A NEW TREATMENT OF LOW PROBABILITY EVENTS WITH PARTICULAR APPLICATION TO NUCLEAR POWER PLANT INCIDENTS

A thesis for the Degree of PhD

by

Octavius Hunt Critchley

of

THE DEPARTMENT OF NUCLEAR ENGINEERING

QUEEN MARY COLLEGE

UNIVERSITY OF LONDON

Submitted in fulfilment of the requirements of the University of London in December 1984

ABSTRACT

'Chacun à son métier'

Technological innovation is inescapable if civilisation is to continue in the face of population growth, rising expectations and resource exhaustion. Unfortunately, major innovations, confidently thought to be safe, occasionally fail catastrophically. The fears so engendered are impeding technical progress generally and that of nuclear power in particular. Attempts to allay disquiet about these disastrous Low Probability Events (LPEs) by exhaustive studies of nuclear power plant designs have, so far, been less than successful. The New Treatment adopts instead an approach that, after examination of the LPE in its historical and societal settings, combines theoretical design analysis with construction site and operational realities in pragmatic engineering, the quality of which can be assured by accountable inspection.

The LPE is envisaged as a singularity in a stream of largely mundane, but untoward incidents, described as 'Event-noise'. Predictions of the likelihood of plant LPEs by frequency-theory probability are illusory because the LPE is unique and not part of a stable distribution. Again, noise analysis seems to lead to intractable mathematical expressions. While theoretical LPE prognostications depend on the identification of fault sequences in design that can either be designed-out or reduced to plausibly negligible probabilities, the reality of LPE prevention lies with the plant in operation. As absolute safety is unattainable, the approach aims at ensuring that the perceived residual nuclear risk is societally tolerable. An adaption of elementary Catastrophe theory to model the prospective Event-noise field to be experienced by the plant is proposed whereby potential, credible LPEs could be more readily discerned and avoided.

In this milieu of increasing sophistication in technology when management in the traditional administrative mold is proving inadequate, the engineer emerges as the proper central decision-maker. The special intellectual capability needed is acquired during his training and experience, a claim that can draw support from new studies in neuropsychology.

The Nuclear Installation Inspectorate is cited as an exemplar of a body practising the kind of engineering inspection needed to apprehend those human fallibilities to which most catastrophic failures of technology are due. Nevertheless, such regulatory systems lack accountability and, as Goedel's theorem suggests, cannot assess their own efficiency. Independent appraisal by Signal Detection Theory is suggested as a remedy.

TABLE OF CONTENTS

(Pages 1 to 432 inclusive)

Section		Pages
	ABSTRACT	2
	CONTENTS	3-8
	GLOSSARY	9-11
	PART ONE	
1	INTRODUCTORY NOTES	13-17
	1.1 The Industrial Revolution	
2	THE CHANGING PERCEPTIONS OF RISK AND THE DECLINE OF FATALISM	18-22
	2.1 Technology reveals its dangers	
	2.1.1 Society comes to grips with industrial hazards	
	2.1.2 Safety regulation and the point of diminishing returns	
	2.1.3 Technology's new aspect of danger: the Low Probability Event	
3	THE SAGA OF SOME CALAMITOUS LOW PROBABILITY EVENTS	23-32
	3.1 Some unexpected explosions	
	3.2 Trouble with bridges	
	3.3 Two tragic but intriguing railway accidents	
	3.4 The grim human cost of coal	
	3.5 Dangers of the sea, technology and the emergence of new hazards	
	3.5.1 Shipwrecks and collisions	
	3.5.2 Two 'incredible' disasters at sea	
	3.5.3 Some mysterious maritime losses	
	3.6 Aeronautical innovations, achievements and accidents	
4	THE ADVANCE OF TECHNOLOGY AND THE NEW HAZARDS OF THE EMERGENT INDUSTRIES	33-40
	4.1 Nuclear Power and Radioactivity	
	4.2 Some serious nuclear accidents	
	4.3 X-rays, Isotopes and Radiography Sources	
	4.4 The generality of radiation accidents	
	4.5 Oil, Petrochemicals and Liquid Natural Gas	
	4.6 Underwater technology and its dangers	
	4.6.1 Oil and the toll of its extraction from under-sea fields	
	PART TWO	
5	THE ENIGMA OF MODERN PERCEPTIONS OF TECHNOLOGICAL HAZARDS	42-51
	5.1 The emergent political potency of public opinion	
	5.2 The growing unease of technological innovations	
	5.3 Anti-technology arguments: supposititious and real	
	5.3.1 Nuclear Power: vestigial risk	

5.4 The riddle of the hostility to nuclear power
5.4.1 Opposition hardening
5.4.2 Fallacious affirmative arguments
5.5 Conditions for toleration of the nuclear power risk

6 THE IMPERATIVE FOR CONTINUING TECHNOLOGICAL PROGRESS 52-59
6.1 Population growth and the inevitability of technical change
6.2 Booms, slumps, the long wave economic cycle and technological development
6.3 The need for new safety concepts
6.3.1 The role of nuclear safety engineering

7 STATE OF THE ART IN RISK SCIENCE 60-78
7.1 Progress in risk and hazard studies
7.1.1 Safety by anticipation - a consequence of atomic energy
7.1.2 Recent additions to the corpus of risk studies
7.1.3 Cultural aspects of risk perception
7.2 The emergence of quantitative probability methods
7.3 The Rasmussen Reactor Safety Study
7.3.1 Criticism and the Peer Group Review
7.4 The German (reactor) Risk Study
7.4.1 Relevance to the New Treatment
7.5 Overview

PART THREE

8 CULTURE, RISKS, 'ZERO-INFINITY DILEMMAS' AND THE NEW TREATMENT 80-111
8.1 The refractory persistence of the cultural dimension
8.1.1 A linguistic explanation for the 'Golden Age' of Greece
8.1.2 The ambivalent societal circumstances of the engineer
8.2 Accidents, Low Probability Events, Risk Prediction and Prophecy
8.2.1 Mortality owing to 'Mundane' causes
8.2.2 Casualties due to odd causes - 'Unusual Events'
8.2.3 Rare and Unusual Events and Statistical Stability
8.2.4 Qualitative characteristics of a Poisson Distribution
8.2.5 New technologies, catastrophic failures and negligible risk
8.3 Risk management and 'The Zero-Infinity Dilemma'
8.3.1 Nine characteristics of 'The Dilemma': an actuarial view
8.4 Engineering interpretations of the 'Zero-Infinity' challenge
8.4.1 Catastrophic failures of uncertain causation
8.4.2 'Ratchetting' investment in engineering safeguards
8.4.3 Low Probability Events and the quandary of open-ended design targets
8.4.4 Protection of the public: major hazards and reactor siting
8.4.5 Control of radiation exposure: dose limits and siting criteria

8.4.6 Verification of accountability and accuracy in risk assessment

8.4.7 Simulated accountability by 'Keeping Score'

8.4.8 Bringing risk assessors to account: some constitutional issues

8.4.9 Illusory aspects of Design and Risk Assessment

8.5 'Lead time': another characteristic of the 'Zero-Infinity Dilemma'

8.6 Overview from the Engineering Dimension

8.6.1 An analogy with 'noise' theory

9 SAFETY ASSESSMENT OF DESIGN: FACTS AND FALLACIES 112-147

9.1 From 'Safety Factor' to 'Design Basis Accident'

9.2 The Maximum Credible Accident (MCA) Doctrine

9.2.1 Limitations of the early MCA approach

9.2.2 The resilience and survival of the MCA doctrine

9.3 The MCA and power reactor siting considerations

9.4 Emergence of the quantitative approach to siting

9.5 The true role of systems analysis in : nuclear safety

9.5.1 A cartesian representation of the theory-practice disjunction

9.5.2 The administrator's need for decision analysis

9.6 Safety Assessment of Design: Illusory aspects

9.6.1 Design Probabilities: Feasible and Metaphysical

9.7 Some matters concerning the nature of probability

9.7.1 Idealism and realism in probability theory

9.7.2 Data collection and risk models

9.7.3 The fallibility of synthetic data distributions

9.8 Overview

10 INDUCTION, PROBABILITY, ENGINEERING AND SCIENTIFIC METHOD 148-160

10.1 Engineering and the ethos of nuclear power technology

10.2 The riddle of inductive inference

10.3 Induction, Scientific Method and the language of technology

10.4 Recapitulatory synopsis

PART FOUR

11 AN OUTLINE FOR THE NEW TREATMENT OF LOW PROBABILITY EVENTS 162-178

11.1 The 'trans-scientific' aspects of Engineering

11.2 Attempts to define some basic principles of safety and reliability

11.2.1 Characteristics of the approach to radiological protection

11.2.2 Principles of the New Treatment

11.2.3 The quandaries of adequate safety

11.3 'Defended Safety' - a holistic concept

11.3.1 The relevance of human factors and accountability

11.3.2 'Bootstrapping' and 'Defended Safety'

11.4 Synoptic Overview

12 ENGINEERING DESIGN, 'EVENT-NOISE' AND THE MANAGEMENT OF LPEs 179-220

12.1 On the nature of engineering design

12.1.1 The Design-Hardware Transform and the concept of 'Event-noise'

12.2 Philosophy and implications of 'Event-noise' theory

12.2.1 Categories of 'Event-noise'

12.2.2 'Event-noise' sources

12.3 The 'Event-noise' stream: Characteristics and singularities

12.3.1 The 'Event-noise' concept and the 'Reactor Safety Study'

12.3.2 An analytical treatment of the 'Event-noise' concept

12.3.3 Engineering and its proper involvement in the defence of safety

12.4 The relevance of Thom's 'Catastrophe Theory'

12.4.1 Some qualitative aspects of the Cuboid Catastrophe Model

12.4.2 The nature of the Catastrophe-function, '$\bar{L}$'

12.5 An interpretation of the Catastrophe/Event-noise approach

12.5.1 Some 'Catastrophe' representations of Event-noise elements

12.5.2 An evaluation of Event-noise/Catastrophe Theory

12.6 Overview

13 EVENT-NOISE: CAUSATION, SIGNIFICANCE AND PRECURSORS 221-229

13.1 Some further deductions from En-Catastrophe theory

13.2 The enigmatic nature of event precursors

13.2.1 A role for technical intuition or engineering judgement

13.3 Loss of resistance to failure, a harbinger of major system faults

13.4 The problem of lethargy and centripetal tendencies

13.5 The assurance of safety and reliability by stability of form

13.6 Overview

PART FIVE

14 PROBLEMS OF INSPECTION IN THE DEFENCE OF SAFETY 231-266

14.1 The nature of 'inspection'

14.2 Aspects of 'engineering inspection'

14.2.1 Orders of engineering inspection

14.2.2 The characteristics of engineering inspection

14.2.3 Quality Assurance, Quality Control and Engineering Inspection

14.3 Some misconceived ideas about inspection

14.3.1 Involvement of the inspector and shared responsibility

14.3.2 'Meta-inspection' - the need for an inspection of inspection

14.4 Some further fallacies of scientistic approaches

14.4.1 The fallacy of the dependence of inspection upon equal expertise

14.5 A role for inspection: a quasi-cultural aspect of safety

14.5.1 The new style of engineering safety regulation

14.5.2 The question of appraisal of inspection and accountability

14.6 The assessment of inspectorial competence by Signal Detection Theory (SDT)

14.6.1 An alternative to the test of market forces in nuclear risk assessment

14.6.2 SDT and the psychophysics of Forward Safety Analysis

14.6.3 A macroscale, synthetic exemplar

14.7 Advantages of the HCA/SDT philosophy of nuclear risk management

14.8 Overview

15 CONCLUDING OVERVIEW AND CONSTITUTION OF THE NEW TREATMENT 267-280

15.1 The essential nature of the New Treatment

15.2 Some matters concerning the public acceptance of nuclear power

15.2.1 The new style inspectorates and public trust

15.3 Synthesis of the New Treatment of Low Probability Events

15.4 A concluding comment with some reservations

PART SIX

16 EPILOGUE 282-284

17 ACKNOWLEDGEMENTS 285

18 NOTES 286-296

19 APPENDICES 297-312

I A synopsis of statutory health and safety regulation in Britain

II Selected Low Probability Events

III On Engineering

20 FIGURES 313-335

(Figures 1 to 15 are also placed in the text near relevant passages)

1 The Five Interacting Branches of Culture

2 Incident Frequencies, Consequences and Public Reactions to Hazards

3 Vistas and Horizons of Technical Design Safety Assessment for a Nuclear Power Reactor: Magnox - AGR - PWR

4 Perceptions of Chance

5 Probability of the Worst Consequences of a US Nuclear Power Station Accident

6 'a' - A conventional vector representation of the relationship between the driving voltage (V) and the current (i) in an alternating current circuit with a reactive load

'b' - An attempt at a multi-dimensional portrayal of the relationships that involve administration, science, design, management-and-practice and technician and artisan skills through engineering ....

7 Prediction and Pattern of Behaviour in Plant and System in the Realm of Very Small Event Probabilities

8 The Realisation of Engineering Design - Theory vs Practice

9 Event-noise Ideogram: Nuclear Power Plant

10 Bathtub Curve

11 Event-noise Display
12 Thom's Catastrophe Graph - Cuboid Modal
13 Design Safety Analysis, Ignorance of Mechanism and Inspection
14 A New Outlook on LPE Causation - The Chilver Failure Triangle
15 Causation Triangle for Low Probability Events
16 Tay Bridge Collapse of 28th December 1879
17 Ronan Point Tower Block Collapse of 16 May 1968
18 Hixon Automatic Level Crossing Crash of 6 January 1968
19 Welder - Over-exposure - Dismemberment - Death
20 Welder - Ionising Radiation Dose Profiles of Exposure of Thighs
21 Welder - Radiation Burns - Degenerative Course

21 TABLES 336-340

(The Tables are also placed in the text near relevant passages)

I Life Expectance Changes
II Accidental Death - Average Risk of Fatality
III Licensee Event Reports
IV Stub Vector Attitudes

22 REFERENCES 341-353

23 ANNEX 354-432

Supporting papers from published works

Document No.

1 'Risk prediction, safety analysis and quantitative probability methods - a caveat',
J. Br. Nucl Energy Soc., 1976, 15, 18-20

2 'Aspects of the historical, philosophical and mathematical background to the statutory management of nuclear plant risks in the United Kingdom',
Proc. Symp. on Radiation Protection in nuclear power plants and the fual cycle, British Nuclear Energy Soc.,
London, 1978, 11-18

3 'Inspection and its Role in the Case for Nuclear Power',
Proc. Meeting on Directions in Nuclear Engineering Research,
Cambridge, 19 September 1980, Inst. Nucl. Engineers,
London, 1980, Paper No. 201

4 'Technological progress, safety and the guardian role of inspection',
Science and Public Policy, 1981, 8, 291-307

5 'Thermal Control of the Magnox Nuclear Heat Engine'
(An abridged revision of an Inspectorate of Nuclear Installations Report, INI/R/19/62, prepared for and published by the Ministry of Power, Millbank, London, October 1962),
Edited version dated July, 1984

GLOSSARY

Note - In a text with a philosophical orientation, the precise meaning of words is important and words may be used in a way that may be unfamiliar to some readers. Some of those words and terms that are uncommon or employed in an unconventional sense have been defined here. The arbiter has, in the main, been Collins New English Dictionary, though the Concise Oxford Dictionary has been consulted and its definitions taken where there has been any great divergence between British and international usage. In those cases where a wider interpretation or one that has specialist connotations has been wanted in a search for the 'mot juste', recourse has been made to the Fontana Dictionary of Modern Thought or to appropriate technical lexicons.

Apperception - perception or comprehension effected by assimilating a perception to ideas already in the mind, or perception with recognition or by association with an idea already perceived.

Bottomry - a contract whereby the owner of a ship borrows money to enable the vessel to complete a voyage and pledges the ship as security for the loan, the lender losing his money if the ship is lost. An agreed fraction of the profit was taken if the enterprise was successful.

Closed system - a term used to describe a risk situation when all the variable factors that create the risk are definitively known or can be allowed for or excluded as insignificant. In a wider context, an experimental scientist aims at establishing a closed system as the environment for his experiment.

Common-mode failure - interaction between systems not normally coupled, for example when a common cause precipitates failure in more than one component, sub-system or system simultaneously. The term is often very loosely used to imply a vaguely defined common cause for failure.

Common sense - in vernacular usage 'common sense' means plain, ordinary good-judgement. A more comprehensive definition adds the qualification that such judgement is tempered by the critical faculty of mind that tests concepts for congruence with learnt knowledge, previous experience, the corpus of commonly held beliefs and persuasions and the personal Weltanschauung, but it is, nonetheless, a faculty that is self-correcting in the course of the evolution of new knowledge.

Consistency - the relationship between propositions which obtains if it logically possible that they should both be true. Two propositions are inconsistent if from the truth of either it follows that the other is false. The notion can be applied to groups of propositions larger than two.

Contingency - a possible but not very likely future event or condition; an eventuality, dependence on chance or circumstances; something dependent on a possible future event; uncertainty of occurrence, chance occurrence, a thing that may happen at a later time.

Credible - capable of being believed, worthy of belief; in the usage of nuclear engineer it means that an envisaged sequence of events, usually of unlikely constitution, can run to completion, probably ending in a plant failure, though there are many variants of this definition.

Defended Safety - an on-going approach to nuclear safety that is essentially dynamic, integrating the techniques of design safety assessment with an inspectional strategy based on foresight rather than hindsight. It is discussed in Section 11.3 et seq. of the text.

Dialectic - the practice of assessing the truth of a theory or opinion by discussion and logical disputation.

Disjunction - the separation of things that have previously been joined; a division formed between parts of a thing that has previously existed as a whole.

Epistemology - the theory of knowledge and particularly the critical study of its validity, method and scope.

Event-noise - an analogy between the continual background of random disturbances in electronic circuits and communication channels and the run of mundane faults, minor incidents and industrial accidents that may be expected to occur on a factory site.

Gestalt - a perceptual pattern or structure possessing qualities as a whole that cannot be described merely as a sum of its parts.

Hazard - a situation that has a potential to cause harm to people or damage to property or the environment.

Heuristic - a method of problem solving or discovery by guided trial and error or by incremental exploration.

Idealism - a group of doctrines in which thought or mind is the only reality and external objects consist merely of ideas. Thus, mind and spiritual values are fundamental to the world as a whole.

Ideogram - a pictorial representation of ideas, particularly of words, ie. logograms. The device is much used in engineering and in engineering design to express complex technical and scientific ideas which are difficult or impossible to communicate by written or spoken language alone, hence ideographical and ideographic.

Idol - a false mental conception; a false notion or erroneous way of looking at things.

Incredible - a state or situation beyond belief or understanding; in nuclear safety, the term is used to define a possible failure mode that would involve mechanisms whose existence is beyond reasonable belief.

Intuition - Immediate insight; knowledge that is empirical in the broad sense of the word, being an extension of experience from sensation to introspection and the immediate grasp of values.

Low Probability Event (LPE) - a sudden, catastrophic and wholly unexpected accident or, more generally, major failure in a technological system, especially a system of an innovatory kind. The LPE is examined further in the Addendum below.

Luddites and 'Ned' Ludd - machine breaking rioters following a legendary leader who blamed the new machinery for their loss of livelihood. There were serious anti-technology riots in the textile manufacturing districts of Nottinghamshire, Lancashire, Cheshire and Yorkshire from 1811 to 1816 which were ruthlessly put down.

Materialism - the doctrine that matter is the only reality and that mind, the emotions, etc. are merely functions of it. Matter thus has a primary position and mind or spirit are secondary dependent realities.

Mechanism - a philosophical attempt to explain phenomena in mechanical terms in which the causation of an event may be defined in clearly discernible antecedents and predictable contemporaneous conditions.

Metaphysics - in popular usage the word means abstruse or highly theoretical with a sense of the occult, but in modern philosphical terminology it refers to enquiry into the kinds of things that there are and their modes of being, namely conception of existence, properties, and events, and into the nature of change, causation, mind, matter, space and time.

Metaphysical - of metaphysics; based on abstract reasoning, abstruse or over-theoretical.

Ontology - the branch of metaphysics dealing with the nature of being, or in logic, the set of entities presupposed by a theory.

Ontological relativism - the principle that it is necessary to test the validity of all the relations and particular values given to the parameters used in a decision model. This implies that all constructs, ie. the things that are put together to make the model should, if the are meaningful, be testable in principle.

Phenomenalism - the theory that only phenomena are real and can be known.

Physical monism - the doctrine that all physical laws are deducible from statistical mechanisms.

Practical, Reasonably Practical - terms originating in the technico-legal vocabulary of indust- safety regulation that have gained a wider currency. A case law definition of 'practical' in respect of measures that an employer must take for the protection of his workers is that they must take into consideration what is possible in the 'light of current knowledge and invention', but not to meet dangers 'scientifically unknown'. The qualification 'reasonably' implies that, although a measure may be possible, judgement can be exercised on what is feasible in the given circumstances.

Pragmatism - the doctrine that practical consequences are the criteria of knowledge, meaning and value. It originated in the latter part of the last century with the American philosopher and scientist, Charles Sanders Peirce who developed a theory of truth that seems to side-step the idealist-materialist debate. It has profoundly influenced American thought.

Probability - in a historical sense, it is a relatively new science, the subtler meanings and practical implications being still a matter of debate. There seem to be three main schools of interpretation, namely the:

(i) Frequency theory or Aleatory Probability which assumes, overtly or tacitly, 'that every class of event shows a statistical regularity of occurrence if only one takes a sufficient number of instances of it';

(ii) Subjective theory according to which probability is to be interpreted in terms of the psychological state of the person making a probability judgement; and

(iii) Objective theory which defines probability as an objective, logical relationship between propositions and events, but one that is always elliptical because it implies that a probability is in a relationship with the data, context and other information from which it was calculated or deduced.

The practical engineering interpretation seems to be that 'we have to treat the probability relation like other fundamental categories, as ultimate and indefinable. It may also well be that each of the rival views is true in one important sense of probability, but not in the others.

Quality Assurance, Quality Control - There is some confusion between the two terms. In this text, Quality Control refers to Viewing inspection, ie. dimensional checks, functional testing, etc., to confirm compliance with specification, whereas Quality Assurance is a broader concept of activities integrated into the management system to ensure that a company's obligations under contract and to the community are met.

Relevatism - any theory holding that knowledge and values are not absolute but are relative to a person's nature, the given situation or circumstances.

Risk - the probability of occurrence of an event that can cause harm or damage to a person, human population or thing of value.

Safeguards (Technological) - may be defined in two categories, namely:

Intrinsic - safeguards inherent in the design concept of an artefact, and

Engineered - a safety feature or system added to the design of the artefact, eg. plant or system, to correct weaknesses or deficiencies revealed in its intrinsic characteristics, for instance provision of an emergency system of control rods in a reactor to effect rapid shutdown compared with the stability given by the negative temperature co-efficient of the nuclear core.

Safety Factor - an engineering concept used in design to allow for overloads and defined as: 'Once the breaking stress has been measured, ... the permitted working stress ... (may be calculated) ... by dividing by the appropriate factor of safety ... a number determined by a variety of considerations, mostly empirical, to provide a margin of reliability to cover such contingencies as imperfections of erection, changes produced during fabrication, deterioration with time and imponderables such as tradition and repute. It may be of the order of 5 to 10 and usually brings the material within the elastic limit with a reasonable margin to spare'. (The underlying concept is basic in reliability engineering, though current applications are far more sophisticated.)

Secundum quid - a term in logic used to identify a deceptive argument which uses a principle or proposition without regard to circumstances which modify its applicability in the given case.

Trans-science - a term proposed by Alvin M. Weinberg (1972) to describe those questions of public decision and debate which lie at the ambiguous junction between science and society that can be stated in scientific terms, but are in principle beyond the proficiency of science to answer. He gives as examples attempts to make precise estimates of the effect of very low doses of ionising radiation to which a population may be exposed and of the probabilities of very unlikely, rare events.

Truth - a word with many and controversial meanings. In popular usage it is the quality of being true, that is genuine, actual or factual as opposed to being false. More philosophically, it is a proposition independent of individual opinions, being the predestined result to which sufficient inquiry would ultimately lead; in other words the outcome of scientific method. Again and pragmatically, it is a 'warranted assertion' or a working, satisfactory or verified hypothesis.

Weltanschauung - a conception of the world, a comprehensive view or personal philosophy of human life and the universe.

ADDENDUM ON THE LOW PROBABILITY EVENT (LPE)

No formal definition of the Low Probability Event (LPE) has been given in the text as the term is largely self-descriptive and the particular meaning has been allowed to emerge in the wake of the descriptive exemplars. More specifically, the term is used to identify those 'incredible' occurrences and potential accidents that present the 'zero-infinity' actuarial risks associated with advanced technological innovations.

No definitive numerical expectancies or failure rates can be assigned to eventualities of such low probability. Nonetheless, any rational approach to the management of these LPEs depends on a concept of probability of which there are three in use. The first is predicated by the aleatory or frequency theory of probability, claiming that a firm failure expectancy within definable confidence limits can be associated with any possible plant LPE despite its being of very low probability, provided that enough data is available. The second is subjectivist. An expectancy may be calculated in a similar way, but its meaning is a product of the assessor's judgement or bias in his treatment of the circumstances, and this can vary grossly among assessors. The subjective risk estimate must be treated accordingly. The third approach follows the objective theory which holds that a numerical probability is only as stable as the data from which it is calculated. Few data distributions are of sufficient stability to justify confidence in such numerical risk estimates. A pragmatic engineering approach finds utility in all three, up to the limit of their relevance in each case to the problem in hand.

PART ONE

THE HISTORICAL, HUMANITARIAN AND REGULATORY BACKGROUND TO A NEW TREATMENT OF LOW PROBABILITY EVENTS

Sections 1 to 4 covering:

The Industrial Revolution, the new dangers introduced by its technology, the beginning of the statutory safety regulation of industry, the emergence of the catastrophic Low Probability Event (LPE) in innovatory technological systems and some disastrous examples of them -

> Explosions, collapsing bridges, coal mine tragedies, shipwrecks and collisions at sea and on railways, the perils of atomic energy and ionising radiations, petrochemical plant and liquid natural gas storage and handling acidents and the hazards of underwater technology;

being an attempt to portray the dangers of modern technology in a historical and sociological perspective in the light of the changing perceptions of risk.

THEMATIC SYNOPSIS

The aim is to set the scene for a study of the LPE that ends in a catastrophic failure in the societal milieu of the reactions of the public as citizens and workers to the risks of innovatory technologies, taking into account the essential (evolutionary) need for continuing technological progress to preserve civilisation and, in particular, progress in the field of energy generation and resource conservation: a study especially concerned with the steps that can be taken to treat the risks created by the new technologies, and by nuclear power in particular, as problems of engineering.

A NEW TREATMENT OF LOW PROBABILITY EVENTS WITH PARTICULAR APPLICATION TO NUCLEAR POWER PLANT INCIDENTS

1. INTRODUCTORY NOTES

> 'The fire broke out at Master Farryner's bakehouse in Pudding Lane, Thames Street, in the early hours of Sunday, 2nd September, 1666, and aided by high winds spread from the TOWER to the TEMPLE and from the THAMES to SMITHFIELD. St. Paul's Cathedral and 89 other churches were destroyed and 13,200 houses. ... In five days it covered 387 acres within the walls and 73 without. It was halted by blowing up houses at Pie Corner, SMITHFIELD.'
>
> The Great Fire of London
> from Brewer's Dictionary
> of Phrase and Fable,
> Centenary Edition, 1977.

In addition to famines and pestilences of which 'The Old Testament' speaks so much and so solemnly, man has also suffered physical disasters which have caused heavy tolls of life and limb and great damage to property. Such events were fortunately rare, were of 'low probability', but usually came very suddenly giving little chance of escape to those threatened because they were seldom preceded by any clearly distinguishable warnings. In past ages, except for fires in great cities like ones in Rome in 64 AD and in London in 1666 and for shipwreck, they have been of natural origin, being earthquakes, volcanic eruptions like that which smothered Pompeii with ash in 79 AD, hurricanes, floods and tsunami (1). In the face of these things there was little that could be done except to take the consequences stoically. However, it has been possible through technology to give man some relief from these afflictions. Modern medicine and sanitation have dispelled the plagues, while the predictive sciences of hydrology, meteorology, seismology and vulcanology can reveal the imminence of cataclysmic terrestrial events so that precautionary measures can be taken, and facilities for effective disaster relief can be promptly and rapidly mobilised by Twentieth Century communications and transport with the saving of many thousands of lives.

Despite the advances which have so strikingly reduced these perils, the threat from disaster of technological origin has grown, and low probability events of an adverse kind from this source seem likely to become dominant over those of natural origin, at least in the more technically developed countries. Besides new dimensions have been added to the calamities attributable to man's activities in that certain damaging factors now exist which are not perceptible to the senses and therefore give no warning of their baneful effects. It is suspected that their consequences may be delayed for many years, even to the extent of emerging in generations subsequent to the one exposed.

Moreover, though the destruction caused by a disastrous event may appear to be limited to the physical domain and its economic consequences, it can often have a veiled though serious detriment in another, though less obvious one. A catastophe causing heavy property damage and process losses which amount to a significant part of a community's wealth or, more widely, of the national product and capital stock, though being of very slight or no harm to humans directly and causing no fatalities, can still be a societal disaster. There is a correspondence between the aggregate economic loss attributable to the event and the well-being of the people afflicted by it which can be related to a reduction in the expected life span (2). While this may be of little importance to any given individual, the sum for the population as a whole may be large and serious.

It is not surprising then that the outlook of many people and influential groups in Western society today is characterised by a growing distrust of technology to an extent which is hard to comprehend. Nowhere are these misgivings more evident than in the case of the safety of its complex, scientific applications in large scale industrial plants and processes of which nuclear power is the exemplar. Oddly, these apprehensions are associated with uneven appreciations of the risks involved. For example, the great and gruesome toll resulting from motor traffic on the roads is accepted with scarcely a murmur, while the nuclear industry which has been appropriately described as 'the safest in the World' is viewed with grave disquiet (3).

Despite the focussing of these fears on atomic energy, they are manifest in rising tempo in respect of other advanced technologies, e.g. liquid petroleum gas and the potent drugs of modern medicine which, except for the occasional tragic mishap, have transformed the scope and efficacy of its practice. The political outcome of these

concerns may prove to be a serious impediment, not only to the scientific and social advances needed for the continuing improvement of man's lot on the planet, but to those related industrial developments, particularly in the field of energy, which are necessary to ease the menacing international tensions caused by capricious restrictions on the flow of oil and the erratic fluctuations in its price. These latter instabilities reflect transient economic trends and political manoeuvring which bear little relationship to the true state of the World's petroleum reserves and the long term dependability of the sources of supply. Oil is an extractive industry and access to it must become progressively more difficult as the oil fields are exhausted in a few decades. The threat to the internal stability of countries almost entirely dependent on it for their transport and for much of their domestic and industrial energy could be grave and unpredictably upset the World balance of power between East and West, unless alternative energy sources of a suitable kind are developed in time. Nuclear power offers an abundant and adaptable one. Like quandaries may be expected as other natural resources become scarce.

1.1 The Industrial Revolution

The adverse influence which technical progress, the consequent mechanisation of industry and the ensuing growth of trade can have on society and the environment have been the causes of disquiet for generations and William Blake (1808) bewailed the 'dark Satanic mills' which were blighting 'England's green and pleasant Land', but as Benjamin Franklin (1760 ca.) observed earlier, 'No nation was ever ruined by trade'.

The profound societal consequences of the rapid and widespread changes in the economies of the occidental countries which have occurred over the past two centuries can be adequately described in the framework of British industrial safety legislation, the enactments of which were made in response to pressure from public opinion to abate the exploitation of workers and to ameliorate bad working conditions. This period of cataclysmic change which began in Britain about 1769, the year in which James Watt took out a patent for his new steam engine, is called the Industrial Revolution, the British experience being its paradigm. In other countries because of a later start and variations in national resources and character of the people, the economic and social transformations took a different, though not wholly dissimilar course, being delayed in Germany until 1860, modified in the U.S.A. by

the scarcity of free labour and in France by a lack of indigenous coal. By 1785 in England, Watt's patents were being fully exploited and steam power soon displaced hand, horse and water as the prime mover in the manufacturing processes, and factories, particularly cotton mills, moved from country settings to towns which grew apace.

Industrial productivity was greatly increased by the new technology and the enhanced output could support a rapid and previously unknown rate of economic growth, and England enjoyed a period of increasing prosperity which continued without major interruption until the outbreak of the first World War in August 1914. Concomitant with the industrial progress were the advances in the humanities, the sciences, medicine and engineering which underpin modern European culture.

In spite of the achievements there were some less happy results. Traditional industries were destroyed and the growing urban proletariat existed in conditions made notorious by Dickens and other chroniclers of their misery. This scene has been pithily described by G.D.H. Cole:

> 'The old, relatively stable conditions of life were dissolved at a prodigious pace; and great masses of country bred workers found themselves flung into an urban way of life .... with no social services except the poor law (of varying dispensations) ... in towns built with almost no regard for sanitation or amenity.'
>
> The Common People 1746-1946,
> Methuen, London, 1947.

But, in spite of this dismal vista in the town slums, the overall picture was one of burgeoning wealth and opportunity and of national economic and cultural progress. The improvements in living standards, housing, sanitation and nutrition, for at least a substantial part of the population, were accompanied by remarkable increases in the expectation of life which rose from 34 years in 1790, a figure which had changed little over the preceding centuries, to 41 in 1850, reaching 50 at the turn of the century and nearly 70 for males and somewhat longer for women by 1950 and the prognosis is for an even further extension of the life span (see Section 6.1). In truth, the economic conditions of the poor in towns were little worse, if not better than in their previous rural state. What differed was that they could be seen as relatively impoverished, huddled masses in their urban environment, whereas previously they had been dispersed

to blend inconspicuously among the rural poor, and as a town based proletariat they provided a receptive audience for reforming politicians and radical publicists.

Attitudes formed in revulsion against the grim conditions of the past industrial environment have played a major part in shaping the way in which the modern British approach to community hygiene and industrial health and safety have developed; now recognised as being amongst the foremost in the World. Accompanying this transformation there has come into being a generation whose birthright is the expectation of a long life endowed with 'a sound mind in a sound body' who demand the right to safe and pleasurable enjoyment of their inheritance. Thus, for the children of today there is a palmy life-style of which those living in a less fortunate era would not have dared to dream. For them, instead, there were:

> 'No arts; no letters; no society; and which is worst of all, continual fear and danger of violent death; and the life of man, solitary, poor, nasty, brutish and short.'
>
> Thomas Hobbes,
> Leviathan, 1651, Pt (i), Ch. 3.

In contrast with this sombre past, modern life is Elysian for the citizens of the caring, democratic occidental states. Living much longer than their predessors, cosseted by health schemes, social security and pensions, they are having 'a taste of immortality' and the more perceptive are loath to give up this heritage and see their Eden spoilt, or their enjoyment of it curtailed. It is not surprising then that they bridle at hints of pollution which would foul their habitat and at threats of disease and death as a consequence of technological disasters or from exposure to industrial toxins or carcinogens. Paradoxically, they are less worried about the risks they may run in satisfying the whims of individual pleasure or convenience, nor do they seem to be much troubled by the ever present threat of a nuclear holocaust.

2. THE CHANGING PERCEPTIONS OF RISK AND THE DECLINE OF FATALISM

'But boundless risk must pay for
boundless gain.'

William Morris, The Earthly Paradise:
The Wanderers (1.1581), 1868-70.

As W.D. Rowe (1977) so succinctly observed, 'Only death is certain', the uncertainty lying in how and when it will be met. Until a little more than two centuries ago, people did not consciously consider that an individual's fate in these respects could be varied.

The casting of one's individuality at the moment of conception is the event of lowest probability that any human can ever experience. From then on survival is continuous exposure to risk unto the end of life. Very few, if any, adults have ever been oblivious to this latter fact, though their reaction can be greatly influenced by the strength of belief in an afterlife. In former times when religious faiths were more strongly held, the prospect of heaven or hell had a profound bearing on the personal attitude towards risk taking, but in the West today it is a factor of less importance.

Our ancestors would, no doubt, have dismissed as trivial the very small risks to which the individual or community are now exceptionally exposed by the occasional low probability failures of a generally benificent technology. The fatalism of the past has given way to profound personal and public anxieties about health and safety.

On the other hand, in earlier times there was much concern about arcane hazards such as 'The End of the World' and apocalyptic strokes of a vindictive providence, portents of which could give rise to great public consternation. There is an apocryphal tale about Dean Jonathan Swift when he was a prebend of St. Patrick's Cathedral in Dublin circa 1670. With jocular intent, he announced that a fictitious eclipse of the Sun was imminent and caused a great tumult in the city.

Accordingly, before the Industrial Revolution had made its mark upon the social, economic and political structure of the Western World, people were little moved by disasters which were nearly all of natural cause and for the most part things which happened far away from their ken. They were looked upon as Acts of God or fate and the private reaction was to secure preservation of self and household as far as this was possible. The state was loath to act and then only in extremis to do little more than to try to check the spread of the peril or to clean up the aftermath, blasting firebreaks, restricting

movement and arranging for death carts for the collection of corpses as was the practice during the Black Death.

The disinterest of a very civilised and moralistic England during the calamity of the potato famines in Ireland of 1846 and 1847 when millions died of starvation was typical of the times rather than heartless.

2.1 Technology reveals its dangers

In Europe before the middle of the last century, knowledge that a new and more efficient manufacturing technique could create industrial hazards would have had but little influence on the decision to adopt it and, thus, on the pace of technological advance. A much more important factor was the effect technical innovation could have on the traditional small scale manufacturing and handicraft industries and, less directly, on the existing social order (4). In the pervading atmosphere of fatalism, concerns about risks to the health and safety of workers were almost non-existent though there were some attempts even in ancient times to control pollution (5). Indeed, had there been the worries about the health and safety hazards of industrial employment which exercise people and their governments today, the phase of rapid scientific, technological and industrial development which started some 200 years ago might well have miscarried and Western civilisation stagnated as has been the case in the Orient.

In view of the social background, it is not surprising that early records of industrial accidents are vestigial and until an Act of 1846, a master had little legal liability for the safety of his workers, even if one were killed in a factory accident. Industrial risks were accepted as inherent in one's way of life and the 'madness of hatters', scrotal malignancy in chimney sweeps and the diseased lungs of miners and glass cutters were taken to be unfortunate and regrettable, but unavoidable. It was likewise for workplace accidents and, though disastrous for a worker maimed and evocative of charity, scarcely newsworthy beyond their locale.

2.1.1 Society comes to grips with industrial hazards

As industrial expansion continued, the value of the gross national product grew and society as a whole became correspondingly more affluent, although the rich benefitted most. Further, the tragic mounting score of factory and mine accidents and disease was bringing a new awareness of the need for safety in industry to the body politic. Movements to improve conditions at work like the Shorter Hours Movement which began in 1830 were awakening public conscience. Important factors of a less idealistic kind not only contribued to the political pressure for change but made it possible. On the one hand it was becoming clear that the detriments of an unregulated industrial technology were no longer confined to the poorer elements of society as the nemesis of the transport accident such as a train crash or shipping disaster did not distinguish between rich and poor and disease and epidemics caused by bad living conditions could not be confined to the slums. Moreover, the loss of a good and skilled hand was a loss to his employer as well as his family. On the other hand, working people were being more effectively organised in unions and could exercise industrial and political pressure for better and safer conditions at work. The most weighty factor of all was that technology had created the wealth to pay for safety.

The foregoing things coincided with the great humanitarian change which had its birth in Europe and America a little more than a century ago. It was a growing trend rather than a sudden change which brought with it free elementary education, laws aimed at ensuring the purity of food and drink and to control foul factory effluents, old age pensions, health insurance schemes, unemployment benefits and, not least, continuing attempts through legislation towards greater safety at places of work. A short synopsis of the history of Health and Safety Legislation in Britain is given in Appendix I.

2.1.2 Safety regulation and the point of diminishing returns

The mundane health and safety hazards of unsafe machines and processes, of gassy mines, on construction sites and in public transport and shipping can be effectively reduced by legislation and enforcement of regulations by inspectors and by designing machines and processes with safety in mind. In consequence, there has been a steady decline in the incidence of industrial accidents and disease until the latter half of this century when it appeared that an end point was being approached.

Barbara Castle, the then Minister of Labour, told Parliament in 1970:

> 'that traditional legislation of the Factories Act type has not succeeded in bringing down the number of industrial accidents to a level which any of us find acceptable. The old approach is inadequate and something new is needed. I am setting up an enquiry to examine the matter.'
>
> Hansard, March 2, 1970, Col. 61.

The Robens Committee of Health and Safety at Work was set up accordingly in that year and it reported in 1972. Its recommendations have been largely implemented in the Health and Safety at Work, etc. Act 1974. The new law aimed at a basic change in the philosophy, style and enforcement of factory safety legislation. Its achievements have yet to be assessed.

2.1.3 Technology's new aspect of danger: the Low Probability Event

Though much progress was being made towards general industrial safety, society was becoming aware that it was being faced with new dangers. Technology, in spite of its benefits, was bringing with it hazards of a less tractable kind and certainly beyond the scope of the traditional regulatory schemes. Accidents of another sort were happening; capricious, rare in any particular mode, seldom foreseen and often disastrous in terms of life, limb and property with effects able to reach well beyond their site of occurrence.

These incidents may be likened to spikes in a background of noise and are defined here as 'low probability events' (LPEs). They are infrequent, unexpected happenings caused by factors either not perceived by the designer of the system which omission is called 'ignorance of mechanism', an actuarial concept discussed in Sections 8.3.1(i) and 8.4.1, or wrongly identified by him as 'incredible' (see Glossary).

The commonplace run of industrial accidents has been the subject of much concern and legislation. On the other hand, the causation and management of the low probability technology event, often accompanied by disastrous consequences to life and property, had received less than due attention until the advent of the atomic energy industries during the last World War when attention began to be drawn to industrial hazards of a new kind. The well-established methods of safety engineering and good management have been shown to be unable to prevent occurrence of these 'low probability events' which need a new treatment, not only in the realms of safety engineering and

regulatory science, but in their interaction with society. The successful approach must therefore be interdisciplinary, mixing sound engineering with social psychology.

3. THE SAGA OF SOME CALAMITOUS LOW PROBABILITY EVENTS

'Fate has terrible power.
You cannot escape it by wealth or war.
No fort will keep it out, no ships outrun it.'

Sophocles, Antigone, 442-441 B.C.

The saga of the 'low probability event' in the form of a sudden and catastrophic accident in a technological system is extensive and continuing. Although rare, such occurrences when accumulated on a Worldwide scale make up a list as numerous as it is diverse. It is possible, therefore, to consider only a few of the ones more relevant to the case here and among them chiefly those of an indigenous kind. They have been separated into 'conventional' happenings, that is, those occurring in well known engineering structure and systems like bridges, aircraft and chemical plant, and into those in advanced technology which include the new energy industries and, especially, nuclear power, although nowadays the dividing line is far from sharp. Some of the selected events mentioned briefly in the sections below are described in more detail in Appendix II.

Whereas in earlier times the pernicious effects of technical innovations were for the most part mundane industrial accidents, disease and local pollution, the new risks of contemporary technology often present in unusual and startling ways. For instance, there are the tragic and unexpected side effects of some of the enthusiastically promoted wonder drugs as in the Thalidomide affair. The preparation which had been subjected to exhaustive testing was offered for sale as safe for human use and widely used in innocent trust throughout Europe in the 1960's until it was found to be the cause of severe deformation in babies born to some mothers who had been prescribed it during pregnancy.

The sudden and catastrophic collapse of a whole section of a seemingly soundly designed and well-constructed tower block of flats in the East End of London brought into question what appeared to be a modern and efficient system of urban residential building. On the other side of the World, the lack of tidal flow through the quiet inland Shiranui Sea,located in the western part of Japan's southern island of Kyushu, turned a prosperous and beneficent industrial development into a malignant, and for a long time unrecognised, source of widespread mercury poisoning for those who lived along its shores. Despite nuclear power's extremely hazardous potential, there have

been but few serious accidents and those that have occurred have been more notorious than damaging to man and the environment.

As a consequence of their unfamiliar and sensational nature, the impact of these rare disasters on what has become international public opinion is greatly enhanced by the assiduous efforts of news seeking journalists and publicists looking for a cause to promote. Accordingly, they are much more disturbing to the body politic than those risks of every day experience which in the aggregate cause more maim and fatalities by far, like the extraordinary toleration of the vast carnage attributable to motor transport accidents. Not only are the grisly features of actual disasters given wide publicity, but those of conjectured ones, like severe nuclear power station accidents, are described in graphic terms (6).

3.1 Some unexpected explosions

The example of powder mill accidents is instructive. They had long been known for their destructive violence and Hounslow Heath was as notorious for these dangerous mills as it was for highwaymen. One such plant provided Guy Fawkes with his gun powder. They were prudently sited in the relative isolation of Hounslow, well outside London, but near the port of Isleworth.

Military and industrial needs had greatly increased the demand for their product. In 1846 Professor Schoenbein, an eminent chemist at the University of Basle, discovered a new explosive, gun cotton, which had several times the impulse of gun powder and which, above all, he had convinvingly proved could be manufactured with great safety in a desensitised state. A factory for its manufacture on a large scale was soon set up at Faversham in Kent and all went well for a few months until at 11.00 a.m. on July 14, 1847, it was demolished by a terrific explosion of mysterious cause which killed 21 people. The shock was not confined to the physical realm and its moral and political repercussions stopped the manufacture of gun cotton in spite of the demand for it. The incident was Britain's first significant experience of the 'low probability event' in the field of advanced technology.

A more recent event occurred on July 17, 1969 when there was an explosion in a large empty oil storage tank standing in an old tank farm at Dudgeon's Wharf on the bank of the Thames oxbow which forms the Isle of Dogs. The top of the tank was blown off with great violence.

Unfortunately a party of six members of the London Fire Brigade had just climbed up on to it to secure a better view of some local oil waste fires in the vicinity. They were all killed. The ignition was caused by an oxy-acetylene steel cutting torch which was being used in dismantling work which had been contracted to a scrap recovery firm. The flame had penetrated the metal membrane near the base of the tank. Another example is the devastasting detonation and fire which destroyed the British Nypro caprolactam chemical plant near Scunthorpe, South Humberside, in which there were 64 casualties among which 28 people died and much damage done in the nearby town of Flixborough. Last there is the casual, and still not fully explained, excursion in a process reactor at the Givaudan chemical plant at Seveso some miles north of Milan in Italy. There was a massive release to the surrounding countryside and nearby town of dioxin which is reputed to be exceedingly poisonous. A large number of people were affected. The full extent and consequences of the contamination of humans is not known, but it was extensive with 150 cases of chloracne in one school alone.

3.2 Trouble with bridges

The collapse of a large and busy bridge is always a newsworthy and sensational event which provides almost invariably important engineering data and design experience, but seldom without the tragedy of loss of human life. Three bridge failures stand out as notable LPEs of extraordinary causality. A central span of the bridge across the Firth of Tay in Scotland, which had been completed only a year and eight months before, collapsed on December 28, 1879 with the loss of 75 lives among whom were many children. The structure failed under the cross pressure of a high wind combined with the load of the train crossing the bridge. The engine and all the carriages fell into the river below. The subsequent Rothery inquiry (1880) severely criticised the engineering and the civil engineer in charge, Sir Thomas Bouch. However, enlighted by a fuller knowledge of the structural mechanics of wide span bridges, it is possible now, 100 years later, to take a less severe view when the circumstances are reassessed in the light of the experineces of more recent bridge failures. Two more recent examples are the collapse on November 7, 1940 of the Tacoma Narrows Bridge which had been built to span the Puget Sound on the West Coast of the U.S.A. and that of a 367 ft. long span of the partially completed box girder West Gate Bridge over the River Yarra near Melbourne, Australia on October 15, 1970. The Tacoma Narrows

incident was the result of aerodynamically induced oscillation in a high wind, an effect not appreciated by the engineers at that time and the Yarra River disaster in which 35 workmen died was due to a lack of understanding by the designers of the nature of the complex stress patterns which would be set up during an attempt to correct an unexpected buckle in some of the plates forming a box. Both of these catastrophic failures occurred because of 'ignorance of mechanism' on the part of the designers. Likewise, although there was negligence on the part of Bouch, he had to solve the problems of load induced stresses in the Tay Bridge design by rule of thumb as structural mechanics was a relatively new engineering discipline at that time. In this he did not succeed.

3.3 Two tragic but intriguing railway accidents

The chronicle of railway accidents is grim and endless, though in comparison with the huge number of passengers carried, the overall safety record is outstandingly good. Railway safety engineering is a well developed discipline, soundly based on long experience in practice. The design requirements for railway rolling stock and signalling equipment specify the highest standards of reliability. When accidents happen, very rarely are they of obvious causation, except in cases of negligent or culpable human error.

One of the points of greatest hazard in railway operation is the point of intersection between the track and a road and, as is to be expected, it is the site of the occasional crash. The one that occurred at Hixon crossing on January 6, 1968 is unique amongst them. It happened where an automatic half-barrier of a well tested type and thought to be almost fool-proof controlled the crossing near Stafford where a busy, though by no means major road, passes over one of the main railway lines from London to the Northwest of England. An experienced heavy-duty road transport crew of 6 with a police escort inadvertently placed a 120 ton mass of steel, an electricity power supply transformer, on the track directly in front of a North-bound oncoming express train travelling at 75 m.p.h. The train driver did not see the obstruction until it was only a few hundred yards ahead of him. A collision was inevitable. The locomotive and five leading rail coaches were destroyed and three others derailed. The casualty roll of 11 dead and 45 injured would have been greater but for the heroism of the transporter driver who stayed at his post in an attempt to pull the transformer clear of the on-rushing engine. Though he did not succeed, his efforts placed the mass of metal so that it was

tossed aside in the impact, permitting the on-rushing coaches to brush past, rather than to crumple concertina fashion or pile on top of one another.

The Moorgate tube station disaster of February 28, 1975 in which 43 people died and 74 were injured was the worst accident to have occurred in the London's underground railway system, excluding a panic in an air raid during the Second World War. Mr. Leslie Newsom, the driver of the morning rush-hour train, approaching Moorgate station at full speed, failed to stop as expected and instead over-ran the platform. He ploughed without any attempt at braking into a short blind-cut tunnel designed as a safety measure for trains over-running the platform. The passengers trapped in the leading compressed and crumpled carriages were thus squeezed together like sardines with no chance of escape.

3.4 The grim human cost of coal

From 1760 onwards, coal mining accidents in those pits which in the light of engineering knowledge at the time were held to be adequately safe and, thus, could be worked without undue danger of a major pit accident, were causing fatalities at a disturbing rate and the rising demand for statutory intervention was becoming irresistable. Doubts were cast about the soundness of many of the accepted practices in mining. One was the single access shaft technique, ventilation being maintained by use of a brattice to separate the downcast and upcast air flows. The terrible accident on January 16, 1862 at the New Hartley pit (near Newcastle-upon-Tyne) when 204 men and boys were entombed and suffocated is an example of how the occurrence of a 'low probability event' can change firmly entrenched scientific ideas. Pit drainage was maintained by a powerful steam driven lift pump actuated by a rod extending to the bottom of the single shaft. The top of the rod was jointed in the end of a massive steel rocker beam so designed that failure under any conceivable load was incredible. The other end of the rocker was motivated by the reciprocating movement of the pumping engine. During a full working shift on that unhappy day, the beam snapped through metal fatigue, a phenomenon about which little was known at the time. The part poised above the shaft fell into it, where it lodged; too heavy to be retracted by any available lifting machinery. Not only did it cut off the sole escape route for the miners but it effectively blocked the air flow. There was a great public outcry and the 'Two Shafts Act 1862' was passed later that year.

Four years later on the two days of December 12 and 13, 1866, two successive explosions tore through the Oaks pit in Yorkshire, killing 361 miners and a number of rescuers. On the 8th of the following November, the Ferndale colliery at Pontypridd blew up killing 178 (Helen and B. Duckham 1973). The ensuing legislation, in addition to requiring a higher standard of ventilation in the underground workings which was recognised to be a key factor in the control of fire damp explosions, contained a new ingredient as the 1872 Act stated that mine managers must be technically competent. The powers of the Inspectorate were also progressively strengthened.

3.5 Dangers of the sea, technology and the emergence of new hazards

The toll of the sea has been historically heavy and until the turn of the 18th Century a merchantman's expected endurance at sea was to make somewhat better than 9 successful voyages out of 10 deep sea sailings. Inability to cast longitude with any measure of accuracy was the root of the trouble. The losses were becoming an intolerable burden upon trade and in 1714 the British Government offered rewards of up to £20,000 for a solution. Technology found a way and in 1773 John Harrison won the prize with his chronometer which was found to be only 5 seconds slow after a 6 weeks sea trial: 'the most famous time piece ever made'. The sea became safer still as better charts, steam, iron ships, wireless and radar followed to aid the shipmaster, but the detrimental aspects of technology soon made their appearance. Collisions rather than rocks and reefs became the hazard and a serious one indeed as the shipping lanes became more and more crowded with the cargoes and passengers of rapidly expanding world trade. Before Harrison shipwreck was commonplace, but marine disasters of the modern world (circa 1776 onwards) have tended to be LPEs of diverse cause and usually with an intriguing technological element. Some characteristic examples are given in the passages and subsections below.

3.5.1 Shipwrecks and collisions

One of the first marine disasters of modern genre to shock international public opinion, an entity which had come into being and was becoming an increasingly important political influence in World affairs in the last two decades of the 19th Century (infra) was the loss of the White Star Liner 'Atlantic' en route from Liverpool to New York with mail, valuable cargo and 1,000 passengers and crew. In heavy gales and short of fuel, her captain tried to make Halifax, N.S. for coal, but early in the morning of April 1, 1873, strong currents,

heavy weather and inaccurate navigation swept her on to the rocks of Mars Head, off Cape Prospect, just 20 miles from her destination. She was a total wreck and only able bodied men, and strong swimmers at that, could save themselves. 750 souls perished among whom were some 300 women and children. The loss some 13 years earlier on February 20, 1860, of the U.S. Mail Steamer, 'Hungarian', which had run ashore on the same rocky coast with the total loss of all 250 lives aboard had much less impact, but that was before the days of international telegraphic links.

These losses were equalled and the horror of the human experience surpassed during the collision in fog between the British Iron Sailing Ship, 'Cromarty', and the French Liner, 'La Bourgogne' off Sable Island, once again near the Nova Scotian Atlantic coast, on July 4, 1898. 'La Bourgogne' was running in poor visibility at some 18 knots, having left New York for Le Havre with 725 crew and passengers. Her captain, an experienced ex-officer of the French Navy had established a full watch and was relying on the power of steam blown fog horn signals from his own and other vessels to confirm that his way ahead was clear. She was rammed amidships by the 'Cromarty' making 4 to 5 knots under reefed canvas: the whistles had not been heard until immediately before the collision. The sailing ship survived as her watertight compartments held and maintained her buoyancy and she put about to pick up survivors. 'La Bourgogne' was holed in the engine room, taking water rapidly and went down in 10 to 15 minutes with the loss of 562 persons, only 163, mostly crew, being rescued. The scenes on deck and in the boats as the ship was abandoned were ugly and deplorable with a total collapse of discipline among the crew. The officers were at a loss to control them. Without firm and proper direction the bewildered and terrified men became so bent on saving themselves that, not only did they do nothing to help the passengers, but they beat back and assaulted those who tried to get into the lifeboats, exhibiting behaviour described as 'fiendish' by eye-witnesses. In the event, no children survived and only 2 women out of 300 female passengers were saved (7). Ignorance of the quirks of sound transmission in fog banks may well have been a contributory cause of this event; if so it will have been another case of 'ignorance of mechanism'.

3.5.2 Two 'incredible' disasters at sea

The foundering of the 'unsinkable' White Star liner, 'Titanic', on her maiden voyage in the early hours of April 16, 1912 with the loss of at least 1503 lives in dead calm seas in the main North Atlantic shipping lanes some two days steaming from New York, after a chance encounter with an iceberg, is a classic 'incredible' LPE (Walter Lord 1976). It came about because of the over-confidence of master mariners and shipping company board rooms in the impressive achievements which had been made in marine technology and navigational science, though in fact they were unaware of the innate fallibility of unproved technological innovation.

Something of similar causation which occurred more than four decades later was the 'radar assisted collision' (L. Oudet 1960, F.J. Wylie 1978) between the superbly designed and equipped Italian liner 'Andrea Doria' and the Norwegian liner 'Stockholm', a ship constructed, maintained and navigated to a similar high standard. It occurred in sight of land at the approaches to New York on July 25, 1956 between two ships operated by companies renowned for the excellence of their seamanship and quality and reliability of their service. It may be classed as one of the first of a series of technological disasters which have revealed hidden dangers from unexpected interactions between mechanical functions and normally routine operational procedures which, in spite of apparently adequate safety provision, are likely to arise in complex technical systems. Both disasters are examples of 'ignorance of mechanism' associated with 'common mode' interaction (see Glossary).

3.5.3 Some mysterious maritime losses

Lloyd's Register of Shipping holds the story of many other grim marine accidents. A series of disasters exhibiting a similar pattern of low probability causality has followed from the 'Titanic' to the present day. Among them are a number of events which have not been explained and they have occurred in spite of the remarkable facilities offered by the new navigational aids, marine safety services and the versatility of the modern life saving equipment carried.

For example, there are the mysterious disappearances of a number of large bulk and specialised carriers of which the three following cases are representative. First are two Norwegian ships of some 70,000 tons in cargo with ore. The 'Berge Istra' was lost on December 31, 1975 and four years later her sister ship, the 'Berge

Vanga' vanished some time after October 30, 1979 on which day the last signals were received from her, nothing being reported amiss. Losses at sea of this kind are usually total, though occasionally some identifiable flotsam has been recovered, the events which caused their fates being unknown beyond insubstantial conjecture. The 'Berge Istra' was certainly lost through an explosion as three crew men who were sunbathing on deck were blown into the sea and were able to climb into a life raft which was fortuitously floating nearby. But why should there be an explosion of such destructive violence in a ship loaded with ore? Of the 'Berge Vanga' there is not a trace. Both ships had carried oil on previous voyages, but their holds had been cleaned and they were fitted with inert gas purging systems.

The third case is that of the German Barge Carrier, 'Munchen'. She was an up-to-date soundly constructed and well equipped vessel of 37,134 tons gross en route from Rotterdam to New Orleans loaded with machinery and barges valued at some £22 million. After signalling on 13 December 1978 that she was in a heavy gale about 450 miles North of the Azores she was not heard from again, vanishing without trace or evidence of cause.

3.6 Aeronautical innovations, achievements and accidents

The First World War established beyond doubt the importance of aeronautical technology and, aside from its military aspects, there were far sighted visions of profitable mass air transport. The lighter-than-air dirigible was seen as the economical and safe way forward and was enthusiastically developed by Britain, the U.S.A. and Germany. It was thought that the dangers of fire and explosion associated with hydrogen could be overcome by good engineering or by using helium instead, the latter approach being taken by the U.S.A. In the decade before Hitler's war, a number of these machines were put into service. Three of them out of five failed disastrously.

The first of the bold ventures was the British 'R-100' and 'R-101' designed as large passenger carrying airships. Encouraged by successful trials with the 'R-100', her sister ship 'R-101' was completed as a luxurious air-liner for Empire service. Confidence that the hydrogen inflammability problem had been successfully solved was so high that smoking was permitted aboard. She was destroyed in a sensational crash in flames over France on October 5, 1930, outward bound from Cardington to India. There was heavy loss of life including the British Air Minister, Lord Thompson. The accident ended British interest in lighter-than-air machines.

The U.S. Navy with assured supplies of the inert noble gas, helium, as the buoyancy medium commissioned the 'Akron' which avoided the hazards of inflammable hydrogen as the lifting agency. After a short period of successful service, she failed through structural collapse in a freak storm off the coast of New Jersey with the loss of 73 officers and men on April 4, 1933. She was not replaced.

The Germans with a long background of experience with lighter-than-air machines, such as their 'Zeppelins' operated during the First World War, built the 'Hindenberg' and 'Graf Zeppelin', both of which had several years of successful and uneventful service. Disaster overtook the 'Hindenberg' on May 6, 1937 when she burst into flames at the end of her 20th North Atlantic crossing while mooring at Lakehurst, N.J. and, though 30 lives were lost, 64 passengers and members of the crew were able to jump clear of the flaming wreck. The cause of the ignition has not been satisfactorily explained. The 'Graf Zeppelin' continued in service for a time.

The structural failure and consequent crashes of the 'Comet' early jet aircraft of British Airways on January 10 and April 8, 1954, were two more accidents attributable to design weaknesses not perceived on the drawing board.

4. THE ADVANCE OF TECHNOLOGY AND THE NEW HAZARDS OF THE ENERGY INDUSTRIES

'The machine does not isolate man from the great problems of nature but plunges him more deeply into them.'

Antoine de Saint-Exupéry
(Writer and aviator):
Wind, Sand and Stars (3), 1939,
trans. Lewis Galantière.

The industrial developments which have been made to meet the vastly increased demand for energy from present day civilised communities have brought with them hazards of a new kind and aspect. The military use of atomic energy in World War II opened the way for the commercial generation of electricity from nuclear reactors and the substantial production of radio-isotopes for scientific, industrial and medical uses. There has been an even greater expansion in the oil industry and in the bulk transport, storage, processing and distribution of petroleum products and liquid natural gas (LNG). Previously, the detriments of technology as sketched in the foregoing passages were confined, for the most part, to the working environment of mill, shop floor, construction site or mine, or to the poorer type of urban residence in the environs of gas works, chemical plant and tannery. In contrast to that milieu, these recent advances in technology, and those of energy and transport in particular, pose threats to whole cities and suburbs, affecting residents in better off areas and even to bother those who could afford to live pleasantly in semi-rural beauty spots. The reaction from this vocal strata of the population has been prompt, energetic and formidable as the aftermath of the Roskill Commission's recommendation (1971) of Cublington, a few miles North of Aylesbury and fringing a residential belt of City, stockbroker and legal types of commuters, for the site of the Third London Airport soon revealed. There have been like reactions to other innovatory proposals adversely affecting residential and other amenities of the superior type elsewhere, and not only in Britain. The realisation that deleterious circumstances could come from technological innovation has to a large extent been brought about by the continuing series of spectacular and disastrous accidents. It is this awareness of disadvantage which has inspired and given cause to the anti-technology movements and lobbies which are able to put a brake on scientific and technical developments in a way that is not

infrequently far from beneficial to the community at large, a matter which is referred to again in the treatment of technological risks set out in another part of this text. Nevertheless, these concerns about safety are not illusory, but real and serious and the circumstances of the several accidents described below give evidence. They are also more fully reviewed among the synopses of those LPEs which, as relevant disastrous incidents of rare and unanticipated causality, have been collected together in Appendix II.

4.1 Nuclear Power and Radioactivity

With the coming of atomic energy, industrial, public and environmental perils of a new compass came into existence: powerful and lethal sources of radiation, local contamination, large scale environmental pollution and the problem of the management of radio-active wastes all presented problems of safe keeping, use and disposal to which there were no easy solutions or even now some of them seen intractable. So serious were the potential dangers of atomic energy that it was recognised from the start with the Manhattan plutonium bomb project that matters of health and safety would have to be dealt with in a new way (Margaret Gowing 1974). Thus, radiation protection was transformed from an obscure speciality into an important and thriving branch of applied physics. Inevitably and in spite of much foresight and heavy investment in elaborate and expensive precautions, some bad accidents have happened, nearly all being LPEs caused by 'human error' (8) or 'ignorance of mechanism' (see Sections 8.3.1(i) and 8.4.1).

There have also been a number of minor incidents which have been harmful to individuals or small groups of workers exposed. They have for the most part happened in the handling of radioactive sources, though there have been several criticality incidents upwards of 10^{15} fissions, some accidental releases of radioactivity to otherwise clean working environments and more numerous inadvertent excessive exposures to intense beams of radiation. It is notable that more than half to perhaps two-thirds of these events have been due to 'human error' in the form of careless mistakes, errors of judgement, but chiefly to negligent or deliberate failure to obey instructions as M.B. Biles (1969) and others since have consistently reported, for example R. Gausden (1979) in the section of his report on 'Over-exposures at industrial premises'.

4.2 Some serious nuclear accidents

Among the plant and process failures which have occurred in the industrial usage of atomic energy, mention must be made of the Windscale plutonium pile fire of October 10, 1957 which, until the Three Mile Island (TMI) affair of March 28, 1979, was probably the worst and potentially most dangerous known failure of a nuclear facility, though in both cases no established harm was done to humans. However, the financial losses in terms of damage to equipment and cessation of services have been very heavy.

One of the most serious near-accidents to threaten a nuclear reactor was the incident of March 22, 1975 which occurred at the Browns Ferry nuclear power station when an electrical technician testing for containment air leaks set fire to the insulation of the instrumentation and control cables in their marshalling vault. Control of the reactor was nearly lost.

There have been persistent and obliquely confirmed reports of a severe radiation accident in late 1957 or early 1958 involving a nuclear facility near Kyshtym, between Sverdlovsk and Chelyabinsk in the U.S.S.R. (J.H. Fremlin 1979), though neither the nature of event nor its consequences are known in the West.

In spite of the foregoing happenings, no member of the public has received a dose of radiation with any significant known health effect (9). The contamination of the environment has been minimal with, once again, the worst case in the West being that caused by the Windscale incident when upwards of 20,000 Ci of fission products were released to the atmosphere from the 400 ft high pile stack. A relatively small quantity of agricultural produce, mainly milk, was destroyed on safety grounds. On the other hand TMI is still a major preoccupation in the disciplines of nuclear safety engineering and regulatory science.

4.3 X-Rays, Isotopes and Radiography Sources

Reports of the severe somatic damage caused by exposure to X-rays were being received less than a year (S.J.R. 1896) after Roentgen's announcement of his discovery of them in December 1895. Until the advent of nuclear technology, radioactive materials of sufficient strength to be of experimental or therapeutic use were available only in tiny quantities, the World's stock of radium amounting to but a few grams. From then on, they could be produced in abundance, both in

amount and type and thereby the risks of injury vastly increased. Gamma-ray sources could now be easily prepared for industrial and therapeutic purposes. Problems of handling, storage, safe use and contamination had to be faced. The solutions drew heavily on the sound, scientifically based approach to radiobiological safety which had been developed over the preceding half-century of experience by medical radiographers and therapists in the use of ionising radiations (Margaret Gowing 1974). In spite of the general efficacy of these precautions, they failed from time to time and these 'low probability events' brought about some serious accidents.

The dangers are principally due to the insidious nature of ionising radiations which even at lethal intensities are imperceptible, so that a very harmful or even fatal dose may be received of which the victim is unaware at the time. The horrible nature of the consequences of a severe overdose of ionising radiations is borne out by the case of an unfortunate welder employed on an oil refinery at La Plata in Argentina. At work during the morning of May 3, 1968 he saw a shiny metal bolt of odd shape lying on the ground which he picked up and carried in his overall pockets for the next two days. At home on the second night, he became ill and in the morning was admitted to the local hospital in pain. He was treated for 'burns of unknown origin' which did not respond to medication. On May 27, the loss of a radiography source was reported. When it was found in his works clothing, it was realised that the man was suffering from a severe radiation overdose. His condition steadily deteriorated with the development of large, dry necrotic scabs on his thighs and desquamation of morbid tissue. By mid-November, it was necessary to amputate the left leg, then the right leg and thigh and finally the left thigh. By January of 1969, the condition of his hands began to deteriorate and further surgery was needed. Finally, devoid of legs and able to use only one hand, he remained a helpless torso until he died of cancer some 18 months later. More graphic details are given in Appendix II.

A recent and no less dramatic incident has been reported by Dr. D. Beninson of the Argentinian Nuclear Regulatory Commission (1984). It occurred at the national RA-2 research reactor late on a Friday afternoon in September 1983. The facility manager, an experienced reactor physicist of about 50, in haste to complete an important experiment, entered the heavily shielded reactor cell after defeating all of a complex pattern of interlocks. He was unaccompanied,

leaving three members of his staff in the control room. With the safeguards inoperative, he was able to re-arrange the core without drawing off the moderator, a time saving manoeuvre that he had repeated several times previously. This time he erred by failing to load absorber in several of the channels. The assembly went prompt critical, there was a Cherenkov flash and he fled from the chamber. Void formation, fuel damage and secondary safeguards prevented a second criticality. The man who was guilty of culpable human error received a whole body dose of several thousand rems. Vomiting and diarrhoea started within 30 minutes. He died of respiratory failure through oedema of the lungs some 49 hours later. He was compos mentis until the end, being able to discuss the circumstances of the incident and improved safeguards and interlocks with official investigators and the facility staff. The excursion was estimated to have released 10MJ with 10^{17} fissions.

4.4 The generality of radiation accidents

In view of the extensive present day use of these extremely dangerous things, particularly gamma ray sources and radio-isotopes, it is not surprising that there are frequent reports of radiation accidents. Owing to the circumspect way in which they have come to be handled and, not least, to the effectiveness of the regulatory controls, the number of the incidents is relatively small. In the U.K. in 1978, there were only 15 'whole body doses' of greater than 5 rems reported to the HSE (R. Gausden 1979). Of them, only one lay in the range of 50 rems to 100 rems and, though this is an undesirably high dose, it is not one considered to be excessively traumatic and not unknown in certain medical diagnostic procedures. As these occurrences are to be identified with the generality of industrial and process accidents, they are not in the category of 'low probability events' and are not considered further here.

4.5 Oil, Petrochemicals and Liquid Natural Gas (LNG)

In spite of the attention focussed on atomic energy and its potential hazards and the hostility directed towards nuclear power, the petroleum industry has been the cause of much greater damage to property and harm to humans. The incidents are numerous, but it will suffice to mention but a few here. An early incident caused by bulk use of liquid natural gas occurred in 1944 when a storage tank in Cleveland, Ohio, ruptured and the liquid ran out into the nearby streets

and sewers. There was an explosion which caused 128 deaths and some 300 injuries (H. Kunreuther 1980). There was a sensational and devastating accident when the French oil tanker 'Betelgeuse', blew up off Whiddy Island in Bantry Bay in Eire on January 8, 1979 killing 50 people, but had the conflagration spread to the adjoining oil storage terminal, the toll of death and damage could have been much greater. The annihilation of half the Spanish holiday camp at San Carlos de la Rapita on July 11, 1978 when 144 campers were burnt to death by a flood of propylene gas which spewed out of a crashing tanker-truck is typical of the hazard posed by overland transport of petroleum products in bulk. Disastrous explosions in giant marine bulk oil carriers continue, in spite of inert gas filling of their oil tanks and other safety measures. The extent of the coastal pollution caused by these vessels is notorious, and unpleasant traces of the 'Torrey Canyon's' disastrous grounding on the Seven Stones Reef between Lands End and the Scilly Isles on March 18, 1967, still linger on the holiday beaches of Devon and Cornwall. She was carrying 171,000 tons of crude oil from Kuwait to England. The wrecked hull was badly holed and upwards of 30,000 tons of her cargo escaped to form a slick 18 miles long by up to a mile wide. Had it not been for energetic salvage and decontamination attempts, the coastal contamination would have been much worse.

4.6 Underwater technology and its dangers

Another important venture of the new technology is the exploration and recovery of the riches of the sea, ocean bed and its mineral bearing strata. Though the gains from the winning of these treasures promise to be very great, to which the present abundant flow of off-shore oil gives evidence, the associated risks are likely to be high, especially to the workers exposed to them. A foretaste of this adverse aspect is given by the toll taken by the efforts to win continental shelf oil so far, let alone that from deeper waters. Since 1976, more than 200 men have died in oil rig sinkings (TIME, March 1, 1982). Furthermore, the vast as yet untapped natural resources of Antarctica offer a challenge likely to bear a heavy human penalty. They can only be tapped by driving through thousands of feet of the thick glacial cap or by working in seas thick with shifting pack ice or at hazard from huge icebergs, often the size of small islands. However, that is a story for the future and the immediate case concerns the price which is being paid for the extraction of off-shore oil.

4.6.1 Oil and the toll of its extraction from under-sea fields

The search for oil, that raw material on which all advanced economies are critically dependent, and its extraction from land sited fields has not proved to be a highly dangerous undertaking, having an accident rate comparable with that of the construction industry. On the other hand, off-shore oil and specially from the open sea has been won only at the expense of many lives, particularly in rough, stormy and unsheltered waters like the North Sea.

Certain phases of the work of drilling for oil and its extraction can not be carried out from large rigs on the surface, but require underwater operations by divers working on the sea bed often at the maximum safe depths from diving bells or at even greater depths by men in small submarines using manipulators. On return to the surface after a stint below, the divers must endure extensive periods of decompression which may last for several days, but the long term effects of the exposure of their lungs and blood stream to mixtures of oxygen and noble gases at high pressure are as yet unknown, though there is some evidence of bone necrosis.

There have been a number of casualties both in the diving bells and submarines through interruption of life support services when supply lines and cables to the surface have been accidentally severed or otherwise cut off. In the case of the large semi-submersible rigs and platforms, upwards of ten thousand tons or more used in deeper waters, the novel engineering and reliability problems which have had to be faced have by no means yet been solved nor even fully appreciated. There have been a series of sinkings with many fatalities and these happenings have been paradigms of the catastrophic low probability event (LPE).

Two of the more recent of these tragic LPEs of which the causes have still to be fully explained involved large rigs thought to be very reliable and able to withstand the most violent of storms. One in the North Sea was the loss of the 'Alexander Kielland' with 123 lives on March 27, 1980 when the rig, a 10,105 tons semi-submersible 'flotel' with 212 men aboard, capsized in a heavy gale, though not excessively high seas. The immediate cause of the catastrophe was the structural collapse of one of the four buoyancy legs. The rig had previously been surveyed and classified as 'absolutely safe'. The other was the sinking of the 'Ocean Ranger', one of the World's largest drilling platforms, off Newfoundland on February 15, 1982. It capsized

in a severe storm and high seas owing to failure of its buoyancy stabilising system. None of the 84 men aboard survived. The rig had been built in Japan in 1976 and was designed to endure the wildest expected weather conditions and to ride out waves of up to 110 ft, much worse than those experienced at the time of the incident.

PART TWO

A REVIEW OF THE SALIENT PROBLEMS OF RISK PERCEPTION, APPRAISAL AND MANAGEMENT IN THE FIELD OF ADVANCED TECHNOLOGICAL INNOVATION

Sections 5 to 7 covering:

The growing public concern about the course of technological advance, evinced in an often largely irrational way, and the hostility to nuclear power evoked by the continuing series of sensational catastrophic failures of technological systems as publicised by the media; the emergence of an informed public opinion as a major political force; further emphasis on the essential need for technical progress if the grave dangers of political and economic destablisation on a world scale due to resource exhaustion in the face of demands for better standards of living by a rapidly increasing population on the planet are to be avoided; the loss of confidence in the kind of health and safety protection provided by conventional regulatory procedures; an appraisal of the state-of-the-art in risk science; a critical review of both quantitative and qualitative methods of safety analysis with reference to the U.S. Reactor Safety Study; the enduring concept of the Maximum Credible Accident (MCA) in safety engineering; the importance of cultural factors in risk perception and management; 'trans-science' - the fringe between science, culture and politics; and the central role of the engineer in the assurance of safety.

THEMATIC SYNOPSIS

Part Two in its review of the grave social and geopolitical problems associated with the growing hostility in the West to technical innovation, and to nuclear power in particular, problems aggravated by rapidly rising, though cyclic, demands for amenities, food and energy in particular, has opened the way for an examination in depth of the methods currently adopted to manage the risks of innovation in technology and for arguments in favour of a new treatment.

5. THE ENIGMA OF MODERN PERCEPTIONS OF TECHNOLOGICAL HAZARDS

'Periculosum est credere et non credere;

. . . . . .

Ergo exploranda est veritas multum, prius
Quam stulta prave judicet sententia'.

(It is dangerous to believe and to disbelieve;
therefore it is far better that the truth be
thoroughly searched, than that a foolish
opinion should pervert your judgement.)

Lucius Phaedrus, 25 B.C.
Fables, Book 3, 10, 1 and 5, 6.

The peculiar, unanticipated disastrous accidents, briefly outlined in Sections 3 and 4 above of which some are dealt with in more detail in Appendix II, expose the odd nature of these 'low probability events' (LPEs). Those chosen, mainly in British settings, are representative examples of these rare happenings, selected from reports of the many, multifarious sad occurrences of the calamitous LPEs which follow one another in endless sporadic series. Besides the catastrophic physical consequences which they bring, almost without exception tragic, their summated effect has profoundly influenced and aroused the social awareness of the bodies politic in the communities affected.

The awakened popular disquiet about technology and its hazards is a feature of the modern entity of sentient public opinion engendered in the masses of people as illiteracy and ignorance have been progressively reduced to little more than negligible residue in the more advanced countries. The source of the discontent is to be found in the advance of technology itself, particularly in communications and transport. The process began with improvements in printing and the introduction of the electric telegraph followed by cables linking the Continents that enabled the successful promotion of the great 'thundering' national newspapers of the 19th and first part of the 20th Centuries which both Abraham Lincoln and Bagehot recognised as powerful political forces.

5.1 The emergent political potency of public opinion

Though there have been few times in the recent past when governments have been able to disregard public opinion, it is now a very influential element in democratic politics. In addition to the spread of literacy, technological progress has made it possible for businessmen, politicians, officials and ordinary citizens to travel to

an extent inconceivable a hundred years ago and has provided facilities for rapid communications through postal services, telegraphy mentioned above and latterly the telephone giving virtually instant communications nation-wide and, now, to all parts of the globe. News of the assissination of President Lincoln on April 14, 1865 took ten days or more to reach London. In contrast, the attempt on the Pope's life on May 13, 1981 was known to all within minutes of the occurrence and could be seen to be true through the technical miracle of television that, since the end of the Second World War has been developed to a perfection whereby events may often be observed in the homes of the viewers as they happen. If the occurrence itself is not caught by TV cameras, then the details are recounted by wellknown and trusted commentators. Thus, the citizens of the Western countries, at least, are well informed about the events which make news and the previous ignorance of the common people about the facts and motives which lie behind the political and economic decisions of governments has been dispelled. Enlightened, they respond if strongly motivated to voice opinions on matters of high policy and are able to influence even the most determined of politicians and administrators. Not only Parliamentary lobbies but factional pressure groups can be quickly brought together to challenge unpopular goverrment plans and actions or to promote a sectional interest. Perhaps one of the first manifestations of the phenomenon of the power of spontaneously evoked mass displeasure was the forced resignation of the British Foreign Minister, Sir Samuel Hoare, on 18 December 1935 by public indignation over the Hoare-Laval proposal to yield Abyssinia to Mussolini.

More recently, strong and often violent protests have been directed against major technological projects, particularly in opposition to the construction of nuclear power stations. This has been expressed in legal prohibitions that in certain cases have brought power station construction work to a halt in the U.S.A. and in violent clashes between anti-nuclear demonstrators and the police in West Germany. More extreme manifestations of hostility to technology have been reported from Spain where the Basque Homeland and Liberty (ETA) group of terrorists by a series of murders, woundings and explosionns over some years in May of 1982 finally forced the constructors to abandon work on the Lemoniz nuclear power station in Northwest Spain, although the plant was nearing completion. The Government had refused a referendum on the siting of the station which the petitioners said was too near the crowded city of Bilbao.

Furthermore, organised groups of concerned citizens and objectors can engage the support of contrary or dissident, but eminently expert and thus formidable, witnesses who have the knowledge and authority to confound the most assured advocates of an officially backed technological project. In fact the pursuit of this kind of adversarial activity has become a minor profession, as for example the efforts of Ralph Nader (1979) and A.B. Lovins. The latter is noted for a strong aversion to nuclear power which should, according to him, 'remain remotely sited in the Sun where it can flourish' (Lovins 1974).

By raising standards of living, by encouraging mass education and literacy and by improving communications, things without which it can not thrive, technology is hoist by its own petard, having articulated its antagonists. Whereas at one time, the principles and formulation of an important engineering project could be decided in camera and then proceed to implementation without extraneous probing and evaluation and would be accepted and sustained by public trust in the officials promoting it and in their expert advisors, this is no longer the case. There are few projects today which can escape public scrutiny and debate if they are likely to bear upon the safety of the environment, workers and general public.

5.2 The growing unease about technological innovations

The opposition to technological innovation is not entirely without cause. Exposed to the endless occurrence of disastrous LPEs and subjected to frequent warnings about the risks of iatrogenic disease or teratogenesis from the use of drugs and remedies on one day asserted to be safe and on the next announced to be harmful, the people of the Western world are not surprisingly sensitised to the dangers that technical innovations may bring. In a report written for the Council for Science and Society Professor John Ziman, summing up the views of his Working Party, wrote that there is evidence of -

> '.... public disquiet at the increasing cost of mistakes in large scale technical projects: mistakes sometimes revealed at the planning stage, sometimes during design and construction, but increasingly often only in operation .... a modern chemical plant explodes, a newly introduced air-liner crashes .... the increasing scale and complexity of human artefacts - machinery, vehicles, buildings, power stations, communication networks, etc., generate a new scale of damaging consequences of failure'.
>
> Superstar Technologies,
> Barry Rose, London, 1976, 'Preface'.

He followed with the observation that -

> 'It is now within our capacity .... to design and introduce a completely new technical system on a large scale without practical experience or tests ..... changes in the social and financial organisation of industry have also weakened some of the forces controlling technological innovation ..... fertile innovators such as Isambard Kingdom Brunel or Thomas Alva Edison carried heavy personal responsibility for the safety and success of their designs and inventions ..... they could not hide this responsibility in the anonymity of a large design team ..... or in a bureaucratic corporation.'
>
> (Ibidem - Para. 1.2.6.)

Thus, the historically established checks and safeguards no longer operate and 'the evolution of successful and safe techniques by natural selection' and exposure to failure in operation, as has been the case in coal mining, can no longer take place. Safety assessment in advance of use and various methods of prediction have to replace the testing experience of failure and proving tests are no longer feasible nor permissible for large scale systems such as a nuclear power plant.

The widespread apprehensions about the possible adverse consequences of further scientific and technical advance not only pertain to the artefacts of engineering and the unpleasant side-effects of new drugs but have deeper roots fertilised by worries which relate to the effect these things may have on human values, the freedom of thought, discussion and the exercise of personal discretion, the family and of intimate inter-personal relations of love and trust and, above all, the ever-present and perhaps growing threat of nuclear Armageddon. As Kirkpatrick Sale in his book 'Human Scale' (1980) has suggested these anxieties may come from a 'primordal human impulse' of self-preservation and instinctive defence of an ecology sensed to be under threat. All these things among other less identifiable influences have helped to feed the present growing tide of suspicion and antipathy which seems to be flowing against technical innovation in general, and against advanced technology in the domain of energy supply and generation in particular. Although of themselves intuitive and amorphous, such fears make fertile ground for the more extreme kinds

of environmentalist advocacy like those of T. Roszak (1972) who portrays technological development as 'malevolent and anarchic' with man as a slave to 'technology out-of-control'.

5.3 Anti-technology arguments: supposititious and real

The cases that the anti-technologists, eco-activists and latter day Luddites (4) advance in support of their opposition to technological progress and innovation usually have superficially plausible factual bases by associating their objections with a hazard, environmental or ecological detriment or threat to a long established trade, being a danger that is known to exist even though it be minimal. When these arguments are pushed beyond their verifiable factual limits, they soon become less rational and are often extended by dubious postulations, speculative inferences, frank emotional appeals or warnings of direct action. Typical of such specious argumentation are the 'hot particle' hypothesis of lung cancer induction following ingestion of traces of plutonium that was publicised by Gofman and Tamplin (1973) and the equivocal extrapolations from technical data so ingeniously used in the anti-nuclear power film, 'The China Syndrome' (6).

The anti-nuclear onslaughts of A.B. Lovins (1974), Bacon and Valentine (1981) and multifarious other polemicists are so committed and intense that it has been suggested by S. Cotgrove (1979, 1982), O.H. Critchley (1980) and F. Sandbach (1980) and others that they are displacement activities relieving deeper concerns about trends and tensions in contemporary society as already suggested (supra). John C. Chicken in his review, 'Nuclear Power Hazard Control Policy' (1982) takes the more specific view that the terrors of nuclear warfare have, by association, coloured public attitudes towards real, but quite different, risk in the matter of nuclear power. This simple, single factor theory is true but insufficient and the circumstances are more complex. There is no doubt that there is an association between the dangers of radiation accidents in nuclear plants and the destructive potential of atomic bombs, especially in relation to fall-out, but there are other important considerations. For example, Flood and Grove-White (1976), two leading environmentalists speaking for the Friends of the Earth, see the 'nuclear threat' in terms of bureacratic centralisation of power and of sabotage and terrorism directed against the country's vital electricity supplies concentrated in relatively few vulnerable units evoking protective responses from the Government inimical to civil liberties.

Despite suspicions that the foregoing grim scenarios of 'hot particles', low level radiation carcinogenesis and teratogenesis and catastrophic nuclear reactor accidents are disseminated as a cloak for more political objections to advanced technology and nuclear power in particular, they can not be lightly disregarded. Taking the nuclear case as an exemplar, there is no doubt that the vision of a sudden and massive release of a cloud of insidiously poisonous fission products, described in the early days of atomic weapons as a 'particularly vicious form of poison gas' (H. de Wolf Smyth 1947), able to spread death, disease and destruction for hundreds of miles from the afflicted plant is frightening. The panic and tumult that followed immediately upon the Three Mile Island (TMI) incident of March 28, 1979 (See Appendix II) give clear evidence that these threats are certainly held in awe. Moreover, it is generally believed by both advocates and critics of nuclear power that a major reactor radiation accident accompanied by casualties clearly attributable to it - there were none from TMI - would bring the nuclear industry to a halt.

5.3.1 Nuclear Power: vestigial risk

Notwithstanding that the chances of a severe radiological accident at a nuclear power station are very small, approaching zero in a soundly designed, well-built and competently managed plant, they are still finite. The worst consequences are truly grave, giving some justification for the foregoing fears. The maximum accident involving an operating installation that has reached equilibrium with its fission product burden has been authoritatively envisaged as posing a worst case threat of 'about 3,400 killed, 34,000 injured and property damage of up to $7 billion' from a 500 MW(Th) reactor according to a wellknown U.S. Atomic Energy Commission sponsored study (H.S. Vance 1957). Present day reactors are larger and the fatalities, harm and damage would be correspondingly greater. A recently updated estimate of the possible consequences of the worst accident to a U.S. type of Pressurised Water Reactor (PWR) is 100,000 deaths and $300 bn in property damage (Sandia Lab. 1982). Furthermore, apart from any direct injury to people or damage to property off the site, the capital, clean-up and revenue losses can be very large. For instance, the General Public Utility (GPU) to recoup themselves for the losses incurred as a result of the TMI incident have sued the constructors, Babcock and Wilcox, for $4 bn for negligence and with failing to inform the Utility of 'the safety hazards at the plant' and the U.S. Nuclear

Regulatory Commission (USNRC) for $4 bn for incompetent regulation (Financial Times Nov. 2, 1982). If the 'loss detriment' relationship hinted at earlier (2) could be quantified, then the huge financial losses incurred by the TMI incident might be expected to cause some reduction in the aggregated life-span of the population upon whom the burden of meeting the cost fell. However, the topic is peripheral to the theme of this research and will not be pursued.

5.4 The riddle of hostility to nuclear power

In view of the foregoing horrific scenarios, despite the fact that it is generally agreed that the chance of such a major reactor radiation accident is minuscule, even the most confident of nuclear engineers, let alone members of the technically informed general public, find the prospect disturbing. However, the reality is that, although nuclear power is admittedly fraught with danger and in spite of a number of serious plant accidents, as far as the public and environment are concerned the hazards have been successfully managed and contained for more than 25 years. Since October 17, 1956 when the Calder Hall nuclear power station went 'on the bars', and until the end of 1981, 272 nuclear power reactors with a capacity of 152,603 MW(e) in 23 countries had been commissioned and were in operation generating 9% of the World's total electricity. These reactors had accumulated some 2600 reactor-years of operating experience (IAEA Report for 1981), during which time no member of the public has been known to have been harmed as a result of exposure to radiation, no property external to the site of any reactor has been damaged and there has been no sensible contamination of the environment. The net picture is one of safe operation of clean and reliable nuclear plants that, unlike power stations burning fossil fuels, emit neither noxious, corrosive nor toxic fumes and in no way make any contribution to the growing menace of 'acid rain' which Robin Porter of the U.S. State Department (1982) has described as 'the most serious environmental problem facing the World'. Besides, the fact that nearly 3,000 reactor-years of operating experience have now been accumulated provides strong evidence in support of the claim that nuclear power can be kept adequately safe, assuming that the existing standards of safety engineering and operational vigilance are sustained. A major nuclear contribution is essential to any longer term World energy balance and efficaceous action to provide it should be taken soon. Therefore, it may be truly said that 'Those who attack nuclear energy show a cynical denial of human ingenuity' (A. Weinberg 1979) and a similar disregard for the needs of mankind.

5.4.1 Opposition hardening

Be all that as it may, hostility to nuclear power seems to be far from abating, indeed, it may well be hardening, confirming Alvin Weinberg's view of some years ago (1977). It has forced the cancellation or postponement of 8 confirmed orders for reactors in the United States and there is no certainty of any new power reactor orders in the coming years (IAEA Report for 1981). Yet, atomic energy is one of the prime sources of environmentally clean power, offering a developed and tried technology with fuel reserves that could last till the end of the next century or longer.

It is true as John Chicken has said (supra) that the adverse reaction to nuclear power has to a considerable extent been inspired among the less well-informed sections of the public by a false perception of the risks which they attribute to nuclear reactors by association with atomic bombs. This effect is waning as a result of educational publicity and is probably of little consequence now. Despite that, there is a related factor that is perhaps less openly acknowledged for its influence on public opinion but nonetheless telling. A nuclear power reactor can, without undue difficulty, be programmed to produce military grade plutonium and provide the transmutational facilities to produce a stockpile of atomic weapons and keep them at the ready. Albeit expensive and sophisticated chemical separation plants are needed, but these can be acquired. In the case of the powerful recognised weapon states, like the U.S.A., Britain, Russia, France and now China, this is of little relevance, but not so for smaller, possibly aggressive, turbulent and unstable nations which make up the large parts of the World. Further, even in the case of those nations that have signed the Non-proliferation Treaty (NPT), their obligations can be abrogated unilaterally on three months' notice. There is, therefore, widespread and due concern that an expansion of nuclear power in the major industrial countries could result in its spread to states that might be less inclined to responsible and self-denying behaviour in the acquisition and deployment of nuclear weapons. This state of affairs coupled with a lack of faith in the effectiveness of restraints that can be imposed by international bodies like the United Nations or, even by the Great Powers on their smaller associates, is disturbing to responsible opinion forming elements in Western countries (Sir Brian Flowers 1976/a).

5.4.2 Fallacious affirmative arguments

Regrettably, the case for nuclear power is not furthered by resort to the ingenuous, but subtly misleading, arguments in which the controversy abounds, for example:

> 'Before discussing the hazards of nuclear power, we would emphasise that in many respects these are not unique. ... . There is a tendency to dramatise the risks in ways which convey quite misleading impressions to people who have no basic knowledge of the subject. It is said, for example, that a piece of plutonium the size of an orange contains enough of the substance to kill everyone on earth. So it does, but it is impossible that it could be so distributed as to have this effect. A very similar statement might be made about other substances that are commonly produced and used in industrial societies. For example, chlorine is a very basic material in the chemical industry and is made in the U.K. alone to the extent of about a million tons per year. Yet a mere 10 mg would be lethal if inhaled; little more than a two-millionth part of our annual production would, in theory, suffice to kill the entire population. It is important to see nuclear hazards in perspective and we have tried to do this throughout our study.'
>
> Sir Brian Flowers,
> Sixth Report: Nuclear Power and the Environment, Royal Commission on Environmental Pollution,
> HMSO, Cmnd 6618, Sept. 1976, S.162.

The argument is, of course, true, but it is not as relevant to nuclear power plant accidents as the Report imputes. In the case of the catastrophic failure of the containment of a large nuclear power reactor consequent on melting of most of its burden of nuclear fuel not only can a very large part of the core's radioactivity be released to the atmosphere, but it would be dispersed with the caprice of the elements and could cause up to 100,000 deaths in the worst conceivable case. The accident is highly improbable but not impossible as with the case of the chlorine. It is an example of the 'Zero-Infinity Dilemma' that at times faces insurers: almost vanishingly small risk coupled with indefinitely large and ruinous consequences, for example that of TMI with $8 bn or more in pending damage claims (supra). It is this kind of calamitous accident that is the true matter of concern in the case of nuclear power and not the toxic effects of minor releases of radioactivity that may be properly likened to other harmful pollutants of industrial society, eg lead in petrol exhaust fumes from motor traffic and the oxides of nitrogen and sulphur in power station flue gases, and the carcinogenic dusts and vapours to which workers are exposed in many factory environments.

5.5 Conditions for toleration of the nuclear power risk

In view of the prevailing doubts, public confidence in nuclear safety is unlikely to be won by attempts to prove that the hazard is so small that it may be ignored by recourse to arcane and elegant risk mathematics that try to present the dangers as sensibly zero and therefore insignificant by obscuring them in a fog of vanishingly small numbers (O.H. Critchley 1982 and elsewhere). The meaningful objections to nuclear power have roots in a different soil than that provided by commonplace accident data, namely one that is composed of the cultural attitudes to risk and chance and of the dominant societal perceptions of the nuclear hazard and of the economic and political changes likely to be brought about in a society that had become largely dependent on atomic energy.

To secure acceptance, or better, toleration of the 'Zero-Infinity' hazard of nuclear power (See Section 8.3 et seq.) the public exposed to the risk must be convinced that exposure to it is in their best interests, that the potential threat can be effectively kept on a firm engineering leash and, further, that the standard of safety management set in the beginning will not relax with time, but remain ever critical and vigilant. This concept of 'safety-by-contained-danger' effectively sustained by continuous alert surveillance is that of 'Defended Safety' - a theme to be elaborated upon in the passages that follow.

6. THE IMPERATIVE FOR CONTINUING TECHNOLOGICAL PROGRESS

> 'Technology made large populations possible, large populations now make technology indispensible.'
>
> Joseph Wood Krutch;
> The Nemesis of Power:
> Human Nature and the
> Human Condition, 1959.

As it has been noted earlier in this text, the long accepted view that technological progress is inherently beneficial and can eventually cure all the ills of the human condition and pave the way to a utopian future, is nowadays seriously questioned and, indeed, is vigorously opposed by some committed groups of social reformers. They advance well argued contentions that technological innovation should be halted or at least changed in direction. Supporting the latter view, David Dickson wrote that:

> 'Contemporary society is characterised by a growing distrust of technology. The many social benefits which technology has helped to bring about are being increasingly counterbalanced by the social problems associated with its use.'
>
> Alternative Technology and
> the Politics of Technical Change:
> Introduction, 1974.

Unfortunately the issue is far from simple. Dickson is wrong in his premiss that 'technology has become an integral part of our social world'. He is wrong because technology is not a thing apart from the human condition. Instead, technology and the social world are, and always have been, integral parts of the same thing, that is the causal means of man's evolution from beast to intelligent social animal. Therefore, technical progress can not be turned off and on like a tap. Man has a choice between continuing technical progress which is, in fact, being subjected increasingly to adaptive and all-embracing controls in the advanced countries of the World and stagnation. Stagnation is a state that characterised the closed Oriental societies of China and Japan until the latter was 'opened up' by Commodore Perry's gunboats in 1854 and the regression that sealed the fate of the Tasmanian aborigines who had lost the art of making fire and were losing that of speech when contact with the White Man finally extinguished their race. That technological progress must continue is a fact; that it must be properly regulated is a necessity. This latter state is being achieved, the problems

of contamination, pollution and resource destruction are being identified and the required regulatory agencies are being created like those for environmental, energy and resource conservation in the U.S.A.

It is not generally realised how deep lies the opposition to technical progress in Western society today. Hostility has been conspicuously focussed on nuclear technology as the front runner on the technical scene. The phenomenon was broadly examined in the preceding Section 5, though with attention directed at its political, psychological and sociological features. As its military aspects are inviolable, it is the civil application in nuclear power that bears the brunt. The disapprobation runs from the open distaste shown by Gofman and Tamplin in 'Poisoned Power' (1973) and their kind to the less than enthusiastic tolerance evinced by the Royal Commission on Environmental Pollution:

> 'Our basic concern is that a major commitment to fission power should be postponed as long as possible, in hope that it might be avoided altogether, by gaining the maximum time for the development of alternative approaches which will not involve its grave potential implications for mankind.'
>
> Sir Brian Flowers (Chairman)
> Sixth Report: Nuclear Power
> and the Environment,
> HMSO, London, Cmnd 6618,
> September 1976, S. 511.

At this point in the argument and before moving on to a more technical line of thought, it may prove helpful to recall an earlier posit about the importance of nuclear energy. The fact must be faced that the existing energy glut is historically only a short, transitory experience. The CEGB may now have 30% or so excess capacity, but this could disappear very quickly. Obsolescent plant is being phased out and the lead time for new plant is of the order of 5 to 10 years.

When, as eventually it must, the present slump ends and industrial activity returns to, and exceeds, its earlier norms, the demand for energy will at least grow in proportion, if not at a much faster rate. Once again, the spectre of resource depletion and an energy famine will emerge. It is then that nuclear power can play a key role. It will be necessary to mollify and overcome the opposition before that time. Essential tasks are to find an acceptable approach to safety assurance in nuclear power technology

and to establish controls that are neither stifling on the one hand, nor too lax on the other, but ones that encourage a due measure of progress and innovation. Above all, it must secure acceptance from the body politic by inspiring confidence in its engineering. It is certain that the forthcoming energy deficit cannot be made good by recourse to an undefined 'Alternative Technology' sans nuclear power that would have to fill the void created by 'the disappearance of contemporary forms of science and technology' as envisaged by David Dickson (1974) and those who, to a greater or lesser degree, share his convictions.

6.1 Population growth and the inevitability of technical change

Posed against the rising tide of hostility to technology are the growing needs of the rapidly increasing populations of the World. Those needs are the result of the medical successes in the fight against disease; of the achievements of public health in providing clean drinking water and sanitation; of the eradication of the vectors that transmit parasites; and of the reduction in infant and maternal mortalities. The accelerating growth of World population is shown in Table I. The step increase that occurred during the latter part of the 18th Century coincides with the onset of the Industrial Revolution. It continued without remission in the West until the First World War when it began to slow down, a phenomenon that has been attributed to the lengthening span of time needed for the education and training of the young in those countries. In the rest of the World, rapid population growth began about the time of the American Civil War, continuing at an accelerating rate since. The population of the World has more than doubled in the last 80 years or so and there are now about 4 billion people on the planet, a number likely to reach twice that size in the next 25 years.

Examination of Table I provides some evidence that the massive increase in the World's population is largely the result of a longer expectation of life from birth. A surprising characteristic is the change in that expectation from some 22 years in the heyday of Rome, a relatively stable and prosperous time, to a span approaching 75 years today. The longer expectation of life, basically a steady change over the centuries of human existence is by no means wholely due to improvements in hygiene, medicine and nutrition (Cosslet P. Putnam 1954). In spite of suggestions to the contrary, the Romans did not die young in mass because of lead poisoning (eg A. McWhirr et al 1982), though no doubt the extensive use of lead did not contribute to good

TABLE I
Life Expectance Changes

THE EXPECTANCE OF LIFE FROM BIRTH IN RELATION TO THE CHANGING POPULATIONS OF THE WORLD, WESTERN EUROPE AND RUSSIA OVER THE CENTURIES

DATE	EXPECTATION OF LIFE AT BIRTH	MILLIONS OF PEOPLE WORLD	MILLIONS OF PEOPLE W. EUROPE & RUSSIA	SOURCE
(B.C. 10,000	18 years	1.0	——	Cosslett Palmer Putnam, Energy in the Future, MacMillan, London, 1954
1 A.D.	22 "	275	(61)*	
1000	(22)* "	285	(63)*	" " "
1450	33 "	375	(83)*	" " "
1650	(33.5)* "	470	103	Everyman's Encyclopaedia, Vol. 10, Readers Union & J.M. Dent, London, 1968.
1750	34 "	694	144	
1800	(35)* "	919	193	
1840	41 "	1091	274 (1850)	" " "
1900	49.2 "	1571	423	" " "
1920	58.3 "	1811	487	" " "
1940	64.6 "	2249	573	" " "
1960	71.0 "	2995	641	" " "
1975	73.0 "	3967	728	Whitaker's Almanack, 113th Edition, 1981.
2000	(>76)* "	(6267)	(947)	

Apply to W. Europe and U.S.A. only

NOTES

(a) The bracketted figures are estimates. An asterisk (*) indicates an interpolation by the writer.

(b) The figures are 'accurate' in the case of those countries in which some form of census has been possible, otherwise they are broad estimates which vary by as much as 20% among those authorities held to be expert.

(c) There is a widely held view that the spurt in growth of the World population after 1650 was not due to increased fertility, but to a fall in mortality, particularly amongst children and young adults which coincided with the increasing standard of living attributable to the growth in the productivity of labour characteristic of the Industrial Revolution.

(d) C. Palmer Putnam does not seem to be wholely in agreement with the opinion quoted in Note (c) above. He observes that the population of China (a country where some sort of attempt to enumerate the total population has been made throughout its long civilised existence) together with that of all the West passed through a minimum in the 7th and 8th Centuries. There was little change until about 1600 when a population explosion began in both areas and which has followed broadly the same continuing pattern ever since. He attributes this, like others, to an increase in life expectancy, though the reasons for this are not fully understood. The effect of improving standards of living is less than might be expected. Some suggest that it might be due to an evolutionary change expressed as lengthening of the human life span.

health. Moreover, the growth of population has little to do with fertility for which there is little evidence of change, but a lot to do with vigour and survival potential. Putnam has suggested that factors as yet unexplained are involved, perhaps an evolutionary change.

6.2 Booms, slumps, the long wave cycle and technological development

One thing is certain, a massive increase in the production of food, goods and services corresponding to the growing size and wants of the human race, not only in the Western nations, but more essentially in the presently backward and deprived countries of the World, is an absolute necessity. There are few, if any, amongst this growing mass of humanity who do not aspire to a fuller, better, healthier and happier life-style and the medium of modern communications by its wide dissemination of knowledge about happenings and conditions of life on other parts of the planet must make their demands ever more insistent.

The problem of meeting the needs of the World today as the Western economies seem to be slipping into another period of cyclic depression corresponding to the 'Great Slump of 1929-1932' (Warren, J.P. 1982) which is currently baffling our politicians and will become even less tractable as we move into the 'Troubled 21st Century' predicted by G. Speth (1980). If the present Western economic distress is in fact a manifestation of a 'Krondriateff' cyclic down-swing, then, as suggested by Sir Bruce Williams (1981), escape can be effected only by extensive restructuring of patterns of production, employment, remuneration and mangement. Changes of this kind have given relief from previous long-term-cycle slumps. The relevant point is that they result in the long run in greatly increased demands for goods and services, substantially raising living standards in the countries that so respond. It will then be necessary to face sooner, not the problems of bounty, but the inevitable exhaustion of many of the planet's natural resources of oil, certain essential ores and other commercially important elements and compounds which will then be in short supply. Furthermore, the productivity of labour of all kinds is dependent on technical aids and, above all, on the availability of adequate sources of energy to power them.

There is then, now and most certainly in the future, an imperative need for continuing technological progress, mostly of an advanced nature, so that not only can the dwindling resources of the Earth be made good, but other kinds of natural wealth can be tapped, for instance from the

sea bed, in Antartica and even from the waters of the oceans themselves. All these things need in addition to bold and innovative technologies, energy in abundance. Hence, the energy generating and distribution industries must flourish, expand and utilise the most advanced methods to provide warmth and light, to drive machinery, to mine and smelt ores, to till and irrigate the soil and to transport man and his goods across the World in pursuit of commerce and friendship. The alternative of 'no-growth' or shrinking economies is not possible, unless man is to slip into a new Dark Age.

If technological advance does not continue and, indeed, perhaps be accelerated, then that 'Troubled 21st Century' (supra) which is less than two decades away will be a nightmare of social turbulence, wars, ecological disasters and starvation. Nuclear power is but one facet of the technological progression that will be necessary to avoid such calamities and, possibly, by no means the most hazardous among many innovations. For example, a hydrogen economy based on nuclear power as the prime energy source as suggested by C. Marchetti (1974), would be accompanied by some very grave risks.

As the result of the concomitant changes in social structures that come inevitably with technological change, confrontations, not only with those motivated by anti-technology and environmentalist sentiments, but, more seriously, with those groups whose employment and social status are threatened, may be expected.

History teaches that social groups whose existence and status is so threatened do not just disappear quietly, but react instead vigorously to the challenge. But, one thing is certain, despite these changes and the hostility they may induce, the World, in the long run, will have to face an ever increasing demand for energy. It is a demand that is most unlikely to be met without a major contribution from nuclear power.

6.3 The need for new safety concepts

The envisaged threats to society and the environment created by the innovation of the new hazardous technologies among which nuclear power plays the foremost place by tradition can be dealt with either by removing or, where that is not feasible, by containing them by physical means. Containment has been achieved with success in the nuclear case, but not in a manner that has disarmed those who persistently impugn its safety.

The commonplace dangers of pollution, contaminated working conditions and other industrial hazards can be met by regulatory action of the familiar kind, for example by the safety regimen imposed on British industry by H.M. Factory Inspectorate (HMFI) which has been indubitably successful and is the paradigm of its type. This is not so for the threat of Low Probability Events (LPEs) in the classes considered in Sections 3 and 4 of this text.

This lacuna in the system of industrial safety surveillance in Britain was acknowledged in regulatory circles after the disastrous explosion at the petrochemical factory at Flixborough on June 1, 1974. Some time before the incident the premises were visited by a member of HMFI who reported no serious breaches of the relevant regulations, though he did ask for the windows in the Control Room to be made shatter-proof (R.J. Parker 1975/a). In the event, the blast of the explosion demolished the Control Room, killed its occupants and wrecked a large part of the plant (See Appendix II).

The subsequent committee of inquiry found that 'The disaster was caused wholly by the coincidence of a number of unlikely errors in the design and installation of a modification' and noted that 'there was no mechanical engineer on site of sufficient qualifications, status or authority' to supervise the work (ibidem - b). The incident therefore seems to have been the result of a management weakness that was beyond the ambit of HMFI to inspect. The occasional occurrence of the unexpected, catastrophic failures like 'Flixborough' and of which to date 'Three Mile Island' (TMI) of March 28, 1979 is the most notorious, are further indications that existing regulatory philosophy and practice, if not inadequate for the safety surveillance of nuclear power plants and other major hazard advanced technology installations, lack the quality to convince the critical public that they provide proper safeguards aginst the occurrence of such incidents.

6.3.1 The role of nuclear safety engineering

In the case of nuclear technology, jobs and ways of working are not at issue and Ned Ludd does not stand in the way. Instead, employment is created because nuclear power offers a much needed and bountiful source of energy. It is in competition with oil rather than coal, a matter of considerable importance in Britain. The opposition to nuclear power has largely associated its case, at least implicitly, with the mystique of 'The Bomb'. This is a cognizable threat by which general public can be swayed. The potential danger

of nuclear fission and the concomitant hazards of disseminated radioactivity have been made abundantly clear by the existence of nuclear weapons, the reality of bomb test fallout and the importance that has been officially attached to the horrific military deterrent potentialities of the former. Though this fallacious apperception seriously handicaps and obstructs the progress of nuclear energy, it is an identifiable objection that can be refuted because it is irrelevant to nuclear power per se. Moreover, the unique dangers also apperceived are more hypothetical than real. In spite of being well written and researched, Ralph Nader and Abbotts in their 'The Menace of Atomic Energy' (1979) fail to make their case that by the year 2000 there will be 12,000 cases of malignant and genetic disease among the general public attributable to emissions of krypton-85, iodine-29, tritium and carbon-14 from nuclear fuel reprocessing facilities. Nonetheless, safety remains the paramount issue for nuclear power and, more particularly, this lies in the real chance of LPEs in the form of the disastrous potential plant accidents that are on the fringe of possibility. Though there are other reasons that inspire the oppostion, these are matters of politics and diplomacy and are patently capable of resolution given the international will to do so. Still the nuclear option must not price itself out by excessive expenditure on safety, an outlay which is already approaching that point (Charles Komanoff 1980).

Taking all the foregoing facts together, there are good and imperative reasons acting to allay the hostility that has been inspired. It can be argued that this is possible through demonstrable good engineering and alert and efficaceous mangement of nuclear power plants that have already proved that the true dangers of nuclear power to the community and environment are minimal, notwithstanding the incident at Three Mile Island in March 1979. Moreover, in the field of technology generally, as Wolf Haefele (1974) has said, nuclear power plays a path-finder role. Hence, as it presents the foremost and best publicised cause, the difficulties in securing its acceptance or, more properly, toleration of the risk it imposes, when overcome, should assist in securing the successful introduction of other advanced technologies that are so urgently needed by present day society. In this connection, among the most demanding of the challenges that nuclear engineers have to meet is resolution of the dilemma of safety versus cost, how to achieve adequacy while avoiding empty, safer-than-safe investment in safeguards.

7. STATE OF THE ART IN RISK SCIENCE

'Only science can hope to keep technology
in some sort of moral order.'

Edgar Z. Friedenberg
(American Sociologist),
Impact of the School:
The Vanishing Adolescent, 1959.

In the previous sections an attempt has been made to review the historical background in which the disastrous low probability events (LPEs) involving technological systems are set, to depict the characteristic circumstances in which these disasters have occurred with reference to some typical LPEs and to give an indication of the progressive changes in public opinion consequent upon the experience of these calamitous happenings, particularly as they have affected the steps that might be taken towards their management. Over the past two decades and since the plutonium pile incident at Windscale of October 10, 1957 (See Appendix II) which seems to have been a watershed in Government and public attitudes towards hazard management in Britain, there has been an enhanced interest in the study of risk in industry and more generally in personal exposure to the multifarious risks of employment and of living, particular attention being directed at those installations and processes considered to present major hazards to the community. These latter potential LPEs are the 'zero-infinity' risks discussed further in Section 8.3 et seq. and saliently those of nuclear power.

7.1 Progress in Risk and Hazard Studies

The cultural impact of a few, but sensationally calamitous accidents, has, not surprisingly, evoked a spate of attempts to analyse the nature of hazards and to treat risks scientifically. Particular attention has been paid to those associated with atomic energy, specially, nuclear power and, more recently, those arising in the petrochemical industry and in the storage and transport of liquid natural gas (LGN), 'Frozen Fire', as it has been dubbed in some environmentalist circles.

The perception of these dangers, both by the official and other executive bodies concerned with their regulation and by the scientific community, has changed progressively over the past few decades. This has been reflected by a growing tendency to refer to them in terms of 'risk' rather than 'hazard', the former having probability connotations. Risk has thus been the subject of numerous

studies and investigations, many of them of a highly mathematical orientation, that have contributed to a considerable literature on the topic.

Notable among the serious and learned works on risk assessment and management which now abound are W.W. Lowrance's 'Of Acceptable Risk' (1976) and more recently W.D. Rowe's 'An Anatomy of Risk' (1977), 'Energy Risk Management' which is a compilation of papers edited by Goodman and Rowe (1979), several compendia of articles by well-known authorities like 'RISK: a Seminar Series' collected by Howard Kunreuther (1982) of the International Institute for Applied Systems Analysis and the publications of the prestigious Safety and Reliability Directorate (SRD) and its associated Systems Reliability Service (SRS) under the aegis of the U.K. Atomic Energy Authority (UKAEA). Works of a more pragmatic genre among the foregoing are those of F.P. Lees (1980) and T.A. Kletz (1982). Of an engineering orientation, they are largely concerned with the realities of loss prevention and the management of risks to employees in industry, and in the chemical industry in particular. The latter's contributions extend to the economics of hazard control in society for both individual and public (Kletz 1976, 1977).

The Directorate (SRD) were commissioned by the Health and Safety Executive (HSE) to carry out a risk assessment of the extensive petrochemical installation on Canvey Island which is on the North bank of the Thames near its mouth (Locke, Dunster and Pittom 1978). The report is a well structured and researched paradigm of this kind of risk study (10). Its conclusions are backed by exhaustive probabilistic treatments of the foreseeable events that could have catastrophic outcomes in fires, explosions and hazardous releases of liquids, vapours and gases. Published under the imprimatur of the Health and Safety Commission (HSC), it is in two parts, an executive summary and the detailed technical report of the investigating team.

Exemplars among a miscellany of other works are the abstruse actuarial essays on 'Credal Probability and Chance' (Isaac Levy 1980) and an earlier proposal to reduce technological risks by 'Channeling Technology through the Law' (L.A. Tribe 1973) which advocated mandatory product and system assessments with liability for damage and injury strictly imposed. This idea has been incorporated in recent British industrial safety legislation through the Health and Safety at Work Act 1974 which in its Section 6 stipulates that anyone who 'designs, manufactures, imports or supplies any article for use at work' shall ensure 'so far as reasonably practicable' that it is safe in use without

risks to health. This assurance must be verified by an assessment of its design and construction and by testing and examination with such supporting research as may be appropriate. Failure to comply has been punished by substantial fines (McLain, Lynton 1977). Further, the U.K. nuclear installations legislation in a succession of Acts of 1959, 1965 and 1970 imposes strict financial liability for hurt or damage caused by the 'nuclear hazard' attributable to the explosive, radioactive, radiotoxic and radiation dangers peculiar to a nuclear installation, that is a nuclear reactor and certain associated plants and processes as prescribed. In an action, for damage to be awarded, negligence on the part of the defendant does not have to be proved; it is sufficient to show that hurt or damage has been suffered (Street and Frame 1966).

One or two studies not committed to mathematical probability have been either observational or interpretative or concerned with creating a constitutional framework in which industrial and public risk attributable to technology and its innovations could be managed. Recommendations along these lines in regard to 'Public Safety' made by the Committee on Safety and Health at Work of 1970-72 (Robens, Chaps 10 and 11, 1972) have been implemented within the HSE by constitution of a Major Hazards Policy Group, supported by a specialist branch of H.M. Factory Inspectorate (J.G.D. Hammer 1980).

An important work that has received less than due publicity is a report to the Council for Science and Society (CSS) by one of its expert working parties which included representatives of the arts, engineering, law, philosophy and the physical and social sciences. Its findings which were of a general nature and of societal relevance led to the conclusion that:

> 'The acceptability of risks cannot be simply derived from a scientific study of quantified probabilities, costs and benefits. The human factor influences the analysis at every point. .....'
>
> It made the single recommendation that 'those who are exposed to risks which are not immediately obvious to them should have a powerful voice - expressed responsibly and on full information and sound advice - in deciding what risks they should be exposed to.'
>
> J. R. Ravetz et al.,
> The Acceptability of Risks,
> 1977 (9.1.1 and 9.2).

The above CSS report is significant by virtue of its being an important interdisciplinary survey of the, then, state-of-the-art in

matters of risks, their management and acceptability. Though the Report (supra) was issued more than five years ago and a vast amount of research in the field has been done since, there has been little progress towards any concord in the contrary views of the schools represented by the participants in the Working Party that assisted in its preparation. The recommendations made in the Report are anything but positive, being limited to a proposal that there be a wide ranging investigation of the agencies and institutions concerned with control and mangement of the industrial, consumer and environmental risks to which people are exposed and may have to tolerate. Nonetheless, the Report was an important contribution to the study of risk and, not least, it revealed the disparate elements in the risk debate which continues in a very open state and is still topical.

7.1.1 Safety by anticipation - a consequence of atomic energy

The advent of atomic energy in circumstances of its accelerated development in a time of military exigency brought with it a change in the nature of the managerial attitudes to industrial safety. The program was driven forward by political considerations that overrode fears of possible risks, but what was lost from circumspection was made up for by prudence. The hazards of exposure to ionising radiations and of the ingestion of radioactive materials were known to be dire through the painful experiences of two generations of radiologists from the time of the discoveries of W.C. Roentgen in 1895 (R.F. Mould 1980). To these dangers, the novel processes of plutonium production added the chance of a fortuitous escape of radioactivity in relatively vast quantities as well as that of a devastating explosion if 'a pile went up'. Many of the scientists associated with the Hanford project thought it too risky to proceed (Margaret Gowing 1974).

The result was a move away from what might be described as a 'determinist' policy of taking steps learnt from the experience of an accident to prevent its reoccurrence, that is 'safety by hindsight', towards 'safety by foresight'. The policy was revolutionary and put atomic energy in the van as the pace setter in the field of industrial safety, a role that was eventually to determine progress in all other areas of industrial risk management.

A salient feature of the new policy was that of the Maximum Credible Accident (MCA) or, to give it a more generalised title, that of the Design Basis Accident (DBA). The distinction is more than semantic because the MCA tends to be identified with siting policy, whereas the DBA is more suggestive of plant technology. The inadequacy

of the MCA in the former context was properly recognised by F.R. Farmer (1967) whose (then new) approach is discussed further elsewhere in this text (infra). Nevertheless, the philosophy of the DBA continues to underlie the recent developments in design safety assessment, the later quantifying methodologies differing from it more in emphasis than substance.

In addition to the schema given below, a fuller account of experience with the DBA/MCA approach with its weaknesses and wider implications is given in Sections 9.1 to 9.3. The passages that follow are an abridged excerpt from the writer's published work on the philosophical basis of hazard control policy for nuclear power in the U.K. and is taken from Document No. 2 in the Annex of Supporting Papers: On the Maximum Credible Accident -

> '24. The ways in which the MCA could occur were examined by fault studies, by qualitative safety analysis programs and by operational research techniques. The assessed likelihood of the accident occurring was then minimised by modifying the design appropriately so as to provide barriers of various kinds against any identified fault initiating a chain of events which could, in the ultimate, precipitate that accident. These barriers, which included containment structures, design limitations, engineered safeguards, operational restraints, regimes of inspection and other such strategems aimed, not only at preventing the accident, but at securing that the consequences of a given MCA were socially and economically tolerable, eg of minimum detriment without the plant boundary or restricted zone.
>
> 25. Beyond the MCA there was envisaged a second tier concept of a possible, highly improbable Maximum Hypothetical Accident (MHA) which could conceivably break through the barriers established at the MCA thresholds. It was posited that the chance occurrence of such a disastrous accident could be made vanishingly small, if not impossible, by appropriate barrier strategies. For example, in the case of a gas cooled nuclear reactor in a pre-stressed concrete pressure vessel catastrophic failure by bursting is virtually impossible and this limits the extent of any conceivable calamity to the core.'
>
> 'Aspects of the historical, philosophical and mathematical background to the statutory management of nuclear plant risks in the United Kingdom',
> Proc. Symposium on Radiation protection in nuclear power plants and the fuel cycle,
> British Nuclear Energy Society,
> London, 1978, pp. 14 - 15.

7.1.2 Recent additions to the corpus of risk studies

The foregoing critique appears to have been confirmed by a very recent and weighty contribution to risk literature, namely the Report of

the Royal Society's Study Group on Risk Assessment (Sir Frederick Werner 1982) which began its work in November 1978. It is introduced by a prefatory remark about the difficulty of reconciling the various, differing approaches of the biochemists, biologists, doctors, economists, engineers, physical scientists and psychologists who took part. The document which covers in depth the nature, estimation, perception and management of technological risks is orientated towards quantitative probability methods of assessing risks, detriments, costs and benefits in order to provide guidance appropriate to the regulatory processes involved. Again, it recognises the dearth of information about the manner in which the public, as distinct from the individual, perceives and reacts to risk. It concludes with a suggestion that 'the relevant institutions', ' the specialists', 'the public' and 'their representatives' should all be drawn into the work of constructing the necessary regulatory processes so as to achieve acceptance of 'a more balanced approach to the inevitable existence of risks and detriments'. In the matter of catastrophic engineering risks and those of advanced technologies and nuclear power in particular, it proposes that the so-called 'determinist approach' of safety factors and design philosophies based on experience of failures be replaced by one which is 'anticipatory'. It is relevant to note that 'the policy of safety by foresight rather than hindsight' has characterised the atomic energy industry since its inception (Margaret Gowing 1974).

A section of the Report on 'Risk Perception' written by a sub-group chaired by Professor T.R. Lee comes to the following insightful and pertinent conclusion:

> 'Probably the main achievement of research on perception is to demonstrate that the public's viewpoint must be considered, not as a form of indulgence or vote catching and especially not as error, but as an essential datum. This is because in matters of illness, injury and even death, or in policy issues involving questions of morality, only the public can estimate the severity of the detriment involved.
>
> The main methodological dilemma is that the most valid data is that which is elicited from ordinary individuals, but this is no guide to action unless it can be aggregated into something that represents 'the public'. The main administrative dilemma is that different sections of the public, and especially those who are directly exposed as distinct from those who are not, have differing perceptions; leaving a considerable role to be played by political judgement that combines expedience with equity.'
>
> 'The Perception of Risks',
> Risk Assessment: Report of
> a Study Group,
> The Royal Society, London, 1982.

The above findings are relevant to some of the propositions about 'major hazard' risk management in relation to nuclear power to be advanced later in this thesis.

7.1.3 Cultural aspects of risk perception

An important interdisciplinary contribution to risk studies has come from Social Anthropology, or Cultural Anthropology as it is termed in the U.S.A., as for example Michael Thompson's work on the aesthetics of risk (1980). Thompson, an Everest climber and mountaineer of some eminence, views risk from the standpoint of the Sherpa and concludes that an individual's risk taking philosophy is embedded in the cultural set to which he has been conditioned by the society of which he is part.

One of the most controversial difficulties in securing agreement in the field of risk assessment and hazard management is that a dilemma arises from the definition of acceptability and consequent administrative action deriving from it. Risk thus becomes a thing that on the one hand is imposed as acceptable by superior decision makers on those who may be either unaware or unable to appreciate the full significance of the hazard or, on the other hand, something knowingly accepted or tolerated by those exposed to it. It is this dilemma or, then, its overtones that are among the principal factors lying at the roots of popular opposition to nuclear power. It is the pith of the ultimate sentence of the quotation from Professor T. R. Lee's contribution to the Royal Society's recent study of risk assessment and management from which an excerpt is quoted in the immediately preceeding sub-section.

A collection of essays called 'Risk and Culture' edited by Mary Douglas and Aaron Wildavsky (1982) may set a new trend in risk studies. They posit that it is inappropriate to define the problem of risk either in objectively calculated physical terms along the lines of N. C. Rasmussen (1975) in the 'Reactor Safety Study' or in subjectively biased physical perceptions as W. W. Lowrance (1976) attempted in his book, 'Of Acceptable Risk'. Instead, between the two approaches lies a particular culture which shapes the perception of the hazard, a concept suggested earlier by Michael Thompson (1980) though in somewhat different terms (supra). However, Douglas and Wildavsky escape the challenging consequences of their seminal proposition by dismissing 'the possibility that the reality of risk has changed in any significant way, essentially ignoring the increased scale and changing

character of technology-induced risk' (Dorothy Nelkin 1982). Their analysis is thus based on tacit acceptance of given American institutional arrangements for risk assessment, management and adjustment: incidentally a lucrative business activity costing that country between $200 and $300 million or more per year for systems analysis studies and computations.

In spite of their creative and stimulating identification of an hiatus which may well have stultified contemporary risk studies, Douglas and Wildavsky, therefore, fail to acknowledge the discontinuity (supra) that has arisen in risk assessment and management as a result of the very cultural changes brought about by continuing rapid technological advance. Nelkin suggests that this may be a consequence of their clear aversion to any radical approach to hazard control policy that, if adopted, might profoundly alter the above mentioned lucrative institutional arrangements.

7.2 The emergence of quantitative probability methods

Those engineers concerned with safety and reliability in the atomic energy industry were from the start able to draw on the emergent new science of probability-based methods of situation analysis which had evolved from Operational Research for military purposes during the Second World War and the parallel development of statistical reliability analysis which had begun to be used for quality control in the manufacture of weapons, particularly in the mass production of military electronics and radar. At first, attention turned to specific safety matters, for instance the management of power reactor fuel elements and, particularly, to those related to components in the provision of which there was a necessary element of redundancy such as control rods and instrumentation sensor networks. Unfortunately, the early scientific papers on the use of these methods in the nuclear industry are not generally accessible for reference because of restrictions on publication. Notwithstanding that limitation, mention may be made of one or two items in this recondite set of works which were cleared for presentation at open meetings or conferences or were circulated without restriction for comment or discussion.

In 1961, N. V. Worthington of the U.K. Central Electricity Generating Board (CEGB) issued a design guidance note on a 'Fuel Element Temperature Criterion for the Operating (Magnox) Reactor'. About this time a design safety assessment study concerning the

adequacy of core themocouple provision in Magnox reactors was prepared for the NII (O.H. Critchley 1962) and circulated for comment throughout the industry (See Document No. 5 of the Annex). More recently, an operational version of the Worthington method was succinctly described by Dale and Harrison (1971) in a contribution on 'Safety in Nuclear Power Plants' to the 4th Geneva Conference on the Peaceful Uses of Atomic Energy under the title of the 'Fire Risk Criterion'.

The possibility of extending statistical probability analysis to more general safety matters was soon recognised. As early as 1964, F. R. Farmer of the Health and Safety Branch of the U.K. Atomic Energy Authority (UKAEA) presented a paper on 'Safety Analysis as related to Reactor Siting' to the 3rd Geneva Conference on the Peaceful Uses of Atomic Energy and this was followed in 1967 by his notable and much cited presentation to a Vienna symposium sponsored by the International Atomic Energy Agency (IAEA) which described a new approach to reactor siting. It employed in a cartesian, graphical representation the probability of major reactor radiation accidents plotted against the consequential release of radioactivity in curies. An accident probability could thus be identified as acceptable or unacceptable according as it fell above or below a transverse discriminating line which represented the criterion.

Since the 1967 disclosure, the concept which has become generally known as the method of 'The Farmer Line' has been further elaborated by Farmer and his associates. A version of it was tabled as a supporting paper during a House of Lords debate on nuclear power reactor safety in late January 1976 (F. R. Farmer 1975). The methodology of the approach which requires the support of a sophisticated data base of reliability information has largely determined the policy of the UKAEA and its Safety and Reliability Directorate (SRD) in matters of nuclear hazard control.

Another early contribution to the topic was a highly mathematical paper in Russian by O. P. Brobrovnikov (1969). It had a 'first time' claim and was read to an IAEA symposium on the handling of radiation accidents.

7.3 The Rasmussen Reactor Safety Study

One of the most important contributions to the science of probability analysis in the field of nuclear power is the U.S. 'Reactor Safety Study' which was the work of a team led by Professor

N. C. Rasmussen and published under the imprimatur of the U.S. Nuclear Regulatory Commission (USNRC) in 1975 . This much quoted document is 'An assessment of accident risks in U.S. Commercial Nuclear Plants' and covers the Boiling Water (BWR) and Pressurised Water (PWR) reactor systems, being conditioned to a program of 100 nuclear plants. The risks arising from a range of conceived plant accidents leading to releases of radioactivity to the environment were assessed by sophisticated methods of reliability analysis. The failure sequences that could cause the nuclear fuel to overheat and release its radioactivity and coincidental failure of clean-up systems and of the integrity of the reactor containments with consequent emission of fission products and other activated matter to the environment were analysed. The 'Study' defined two broad types of situations that might potentially lead to a melting of the reactor core: the loss-of-coolant accident (LOCA) and transients. The latter term referred to any one of a number of conditions which could occur in a plant and require the reactor to be shut down. Following shut-down, the decay heat removal systems should operate to keep the core from overheating. However, certain failures in either the shut-down or decay heat removal could also cause the core to melt. The method of analysis used had two aspects, namely:

> 'An Event Tree which defines an initial failure within the plant. It then proceeds to examine the course of events which follow as determined by the operation or failure of various systems that are provided to prevent the core from melting and to prevent release of radioactivity to the environment. Event trees were used ... ... to define thousands of potential accident paths which were examined to determine their likelihood of occurrence and the amount of radioactivity they might release.
>
> Fault Trees which were used to determine the likelihood of failure of the various systems identified in the Event Tree accident paths. A Fault Tree starts with the definition of an undesired event, such as the failure of the system to operate, and then determines, using engineering and mathematical logic, the ways in which the system can fail. Using data covering 1) the failure of components such as pumps, pipes and valves, 2) the likelihood of operator errors, and 3) the likelihood of maintenance errors, it is possible to estimate the likelihood of system failure, even where no data on total system failure exists.

> The likelihood and size of radioactive releases from potential accident paths were used in combination with the likelihood of various weather conditions and population distributions in the vicinity of the reactor to calculate the consequences of the various potential accidents.'
>
> U.S. Reactor Safety Study:
> Executive Summary - WASH-1400,
> U.S. Nuclear Regulatory Commission,
> October 1975, Section 2.21.

The results of the Study in probability terms were compared with those of various other natural and manmade hazards suffered by inhabitants of the continental territory of the United States. These risks were equated with those presented to the same individual by a program of 100 operating nuclear power plants for which the chance of fatality through a nuclear accident was put at 1 in 5,000,000,000 per year compared with the risk of death from all accidents, manmade or natural, of 1 in 1,600 per year, a ratio of about 3,000,000/1. The result of the Study put the risk of death from a nuclear accident as about the same as that of being killed by a meteor, a very real threat, but so small that nobody worries about it. Ergo, the U.S. commercial reactor program in acceptably safe.

7.3.1 Criticism and the Peer Group Review

Other than by the committed nuclear establishment and its supporters, the Study was skeptically received. The calculations were clearly complicated, especially those involving common mode failures and obscure in that they were inadequately described, a deficiency which has drawn unfavourable comment.

The American Physical Society thought that their own 'experience with problems of this nature involving very low probabilities' gave them no confidence 'in the presently calculated absolute values of the probabilities of the various branches' (N. C. Rasmussen 1975/a). The U.S. Environmental Protection Agency found that 'the area of human reliability appears to be improperly or incompetently considered' (Ibidem/b), a view not irrelevant in light of the accident at Three Mile Island (See Appendix II). The National Aeronautics and Space Administration (NASA) were discretely covert in their criticism, saying that they did not have the technical effort available to validate the numerical assessment. They further observed that with a small factual data base they favoured an empirical, evolutionary technique (Ibidem/c). This has been described

as a method of design which is inter-penetrant with practice using a 'design-make-test-fail-fix' iteration that enables a very high standard of reliability to be attained for space vehicles and other high risk systems (W. M. Bryan 1975).

As a result of the criticism, the USNRC commissioned Professor H. W. Lewis to chair a 'Peer Group' to review the Study. Its report was issued in September 1978. The Peer Group found that the Rasmussen methodology provided a useful tool for the work of reactor safety analysis, but considered that the presentation 'was inscrutable, it being exceedingly difficult to follow the detailed thread of any calculation to a conclusion'. The uncertainties involved in the data and calculations were not sufficiently emphasised. It suffered from a lack of data on which to base input distributions which were 'associated with the invention and use of wrong statistical methods'. The general conclusion of the Peer Group was that the Study was 'a pioneering step leaving much to be desired', but one which had potentialities for further development. Its use to judge the acceptability of reactor risks was deprecated. In their wider influence, the findings of the Peer Group Review provided the orientation for the 'German (reactor) Risk Study' (infra).

At present the balance of opinion on the U.S. Reactor Safety Study divides between administrators, physical scientists and politicians who favour nuclear power on the one hand and the engineers concerned with the realities of designing, constructing and operating nuclear power plants on the other (See Section 8.1). Whereas the former group have largely maintained their enthusiasm for the Rasmussen findings, like Lord Rothschild in his 1978 Dimbleby lecture on 'Risk', the latter remain skeptical. Instead, the method is accepted as a supplement to established engineering practice and principles rather than as any true way of forecasting a low probability risk in the circumstances of an operating plant beyond the conjectures of the design situation (infra).

It also offers a means for rational management of investment in safeguards which can thereby be more effectively apportioned over the design as a whole. Excessive involvement with a particular feature to the detriment of others not so immediately salient can thus be avoided.

7.4 The German (reactor) Risk Study

Another important, but more recent, study of the risks attributable to a thermal nuclear power plant, in this case the German version of the PWR, was made by the West German Reactor Safety Institute, namely, die Gesellschaft fUr Reaktorsicherheit (GRS) mbH, at the request of, and under contract to, the Federal Ministry of Research and Technology (A. Birkhofer 1979 and infra). A summary of the work, pending full publication, was presented in Bonn in August 1979. The terms of reference were to:

(i) Assess the 'collective risk' attributable to nuclear power plant radiation accidents in the light of German conditions, and

(ii) Compare the findings with the U.S. 'Reactor Safety Study' (supra) in order to be able to evaluate differences in engineered plant features and site conditions.

The direction of the German investigation was influenced by the critical appraisal of the U.S. 'Study' made by the 'Peer Review Group' (supra) led by Professor Lewis. The German study is reserved in its approbation of the U.S. work. While recognising the merits of the latter and the usefulness of the quantitative probability analyses on which Rasmussen's investigation relies, reference is made to its limitations and due acknowledgement is accorded to 'the proven worth' of the traditional qualitative approach, that is the use of the concept of maximum, inclusive credible accidents (MCAs) or, in other words, Design Basis Accidents (DBAs). It also draws attention to certain counter-productive aspects of quantitative methods of hazard assessment when applied to suppositious LPEs in respect of nuclear power plants. Three relevant excerpts from the summary of the German 'Study' are reproduced below:

On the Design Basis Accidents - from 1. INTRODUCTION

'The safety review of nuclear power plants includes a comprehensive accident analysis. Safety-related requirements, in particular those for the design of safety systems, are set up against the background of design basis accidents, i.e. the accidents involving the largest loads and thus the most stringent requirements. The design of the safety systems is based on these requirements. The demonstration that these accidents will be coped with in terms of safety features includes at the same time the evidence that less serious accidents involving smaller loads than the design basis accidents will be coped with as well. As a result of the safety precautions which have been taken, accidents involving more serious consequences than the design basis accidents are considered to be so unlikely that they can be precluded as far as one can judge.

Experiences so far show that this safety concept has proven its worth. At a worldwide level there is now available the experience of some 1,500 reactor operation years over a period of about 25 years. During this time, neither deaths nor other health effects due to activity release have occurred in the environment of nuclear power plants.'

On quantitative methods - from 7. EVALUATION OF RESULTS

'In the safety-related design of nuclear power plants, a probability concept has always been used implicitly when, on the basis of existing engineering experience, a decision has to be made as to which accident sequences will have to be coped with by the safety features. In many cases, decisions on protective requirements with regard to external events are made dependent on their occurrence frequency. Findings with respect to typical accident sequences may be used for the planning of emergency measures.

.....

However, the possible applications of risk analyses are limited. Risk analyses use probabilities which are, in most cases, small or very small. Thus, the results, whose character is that of an estimate anyhow, will become even more uncertain with decreasing probability ... It has to be doubted whether the state of the art is sufficient, in the case of events involving probabilities of 1:1,000,000,000 per year, to determine somewhat reliable results which can serve as a basis for assessment and decision. Furthermore, it remains doubtful whether events involving the frequency mentioned before or an even smaller frequency can still be made part of realistic considerations at all.

On counterproductive aspects of risk studies - from 7 ibidem

'The implementation of risk analyses will also lead to problems of a psychological nature which may counteract the purpose of risk analyses. Events which are impossible as far as one can humanly foresee will assume a real character as a result of a detailed analysis. Thus, people are made aware of possible hazards which in all probability will never result in fatalities and which do not play any role in the minds of most people. This may involve the paradoxical consequence that certain risks are demonstrated to be minimal but that fear of these risks is increased by the very demonstration, whereas far greater risks which may not have been investigated in detail will not be taken note of at all.'

Professor Dr. A. Birkhofer,
The German Risk Study: Summary,
Gesellschaft für Reaktorsicherheit,
Cologne, August 15, 1979.

7.4.1 Relevance to the 'New Treatment'

The rather lengthy excerpts from the officially backed German reactor safety centre have been quoted because of the general support they give to the philosophy underlying the research reported in this thesis. Further, the first two of them show that German nuclear safety engineers have followed a path similar to that of the British Nuclear Installations Inspectorate (NII), at least up to 1 January, 1975 when the NII was merged into the Health and Safety Executive (HSE). From that time onwards, its policy began to be influenced by the propinquity of the much larger and dominant H.M. Factory Inspectorate and its administrators whose safety policies derive from a more formal and legalistic tradition. The basis of the then NII's approach to the design safety assessment of the nuclear power reactors for which it had statutory licensing and safety responsibility was the predominance of sound and well based engineering judgement backed by field experience over ad hoc scientific studies and mathematical computations. Recourse was made to scientific research and sophisticated mathematical techniques, probabalistic safety analyses and reliability studies, when these aids were appropriate to the safety investigations in hand (Gronow and Gausden 1975/a).

None of the above comments derogate from the value of quantitative safety and reliability analyses of the kind offered by the Safety and Reliability Directorate of the UKAEA when the approach is appropriate to the task. However, the line taken in the New Treatment is that these quantitative methods can only provide an adjunct to the discipline of nuclear safety engineering which must take account of the realities of the construction site and reactor control room as well as accommodating to theoretical appraisals coming from specialist bodies, computer offices and other 'centres of excellence'.

7.5 Overview

The preceding brief review of the state of the art in risk science reveals it as an area of study that has been researched widely and in depth. It has been the subject of numerous inquiries, conferences, symposia and working parties. The published reports and papers describing the results of these activities provide an

extensive literature that might be expected to cover every aspect of the topic. What place then can a new treatment of risk and its management in the domain of low probability events find in this well tilled field of knowledge? What contribution can it make when apparently everything important and relevant has been thoroughly investigated already?

It is obviously true that few aspects of risk have not been covered, but most of the numerous studies, reviews and researches have been classic, mathematical applications, tending to a traditional scientism and characterised by the Poissonian approach adopted by Green and Bourne in 'Reliability Technology' (1972), in the U.S. 'Reactor Safety Study' (N.C. Rasmussen 1975), in a compendium called 'Nuclear Reactor Safety' published under the imprimatur of the Safety and Reliability Directorate of the UKAEA (F.R. Farmer et al. 1977) and by Locke et al. in 'Canvey Island' (1978). These authors assume that, if adequate data are available, then almost all risk can be expressed meaningfully in quantified form, a momentous concept currently much exploited. Implicit in this assumption is a conventional idea that pervades Western civilisation of an underlying order in the cosmos and, thereby, in the universe of technology in particular. Though widely supported in the most eminent of scientific circles, it is by no means universally accepted as valid. It has been challenged in principle by authorities among whom John Maynard Keynes (1922), E. Barankin (1956), Bruno de Finetti (1972) and J.R. Ravetz (1977) may be cited. More pragmatic criticism of the quantification of overall nuclear power plant risks has been voiced by some well-informed engineers, including Hanauer and Morris (1971), W.M. Bryan (1974), Gronow and Gausden (1975/a) and O.H. Critchley. The argument is of much greater profundity than at first might seem to be the case. Moreover, it is of considerable importance as it can significantly affect the approach to risk assessment and the measures adopted for hazard control.

There is growing acknowledgement that an entity called 'The Public' is a key factor in risk acceptance by the body politic and that the acceptability of risk is a very complex thing not susceptible to a purely scientific analysis leading to precise numerical risk indices. This is coupled with a realisation that they way in which risks are perceived and the reactions of people to them vary and the response of an individual as such does not necessarily correspond with that of the same person identified as a member of 'The Public'.

In addition to exploring the foregoing aspect, Douglas and Wildavsky (1982) studied the response that may be evoked from a community by those hazards of wider consequence that have general or latent rather than specific effects among the population, for instance, low level dispersed radioactivity such as that attributable to releases from various nuclear plants in normal operation. They claim that these apprehensions are features of the societal dimension of risk, being peculiar to the indigenous culture (supra). As in the case of the threat posed by a potential catastrophic LPE, say that of a major nuclear accident, social phenomena in this class show little or none of the proportionality between the magnitude of the agency or stimulus and the response that is characteristic of the reactions observed in the physical and life sciences. They exhibit instead what might be called 'irrationality', a term often used to describe apperception of a risk by 'The Public', but far from appropriate in the circumstances. The use of the word 'irrationality' in this sense is an example of an all too common solecism that may be attributed to a general tendency to have recourse to classic scientific method under the illusion that it is generally applicable to the solution of all problems, whereas it is not.

Risk apperception is a subject in the domain of 'Trans-science' to use the term coined by Alvin Weinberg (1978) and ranges into intellectual territory beyond the bounds of the physical and life sciences, but where the engineer must perform effectively.

The investigation of those major accidents - LPEs - that have afflicted nuclear power plants, for instance, the Windscale Plutonium Pile fire of 1957, the Browns Ferry cable vault fire of 1975 and the loss of coolant at Three Mile Island in 1979 revealed that the causation of these, and other events like the explosion at the Flixborough chemical plant in 1974 (See Appendix II), involved factors outside the physical event schema and fault sequences envisaged in their design safety analyses. To account for this deficiency in the method of analysis there has been a comparatively recent recognition that an unanticipated and capricious agency, so-called 'Human Error', is an important element. Attempts have been made to measure it in a quantitative way. Once again, it is an indefinite statistic whose treatment lies beyond the bounds of quantitative science. Nonetheless, it is a potent and ubiquitous thing that must be taken into account in technical safety analysis.

In spite of all the studies, learned papers, committees, conference deliberations and reports there has been little real progress in foreseeing and abating the severe but very rare disastrous failures that have come to be associated with the introduction of advanced technologies in industry, transportation and medicine. Neither has public confidence been won in the officially sponsored hazard control measures that have been introduced to allay public concern about the safety of certain innovations, notably nuclear power. Instead, their anxiety has been fed by the occasional, unlikely and unanticipated accidents that continue to occur sporadically with new drugs, in public transport and in industrial plants and processes, all of which things were presumed to be adequately safe before the failure.

There are few who would not agree that absolute safety is not attainable, but that a compromise between reasonable cost and a safety asymptotic to that state is. As far as advanced technological processes or systems are concerned, the task is not only to attain the latter in such technical respects as are practicable, but to win the public to acceptance of its reality. Further, not only must this state of tolerable safety be achieved, but the resultant must relate to something that is needed by the community exposed to the risk or otherwise desired by it.

The means are, therefore, almost as important as the end and so there must be a proper apportionment of publicly observable responsibility amongst the disciplines that have to act in concert to achieve that essential minimum condition of safety needed to obtain public toleration of a hazard presented by a given technological innovation. It was this kind of inter-disciplinary co-operation that was so effective in the atomic energy industry during its early years of rapid progress (Margaret Gowing 1974, O.H. Critchley 1977). Distributing duties accordingly, it is the province of the scientist to gather the relevant technical facts; that of the administrator to handle the politics and finance; but the engineer has the central managerial role of bringing these three things together to fruition in a demonstrably safe plant or system. It is he who spells out the concept in terms of an engineering design and who effects its realisation in construction and operation of the end product. Besides, it is at the interface of design implementation with the day-to-day realities of interaction among drawing office, shop floor, construction site and control room that the engineer exercises governance and accepts

responsibility. It is odd that these facts have escaped due acknowledgement by those senior administrative and political echelons who form certain of the Western national establishments and, not least, by the scientific community itself. This oversight has been lamented by Sir Alan Cottrell (1976). It is discussed further in the following passages and in Appendix III.

PART THREE

THE HAZARDS OF ADVANCED TECHNOLOGY IN THE LIGHT OF RISK PERCEPTION AS A CULTURAL PHENOMENON AND THE ENGINEER AS THE DEFENDER OF SAFETY

Sections 8 to 10 comprising:

An outline of the cultural frame of reference in which today's technological risks are perceived and tolerated, the orientation of the Western intellect towards logic and science ascribed to the persisting influence of Aristotlean philosophy, a linguistic and neurological explanation for the liberating 'miracle' of ancient Greek thought; aspects of the widening disjunction between the purely intellectual realms of administration, law, politics, theoretical science and the humanities, defined as 'The Word', and the pragmatic domains of technology and the useful arts, defined as 'The Deed', engineering as the bridge across the divide; an analogy with 'noise theory' in the classification of industrial accidents and process faults and incidents, the singularity of the Low Probability Event (LPE) of catastrophic failure and the difficulty of the actuarial assessment of the potential LPE which presents a 'Zero-Infinity Dilemma', an engineering interpretation of the nine features of the 'Dilemma'; the question of the lack of accountability of technological risk assessors in government agencies and large public utilities; illusory aspects of convential methods for the safety assessment of design and of the probabalistic approach to risk appraisal; human error as the most common element in accident causation, and the engineer as the bedrock of technological safety and of public confidence in hazard management.

THEMATIC SYNOPSIS

The ground has been prepared for the development of a New Treatment of Low Probability Events as an engineering response to the threats posed by modern innovatory technologies, one that the engineer per se is singularly well-suited to perform owing to his professionally adapted intellectual capabilities. As the qualitative methods of technical risk appraisal have been shown to be inadequate and the quantitative ones to be illusory, new methods in an engineering dimension are needed. Moreover, owing to the ubiquity of human error in its penetration of all systems and processes, the certain assurance of competence, not only in the performance of mechanical and technical tasks, but in all functions of management is necessary. For this purpose, the new style of engineering inspection that has evolved in the nuclear industry can provide a basis.

8. CULTURE, RISKS, 'ZERO-INFINITY DILEMMAS' AND THE NEW TREATMENT

"Twice two equals four: 'tis true,
But too empty, and too trite.
What we look for is a clue
To some matters not so light."

Sir Karl R. Popper,
'Some comments on truth and
the growth of knowledge',
Proc. Int. Congress on Logic, Methodology
and Philosophy of Science, (Ed. by
Nagel, Suppes and Tarski), Stanford
University Press, California, 1960, p. 290.

Throughout the Western world, the public shock at certain technological disasters has been sharp and vigorous and their consequences have evoked profound concern. Several have had serious legal aftermaths and the corporate bodies culpable have had to bear the cost of heavy claims for compensation. Two notorious cases among them were the Thalidomide and Minimata tragedies involving respectively the teratogenic effects of an apparently harmless tranquiliser and the insidious poisoning of a whole Japanese community over a number of years by a factory effluent reasonably held to be innocuous but discharged into a bay that had an unusual confining flow pattern (See Appendix II).

A characteristic of both cases was the strange reluctance of the public authorities and corporations responsible to accept the fact that these activities were causing serious harm in face of proof positive that this was so. Yet, those wealthy and powerful corporations responsible were, overtly at least, public spirited bodies and not ungenerous in their support of charitable and cultural programs conducted for the benefit of the community, locally and more widely.

Another phenomenon of relevant interest is the lack of opposition to the huge nuclear power program which is currently underway in France (Pierre Papon 1979). Though it has been anything but free of serious technical problems and reputed near accidents, those failures which have occurred have aroused surprisingly little hostility among the French public. The relative lack of objectors and weakness of such popular opposition as has been evident may not be unrelated to the country's paucity of indigenous energy sources. This deficiency had placed a serious brake upon her industrial development until large supplies of oil became readily available during this century. Continuing dependence on exotic energy supplies that could be easily restricted or

cut off by hostile actions and are in sight of exhaustion in any case makes France extremely vulnerable to foreign political pressures and is clearly unpalatable to the very nation-conscious and patriotic 'People of France'.

8.1 The refractory persistence of the cultural dimension

In the earlier Section 7.1.2, a brief reference was made to the work of Mary Douglas and Aaron Wildavsky (1982) who with Michael Thompson (1980) and others have shown that the evocation and nature of the response to a risk by both individuals and the community as a whole are shaped by the culture in which the risk arises, is perceived and recognised as a threat. In addition, these cultural determinants or mores which are the efficient causes of such apperceptions are very enduring and resistant to change. Besides, the mores of a society are particularly relevant in the case of those technological risks of very low probability that combine dire consequences with vestigal chance of occurrence where apparently irrational attitudes to them can emerge. Therefore, in view of the dominant part that societal things of this kind can play in the formation of the notions held by individuals and the general public about such risks, the nature and sources of origin of these mores must be known if the complex and enigmatic phenomenon of risk apperception is to be properly understood and managed.

In the Occident, each indigenous Weltanschauung derives largely from the ancient Greek scientist-philosophers whose seminal ideas on the nature of the physical, political and ethical world did so much to set European civilisation on its remarkable upward path. The eminent French academic, Arnold Reymond (1955), in assessing the influence of their thought wrote that the originality, insight and penetration of these Greek thinkers 'constitutes a veritable miracle', for which there is an intriguing scientific explanation (infra). The most important of them was Aristotle (388-322 BC) whose philosophy has laid the basis of the European Christian ethos and even that of its main deviant trend, Marxism. As interpreted by St. Thomas Aquinas (1224-1274) in what Vernon J. Bourke (1967) has described as a rethinking of Aristotelianism, it still endures as the dominant theme in Catholic theology today and certainly in the whole of Christendom until the Reformation (circa Diet of Worms 1521) when Luther weakened the grip of Aristotle on Western philosophy and science: weakened but not overcome and not least in the mind of Luther himself (11).

It is a story that began nearly 3,000 years ago in the melting pot of cultures, languages, religions and technologies that existed in the Greek peninsula and archipelago and along the coasts of Asia Minor. Until the advent of Socrates (470-399 BC), the attention of these early scientist-philosophers was directed towards an attempt to understand man's natural environment. However, the time of Socrates is associated with a shift of interest from natural philosophy to politics and ethics that represented a change in the condition of society produced by the growth of the institution of slavery. By this time it had been transformed from a domestic institution of household retainers into a system in which most manual work and particularly mining, agricultural and industrial processes and the laborious tasks of transportation were performed by alien chattel slaves. Thus, the ideal was established of the citizen as one who did not engage in manual work. A far reaching and evil consequence of this was that technology and the knowledge essential to many branches of science passed into the hands of slaves and became associated with their subculture.

Professor Benjamin Farrington (1947) has described this watershed in the development of human thought thus: "the 'word' was the concern of the citizen, the 'deed' was the concern of the slave". The practioners of applied science were in consequence despised and remained in this condition until Robert Boyle (1627-1691) provided a rationale in his 'The Skeptical Chymist' (1661) for the movement that secured the eventual release of chemistry and the physical sciences from the bondage of alchemy by the turn of the 18th Century. But engineering has not fared so well. Owing to his ability to fashion engines of war and to design and build public works, the engineer was usually allowed to pursue his task as a free man, but always in a lowly rank. For reasons that are not clear, his profession has yet to acquire the modest esteem accorded in our times to the scientist and the traces of the ancient prejudices against the engineer and his technicians and craftsmen remain to this day, a matter commented on in Appendix III.

The influential Aristotlean philosophy of idealism which is entrenched in the ideology of 'The Word' is particularly resistant to change. The history of the progress of science and technology has been a continuing fight in favour of the materialism of 'The Deed': that is the pursuit and establishment of knowledge and progress determined and supported, not by Ivory Tower speculation, but by the theory and practice of empirical science justified by experimental evidence. This battle has

not yet been won and the latter part of this century is seeing a 'Drift from Science' (Nature-Editorial 1980; Anthony Smith 1980). It took a century or more for the Heliocentric Theory to gain acceptance; Professor Ohm was castigated for his 'preposterous theories'; the brilliant French physicist, Sadi Carnot (1796-1832), a founder of Thermodynamics, did not disclose his ultimate denial of the Caloric Theory of Heat, confining his thoughts to private papers, which were not published till long after his death. In our time there has been the extraordinary rejection of the Quantum Theory by Einstein on idealist grounds, 'The Gods do not play dice' (W. Ehrenberg 1977). The role of mathematics has been ambiguous and its 'Pernicious influence' on science has been decried by Professor J. Schwartz (1962) because of its use to underwrite often dubious hypotheses lacking empirical verification.

Assuming the validity of the foregoing premises, there is good reason to suspect that the persisting idealism still deeply embedded in Western thought with its concomitant hostility to the pragmatism of engineering has affected the approach to risk science and the management of the new technological hazards. If so, it has encouraged ones that lean towards the theoretic and scientistic rather than to the engineering commonsense that comes from practical engagement with reality. Present day examples of this tendency are the quantitative systems methodologies of risk assessment and hazard control that have emerged over the last 25 years in the domain of advanced technology and in particular that of nuclear power. The best known enunciations of its use in the latter field are due to F. R. Farmer (1978) and N. C. Rasmussen (1975) in the latter's 'Reactor Safety Study', matters reviewed in Section 7.3 et seq. While it cannot be denied that the introduction of these techniques has been a major advance in nuclear safety engineering, the preoccupation with which they have been espoused has shown a certain lack of balance.

8.1.1 A linguistic explanation for the 'Golden Age' of Greece

The extraordinary development of Greek intellectual life and its lasting effect on European culture discussed in the foregoing passages has long baffled anthropologists and historians seeking a convincing explanation for its cause. J. R. Skoyles (1984) has offered an intriguing linguistic explanation that has neurological support. Before the dawn of their Golden Age about 600 BC, the Greeks had developed and become proficient in the use of an alphabet that was unique in giving

them a fully phonetic representation of language. This limited the management of writing in the brain to the left cerebral hemisphere. The restriction does not apply to non-phonetic writing systems which can use reading strategies that engage the right hemisphere in the recognition of logograms. Neurological studies show that hemispheric representation of non-alphabetic writing systems differs markedly from that of alphabetic ones. Supporting clinical evidence comes from Japan where 'Kanji', the non-phonetic system, is vulnerable to different areas of brain injury from 'Kana', the phonetic writing system (23). The right hemisphere is fully competent, and probably more so, than the left to read hieroglyphics, logograms and other non-alphabetic writing. Such competences compete in the brain for expression and, in an analogy with Mendelian genes, the competences of the mind can have a dominant or recessive relationship to each other. Skoyles then posits that the alphabet, by producing a unilateral representation of lexicals in the left hemisphere, freed the recessive competences in that hemisphere which underlie rational, analytic and logical thought. Thus liberated from the inhibitions imposed by the right hemisphere, the left was able to develop fully its peculiar analytic and logical power. The implications for engineering in which thought is dependent on the ideograms of drawings and circuit diagrams are profound.

8.1.2 The ambivalent societal circumstances of the engineer

Any attempt to treat the catastrophic LPEs of modern technological society must be compatible with the cultural setting in which it has to be accepted and applied. The school of Aristotle has not only fashioned Western thought, but has helped to legitimate its social structures, even those appearing to be the most diverse. In affairs of management this is expressed in a view that there is a clear divorce between those in a position to order the affairs of the World, the realm of 'The Word' and those naturally subordinate to them charged with the performance of tasks, the domain of 'The Deed', with engineers and, until recently, scientists, falling into the lower bracket. C. P. Snow (1959) described the division as the 'Two Cultures' as discussed in Section 8.1

Despite the fact that European culture has been famed for its achievements in the domains of literature, mathematics, music, philosophy and politics, until the onset of the Industrial Revolution technology made relatively slower progress. It is relevant that the Industrial Revolution which began in Britain was associated with the growth of an educational form called the Mechanics Institute. The Institute provided

a technical education for able boys from the middling classes directed towards the mastery of the ideograms and non-linguistic concepts of engineering. They flourished and by about 1830 there were several hundred in England. By then the demands of the Empire for administrators, army officers, colonial officials and higher grade clerks brought into being new grammar and public schools which offered a liberal education in which classical learning and linguistic attainments took pride of place. The Mechanics Institutes suffered a corresponding loss of favour and by the end of the Nineteenth Century only a few of exceptional merit had survived. British engineering and technology which had led the World until about 1870 suffered a similar decline, though with a time lag of a generation. The unfortunate national consequences of this phenomenon are matters of major public interest today, a subject pursued further in Appendix III.

Over the past millenium, this cultural divide has no doubt stabilised society and enabled intellectual, economic and social betterment to be achieved within an accepted framework. However, technical advance since the Industrial Revolution has reached a stage when the technological tasks of 'The Deed' have acquired a complexity that has brought with it a qualitative change in their nature. Thus, technology and those who practice the intellectual disciplines of engineering are fast becoming transcendent elements in the social and cultural scene that are making structural changes in the social order inevitable. Engineering can now be identified as a discipline distinct from Science as depicted in Figure 1.

There is evidence of a growing recognition of the importance of engineering and technological cultural elements in their own right . In his controversial Rede lecture that forced British academia to acknowledge 'Science' as a second culture rather than an inferior calling, C. P. Snow hinted at the existence of a still submerged third, that of 'Engineering'. He had in fact been long and specifically pre-empted by Auguste Comte (1825) who identified a new class emerging in the scientific body, 'Engineers distinct from the savants properly so called' whose task it was to interpret and apply the scientific discoveries of the latter. A recent sign of the times is the report of the Finniston Committee (1980).

8.2 Accidents, Low Probability Events, Risk Prediction and Prophecy

Despite the repetition in saying that any serious treatment of unexpected disastrous failures in technological systems requires an

THE FIVE INTERACTING BRANCHES OF CULTURE:
THE HUMANITIES SCIENCE MEDICAL SCIENCES ENGINEERING COMMERCE
WITH THEIR SATELITE ASPECTS AND SOCIETAL FIELDS

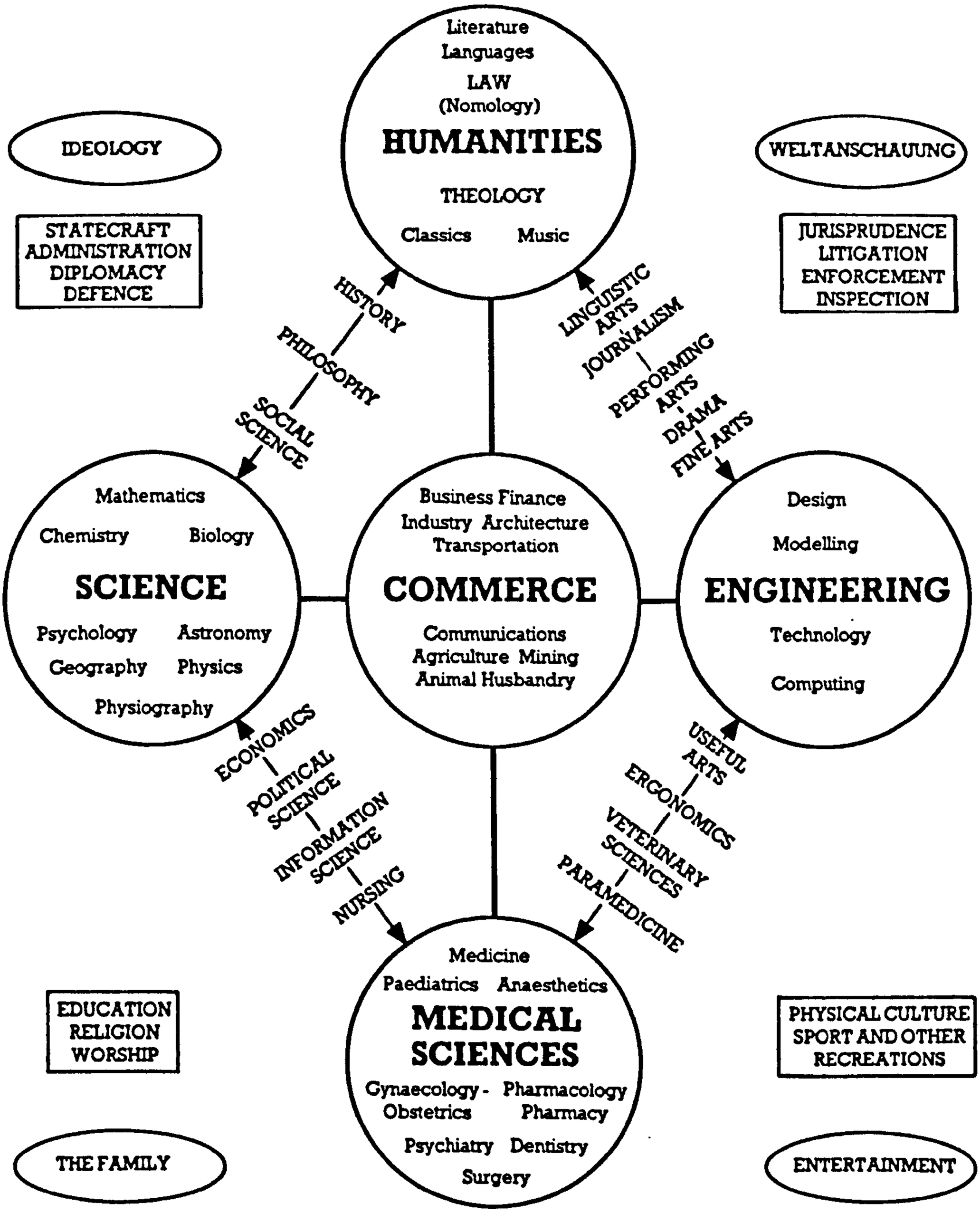


Fig 1

estimate of the chance of occurrence of the given LPE together with an assessment of its consequences, it is necessary to consider certain aspects of the matter more fully. Again, the manner of estimating the two parameters of chance and consequences is an aspect of risk analysis that has already been examined in some depth in Section 7 above. Some doubt has already been cast on the extent to which numerical evaluations can be used to represent low probability risks except in certain special cases.

Beyond the foregoing tautologies, an important consideration in the treatment of LPEs is that meaningful assessment of the chance that this or that rare failure may happen differs qualitatively from the usual experience of handling the random adversities of normal life. For example, the most common essay into the realm of prediction is the judgement involved in placing a bet with a bookmaker, but here the numerical odds against success are comprehensible within the span of human appreciation. This is not so when the odds against an event are very great.

Excluding considerations of material loss, the magnitude of an adverse event may range from minor somatic injury to loss of life itself. However, for simplicity of argument, it is convenient to treat the extreme calamity of death rather than to attempt to scale injuries and harm. Consequently, the typical risks listed in Table II relate to the single dimension of potential fatality. There are three main groups, namely, those that are commonplace or 'Mundane', those that are 'Unusual' in the sense of being infrequent and of less common causation and, lastly, truly rare, that is to say, 'Low Probability' risks which are the Low Probability Events (LPEs) of our inquiry.

8.2.1 Mortality owing to 'Mundane' causes

Most people can expect to pursue their lives without early death from disease or fatal somatic catastrophe until the age of 'three score years and ten'. Their graver experiences of danger, harm and death and their perceptions of risk and its management come with the knowledge of the fatal accidents of which they have personal experience, that is to workmate, colleague, neighbour, friend or kin. The risk of accidental death borne by the average citizen of the U.S.A. or Great Britain is about one chance in 1250 per year, varying with age, occupation, place of residence, sex, social class and mode of compilation of the statistics (G. D. Bell 1977). The causes are mainly of the kind classed as 'Mundane' in Table II. They are the mortality caused by

TABLE II

Accidental Death – Average Risk of Fatality

PROBABILITY CLASS	CAUSE OF DEATH (Accident Type)	INDIVIDUAL'S CHANCE OF FATALITY (Annual risk to member of group exposed to the hazard – rounded-off figures)	SOURCE OF DATA
MUNDANE	Industrial Accidents (Construction sites, factories and mines)	1 in 2,500 (employees – UK)	(a,b)
"	Falls at home (Age group 45 – 65 years)	1 in 3,000 (UK)	(c)
"	Traffic Accidents	1 in 4,000 (UK and USA)	(c,d)
UNUSUAL	Fires	1 in 25,000 (USA)	(d)
"	Drowning	1 in 30,000 (USA)	(d)
"	Air Travel	1 in 100,000 (International)	(d)
"	Railway Passengers	1 in 400,000 (UK)	(e)
"	Struck by lightning	1 in 2,000,000 (UK and USA)	(c,d)
LOW PROBABILITY GROUP OF EVENTS		(Chance of death due to given cause not calculable. Data exiguous and unstable. Zero-Infinity hazards presenting vestigal risk of unlimited losses.)	
Actual	'Titanic'	1503 fatalities	(f)
"	'Andria Doria'/'Stockholm' collision at sea	59 "	(f)
"	Collapse of tower block flats – Ronan Point	4 "	(f)
"	Explosion at Flixborough petrochemical plant	28 "	(f)
"	Three Mile Island nuclear power plant	No casualties, but financial losses greater than $4 billion	(f)
Hypothetical		(These are potential accidents for which the assessed risk has been formally quantified)	
"	Canvey/Thurrock petrochemical installation (See note 'h' below)	1 in 10,000 – Notional estimate using data from analogous actual happenings	(g)
"	Nuclear Power – for a program of 100 reactors – Radiation accident – casualties among the public	1 in 5,000,000,000 (USA) Estimate derived by quantitative analysis of synthesised model	(d)

NOTES

(a) Report by H.M. Inspector of Factories for 1973.
(b) Wickenden and Mayhew, ATOM, June 1980, UKAEA house journal.
(c) F. R. Farmer (Ed.), Nuclear Reactor Safety, Academic Press, 1977.
(d) N. C. Rasmussen, U.S. Reactor Safety Study – Main Report, WASH-1400(NRC), 1975.
(e) Chambers's Encyclopaedia, Vol 11, 1950, p. 502 (tends to be an invariant statistic).
(f) See Appendix II.
(g) Locke, J. et al., CANVEY, HSE, London, 1978, Table 4, p. 25.
(h) Included as an exemplar of a hypothetical risk prediction, but anomalously placed in the Low Probability Group of Events. Note 10 refers.

accidents at work, in the home and on the streets that come in a steady dreary stream of every conceivable variation. There is thus no lack of data about them for quantitative statistical analysis. It is stable and is an important ingredient in those actuarial tables compiled by insurance company accountants so remarkable for the accuracy of their predictions. Such data is characteristic of that taken from a 'closed system', (12) examples of which from the realm of natural science include radioactive decay, tides and the movements of the planets and their satellites.

8.2.2 Casualties due to odd causes - 'Unusual Events'

From time to time in addition to the deaths that are the result of commonplace incidents of the type that have been classed in the sub-section immediately above as 'Mundane', there are occasional fatal accidents attributable to less familiar causes. Among them are death in a fire, by drowning, by a stroke of lightning or in an air or rail disaster when many people may be killed or injured at one time. A few instances are listed with their expectations in the 'Unusual' grouping in Table II. Despite their local rarity, enough data about these events can be collected on a countrywide or international scale to provide material that is sufficiently abundant for meaningful statistical analysis by assuming a Poisson distribution. A much quoted and classic example is the treatment by L. von Bortkiewicz (1898) of the mortality among Prussian army grooms caused by kicks from frisky horses. The case is of interest because it affected wide areas of scientific thought beyond mathematics. The conclusions Von Bortkiewicz and others have drawn from it were considered by many eminent mathematicians to be far-fetched and misleading, 'compromising mathematical science'. As a result probability theory languished in its development outside academic mathematical studies until early this century (L. E. Maistrov 1974/a). The subject is still one of recondite controversy and is discussed further in Section 9.7.

8.2.3 Rare and Unusual Events and Statistical Stability

Ladislaus von Bortkiewicz, a mathematician of superlative skill, attempted to use the regularity exhibited in the stable experiences of the cavalry men of the Corps of Guards (supra) and in like 'piquant' examples to establish his 'Law of Small Numbers'. By this he sought to explain the shrewd and remarkably efficaceous intuition of insurance actuaries in judging proposals bearing a concentration of risks, however small. A recent and relevant case is presented in the insurance industry's

reaction to the 'Zero-Infinity' characteristic (See Section 8.3 et seq.) of the nuclear risk that has brought into being new methods of underwriting and required legislative changes on an international scale (Street and Frame 1966). J. M. Keynes in his 'Treatise on Probability' (1922/a) dismisses this presumption as nothing more than another case amenable to Poisson's 'Law of Large Numbers' (1837), describing Bortkiewicz's mathematics as clever algebra rather than a recognition of reality. More significantly, Keynes (1922/b) rejects as 'certainly false' Poisson's idealist concept 'that in the whole field of chance and variable occurrence' there exist 'underlying discoverable systems' particular to the circumstances that can be revealed if enough instances of any given case are taken. He attaches great importance to the concept of 'stability' (infra) and, though much influenced by the German theoretician W. Lexis, developed an independent view (Ibidem - c). Keynes also observes that the existence of a fairly numerous set of statistics in respect of a phenomenon (say failures in large coolant circulating pumps for nuclear power plants - author's note) does not, a priori, justify an assumption that 'the observed degree of frequency is therefore stable'. Data of this kind may show:

> 'That some statistical frequencies are, within narrower or wider limits, stable. But stable frequencies are not very common, and cannot be assumed lightly.'
>
> J. M. (Lord) Keynes,
> Ibidem, p. 368.

Nonetheless, it has long been known that there is a remarkable regularity about many comparatively rare events among which may be listed suicides, certain organic diseases and genetic abnormalities, eg Down's syndrome. But, in each case there will be a closed system of causation that can be discerned and the degree of frequency attributable to it is therefore stable. Bortkiewicz's grooms existed in anything but a chaotic universe as the Prussian army's elite Corps of Guards was a body centred on discipline and good order. In such a system one would expect to find a matrix of regularities shaping events and the frequencies of the occasional abberations would be as stable as the observances of the regime from which they deviated. Fallacious attempts to identify regularities and stable patterns in what are inherently labile or chaotic event fields abound in risk analysis, notably in the domain of adventitious human errors of judgement and action.

8.2.4 Qualitative characteristics of a Poisson Distribution

If a rare event is of such a nature that it can be shown to share a common pattern of causation with like occurrences, that enough instances of kindred events have been reported to justify analysis and that there is reason to believe that such data is stable, then it may be treated as a member of a Poisson distribution. These are the criteria for classification in the 'Unusual' category that comprises the second part of Table II. In addition to those listed there, one may include the unexpected dangerous faults that emerge in a set of mass produced articles previously thought to be safe and reliable. For instance, 200,000 Austin-Morris 'Mini' motorcars had to be recalled for examination of their brake system master cylinders because there were a few otherwise unidentifiable defective units amongst them (Austin-Morris type fault 1978). These are once again events or potential events in virtually 'closed systems' (12).

8.2.5 New technologies, catastrophic failures and negligible risk

In Sections 8.2.1 to 8.2.3 above, it has been posited that the familiar run on untoward, but relatively infrequent events identified as 'Mundane' and 'Unusual' is comprehensible in terms of a probability distribution. These unfortunate happenings of which there are several examples in the first and second parts of Table II account for most of the fortuitous deaths and serious somatic injuries that afflict Western societies, for instance those caused by industrial accidents. They are generally amenable to statistical treatment as events forming particular Poisson distributions. Though these data are stable enough for the purpose, the conformity is by no means exact. In spite of that the deviations from the expectations predicted by the Poisson model are usually small and can be attributed to accident proneness, personality factors and variations in local circumstances of exposure to the given hazard. It is thus possible to calculate in finite terms the risk or chance of failure that can be associated with a given accident or fault.

While these 'Mundane' and 'Unusual' happenings are manageable in terms of quantitative risk analysis and meaningful predictions of the likely frequencies of occurrence of particular accidents may be calculated, say the number of motor vehicles that might be expected to go out of control and cross the central reservation of a motorway in the circumstances of some assumed traffic density, there is a third class of event for which this is not so. These Low Probability Events

(LPEs) are those very rare, random catastrophic failures of sporadic occurrence in technological processes, plants and systems and chiefly those of an innovatory kind, that distinguish themselves by being expected not to happen: yet in spite of that occasionally they do, being described in popular parlance as the 'once-in-a-million' chance. They are truly in a category in which the expectation tends to zero, seldom, if ever, occurring twice in any closely similar mode. The weaknesses that give rise to them are usually eliminated from plant and system designs because the lessons learnt from one disastrous and well publicised event almost invariably ensure that such identifiable defects do not remain uncorrected. A few exemplars are given in the 'Low Probability' and third section of Table II. It has sub-classifications of 'Actual' and 'Hypothetical', the former being things that have happened and the latter those that might. These calamitous occurrences are drawn from a fuller and more representative list with short descriptions of the causation and consequences provided by Appendix II. Other examples of low probability catastrophic failures, sometimes called 'negative-valued events', are legion. Nonetheless, these collectively not infrequent collapses, collisions, crashes, explosions, sinkings and releases of toxic fumes, vapours and polluents are characteristically rare individually, being occurrences of a diverse nature, each having its own peculiarities. As a result they present no statistical distributions in the realm of reality, let alone the stable ones required for meaningful quantitative probability analysis.

8.3 Risk management and 'The Zero-Infinity Dilemma'

L. von Bortkiewicz in his 1898 paper, 'Das Gesetz der kleinen Zahlen', attacked a clearly defined problem in a closed situation, when he calculated the death risk faced by Prussian Army grooms. The actuarial task of assessing rates for compensating the military authority for the cost of loss of men would have been straightforward. Not so for that posed by total plant investment and societal loss cover for a modern major hazard technological complex, eg the Canvey Island/Thurrock petrochemical and liquid natural gas installation (Locke et al. 1978). Here there is a presumption of a very low probability of an event or series of events leading to a very large loss. This is the 'Zero-Infinity Dilemma' (infra) with its risk-cost imbalance which has been identified by Talbot Page (1978) as the most difficult problem facing the proximate decision makers, both commercial and political, who must promote, finance, authorise and regulate the

industrial exploitation of advanced technologies, particularly in the evaluation of 'prospective energy alternatives' in which class he names nuclear power. They are also policy areas in which matters of project acceptance by the body politic and its acquiescence in the selection of sites are complex and sensitive.

Owing to the magnitude of the hazard consequent upon a major plant failure combined with the exceedingly small chance of its occurrence, the engineering, commercial and public experience of accidents upon which risk acceptance and management are normally built up does not exist. The questions of decision making about an innovation that brings with it the threat of a catastrophe of almost zero probability, but of virtually unlimited extent, in financial terms even though human life and limb may not be lost, has been brought into focus by the continuing and apparently endless debate about nuclear power. This 'Zero-Infinity Dilemma' poses a serious problem for the insurance industry owing to the scale, extent and new dimensions of risk that have to be underwritten if essential technical progress is not to be hindered. Among the many hazards of advanced technology in addition to atomic energy, those of the petrochemical industries and that of liquid natural gas (LNG), 'Frozen Fire', loom large. The dangers attributable to the latter are so grave that the U.S. Federal and State Governments have imposed special siting regulations for LNG installations, limiting population density to an average of no more than 60 people per square mile within 4 miles of a marine terminal and a lower population zone of not more than 10 within one mile of the installation (H. Kunreuther 1980). A very serious accident occurred in Cleveland, Ohio, in 1944 when the LNG flowing from a storage tank ruptured by brittle fracture ran into sewers where it evaporated and exploded, killing 128, injuring 300 and damaging $7 million in property.

The potential scale of the hazard which was assessed in the case of the Oxnard proposed terminal in California to present a worst case scenario of a severe threat to 50,000 residents caused the State Government to refuse permission for its construction (ibidem).

Another disastrous low probability event in the 'Zero-Infinity' class was the collision between the 'Aegean Captain', a 210,000 tons bulk crude oil carrier, and the 'Atlantic Empress' of 288,000 tons, also carrying crude oil, off Tabago on 20 July 1979 in which 26 men were killed. The insurance claims were of the order of £66 millions. The accident occurred through confusion in the interpretation of radar screen displays, both ships being adequately manned, equipped with the most up-to-date facilities and fully seaworthy.

8.3.1 Nine characteristics of 'The Dilemma': an actuarial view

The insurance industry in the West has had long experience of risk management and assessment and will provide cover for almost any imaginable risk, from compensation for multiple births to the career valuation put upon a film star's legs, but the new ones of the zero-infinity kind have posed special problems. Failure to assess a set of risks properly can mean bankruptcy, either through ruinous imbalance between claims and premiums or loss of business to competitors offering more attractive rates. The competition is fierce and in this adverse environment Lloyd's of London has survived for three centuries, 'never having failed to pay out a justified claim'. There should be valuable lessons that the engineer involved in the obviously analogous work of the assessment and management of the risks presented by the new hazardous advanced technologies, and not least those of nuclear power, can learn from the savoir-faire of his opposite number in the world of insurance who faces decision making of a similar kind.

Talbot Page's actuarial analysis of 'The Zero-Infinity Dilemma' (1978) is very relevant to the treatment of the disastrous LPEs that are the concern of modern engineering and deserves due consideration therefore. He distinguishes some nine common characteristics in the zero-infinity dilemma that is presented by certain advanced technologies, though not all are directly related to physical risks and thus to the engineering features of their management. They are:

(i) 'Ignorance of mechanism' which is perhaps the most important. It is lack of knowledge about the way in which the causes that lie behind a risk emerge to create an accident. It characterises all manner of risks, for instance, the chance of a major structural failure, a nuclear power plant incident, the transmission to man of radioactivity or other toxin that has adventitiously escaped into the food chain or the greivous harm that can be inflicted on a community by a medicine confidently promoted as safe. 'The mechanisms of generation, transmission and response are so poorly understood that the management of the problems arising is truly decision making under perverse uncertainty'.

(ii) 'Potential for catastrophic costs and harm to humans' is again an indeterminate decision criterion as it is specifically related to mechanism which is the principal area of ignorance.

(iii) 'Asymmetry between benefits and costs' as in the case of nuclear power when further investment in safeguards brings a modest reduction in risk. For example, the addition of an expensive safety feature is required to meet a vague danger which can not be precisely specified, but yet which can not be denied.

(iv) 'Low subjective probability' of catastrophic outcome has a commonsense influence in limiting safeguarding investment, though this again lacks specificity because of ignorance of mechanism. This is perception of the finite but near zero risk aspect of the 'dilemma'. It presents a particularly difficult problem for the safety assessor as on the one hand he must direct design investment toward the reduction of risks, yet on the other he must abdure empty safeguard engineering.

(v) 'Internal transfer of benefits' is an economic concept bearing on transfer of the benefits of the technology, eg cheaper nuclear generating costs per unit, through the market to the consumer by tending to lower product prices.

(vi) 'External transfer of costs' is another economic concept describing 'the direct non-market transfer of an effect'. The catastrophic costs of a nuclear plant accident of serious dimensions could not be transferred to the consumers through the mechanism of market prices of electricity and must be met from elsewhere, by government subventions. The high potential costs arising from a severe accident involve large safeguarding expenses which could not be borne wholly by the industry and are transferred to the general exchequer through direct government or subsidised institutional research, ie UKAEA. The failure of the market mechanisms to deal with this aspect of technological innovation is a primary reason for regulatory intervention in addition to public and environmental safeguarding. The commercial insurance market could not bear the strain of the catastrophic costs of a major nuclear power station accident, and the claims they are required to meet are limited by law with the government bearing the excess.

(vii) 'Collective risk' is one borne by many people simultaneously as major environmental risk problems have the potential to affect large numbers of people at the same time. The effectiveness of insurance, liability law and other traditional compensatory mechanisms in protecting against loss resulting from risk is limited in the collective case. This also has engineering and regulatory overtones as the plant and process must be designed to reduce collective risk, eg discharges of radioactivity from nuclear installations are regulated by law, overall shielding of the reactor to minimise radiation exposure of the public and the design of the plant are subject to regulatory safety scrutiny.

(viii) 'Latency' is the often extended delay between initiation of the adverse effect, eg massive release of radioactivity as the result of a nuclear accident, or exposure to the effect and the manifestation of its damage or detriment. Latency can be from 20 to 30 years and has regulatory significance in that operator of the hazardous installation may enjoy a limited period of responsibility for harm caused but not revealed during the operation of the plant or process. In the UK, the

operator of a nuclear installation may not have to meet claims for loss attributable to a nuclear incident when such claims are presented more than 10 years after he has been formally relieved of his period of responsibility for that installation.

(ix) 'Irreversibility' refers to the lingering consequences of adverse effects of the hazard or as a practical matter reversal or removal of the effect takes a long time or is very costly. It applies particularly to contamination as for example that of plutonium which is highly toxic in minute traces and has a half-life of 24,000 years which is considered to be absolutely irreversible.

Commenting on the above nine characteristics of the extra risks that advanced technology projects present to the insurance industry, Talbot Page (1978) considered that 'latency and irreversibility of effect have profound ethical and institutional implications. They raise questions concerning fair distribution of risk over time and how institutions can be designed to anticipate these adverse effects, rather than merely to react to existing known effects'. Not all of the nine are likely to have any direct influence on the formulation of an efficaceous treatment designed to anticipate and inhibit those causes that could bring about a catastrophic low probability failure of the zero-infinity kind in a technological system. Nevertheless, all of them, to a greater or lesser degree, will have a significant bearing on the thought processes that underlie such a treatment and some will determine the course taken by the designer to assure the safety of the system in question, but that is a matter of engineering.

8.4 Engineering interpretations of the 'Zero-Infinity' challenge

While the foregoing characteristics of 'The Zero-Infinity Dilemma' as perceived by Talbot Page (supra) are of an actuarial nature, they are, nonetheless, in accord with the general milieu that exists in Western society today, a milieu that has been largely created by the important part that the new technologies have played in fashioning its organisation and structure. Thus, the body politic has, at last, had to yield to penetration by the engineers who have even been accorded status be being dubbed 'the technical intelligentsia' and the cultures of the advanced countries have had to adapt their mores to their needs. On the other hand, the conservative discipline of engineering has had to broaden its horizons and admit that it has interdisciplinary interests touching on subjects like ergonomics, health physics and management. Design per se has emerged as an important study (Malherbe and Ogorkiewicz 1962, A. Moulton 1976, Bruce Archer 1979). There are many new sub-disciplines

that share a community of interest with the life and social sciences which in nuclear engineering include safety technology, siting and radiation protection. Neither has engineering escaped the challenge of the 'Zero-Infinity Dilemma'. There are, in fact, close comparisons between the quandary of the insurance risk assessor and that facing the engineer concerned with investment in the safeguarding of a major hazard installation, in our case a nuclear power plant, against a potentially catastrophic LPE.

Out of the nine characteristics of the risk assessor's perception of the 'Zero-Infinity Dilemma', all but two are relevant to the analogous situation that can face a nuclear engineer. The transfer of costs and benefits, Talbot Page's fifth and sixth categories, are matters of economics and, as such, have no direct bearing on the management of LPEs. However, the sixth, 'External transfer of costs', was a factor that largely determined the peculiar and novel form of the statutory regulation of commercial nuclear power in Britain and the U.S.A., the legislation being drafted in part to meet the needs of the insurance industry (Street and Frame 1966).

8.4.1 Catastrophic failures of uncertain causation

(Re Page's 'Potential for catastrophic costs and harm to humans'

and

'Ignorance of mechanism')

Owing to political and societal pressures, a major technical innovation may be put into use before enough is known about it to enable its reliability and safety to be fully assured. In many cases access to the foreknowledge needed is difficult or impossible to obtain. If the potential modes of failure are unknown, then there is ignorance of that mechanism which might precipitate a catastrophic accident and it would not be feasible to take every conceivable precaution against a possible, low probability event of uncertain causation. Hence, occurrence of a catastrophic LEP cannot be absolutely excluded. From its earliest days, the nuclear branch of engineering science recognised this danger and met it be developing a new approach to the technologies of reliability, safety and risk management, leading the field in these matters, the philosophical inspiration being 'safety by foresight' (Margaret Gowing 1974).

The characteristic of 'Ignorance of mechanism' together with that of a potential for the catastrophic outcome of a possible failure sequence are the sources of most of the problems relevant to safety that

are likely to arise when a new technology is exploited, something indubitably true in the case of nuclear power.

8.4.2 'Ratchetting' investment in engineering safeguards (Re Page's - 'Asymmetry between benefits and costs')

While engineers may be well aware that a certain technical innovation has an inherent tendency to suffer from a fault potentiality that could lead to a catastrophic accident, they may well be ignorant of all the efficient mechanisms capable of bringing the event about. As a result of their lack of perception of the true nature of the overhanging threat, the decisions that involve efficaceous engineered or operational safeguards may in consequence be indeterminate. This circumstance arises because, although a precaution taken may appear to be sufficient at the time of its introduction, further knowledge shows that it can be circumvented by another failure mode which, though perhaps a little less likely, is equally efficient. To meet the new threat, an additional step of safeguarding investment is made. But, continuing inquiries reveal that there is still yet another failure mode that can precipitate the accident and the engineer is called upon to make a further investment in safety. As the approach to full safety confidence is generally asymptotic, there can be continued iteration and 'ratchetting' of investment in the particular provision of safeguards with 'asymmetry between benefits and costs'. The problem of determining the point at which investment in safety can be seen to be adequate is one of the most difficult problems facing nuclear engineering.

8.4.3 Low Probability Events and the quandary of open-ended design targets (Re Page's 'Low subjective probability of catastrophic outcome')

The designer of a hazardous technological system is confronted with a wide spectrum of potential faults, any one of which might initiate a sequence leading to a catastrophic failure. In the case of nuclear reactor design, his quandary is profound. Not surprisingly then, the problem of how to set realistic design targets which embody demonstrably adequate protection against the very real threat of a calamitous radiation accident of very low, but finite probability has exercised the nuclear power industry from its inception. Many of the more intractable of these faults can be designed out of the system entirely, as for instance the replacement of the steel membrane which formed the pressure vessel surrounding the core of a Magnox reactor by a pre-stressed concrete shell that made explosive rupture of the reactor's

main containment impossible, and 'fulfilled the requirement of unquestionable safety' (Kirk and Taylor 1971). Nonetheless, there remain those faults that cannot be eliminated in such a definitive way and, indeed, their very existence may be unsuspected. The true threat posed by these residual, but grave, weaknesses in the fabric of reactor design remains enigmatic, chiefly because of their low subjective probability. Despite their elusive character, the threat they present cannot be dismissed and design for safety in such circumstances is necessarily open-ended. Attempts made so far to escape from the quandary, at first by qualitative and more recently by quantitative methods of design safety assessment, have been less than wholely successful and the problem remains an obstacle in the way of the further development of atomic energy as a source of commercial power.

8.4.4 Protection of the public: major hazards and reactor siting (Re Page's 'Collective Risk')

The dangers that a major hazard installation can impose on the community in which it is located may extend to a considerable distance beyond its boundaries. As a result, people and property in the surrounding area are at risk collectively. Among the dangers to which they may be exposed are missiles and blast from an explosion, toxic fumes, gases and ejected particulate material and, in the case of a nuclear power plant, effusion of radioactivity and direct radiation from the process. While it is only recently that attention has been paid to the generality of industrial activities presenting hazards of this kind, siting restrictions have long been applied to nitration plants and to factories manufacturing and storing commercial explosives and munitions. In the case of nuclear power, the dangers were recognised from the beginning. At first attention was paid chiefly to site perimeter radiation levels and the massive adventitious release of radioactivity that could follow a radiation accident. More recently, it has been directed to the steady effusion of radioactivity resulting from normal operation as well which can contribute to low level doses to the general population over a wide area. Siting policy has always played an important part in nuclear safety regulation in Britain, but it has tended to remain in a traditional mold in spite of attempts to put it on a quantitative basis. While remote siting, as far as this has been feasible, has been accepted as appropriate to the risk, the economic inducements to bring power reactors closer to the main centres of population are strong. Undoubtedly, siting policy is likely to be a continuing matter of debate.

8.4.5 Control of radiation exposure: dose limits and siting criteria (Compare Page's 'Latency' and 'Irreversibility')

The characteristics of 'latency' and 'irreversibility' have no direct engineering relevance to the anticipation of LPEs, nonetheless they are important because they are factors taken into account in setting the permitted levels of ionising radiation and radioactive contamination to which people may be exposed and in prescribing limits for the amounts of radioactivity that may be released to the environment. The specific values and associated norms are set nationally, but in accordance with the Recommendations of the International Commission on Radiological Protection (ICRP), though with certain local variations in interpretation. By virtue of their regulatory status, they become determinants in the formulation of engineering design criteria for shielding, controlled discharges of radioactivity to the environment, radiation protection in the fuel cycle generally and for the initiation and planning of emergency action in the event of a radiation accident and in the prescription of siting criteria.

8.4.6 Verification of accountability and accuracy in risk assessment

Long experience has taught insurers to be wary of big risks with very low probabilities which 'create such a problem to the industry that it rather tries to avoid the insurance of such risks'. Nuclear risks in this class are underwritten only with specific government guarantees that are further covered by international conventions on liability, and premiums are arbitrary. Talbot Page posits that normal acceptance of risks of this kind, and nuclear ones in particular, can only be secured by establishing trust amongst the underwriters and the body politic. The industry in question, nuclear power, does not have to be shown to be absolutely without major risks, for that is impossible, but the institutions responsible for assuring the safety of nuclear power and the individuals who comprise and represent them must be known to be worthy of trust. Similar conditions apply to acceptance, or better toleration, of the nuclear risk by the concerned and politically aware elements of the public in the West, but with a more general proviso that they must also be convinced that the nuclear option is a necessary contribution to the World energy balance. And, this theme underlies the New Treatment.

In these circumstances, Talbot Page's proposed solution to the zero-infinity dilemma of nuclear power is relevant, profound and worthy of study. In advancing an actuarial thesis, Page notes as 'curious' a

situation in which insurance companies appear to have long used probability in their assessments of risk, but 'when this approach flowered later in the enormous complexity and sophistication of the Rasmussen report and similar treatments of decision trees, public confidence in them in fact declined'. He sets aside the suggestion made by certain specialists in risk assessment that the public is irrational and lacks understanding in the techniques used. Instead, he attributed 'the growing scepticism' and lack of confidence in risk assessors to ad hominem considerations such as 'of course he assesses the risk as very low, but then his career is invested in nuclear power'.

There are three salient things that make risk assessment in Western society of today different in quality from that to which the insurance industry had become conditioned. Previously, business in each class of cover was written against an experience of loss adjustment that was adequate for the given risk accepted. Secondly, the mechanism likely to precipitate a loss was largely known and understood, including the heavy losses occurring from time to time in air, marine and rail transportation. And lastly, the risk assessor's advice was validated against the continuing test of market forces, poor advice being an almost certain prescription for financial collapse of the underwriting syndicate. The sanction of accountability has proved the soundness of the renowned insurance corporations of today who enjoy public approbation and trust.

8.4.7 Simulated accountability by 'Keeping Score'

In a subsequent analysis of the actuarial enigma created by zero-infinity risks, Talbot Page (1979) identified 'Ignorance of Mechanism' as its first and most important characteristic. Owing to the potentiality of these new risks for a catastrophic outcome (Page's second characteristic), business of this kind has only been accepted on a basis of absolute liability without recourse and within maximum limits of loss supported by government guarantee for any excess. This latter involvement of the state has had far-reaching consequences. To the foregoing, he has added a third salient characteristic of 'Latency' which by a turn of logic is extended from his earlier definition (1978) (meaning the long delay between a calamitous event and its full consequences) to embrace the patent loss of trust now displayed in the new style of risk assessors. As a consequence of state involvement, they are, for the most part, employees of government agencies or sponsored bodies and as such bear no

direct responsibility for their advice and other interventions, working to a philosophy described as being 'concerned with influencing attitudes and creating a framework' and 'not with detailed prescriptions' because 'the primary responsibility lies with those who create risks' (Robens 1972/a). Indeed, any direct responsibility is constitutionally eschewed. Yet, these experts are the assessors who effectively determine whether or not this or that risk should be imposed. Page opines that this combined with 'latency' has been inimical to credibility. Nonetheless, he suggests that the credibility so essential to the work of risk assessment agencies could, in fact, be built up by simulating the actuarial obligation of accountability that has proved successful in maintaining the high standards of the insurance business and the trust so readily accorded to it. While it would not be feasible to establish direct responsibility for the circumstances that led to a rare and unusual accident, it would be possible to test nuclear risk assessors against a lower tier of faults and incidents that are of relatively frequent occurrence, although they do not progress to the final stage of disastrous consequences. He proposes an analogy with a game which he called 'Keeping Score', whereby assessors could be rated against their successes in predicting 'intermediate events and partial chains in their major decision trees' (Talbot Page 1979). By this device there would be more events and 'latency' would be less of a problem because such minor failures could be readily identified and reported with much less of a hiatus between expectation and occurrence. The process would have the teeth of accountability by imposing sanctions on the agencies and their assessors by rewarding success and penalising failure. The idea is developed further in Section 14.6 et seq.

8.4.8 Bringing risk assessors to account: some constitutional issues

Despite the profound insight that Page's proposals give into the vexatious problems that arise in the management of zero-infinity industrial risks, serious difficulties, both organisational and practical, stand in the way of their introduction. His case which is administrative and actuarial in essence involves an institutional extrapolation from the clearly defined task performed by risk assessors for underwriters in the insurance industry into the vague and almost inchoate situation in which advice is sought and received by the proximate decision makers in government departments, state industries and boards, public utilities and large commercial corporations. Furthermore, for 'Page' to be effective, profound changes of a constitutional kind are essential

because policy formulating authority over a wide technological area would have to be ceded by entrenched administrative officials in whose hands it traditionally rests to engineers in bodies like the U.S. Nuclear Regulatory Commission (USNRC) and the Nuclear Installations Inspectorate (NII) in Britain. In accepted constitutional practice, the latter two bodies are assigned inspectional functions to be properly exercised under higher tier administrative direction that precludes excursions into matters of policy, say direct involvement in the debate about choice of a nuclear reactor system, for instance Pressurised Water (PWR) versus Advanced Gas Cooled (AGR) reactor technology. But, owing to the complexity of the work undertaken by the USNRC and the NII both bodies and particularly the latter have acquired an unusual degree of autonomy in the policies they pursue and the actions they undertake in matters that are constitutionally beyond their competence. For instance, the NII exercises powers of licensing, is involved in the drafting of legislation and negotiates with public and official bodies to an extent that is unusual in the execution of an important Act of Parliament (O.H. Critchley 1977). The substantial further delegation of Ministerial authority in matters of nuclear power envisaged by Page (supra) would be seen as establishing a precedent of far reaching constitutional significance and, as such, would be likely to be resisted.

The issue at stake lies deeper at the interface between the administrative realm of 'The Word' and the functional one of 'The Deed' where the engineer is intruding to exercise the new societal role that Auguste Comte identified (See Sections 8.1 and 10 et seq). Similar difficulties face the New Treatment, but in matters of atomic energy some of the necessary delegations have already been acquired in practice and wide areas of precedent established (supra). Further, the New Treatment is in the engineering dimension and that adds a legitimacy to its case that Page's constitutional challenge lacks.

8.4.9 Illusory aspects of Design and Risk Assessment

The fault and event decision trees of the U.S. Reactor Safety Study (See Section 7.3) are cited by Talbot Page (supra) as products of an analysis of the zero-infinity risks of nuclear power of the kind that could provide suitable material for appraising the competence of risk assessors. As an example, he notes that the assessors did not allow for the possibility of the human error that initiated the Browns Ferry accident (See Appendix II). Notwithstanding the considerable value that an analysis in depth of the Rasmussen kind can confer upon a complex

design concept by improving its quality and safety and, not least, by disclosing oversights, hidden weaknesses, unrecognised common mode fault potentialities and other less obvious causes of system failure, it is not possible for the assessors to foresee more than a part, though perhaps a large part, of the future situation. The writer in commenting on the assessed individual major accident risk of 2×10^{-9} per year per reactor predicted in the U.S. Reactor Safety Study (N.C. Rasmussen 1975 - 2) puts it thus:

> 'A risk so forecast cannot be true. The true hazard is given by the summation of the occurrence probabilities of all the accident-producing causes which includes an almost infinite spectrum of unexpected, unusual or highly improbable though possible happendings or occurrences. At the present time, at least, the task of catching such a large number of rare, random and diverse things is Sisyphean.'
>
> O. H. Critchley,
> 'Risk prediction, safety analysis and quantitative probability methods - a caveat,'
> J. Brit. Nucl. Energy Soc., Jan. 1976, 15(1), 19
> (See Document No. 1 in the Annex of Supporting Papers).

The foregoing is in keeping with established philosophy in modern plant engineering, for example Professor Frank P. Lees (Plant Engineering, Loughborough Technological University) writes:

> '9.1.8 Engineering Feasibility... ... There is obviously a limit both to the degree of plant reliability that can be achieved by even the best engineering practice and, equally important, the degree of confidence that can be placed in such assessments of plant reliability.
>
> A figure quoted for the reliability to which plants can be engineered is a hazard rate of 10^{-5} events/year (Bowen 1976). The reason that it is difficult to achieve lower hazard rates is that at this level the risk begins to be affected by rather improbable failures and common cause faults.
>
> It is important not only to be able to achieve low hazard rates but to have confidence in the estimate made of this rate.'
>
> Loss Prevention in the Hazard Industries:
> Hazard identification, assessment and control, Volume 1,
> Butterworths, London and Boston, 1980,
> pp. 180-181.

It is therefore hard to see how an assessor could find the time to cover enough of the vast field of possible happenings to include the odd human error that led to the Browns Ferry incident (supra). The Reactor Safety Study consisting of a Main Report and eleven substantial volumes

of supporting material was described by the Peer Review as inscrutable, difficult to follow and lacking in adequate data (See Section 7.3.1). Yet, it took a large team under the direction of Professor Norman C. Rasmussen of M.I.T. assisted by many supporting research bodies some two years to produce. In spite of its wide ranging and sophisticated survey of possible accident sequences which included human errors, the text has to be tortured to extract from it any hint of the precursors of the Three Mile Island incident of 31 March 1979. By comparison the safety study for the inquiry chaired by Sir Frank Layfield into the Central Electricity Generating Board's (CEGB) proposal to site a Pressurised Water Reactor (PWR) at Sizewell near Leiston in Suffolk is even more massive (13). Assuming a positive recommendation from the inquiry, it will be a decade before event reports from operations of the PWR will become available for comparison with the decision trees.

In view of these long lead times, the idea of retrospectively bringing an assessor or his team to account for failure to predict some catastrophic failure seems chimerical, if not improper. Nonetheless, Page's suggestion (supra - 8.4.7) of rating assessors against their contemporaneous performance in predicting the occurrence of faults in the numerous 'intermediate and partial chains' has merit. Analogous data that met the criterion of ontological relativism as defined in Section 9.7.2 et seq. could be obtained through the licensee event reporting systems of which samples are displayed in Table III.

8.5 'Lead time': another characteristic of 'The Zero-Infinity Dilemma'

Talbot Page (1979) in his penetrating analysis of 'The Zero-Infinity Dilemma' recognised the importance of the often very considerable delay between cause and effect. In his earlier actuarial approach of 1978, he saw it in the limited terms of a detriment that confounded evaluation of a risk, defining it as 'latency' (See Section 8.3.1 - viii), citing as an example the long induction period between exposure to ionising radiations and the appearance of deleterious consequences. However, he overlooked another aspect, the delay, which, although it has long been known as an impediment in engineering, could seriously compound treatment of 'The Dilemma'. This is the engineering factor of 'lead time', no longer a confidently predictable feature of design, but an incommensurable element in the complex mix of latter day technology, for example the excessive, though unforeseen lead times that have distinguished the 'Concorde' airliner and the Dungeness 'B' AGR nuclear power plant. Although it properly makes an independent and tenth characteristic of the dilemma, Page identifies it with 'latency', stretching that

TABLE III

Licensee Event Reports

(Two specimen sets of Licensee Event Reports excerpted from returns by U.S. nuclear power plant operators to the Nuclear Safety Information Center and issued after processing in February and April 1980)

FEB 24, 1980 — LER MONTHLY REPORT SORTED BY FACILITY
PROCESSED DURING FEBRUARY, 1980 FOR POWER REACTORS

FACILITY/SYSTEM/COMPONENT/ COMPONENT SUBCODE/CAUSE CODE/ CAUSE SUBCODE/MANUFACTURER	DOCKET NO./ LER NO./ CONTROL NO.	EVENT DATE/ REPORT DATE/ REPORT TYPE	EVENT DESCRIPTION/ CAUSE DESCRIPTION
ARKANSAS-1 FEEDWATER SYSTEMS + CONTROLS PUMPS OTHER DEFECTIVE PROCEDURES NOT APPLICABLE ITEM NOT APPLICABLE	05000313 79-022/03L-0 827112	011979 021679 30-DAY	DURING PLANT HEATUP TO HOT SHUTDOWN CONDITIONS, THE OPERATIONAL TEST (OP 1106 06) OF THE TURBINE DRIVEN EMERGENCY FEEDWATER PUMP (P7A) WAS NOT PERFORMED. HOWEVER, THE REDUNDANT MOTOR DRIVEN PUMP (P7B) WAS TESTED SATISFACTORILY WHILE IN COLD SHUTDOWN CONDITIONS ON 11-12-79 AND 11-28-79 THE P7A EMERGENCY FEEDWATER PUMP WAS SATISFACTORILY TESTED. THERE HAVE BEEN NO SIMILAR OCCURRENCES. REPORTABLE PER T.S. 6.12.3.2(B). THE P7A EMERGENCY FEEDWATER PUMP WAS NOT TESTED PER OP 1106 06 DUE TO A SCHEDULING MISTAKE WHICH WAS NOT COVERED BY THE STARTUP PROCEDURE 1102 0 2. THEREFORE, A STEP WAS ADDED TO THE STARTUP PROCEDURE TO PROHIBIT ANY FUTURE SIMILAR OCCURRENCES.
ARKANSAS-1 FEEDWATER SYSTEMS + CONTROLS TURBINES SUBCOMPONENT NOT APPLICABLE COMPONENT FAILURE MECHANICAL TERRY STEAM TURBINE COMPANY	05000313 79-024/03L-0 827883	020679 021080 30-DAY	DURING THE OPERATIONAL TEST (OP. 1106 06 SUPP. II) OF THE TURBINE DRIVEN EMERGENCY FEEDWATER PUMP (P7A), THE PUMP WAS DECLARED INOPERABLE ON LOW PUMP DELTA P. THE REDUNDANT PUMP (P7B) WAS STARTED AND PROVED OPERABLE. ON 12-6-79, THE P7A EMERGENCY FEEDWATER PUMP WAS REPAIRED AND SUCCESSFULLY TESTED. THERE HAVE BEEN NO SIMILAR OCCURRENCES. REPORTABLE PER T.S. 6.12.3.2.(B). THE SPEED GOVERNOR LOCK NUT WAS FOUND TO BE LOOSE ON THE TURBINE PUMP DRIVE. THIS CAUSED THE PUMP SPEED TO BE LESS THAN NORMAL. THE PUMP SPEED WAS INCREASED TO ALLOW NORMAL OPERATION AND THE LOCK NUT WAS TIGHTENED
ARKANSAS-1 CHEM, VOL CONT + LIQ POISN SYS PUMPS CENTRIFUGAL PERSONNEL ERROR LICENSED & SENIOR OPERATORS ITEM NOT APPLICABLE	05000313 79-023/03L-0 827964	122179 011880 30-DAY	DURING A NORMAL MAKEUP OPERATION TO THE RCS, THE BORIC ACID PUMPS WERE INADVERTANTLY LEFT OPERATING. THIS RESULTED IN OVER BORATION OF THE REACTOR COOLANT AND AUTOMATIC WITHDRAWAL OF RODS ABOVE THE LIMITS PER T.S. 3.5.2 3.5. THE RCS WAS IMMEDIATELY DILUTED AND THE ROD INDEX WAS RETURNED TO THE NORMAL RANGE WITHIN THE ALLOTTED 4 HOURS. LER 50-313/78-025 WAS A SIMILAR OCCURRENCE OF THE ROD INDEX OUT OF LIMIT. REPORTABLE PER T.S. 6.12.3.2.B. DURING A NORMAL MAKEUP OPERATION TO THE RCS, A REACTOR OPERATOR INADVERTANTLY FAILED TO SECURE THE BORIC ACID PUMPS. THE OPERATOR WAS COUNSELED AND COPIES OF THE FAILURE REPORT WERE DISTRIBUTED TO ALL LICENSED OPERATORS.
ARKANSAS-2 OTHR INST SYS REQD FOR SAFETY INSTRUMENTATION + CONTROLS TRANSMITTER COMPONENT FAILURE OTHER FISCHER & PORTER CO.	05000368 79-008/03X-1 825219	011479 011880 OTHER	DURING MODE 1 OPERATION, REFUELING WATER TANK LEVEL TRANSMITTER, 2LT-5639-3, SENSING LINE FROZE, MAKING THE TRANSMITTER INOPERABLE. THE LOW-LOW LEVEL TRIP (RAS) SIGNAL ON PPS CHANNEL "C" WAS BYPASSED PER THE REQUIREMENTS OF ACTION STATEMENT T.S. TABLE 3 3-3.6.B 09. THE REMAINING RWT LEVEL INDICATIONS WERE VERIFIED TO BE NORMAL. SIMILAR OCCURRENCES ARE LER'S 50-368/79-002 & 79-001. REPORTABLE PER T.S. & 9.1.9 B. INVESTIGATION REVEALED THAT THE TEMPORARY HEAT LAMP PLACED IN THE TRANSMITTER BOX HAD BURNED OUT. THE LAMP WAS REPLACED AND REMAINED IN SERVICE UNTIL NOVEMBER, 1979, WHEN HEAT TRACING WAS PERMANENTLY INSTALLED.

APR 24, 1980 — LER MONTHLY REPORT SORTED BY FACILITY
PROCESSED DURING APRIL, 1980 FOR POWER REACTORS

FACILITY/SYSTEM/COMPONENT/ COMPONENT SUBCODE/CAUSE CODE/ CAUSE SUBCODE/MANUFACTURER	DOCKET NO./ LER NO./ CONTROL NO.	EVENT DATE/ REPORT DATE/ REPORT TYPE	EVENT DESCRIPTION/ CAUSE DESCRIPTION
BEAVER VALLEY-1 PRCS + EFF RADIOL MONITOR SYS COMPONENT CODE NOT APPLICABLE SUBCOMPONENT NOT APPLICABLE OTHER NOT APPLICABLE ITEM NOT APPLICABLE	05000334 80-015/04T-0 838535	030880 032180 2-WEEK	WHILE PERFORMING THE MONTHLY RADIATION MONITOR SURVEILLANCE TEST, IT WAS DISCOVERED THAT THE COMPONENT COOLING WATER RADIATION MONITOR HIGH-HIGH LEVEL ALARM DID NOT FUNCTION. THIS RADIATION MONITOR SERVES NO AUTOMATIC CONTROL FUNCTION AND IS BACKED UP BY THE RIVER WATER RADIATION MONITORS. THERE WAS NO SAFETY IMPLICATION INVOLVED WITH THIS INCIDENT. THE COMPONENT COOLING WATER RADIATION MONITOR HIGH-HIGH ALARM DID NOT COME IN WHEN THE TEST SIGNAL INPUT WAS HIGH ENOUGH TO CAUSE THE METER TO INDICATE OFF-SCALE, HIGH. SUBSEQUENT INVESTIGATION BY MAINTENANCE PERSONNEL REVEALED THAT THE ALARM POTENTIOMETER WAS OUT OF ADJUSTMENT.
BIG ROCK POINT DC ONSITE POWER SYS + CONTROLS BATTERIES + CHARGERS SUBCOMPONENT NOT APPLICABLE COMPONENT FAILURE OTHER EXIDE INDUSTRIAL DIV	05000155 80-002/03L-0 838237	012480 022180 30-DAY	DURING MONTHLY SPECIFIC GRAVITY CHECKS, CELL 14 OF THE BATTERY FOR CHANNEL C OF THE REACTOR DEPRESSURIZING SYSTEM, READ 1.191. THIS IS BELOW THE LIMIT OF 1,200 SPECIFIED IN TECH SPEC 11.4.5.3.A.2(B). ALL OTHER CELLS EXCEEDED SPECIFICATIONS AND THE CHANNEL IS DEEMED OPERABLE FOR THE SPECIFIC DEFICIENCY. THE BATTERY WAS PUT ON EQUALIZING CHARGE. INCIDENT SIMILAR TO RO-79-26 AND RO-78-34. NO HAZARD TO THE PUBLIC OCCURRED. THE CELL DID NOT RESPOND ADEQUATELY TO THE EQUALIZING CHARGE AND THE CHANNEL WAS REMOVED FROM SERVICE, AS ALLOWED BY TECHNICAL SPECIFICATION 11.3.1.5, TO REPLACE THE DEFECTIVE CELL ON 1/29/80. REPORTABILITY BASED ON TECH SPEC 6.9.2.B(2).
BIG ROCK POINT CNTNMNT ISOLATION SYS + CONT VALVES CHECK COMPONENT FAILURE NATURAL END OF LIFE UNION PUMP COMPANY	05000155 80-007/03L-0 838446	022480 031980 30-DAY	DURING ROUTINE OPERATION AT 1700 HOURS, EXCESSIVVE VIBRATION WAS NOTED ON CONTROL ROD DRIVE PUMP 02. THE PUMP WAS REMOVED FROM SERVICE AND 01 PUMP WAS PLACED IN SERVICE. INVESTIGATION REVEALED THAT THE SUCTION POPPET VALVES WERE DEFECTIVE. THE PUMP SUCTION VALVE WAS MANUALLY CLOSED ON 2/24/80 TO PROVIDE A REDUNDANT CONTAINMENT BOUNDARY PENDING COMPLETE REPAIR TO THE VALVES. NO HAZARD OCCURRED. REPORTABLE BASED ON TECH SPEC 6.9.2B(2). INVESTIGATION REVEALED WORN SUCTION POPPET VALVES ON THE PUMP AND DAMAGE TO PUMP PIPING HANGERS FROM THE VIBRATION. THE POPPET VALVES WERE REPLACED AND LAPPED AND THE HANGARS REPAIRED AND THE PUMP TESTED SATIFACTORILY ON 2/26/80. SIMILAR TO INCIDENT REPORTED AS RO-77-29.
BROWNS FERRY-1 DEMIN WATER MAKE-UP HANGERS,SUPPORTS,SHOCK SUPPRSS OTHER OTHER NOT APPLICABLE TENNESSEE VALLEY AUTHORITY	05000259 79-016/01T-1 826778	082379 031180 2-WEEK	WITH UNIT IN NORMAL OPERATION AT 95% POWER, INSPECTIONS WERE MADE IN ACCORDANCE WITH IE BULLETIN 79-14. DURING THIS INSPECTION, IT WAS FOUND THAT RESTRAINTS ON CERTAIN CSSC SYSTEMS WERE INOPERABLE IN THAT THEIR CONFIGURATION DID NOT CONFORM TO THE DESIGN SPECIFICATIONS. THERE WERE NO RESULTING SIGNIFICANT OCCURRENCES, NO PREVIOUS SIMILAR EVENTS AND NO DANGER TO HEALTH OR SAFETY OF THE PUBLIC. THIS EVENT WAS REPORTED UNDER T.S. 6.7.2.A(9). PIPE VIBRATION AND/OR IMPROPER INSTALLATION DURING CONSTRUCTION CAUSED THE INOPERABILITY ON RS TYPE RESTRAINTS, ON RMRSW. FIFTY OF THESE RESTRAINTS IN UNITS 1, 2, AND 3 WERE INSPECTED WITH REPAIR WORK REQUIRED ON NINETEEN OF THESE. THIS IS A FINAL REPORT.

Licensee Event Reports (LERs) are made by U.S. nuclear site licensees' to a data base at the Oak Ridge National Laboratory (ORNL) maintained by the Nuclear Regulatory Commission (NRC), the Advisory Committee on Reactor Safeguards (ACRS) and the Nuclear Safety Information Center (NSIC). After being collated and summarised, the LERs are issued monthly by the Licensee Operations and Evaluation Branch of the NRC. (Situation as at August 1980. See also Note 15.)

characteristic to explain the futility and, indeed, impropriety of holding the risk assessors concerned with zero-infinity risk, like those engaged in the safety assessment of nuclear power plants, directly accountable for the accuracy of their predictions.

The foregoing long and unforeseen lead times associated with modern innovatory technology and particularly with nuclear power have not allayed public concern about its hazards and, not least, have helped to undermine confidence in officially sponsored claims for its safety. Furthermore, a long and indeterminate hiatus between the commencement of a major project and its completion destroys the continuity between the team that conceived, synthesised and assembled the information presented in the design packet and the engineers who at some much later date must construct, commission and operate the plant according to the design instructions.

A long lead time can impair the clarity with which a design can be interpreted and the fidelity of compliance with its instructions. The confidence that can be placed in any risk assessment based on that design is thus further diminished. The deviations from the design and other failures to realise its intent cannot be made good by actuarial judgement or allowed for in the process of assessment because their incidence cannot be foreseen with any certainty. They can only be corrected after detection during engineering work in the field as the plant is constructed and brought into operation. The concept of such monitoring is central to the New Treatment and is the theme of 'Technological progress, safety and the guardian role of inspection' (O.H. Critchley 1981) which is offered as Document No. 4 of the Annex of Supporting Papers.

8.6 Overview from the Engineering Dimension

The modern disastrous technological LPE has been portrayed in its historical setting as an inevitable consequence of the progress of technology in Western society, something made necessary by population growth and associated pressures from the people for a healthier, better and fuller life. To meet their needs, it has been necessary to harness ever more powerful agencies and forces that carry risks which have risen in proportion to the potency of the instrumentalities used. Better technology has enabled man to live a longer and richer life, but at a price of suffering a greater toll of accidents which to the average person in the West now presents a risk of fatality of about 3.8×10^{-4} per annum of which 2.5×10^{-4} can be attributed to traffic accidents,

although industry as a whole has become much safer. In this steady and largely stable flow of untoward events, the LPE, unexpected, unpredicted, catastrophic and costly in life, limb and property, presents itself as a singularity, like a crashing spike of random noise in an electronic communication channel. It inflicts a cultural shock on the community afflicted, often spreading to people far from its site of occurrence, evoking intense interest, concern and, sometimes, fear. However, as Professor R. Wilson (1975) has observed, the response is odd and anything but linear, a situation depicted in Figure 2. Typical among these catastrophes may be picked out the 'Titanic' (1912), 'Aberfan' (1966), 'Minamata' (1959-1971), 'Flixborough' (1974) and 'Three Mile Island' (1979) which are all mentioned in Appendix II.

Characteristic of their causation is a combination of physical and human systems failures, usually involving glaring errors of action and judgement. Therefore, any attempt to reduce their incidence and to ameliorate the societal shock that is associated with major LPEs must recognise them as, not merely physical events of death, maim and destruction, but as events embedded in the contemporary culture, being due more to frailties of behaviour and management than to failures of plant or equipment. Despite that, the current interests of safety science seem to have been concentrated on scientistic rationalisations of the way in which people perceive risk and on the perfection of design through quantitative analyses of presumed plant function. The latter trend has led to some very sophisticated investigations of great complexity and depth like the U.S. Reactor Safety Study (N.C. Rasmussen 1975).

The quantitative approaches which were promoted largely as ways of resolving the problem of LPEs in nuclear power plants and thereby presenting a safe image of the technology were initially received with almost universal acclaim, although doubts were expressed by many informed engineers. There is now general agreement in the latter circles that they offer an effective way in which to make an exhaustive safety assessment of a design, but they are of little relevance to things that might precipitate an LPE in a spatially remote situation after a long lead time. Besides, there is growing scepticism of more presumptive claims.

The early uncritical rush of support for the methods of quantification that are still favoured in some of the most august scientific circles, albeit out of the field of pragmatic engineering plant risk management, is of itself a phenomenon of societal interest. It arises in the

INCIDENT FREQUENCIES, CONSEQUENCES AND PUBLIC REACTION TO HAZARD

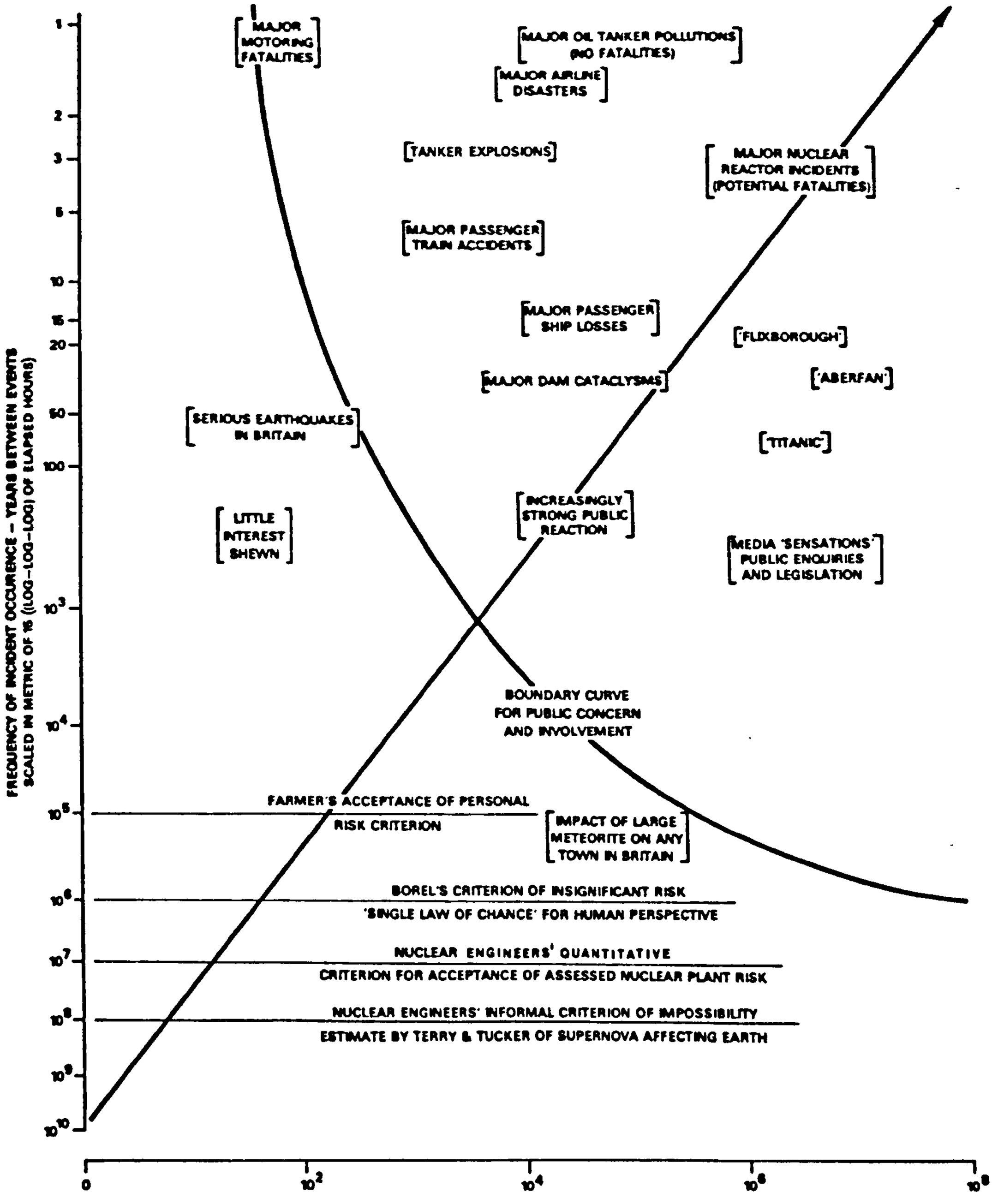


Fig 2

Aristotlean idealist Weltanschauung that still dominates Western thought (11). Causation is believed to act in a cosmos of underlying order and obedience to universal natural laws, despite what may appear to be superficial chaos. Adherence to this ideal led Albert Einstein to question the Quantum theory even until his death, still expecting an alternative to be discovered. It follows logically that by collecting enough data, it should be possible to cast a true quantitative probability that can define the likely behaviour of a system, despite any immediate inference of uncertainty. The random elements can be contained within confidence limits that may be established with sufficient stability for sound decision making to be based on the result.

A not unrelated recent trend, inspired by the impressive developments in computer based information technology, is to build into the control circuits of a complex, potentially hazardous plant, eg a nuclear power station, automated safety, able to override the actions of the operators in the control room. Once again the idea is initially reassuring, but there are engineering doubts and the Air New Zealand disaster that overtook its DC - 10 on Mount Erebus in Antartica on November 28, 1979, has disturbing implications. It seems likely that it was a computer assisted crash (See Appendix II , also Gordon Vette 1982).

The validity of the idealist position will be challenged in the passages that follow and the New Treatment will offer an alternative approach in the engineering dimension that accepts a random and ultimately unforeseeable incidence of LPEs. Their causation will be attributed to the ubiquitous and unpredictable propensity of human beings to behave erratically, even when the most skilled people are engaged in familiar tasks. Severe accidents in well-managed and established systems are seldom, if ever, caused by failures of equipment or components alone without a compounding element of human error (Glin Bennet 1983).

8.6.1 An analogy with 'noise' theory

The New Treatment draws an analogy with noise theory in which the LPE is identified with the spike of noise that is often observed in a communications circuit, both being surges of anomalous causation that disrupt the normal performance of the system by overloading, causing damage if they are of sufficient magnitude. Features of the phenomenon include an impulsive disturbance intruding from without the system, a sudden change of state within it due to release of internal stresses or tensions or a confluence of random events, usually faults or breakdown

of a component. These things, separately or in combination, build up to a major electrical surge or a fault sequence leading to an incident that may be catastrophic for a nuclear power plant.

In the case of a severe plant LPE, the precipitating events might be failure of the electric grid supply, irregular operator actions consequent upon person or inter-personal tensions and additive combinations of equipment faults and human errors. As noise theory can do no more than to identify the foregoing causative elements as signals indicative of the plant state, some interpretative process is needed. Catastrophe theory is introduced to assist the safety analyst in understanding the significance of these potential harbingers of failure.

In the combination of Noise and Catastrophe theories, a nuclear power plant in its operational phases is envisaged as moving in a probabilistic behaviour field, being steered by human agencies to avoid those anomalies in the surface of the field that could destabilise the system, leading in an extreme case to catastrophic failure. Successful operation then depends on the quality of the engineering in all aspects of the management of the plant, a function that can be monitored and attested by inspection.

In the light of this kind of pragmatic hazard management, acceptance of the 'zero-infinity' risk of disastrous accidents is unavoidable. The aim is to reduce the chance of their occurrence to the negligible, a state that can be recognised as such by a community willing to tolerate the residual hazard so that the benefits of the technology may be enjoyed. There is evidence to show that such a treatment can win the support of a responsible and properly informed body politic. Reference has been made to the experience of the Netherlands that has long existed under a ceaseless threat from the sea which is kept out by an extensive and complicated system of dykes, sluices and sea-walls maintained by the country's civil engineers. Despite the over hanging menace, the Dutch continue to live in their fertile and prosperous land, confident in the adequacy of their protection, notwithstanding the calamitous failure of these sea defences during the past millenium, one of which occurred this century.

9 SAFETY ASSESSMENT OF DESIGN: FACTS AND FALLACIES

> 'It may be noted that it is the use of appropriate and precise methods of observation and reasoning which make an investigation scientific. The fact that the material is scanty, as may sometimes be the case in operational research, does not of itself render an investigation unscientific, although no amount of scientific method can get more out of data than there is in them.'
>
> P.M.S. Blackett (Lord)
> 'Operational Research', Part II -
> Studies of War: Nuclear and Conventional,
> Oliver and Boyd, Edinburgh & London, 1962, p.200.

The New Treatment is an engineering approach to nuclear power risk management that proposes a specific application of the Scientific Method, whereas the existing approaches have become orientated towards theory rather than practice. Owing to the societal pressures on the industry, their significance is more cultural and promotional than scientific and has the marks of the dominance of 'Word' over 'Deed' that is characteristic of Western civilisation. A consequence has been a preoccupation with studies of design itself rather than a proper attention to the realisation of a given design in the hardware of the operating nuclear power reactor on site. The U.S. Reactor Safety Study (N.C. Rasmussen 1975) is almost exclusively concerned with problems of design and the quantification of elusive possible fault sequences. Obviously, it is essential to have a sound design, as fault free as reasonably practicable, but proving that a potential event known to have a very low probability has an even lower one is of little relevance to operational safety.

Safety assessment of a kind has long been practiced as a normal part of industrial plant design. In the nuclear power industry where the grave nature of a major radiation accident was immediately manifest, a meticulous and structured system for the safety assessment of design has evolved. In the commercial field, it has become a statutory part of the licensing process, the applicant being required to submit a Safety Report which may be in several parts, giving a comprehensive description of the design of the plant and its safety provisions (R. Gausden 1982). The safety case presented in such a Report which would embrace all the technical design matters depicted in Figure 3 is then subjected to an exhaustive official safety assessment that may result in mandatory requirements for major design changes. These scrutinies were at first largely qualitative, but over the past decade

VISTAS AND HORIZONS OF TECHNICAL DESIGN SAFETY ASSESSMENT FOR A NUCLEAR POWER REACTOR: MAGNOX–AGR–PWR

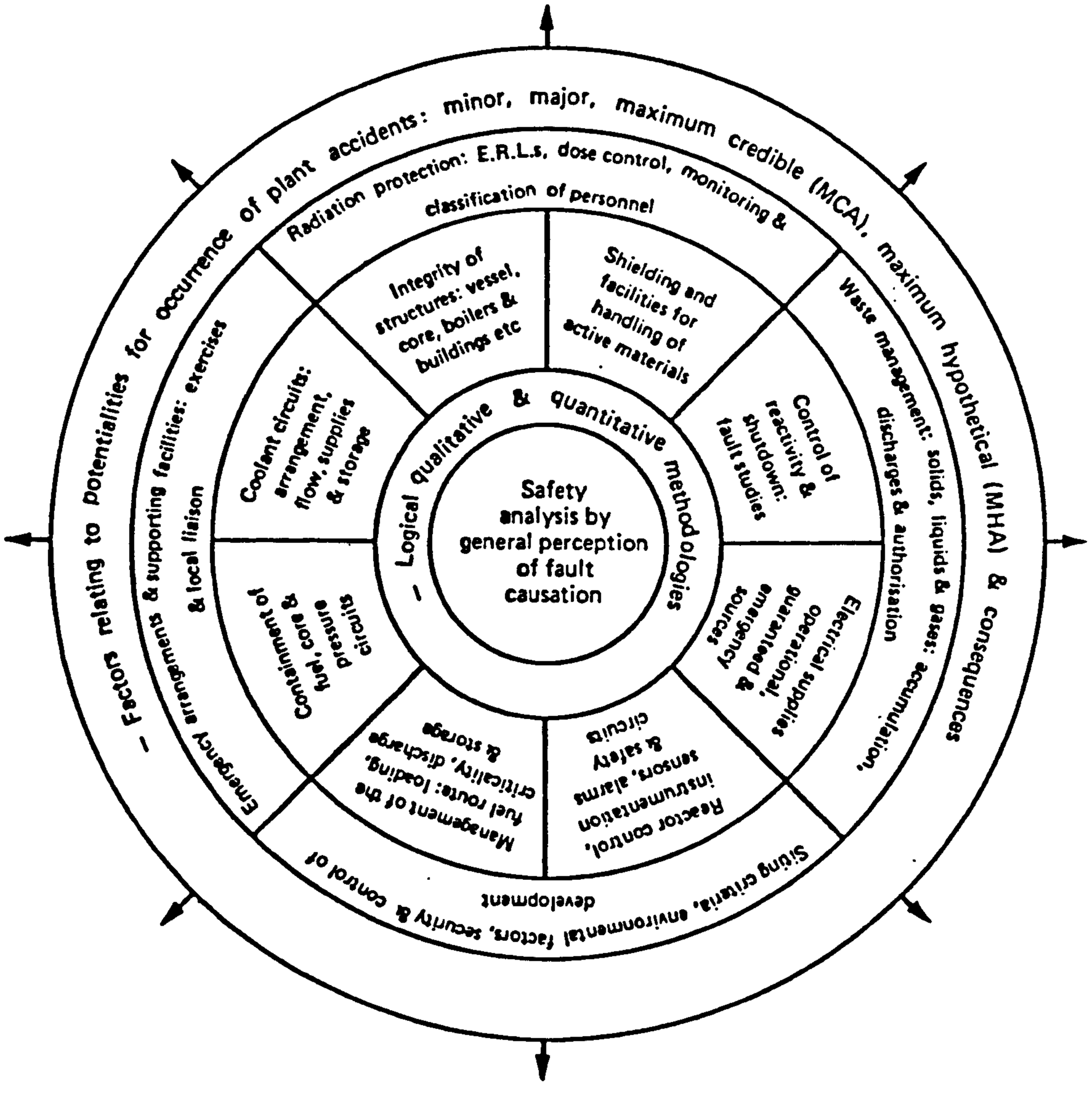


Fig 3

there has been increasing pressure to adopt quantitative methods of the decision analysis kind (See Section 7.2 et seq.).

9.1 From 'Safety Factor' to 'Design Basis Accident'

Early attempts to achieve safety and reliability in the design of the major artefacts of engineering, except in a few special fields like architecture and structural and aeronautical engineering, were largely matters of following established drawing office and shop floor procedures and rule-of-thumb. When faced with an innovation, the designer of a technically advanced industrial installation had little information and no prior experience from which definitive guidance could be gained. Consequently, there was ignorance of the true nature and extent of the failure possibilities and safety provisions were often the result of trial and error at the best and guesswork at the worst. On cost grounds alone, it is not feasible to provide engineered safeguards or administrative controls to prevent or abort every conceivable fault sequence. Absolute safety is unattainable if an iota of risk remains, as there is always some way in which the vestigial chance can precipitate a catastrophic failure. The aeroplane is a case in point as there can always be a crash while it is in flight no matter how many precautions are taken. To eliminate all but the most improbable causes of an unlikely accident would render the extra-safe machine useless, with little or no payload.

In order to ensure that his work had an adequately safe and reliable outcome, the engineer has traditionally followed a course determined by his experience, technical knowledge and competence, striking a rational balance between his estimate of the likelihood of failure and the cost of the safeguards thought to be necessary, an exercise of skill called 'Engineering Judgement', a matter of some profundity dealt with further in Section 13.2.1. Though a conservative approach to failure margins has always distinguished sound engineering, in the absence of theory it was inevitably ingenuous. Attempts at an overtly scientific treatment were first formalised in the 'Safety Factor' concept (V.H. Searle 1950), becoming generally established practice towards the middle of the last century.

Notwithstanding the rule that a Safety Factor is determined by calculations based on strength of materials or like data, many imponderables, judgements and precedents enter into the process. With the innovation of heavier-than-air flight, the art of Safety Factor estimation in aeroplane design became an important engineering

discipline in its own right. By the outbreak of the Second World War, that of the 'Stress Man' had become an important and well-paid vocation. His achievements contributed in no small measure to the outstandingly reliable aircraft supplied to the RAF and British civil aviation.

The airship disasters of the decade and a half before the outbreak of the Second World War (See Section 3.6) coupled with the great expansion of civil and military aviation during 'The Thirties' had stimulated an awareness of the need to improve the safety and reliability of products of the aeronautical industry. Statistical methods of quality control were being introduced into the production lines with very fruitful results in the manufacture of electronic and associated matériel. The scene was thus set for the bold steps forward that were about to be taken to assure the safety of atomic energy that by 1941 was being exploited in a 'crash' program to produce 'The Bomb' (Leslie R. Groves 1963).

The dangers of the new technology were unknown, except for those of its radiation hazard through experience that had been gained by radiologists (R.F. Mould 1980). The nuclear energy risks were thought to be of such a potential magnitude that 'some scientists doubted whether the programme could or should be prosecuted (Margaret Gowing 1974). There may have been no conscious technology transfer, but positive philosophies of safety had evolved in the form of radiological protection from the field of medicine and by way of design foresight in engineering through the developments that had taken place in the Safety Factor doctrine. Intellectual ground was thus ready for emergence of the 'Design Basis' (DBA) or, in other words, the 'Maximum Credible Accident' (MCA) criterion. The MCA has since formed the cornerstone of safety policy in nuclear engineering (O.H. Critchley 1977), giving an effective pragmatic answer to the 'zero-infinity' risk quandary (See Section 8.4 et seq.).

9.2 The Maximum Credible Accident (MCA) Doctrine

Despite the fact that it is often mentioned, there are few explicit descriptions of the MCA method. With the exception of an excellent review by T. Coxon (1971) of its use in the design of an Advanced Gas-cooled Reactor (AGR), those that have been published are often vague or meagre. On the other hand, criticisms of the MCA concept and expositions of the quantitative probability approaches that are claimed to be alternative to it abound. The MCA is a hypothetical LPE envisaged after a critical review of the possible fault sequences in a

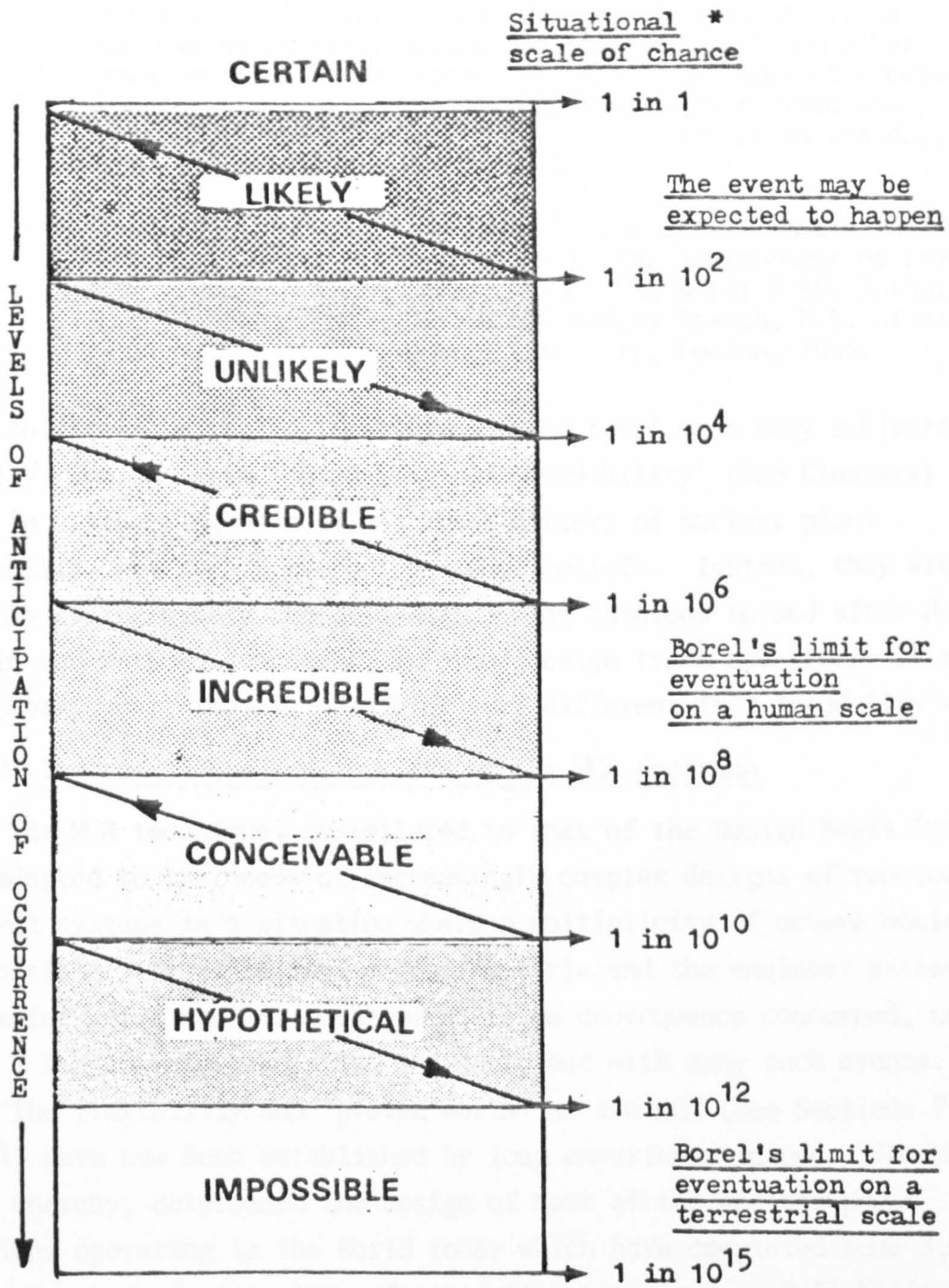
reactor system that might lead to a catastrophic nuclear plant accident and the release of radioactivity to the environment. By the exercise of balanced engineering judgements made on all the evidence available, the maximum accident that appears to be credible (See Glossary) is identified. The MCA so conceived is taken to embrace all lesser accidents. These credible fault sequences are then studied to identify those components, plant elements and systems that could be modified or adapted to block progress of the faults along each of the given sequences. Those failure modes that it is not possible to design out are managed by instrumented limit trips, alarms or administrative controls. As a result of the safety measures taken to prevent the MCA, hypothetical accidents with more serious consequences are considered to be so unlikely that they may be precluded. An attempt to give a comparative measure of these subjective probabilities in numerical terms is made in Figure 4.

Imponderable factors make it difficult to calculate the expected fission product release in the event of an MCA. Nevertheless, decisions about the location of nuclear power reactors have had to be made. Siting regulations in the UK and USA 'seem to assume explicitly or implicitly, a release of 10^3 curies' (F.R. Farmer 1975). In consequence, this value or a figure somewhat greater has provided a basis for siting policies in the two countries (Shaw and Palabrica 1974, Charlesworth and Gronow 1967).

9.2.1 Limitations of the early MCA approach

With increasing complexity of existing reactor designs and the introduction of more sophisticated types such as the Advanced Gas-cooled (AGR), the Steam Generating Heavy Water (SGHWR) and the Fast Breeder Reactor (FBR), the technical safety assessment of design was becoming an ever more formidable task. The field of technical problems facing the nuclear power reactor design safety analyst is shown in Figure 3. Not only was it now necessary to make comparisons between reactor types, but to take decisions on the apportionment of investment among the engineered safeguarding features which had become very elaborate. Furthermore, safety studies, often instigated by groups hostile to nuclear energy, were revealing new modes of failure which, though of very low probability, could result in major radiation accidents, for example the controversy over the integrity of emergency core cooling systems (ECCS) incorporated in U.S. light water reactors.

PERCEPTIONS OF CHANCE



Borel's probability limits

Metaphysical probabilities - See Section 9.6.1 and Note 14.

* Situational chance - nuclear

The chance that a specific event will occur during the operational lifetime of a nuclear power plant.

FIG 4

Doubts about the adequacy of the MCA doctrine were voiced. John Ablitt thought the approach outmoded:

> '4. The Maximum Credible Accident Concept has always suffered from the disadvantage that a sequence of events credible to one person could be utterly incredible to another, since credulity is an intensely personal attribute which varies considerably between individuals and can be strongly influenced by commercial and other pressures. Even as regards its use as a comparator between reactors, its value has been adversely criticised and whereas it may have been a convenient device in its day, its limitations are now recognised.'
>
> The contribution of systematic incident evaluation to the achievement of reactor safety, Report AHSB (S) R 89, Authority Health and Safety Branch, U.K. Atomic Energy Authority, London, 1965.

Ablitt was right in identifying 'credulity' as a very subjective faculty, but the terms 'credible' and 'credibility' (See Glossary) as used in engineering discussions about matters of nuclear plant reliability and safety are not personal beliefs. Instead, they are soundly based, widely accepted engineering opinions formed after debate within and between competent, informed design teams and groups of safety assessors. But, that is something very different from 'credulity'.

9.2.2 The resilience and survival of the MCA doctrine

The MCA technique, assimilated to that of the Design Basis Accident, has adapted to the needs of increasingly complex designs of reactor and control systems in a situation where a multiplicity of severe accidents is possible. It is in fact a generic title and the engineer assessing the safety of a nuclear power plant is in consequence concerned, not with a single major radiation incident, but with many such events.

The flexibility and 'proven worth' of the MCA (See Sections 7.1.1 & 7.4) have now been established by long experience in use. The MCA has, thereby, determined the design of most of the nuclear power stations operating in the World today which have completed some 3,000 reactor-years of virtually safe operating experience. Reliability analysis and associated quantitative methods have always formed an important part of its broadly based scheme of safety assessment. Indeed, the MCA doctrine may be said to embrace the methods of quantitative safety analysis that have been developed over the past decade. By contributing a rationally structured procedure that the MCA previously lacked they have in fact enhanced its power. A widely

held view amongst engineering safety assessors is that the final judgement taken about the safety of a reactor design is inevitably qualitative, quantitative methods, although they may give essential help in reaching it, are inadequate to the task of making the ultimate design decisions (Hanauer and Morris 1971, Gronow and Causden 1975/a). Thus, the MCA still rules in the domain of safety analysis. And this despite establishment advice to replace it by the quantitative approach (Robens 1972/b, Sir Brian Flowers 1976/b) which was underwritten by the motion in the House of Lords (1976) mentioned earlier.

9.3 The MCA and power reactor siting considerations

The MCA is by definition the peak of a hierarchy of possible plant failures and untoward occurrences that can result in the massive release of radioactivity to the environment about a power reactor site. As noted earlier, it is envisaged as a very rare event and one that is not expected to happen, but there are many lesser ones that do, and some of them repeatedly. There is thereby a continual escape of small quantities of fission products from a power reactor to its surroundings. For example, an operating gas-cooled Magnox or AGR plant may be expected to lose between 1 to 50 tonnes of CO_2 per day owing to leakage from the coolant gas circuit at penetrations, pipe joints, glands and mechanical seals on the shafts of blowers, pumps and valves. In spite of the best precautions, the coolant will suffer some contamination from the nuclear fuel that cannot be immediately removed by the clean-up filters. The escaping gas is thus faintly radioactive, if not all the time, then for some of it. In addition there are further fortuitous escapes of coolant during maintenance, from planned operational activities and by inadvertent blow-downs. Radioactive cesium, iodines, noble gases and small amounts of other nuclides as fine particulates are carried into the atmosphere to make the ambiance within a few miles of the reactor slightly radioactive.

Any hazard from such minor leaks of radioactivity can be met by locating the installation in the centre of a zone of very low human occupational and residential usage. This requirement is met by the current practice of 'specifying the boundary of a low population area within a radius of 1 km', with emergency action, ie. evacuation procedures, envisaged out to a further periphery of 2 miles from the reactor. Both boundaries have been confirmed in a study by Shaw and Sina (1976) for a postulated 'unit release' of 10^4 curies in the stable weather conditions (F. Pasquill's 'Category D', 1962) that usually

prevail in Britain, although they put the evacuation perimeter at 3 km (1.86 miles). Their 'unit release' corresponds to a dose of 170 rem to the thyroid of a 0 - 5 year old child and is an order greater than the 'nominal 1,000 curies release' said by F.R. Farmer to be characteristic of siting regulations (supra).

Recognition of the MCA as the chief hazard of nuclear power with its concomitant release of radioactivity in large quantities has justified the prudent policy of the remote siting of reactors, for instance the ones meeting Class I criteria in the long standing UK scheme (Charlesworth and Gronow 1967, Shaw and Palabrica 1974) were those of choice. Unfortunately, the policy of remote siting involves a heavy cost in power transmission and, in a densely populated country like Britain, the number of such sites is limited, Shaw and Sina (ibidem) finding only Dungeness in East Sussex effectively so isolated, though they failed to evaluate Hinckley Point on the coast of Bridgewater Bay in Somerset.

The difficulties that have to be faced in formulating a realistic policy for power reactor siting in the UK are exposed if one considers a possible MCA releasing some 10^6 curies when the evacuation perimeter might have to be extended to 20 miles. In the case of Dungeness, this would involve the evacuation of Hastings (75,000), Folkestone (45,000), Dover (34,000) and Ashford (23,000) and some 2 dozen smaller centres of population like Lydd (4,500). There are few feasible sites in Britain that could be styled as truly 'remote' other than Dounreay near Thurso, Caithness (now called the Highland Region), on the Northeast tip of Scotland.

9.4 Emergence of the quantitative approach to siting

Siting restrictions when combined with the difficulties to be faced by a utility seeking proximity of electricity generation to centres of load and having to acquire tenure of suitably located land could pose serious obstacles to an energy policy that made nuclear power its principal source.

Referring to the need to escape from the foregoing constraints, F.R. Farmer recalled that:

> 'During the period of the mid-1960s, there was a move to bring reactors closer to populations; this required an amendment of the maximum credible accident to become more realistic and required more confidence in the functioning of safety equipment.'
>
> Nuclear Reactor Safety: Preface, Academic Press, New York, San Francisco, London, 1977, xii.

A way out of the quandary is to reduce, if not the true seriousness of the MCA as postulated, then the perception of its gravity. A new policy was advocated by certain design and research authorities that aimed at achieving this end by rationalising the conception of the detriments of nuclear power. For example, Farmer opined thus:

> 'I had worked on the problem of how sites might be specified for power reactors in a thickly-populated country such as the UK.
>
> ... ...
>
> This led me in 1967 to consider a scale of probabilities for accidents according to a risk concept in terms of a possible casualty rate within a sizeable nuclear programme of, say, 1,000 reactor-years. ... ... I chose a target line weighting somewhat against the more serious events.... ... I reasoned that even a small release - say the nominal 1,000 curies release envisaged in many siting regulations - obviously occurred very rarely - I guessed at a figure of once per 1,000 reactor-years ... ... Thus, I was led to a required rate for a 10^6 curies release of not more frequently than once in 10^7 reactor-years.'
>
> 'Advances in the reliability assessment of reactor systems', ATOM 230, December 1975, United Kingdom Atomic Energy Authority publication, p. 218.

The outcome of his cogitation was 'The Farmer Line' approach to siting referred to in Section 7.2 above, the reactor design being matched on a probabilistic fault-sequence-release assessment to the category of the site in terms of the rate at which thyroid malignancies would be expected to be induced in the event of a range of accident scenarios of ascending gravity and declining probability (F.R. Farmer ibidem). The 'Line' is a representation of the concept of probability assessment rather than a tool for specific application in solving design and siting problems.

Another probability-based approach with much the same purpose is the U.S. 'Reactor Safety Study' reviewed in Section 7.3 (N.C. Rasmussen 1975). The method was devised specifically for the probabilistic

safety assessment of the American BWR and PWR nuclear power plants and applied to that end.

It found the chance of the worst accident happening to a U.S. light water nuclear power plant, BWR or PWR, as 'once in 1,000,000,000 years of reactor operation' (See Figure 5). The Study's estimate of the overall personal risk of fatality through the existence of a nuclear power station within 25 miles of the individual's domicile is put at 7.5×10^{-8} per annum or roughly 10^{-7}.

Both methods aggregate the radiation detriments of nuclear power by taking together the whole spectrum of exposures of a population to radioactivity from routine operational releases, smaller accidents and the most unlikely massive escape of fission products attributable to the MCA or greater hypothetical accident, spread over a probability range from certain to the exceedingly remote. The risk is then averaged out over the lifetimes of the individuals likely to be affected and in these terms may be compared with the other risks, 'Mundane' and 'Unusual' (supra), to which they may be exposed in their daily life and listed in Table II. In this context, the nuclear power risk appears to be trivial, 10^{-7} against 7×10^{-3} per year from all causes at the age of 50. These figures, although they differ from those given brief mention in Section 7.3 above, are consistent with them. Death 'from all causes' includes disease as well as accidents and the greater nuclear risk relates to those living near a nuclear plant, compared with the national population.

At this stage it is impossible to foresee how much influence these two probabilistic strategies will have on power reactor siting. It is suspected, however, that, in the UK at least, this will continue to be determined more by practical and political expedience than by abstract theory. Nevertheless, if nuclear power is to make an eventual major contribution to the economies of the developed countries, then either nuclear power plants must be moved in closer to centres of population and in densely populated countries semi-urban sites used or more economical methods of power transmission from remotely located reactors developed. An attractive option in the latter case would be the production of hydrogen and oxygen rich by-products by the endothermic utilisation of nuclear heat to be sent by pipeline for use, mainly as energy sources, in centres of industry, cities and other heavily populated residential areas with electricity distributed from local power stations burning or otherwise converting the hydrogen to electrical energy. This scenario as envisaged by C. Marchetti (1974) has been briefly commented on in Section 6.2 above.

PROBABILITY OF THE WORST CONSEQUENCES OF A US NUCLEAR POWER STATION ACCIDENT

(Rasmussen – Bulletin of the Atomic Scientists 'The Safety Study and its Feedback' Vol 31 1975 p 28)

TIME INTERVAL BETWEEN EVENTS IN A GIVEN PLANT

Time span between events 10^9 years	=	Precipitating event occurs once every 1,000 years	×	Safety system (worst breach) occurs once in 1,000 years	×
		Worst weather conditions occur once every 10 years	×	The highest population density to be affected will be present once every 100 years	

In frequency terms the probability per plant per year is:

Probability of worst consequences @ 10^{-9}	=	Probability of initiating event @ 10^{-3}	X	Probability of worst breach of safety defence system @ 10^{-3}	X
		Probability of worst weather conditions @ 10^{-1}	X	Probability of exposure of area of highest population density @ 10^{-2}	

Note All events are presumed to be independent of one another, there being no common modes.

The above probability of 10^{-9}, that is a chance of eventuation once in One Thousand Million Years, is metaphysical and the accident sequence or sequences so predicted will never happen. Nevertheless, a catastrophic failure outside the fault-event systems conceived by the analyst remains a possibility, given the existence of a true hazard potential.

Fig 5

9.5 The true role of systems analysis in nuclear safety

The application of the quantitative methods of reliability analysis to nuclear plant siting advanced by F.R. Farmer (1967) was part of a more general move to extend quantitative probability over the whole field of technical design safety assessment, a policy which he subsequently described more fully in his 1975 ATOM paper and elsewhere (26). It was put into effect in the Canvey Island/ Thurrock petrochemical complex risk study mounted by the Health and Safety Executive (J.H. Locke et al. 1978) and in the U.S. Reactor Safety Study (N.C. Rasmussen 1975). Together with other decision methodologies, the foregoing quantitative techniques have their antecedents in operational research that was extensively developed for military purposes during and after World War II (P.M.S. Blackett 1962, D.J. White 1975/a). All are examples of inductive reasoning which, in its application to nuclear safety, has been examined by O.H. Critchley (1978) in his work on the historical, philosophical and mathematical background to nuclear plant risk management in the U.K. (See Document No. 2 in the Annex of Supporting Papers).

The attractions that these methods offer to proximate administrative decision makers, politicians and certain theoretical scientists are understandable, and if their limitations are recognised, are not without justification. They lie in the idealistic Weltanschauung that has deep roots in Western society and dominates most of its non-technical divisions. This holds that causation has its place in a cosmos of underlying, though generally not superficial, order and that it obeys the universal laws of nature. Some of the profound, but misleading inferences drawn from this concept were mentioned in Section 8.2.3. One most relevant to safety engineering is that it should be possible, if not to make an accurate forecast of what may happen in the future, then at least to predict the chance of an LPE, say the catastrophic failure of a major artefact like a nuclear power reactor, assuming as Poisson (1837) did that a positive mathematical probability may be calculated for any situation with an element of chance in its outcome, given access to adequate data. Besides, in the case of major innovatory technologies like nuclear power where actual experience of catastrophic incidents is minimal, it is claimed by risk and systems analysts that the dearth can be made good by synthetic data distributions compiled from information about the behaviour of analogous and comparable components, equipment, plants

and systems. The topic is examined further in later sections of this chapter.

On the other side of the ideological division, engineers tending naturally to the pragmatic philosophy of 'The Deed' place greater confidence in more traditional and established empirical methods. Their approach in dealing with the safety analysis of design and the practicalities of construction and operation of technological undertakings, and particularly nuclear power plants, is to use a method based on a concept of limiting possible accidents which has been discussed as the Design Basis (DBA) and Maximum Credible Accident (MCA) methods in Section 9.2 et seq. above.

The issue of idealism versus pragmatism has been, and still is, at the root of a serious debate about nuclear safety that has reached the most imposing official levels, and at least two major public inquiries, one chaired by an eminent scientist (B. Flowers 1976/c) and the other by a distinguished member of the bar (R.J. Parker 1978) have found in favour of the quantified probability approach to safety assessment, disparaging MCA practice. Nonetheless, this approbation of quantified systems analysis, and certainly its application to the forecasting of LPEs in hazardous technologies, is by no means universal and has many critics among professional engineers and from academia. The matter is of paramount importance in the safe exploitation of advanced technologies and is central to the development of the New Treatment. Moreover, it is held that the concept of the DBA/MCA is fundamental and proper to the achievement of reliability and safety in nuclear power technology, and for that matter in other technologies presenting similar 'zero-infinity' risks. Consequently, the systems methodology in the form of quantitative safety analysis comes as a valuable adjunct to nuclear safety engineering, but cannot provide its central core.

9.5.1 A cartesian representation of the theory-practice disjunction

The foregoing differences in outlook between those who practise the intellectual skills of engineering and technology and those involved in the arts, administration, jurisprudence, politics and certain aspects of theoretical science and mathematics lie deep in the structure of Western society, a matter which has been discussed earlier (Section 8.1). Nevertheless, an understanding of the disjunction may, perhaps, be assisted by an analogy that can be drawn for the divorce between theory and practice and the way in which a similar conceptual

partition is used to represent the two aspects of alternating current (AC) in electrical engineering as shown in Figure 6a. Without such an approach, AC technology would be both perceptually and practically intractable, but the analogy can be taken no further than an appreciation of the similarity. It is given diagrammatic form in Figure 6b, where the intellectual gulf between those things which may be properly associated with 'The Word' are depicted in cartesian form as lying in the j-direction (along the y-axis) and those of 'The Deed', including applied science and theory with empirical verification, technology, the useful arts and manual skills, lying in the real plane (along the x-axis). Those activities which bring together aspects of both 'Word' and 'Deed', as in the case of engineering that achieves its ends by utilising scientific theory in association with technology, technicians' skills and handicrafts, may be represented by intermediate axes as shown in the Figure. Then, technical safety assessment of design would lie on the upper or 'Management' side of a 45^{o} axis and the construction and operation of the plant so designed would lie on the lower or 'Technology' side.

Such a graphical portrayal of the foregoing sets of cognitive entities that are respectively co-ordinate in theory and practice is indicative of their essence rather than their magnitude. It can also help to establish the relevance of the metaphysics, that has been discussed, to the acquisition of foreknowledge about the imminence of catastrophic LPEs in nuclear power plants, to the provision of means by which they might be inhibited, to prudent anticipatory measures such as siting and, not least, to assessment of the validity of some of the procedures for risk prediction and safety analysis.

The disjunction may also be seen as a consequence of 'The Information Explosion'. Thus, Figure 6b may be envisaged as two orthogonal radii lying in the surface of a diametral slice of the expanding sphere of human knowledge, the aspect so presented depending on the direction of the cut in relation to the branches of culture depicted in Figure 1. The length of the arc joining the ends of these radii, associated as they are with 'Word' and 'Deed', namely administration-theory-design and practice-technology in the given case, is then a measure of the extent of the divorce between the two domains. Clearly, at some stage in the expansion of scientific and technical knowledge, the gulf between the two domains will grow too wide for effective executive authority to be exercised across. Until now, an able administrative mind could readily span the intellectual gap between

A conventional vector representation of the relationship between the driving voltage (V) and the current (i) in an alternating current circuit with a reactive load

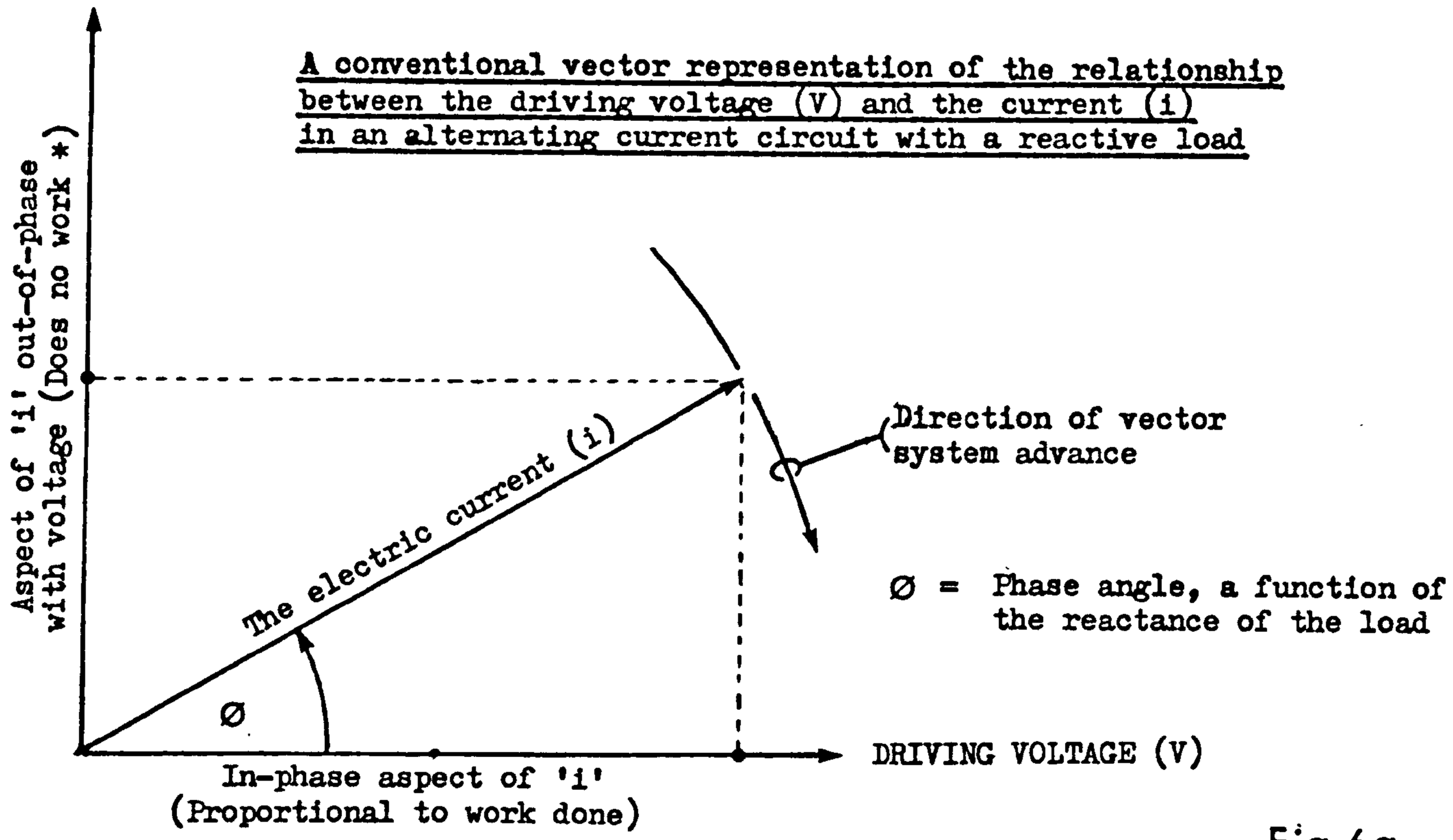
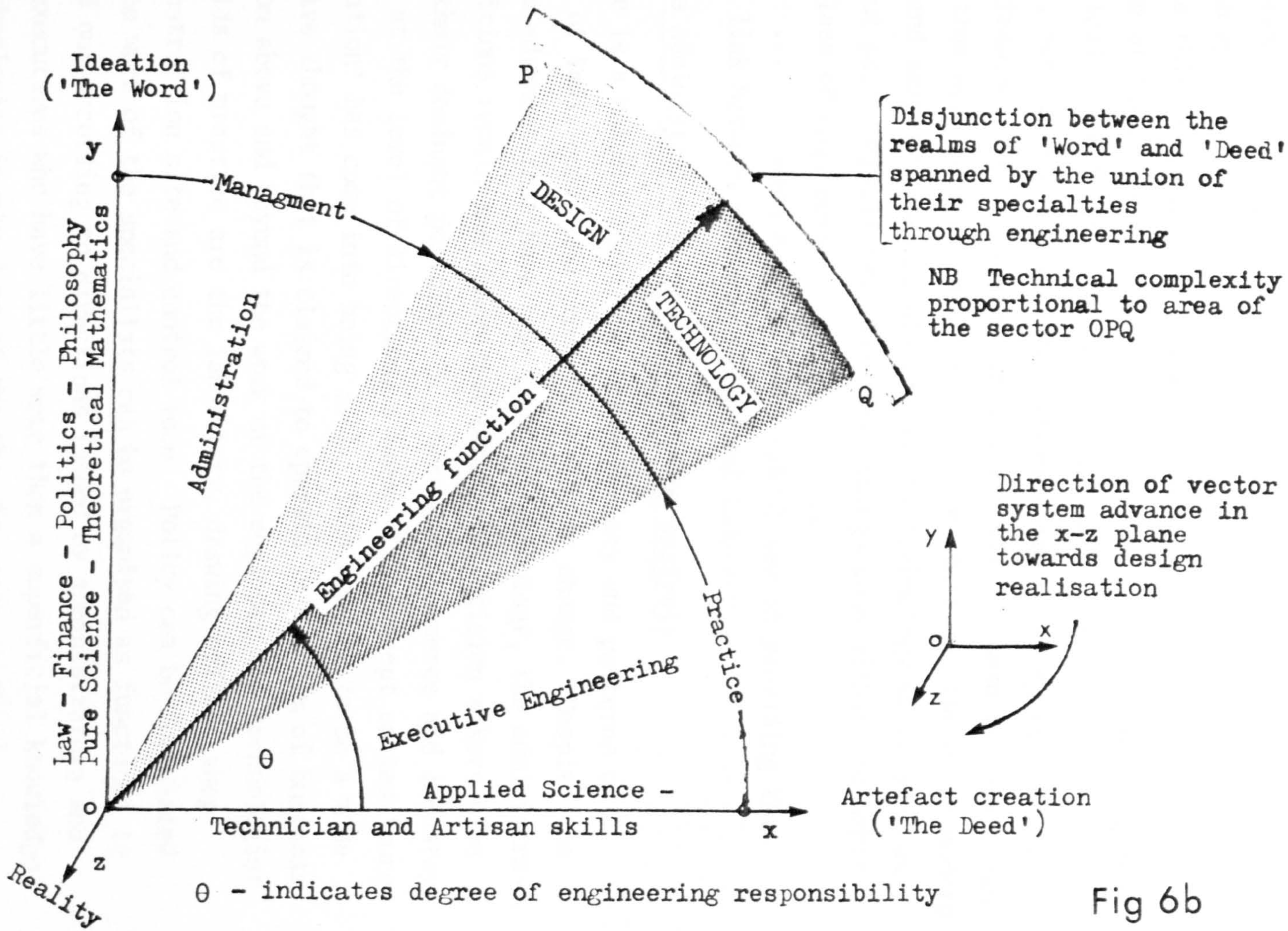


Fig 6a

* - a consequence of a loss-less energy exchange due to the reactance which the load presents to 'V'

The vector representation given above of the flow of an alternating electric current in a circuit containing reactance is an example of an engineering ideogram that enables an abstract technical situation to be presented as a manageable intellectual concept. Such pictograms abound in the language of technology, indeed communication and reasoning in engineering would be very difficult, if not impossible, without them.

An attempt at a multi-dimensional portrayal of the relationships that involve administration, science, design, management-and-practice, and technician and artisan skills through engineering in the creation of a technological artifact



θ - indicates degree of engineering responsibility

Fig 6b

'Word' and 'Deed' by acquiring a sufficient grasp of the salient features of a given technology to make wise and rational managerial decisions, referring as appropriate to engineers and scientists on tap. This is fast ceasing to be the case. Technology in our times presents technical and associated societal problems of another order of complexity. The technical features are often recondite and the full consequences of many important innovations impenetrable to those without an appropriate scientific and technical background. To appreciate this, one has only to compare nuclear power with the combustion of fossil fuels, computerised data processing and xerography with clerical paper filing routines and hot metal typographic processes, aerospace and satellite communications linking continents with sea transport and submarine cables, and all of these earlier forms in their time were leaders in technology. In addition, there are modern medicine and surgery, pharmaceuticals and biotechnology which are new and without past comparisons. All these things come within the ambit of 'the class of engineers' ... ...
... ... whom Auguste Comte (1825) saw as providing the practical link between science as such and industry.

9.5.2 The administrator's need for decision analysis

There is a natural inertia in human society and patterns of behaviour of individuals and groups are slow to change. Despite the remarkable advances that have been made in technology, the administrative traditions remain and generalist proximate decision makers have retained their dominant positions in government, commerce and industry. Moreover, at the level of direction, a managerial concept called 'pure administration' has come into being (24). This appears to be a mode of executive thought that is claimed to operate in a realm of business abstraction above and beyond the work of the engineer and technologist whose fields of practice are the laboratory, drawing office, shop floor, construction site and control room. Policy can be formulated whereby the work of the specialists can be organised as functions to be carried out according to directions issued by administrators and business executives who have little more than a superficial knowledge of the technologies involved or of the thought patterns those technologies require for their successful exploitation. Integrated and participating management is replaced by two fields separated by the interface between policy formulation and business direction on the

one hand and productive operations and their subordinate functions on the other through which management information must pass.

In both private industry and public sector activities involved in the exploitation of advanced and particularly innovative technologies - and in the West today there are few that are not, most major business decisions are complicated by the profundities and societal ramifications of the given technology. The generalist administrator or director of today is, therefore, likely to be ill-equipped to draw together in full comprehension all the technical complexities that interact with his other corporate duties. Decision theory and systems analysis appear to offer an escape from such quandaries by reducing difficult concepts to readily appreciated numbers. The magic of being able to solve refractory problems by transforming them into impersonal mathematical operations is obviously attractive. Besides, systems analysis has very reputable origins in operational research that made an important contribution to victory in the last war (P.M.S. Blackett 1962). As well as offering a process with a stamp of scientific objectivity, the administrative decision maker can associate his mistakes with faults in the methodology, rather than to imperfect judgement on his part. It is not surprising that the methods of systems analysis are much in favour in the boardroom and with officialdom. But, the circumstances are no longer simple. It took no technical knowledge to understand the statistics of wartime convoy management or the tactics of pattern bombing: nuclear power and information technology are in another intellectual class requiring the professional background and trained judgement of the engineer for their proper comprehension.

While a systems approach can rationalise a complex and apparently intractable business or financial problem, it cannot supply the professional judgements that must come from the engineering dimension. As Professor Ida Hoos observed in her critique of systems analysis:

> 'There is a confusion between a systematic approach and a systems analysis approach.... ... Unfortunately, the lack of factual knowledge of conditions existing in the real world forces the model builder to base many if not all his general conclusions on all kinds of apriori assumptions.... ... Uncritical enthusiasm for mathematical formulation tends often to conceal the ephemeral substantive content of the argument behind the formidable front of algebraic signs.'
>
> Systems analysis in public policy: a critique,
> University of California Press,
> Berkeley, Calif., 1972, p. 37.

9.6 Safety Assessment of Design: Illusory aspects

There are some profound logical, philosophical and practical weaknesses in the claims made for the existing methods of risk and reliability analyses when they are used as the main basis of support for safety claims about nuclear power plants. The leading techniques of which there are two, both centred on the safety assessment of design, have been described earlier. One is that of the Maximum Credible Accident (MCA), sometimes called the Design Basis Accident (DBA), which has been described earlier in this section and the other is that of Quantitative Safety Analysis (QSA) used in the Reactor Safety Study described in Section 7.3. The latter which is the better known among several systems approaches was a large scale and exhaustive assessment of the two designs of American light water reactors of the BWR and PWR types, with a program of 100 reactors in mind. The two designs were taken as representative of the reactor types concerned, the Study being thus generic rather than specific. Its terms of reference specified that 'quantitative risk analysis methods' should be further developed to dispel the uncertainties about their applicability. QSA methods of a sophisticated kind were already in use at the UKAEA's Safety and Reliability Directorate's laboratories at Culcheth in Lancashire where they had been developed to supercede the MCA method (F.R. Farmer 1975). The attempts to forecast the occurrence of catastrophic LPEs in nuclear plants by the above methods of safety assessment are centred on studies of design of the plant types concerned and their validity is dependent upon the extent to which the plant as actually built and operating replicates the design in reality, whereas in practice there may be marked differences between them. Lead times preclude retrospective adaptions of the assessments to take into account deviations and modifications from the design in the state it was when assessed earlier. While both the MCA and QSA methods can explore in depth the intricacies of the design and improve its quality by exposing weaknesses and, in the case of the QSA, adjust a lack of balance of investment in safe-guards, they remain studies of design. Their estimates of the chances of occurrence of catastrophic LPEs in the entity conceived by the design thus relate in principle only to the reality of the operating plant that will exist at the end of the construction process.

Furthermore, both the MCA and QSA approaches are exercises in inductive reasoning which is the subject of much doubt as to its logical validity, though scientific method and commonsense escape from the

dilemma by recourse to probability (infra). It is in the domain of probability that the main differences between the MCA and QSA methodologies lie. The MCA method is one of objective probability that is mainly qualitative with subjective overtones, though quantitative reliability analysis is much used when deemed to be appropriate. As an example the paper presented as Supporting Document No. 5 in the Annex is part of an MCA assessment pertaining to nuclear core temperature management in a Magnox reactor.

It must be said in favour the MCA technique that prediction was never its aim as it was devised to give a safety target for the design office and, indeed, the synonym for the MCA is the DBA which says so in its title. For specific risks, QSA as practised by SRS can be commissioned for the safety assessment of plants and processes presenting a major hazard. One such assessment was the Canvey/Thurrock petrochemical installation risk study (See Section 7.1) and a massive investigation with a QSA orientation has been made in support of the Central Electricity Generating Board's case for its prospective PWR nuclear power station at Sizewell and tabled at the current inquiry (13).

9.6.1 Design Probabilities: Feasible and Metaphysical

As suggested earlier, the advanced methods of technical design assessment now available to engineering provide penetrating and, indeed, inestimably useful tools for the safety and reliability analyses of design. To restate the case, the weaknesses and covert fault sequences so disclosed can be designed-out or corrected by modification of the design feature involved to give intrinsic safety, to introduce an engineered safeguard or to devise an administrative control. The Maximum Credible (MCA) and Design Basis (DBA) Accident methods, being engineering rather than predictive techniques, do not lend themselves to the estimation of very low probability risks other than in terms of 'credibility'. On the other hand, Quantitative Safety Analysis (QSA) as exemplified by the U.S. Reactor Safety Study has been promoted with quantitative prediction in view. Despite doubts about the true worth of such attempts at prophesy, QSA imposes a disciplined approach and can give guidance to a design office about the apportionment of investment among competing safeguarding features. Clearly, a judicious combination of the MCA/DBA approach with that of QSA is desirable.

In their treatments of design, both the MCA and QSA approaches reduce effectively to much the same thing, namely the identification of potential fault sequences, and particularly low probability ones, that could derogate from the safety and reliability of the plant. The substantial differences between the two arise at the fringe between tangible probabilities and hypotheticalities where the MCA method sets a limit to specific safeguarding actions by a concept of 'incredibility' which is a matter of engineering judgement, whereas QSA defines similar bounds in terms of assessed low probability limits of reliability expressed in numerical terms. F.R. Farmer (1975 -2) has suggested that the quantitative decision point should be related to an individual risk of 10^{-5} per year per reactor program, with a reservation on political grounds that 10^{-6} to 10^{-7} would be advisable.

However, beyond the foregoing decision points, the probabilities may become metaphysical, an aspect of objective probability identified by J. Le R. d'Alembert (1717 - 1783) as cited by L.E. Maistrov (1974/b) and by Emile Borel (1950) as his 'Single Law of Chance'. Both authorities posit that very rare events never happen, though this must be qualified by reservations about the nature of the system in which the action is conceived (14). Hence, very low fault probabilities of less than 10^{-6} per annum are too unlikely ever to occur and certainly not in the relatively short life time of any real nuclear plant. This does not mean that a nuclear power plant bears no chance of suffering a catastophic failure, for an event of this kind is always possible where there is an actual risk, even though it may be very small. The real hazard is due to a spectrum of small risks, both identified and unrecognised, that fluctuate with time and circumstances. The LPE that might occur is, therefore, most unlikely to be the one predicted by QSA. Furthermore, the message contained in the design by which the plant will be constructed and operated inevitably suffers distortion and modulation during its 'noisy' translation from concept into the reality of an operational nuclear power plant. In consequence, there will have been brought into existence a field of failure eventualities that lie beyond the scope of design analysis per se and thus will have escaped the scrutiny of the assessor. The circumstances are depicted in Figures 7 and 8. The disastrous happenings at 'Browns Ferry', 'Three Mile Island' and other catastrophic industrial plant LPEs such as thatat 'Flixborough' (See Appendix II) are examples confirming the general experience.

PREDICTION AND PATTERN OF BEHAVIOUR IN PLANT AND SYSTEM IN THE REALM OF VERY SMALL EVENT PROBABILITIES

TWO DIMENSIONAL REPRESENTATION OF AN N DIMENSIONAL EVENT SPACE

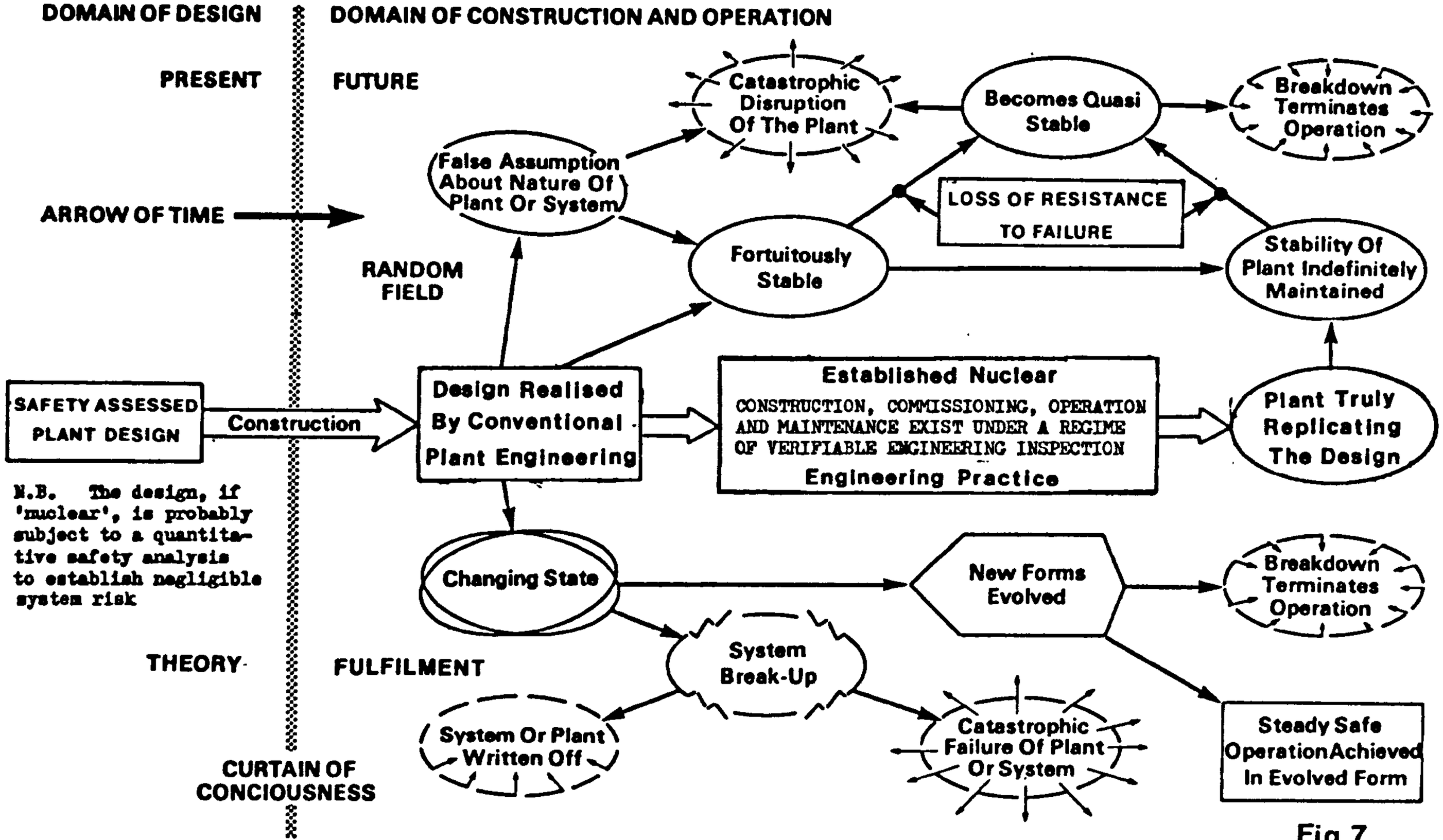


Fig 7

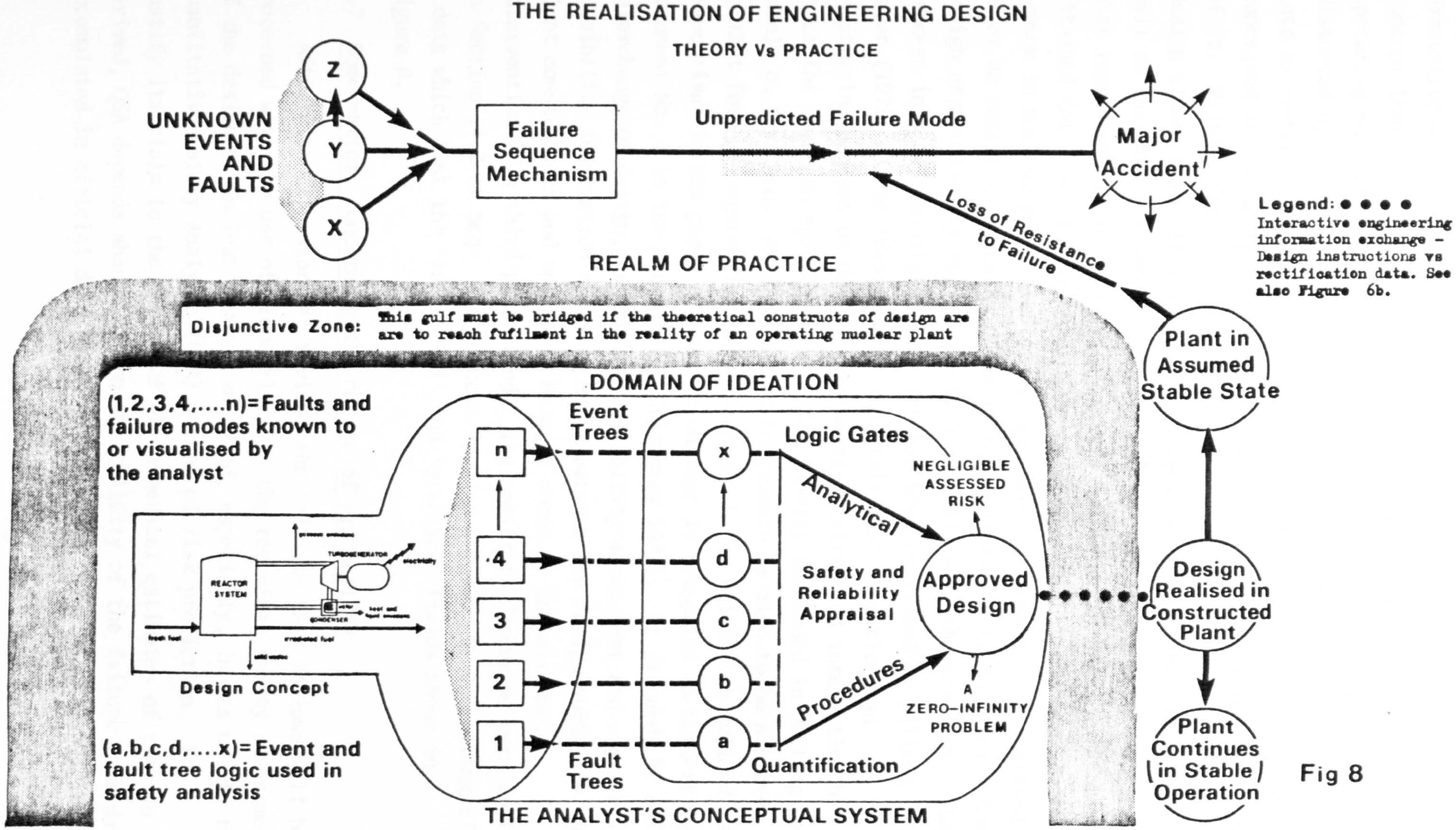

THE REALISATION OF ENGINEERING DESIGN
THEORY Vs PRACTICE
UNKNOWN EVENTS AND FAULTS
Z
Y
X
Failure Sequence Mechanism
Unpredicted Failure Mode
Major Accident
Loss of Resistance to Failure
Legend: ● ● ● ● Interactive engineering information exchange - Design instructions vs rectification data. See also Figure 6b.
REALM OF PRACTICE
Disjunctive Zone: This gulf must be bridged if the theoretical constructs of design are are to reach fufilment in the reality of an operating nuclear plant
Plant in Assumed Stable State
DOMAIN OF IDEATION
(1,2,3,4,....n)=Faults and failure modes known to or visualised by the analyst
Event Trees
Logic Gates
n
x
NEGLIGIBLE ASSESSED RISK
Analytical
4
d
Safety and Reliability Appraisal
Approved Design
3
c
Design Realised in Constructed Plant
2
b
Procedures
A ZERO-INFINITY PROBLEM
1
a
Fault Trees
Quantification
Plant Continues in Stable Operation
REACTOR SYSTEM
TURBOGENERATOR
CONDENSER
Design Concept
(a,b,c,d,....x)=Event and fault tree logic used in safety analysis
THE ANALYST'S CONCEPTUAL SYSTEM

Fig 8

Finally, to repeat, any system of design assessment, even one as exhaustive as the U.S. Reactor Safety Study, pertains to a design concept that remains as 'marks on paper' until it is realised as an operating nuclear power plant, many features of that concept being distorted by 'noise' in the process (supra). What is eventually brought into existence as hardware is, thus, something other than the entity conceived in the design, although it may be a very good representation of it. Valid safety assessments cannot be derived from studies of design alone, but must involve immediate knowledge of the artefact as well so that the assessment embraces not only the design, but the entity that represents it in reality. Such correspondence is seldom, if ever, attained for novel designs exhibiting those major innovatory elements common in nuclear power plants. Congruence can, however, be achieved after an interactive series of evolving replications through which the design asymptotically approaches full identity with the artefact. The process in a reliability application has been described by William Bryan (1975) as the 'design-make-test-fail-fix' iteration, an engineering process of design-assessment-construction interaction by which the American space agency (NASA) finally succeeded in putting men safely on the Moon. An approach to congruence is also to be achieved by that form of engineering inspection which the writer has defined as 'Executive' in his paper on inspection that is presented as Supporting Document No. 4 in the Annex (O.H. Critchley 1981). It proceeds by an interchange of design, safety and reliability assessment and engineering feasibility information and judgements between the design authority and plant constructors and operators brought about by inspectional intervention of a third-party kind. The matter is discussed more fully in Section 14.2 et seq. The process is also depicted by the string of 6 dots which link the 'ideational' and 'practice' fields shown in Figure 8.

9.7 Some matters concerning the nature of probability

After a short historical review, the critique that follows will be concerned with the use of probability in the technical safety assessment of the design of nuclear power plants and, especially, in its use in the Quantitative Safety Analysis (QSA) method of risk prediction. To justify its claim to the verity of the numerical estimates of risk so derived, QSA depends absolutely on the validity of the failure rate data accumulated in official data banks (F.R. Farmer 1975, S.R.S. 1984) that

are largely sponsored by public agencies. The claim is questionable for reasons that will be given in Sections 9.7.2 and 9.7.3 below which bear on the difficult subject of sampling.

Probability which is the essence of safety assessment has long been a subject of controversy over its meaning and applicability. The general tendency abroad today to treat probability measures as if they were among the physical attributes of an entity or system, like Lord Rothschild's concept of risk (1978), has by no means received universal acceptance, even being facetiously described as a 'Phlogiston theory' (S.R. Watson 1981).

It is a relatively new field of mathematics that emerged little more than 250 years ago when 'probability theory was raised to the status of a science and began a new era in its development' by James (Jacques) Bernoulli's treatise, 'Ars Conjectandi', that was published in 1713 (L.E. Maistrov 1974/c). The part it could play in the burgeoning insurance industry that had come into being as an essential economic support for the rapidly expanding commerce of an age on the threshold of the Industrial Revolution (See Section 1.1) was an important factor in its growth. Nevertheless, it can be argued that gambling was its true mainspring because this was the underlying theme of many of the early works on the subject, for example Christiaan Huygens' essay, 'About Dice Games' published in 1657 and Gerolamo Cardano's 'Book on Games of Chance' published posthumously in 1663 some 90 years after his death (L.E. Maistrov 1974/d). While this is true, it is not inconsistent with the former view as all business ventures of the time beyond the traditional craft industries were gambling in the sense of their very high risk element. For instance, until the revolution in the art of navigation that followed on acceptance by the British official 'Board of Longitude' of John Harrison's marine chronometer in latter half of the 18th Century (See Section 3.5), deep sea merchant shipping was a hazardous undertaking. Accordingly, financial cover for such risks was very costly and bottomry (See Glossary) rates ran at seldom less than one-sixth of the valuation of ship and cargo per voyage.

Though the mathematics of probability has made impressive progress, especially during the past 150 years, notably through the work of Siméon-Denis Poisson (1781 - 1840), Adolphe Quetelet (1794 - 1874) and Ladislaus von Bortkiewicz (1868 - 1931), its philosophical and societal interpretations are still matters of continuing dispute. The history

of the development of the science has been described by J.M. Keynes (1922/d) and more recently and comprehensively by L.E. Maistrov.

The latter observed that:

> "... ... Poisson's main work on probability theory, 'Recherches sur la probabilité des jugements en matière criminelle et en matière civile' (was) published in 1837.
>
> ... ...
>
> The ideas and conclusions in Poisson's book were supported in the first place by mathematicians who considered it natural to apply probability theory to problems of legislation, jurisprudence and the political and economical sciences. ... (But) a number of mathematicians were very much against such an application of probability theory. They accused Poisson and his followers of compromising mathematical science.
>
> ... ...
>
> (In spite of this important and fruitful initial period in the development of the philosophical basis of the science there followed) an indifferent attitude towards probability theory in the West and a definite rejection of the possibilities of utilising its methods in studying natural phenomena. This led to a long period of stagnation ..."
>
> L.E. Maistrov (Trans Samuel Kotz)
> Probability Theory: A Historical Sketch,
> Academic Press, New York and London,
> 1974, pp 158 - 161.

Except in certain special applications where the interpretation and management of error were of obvious importance, an appreciation of the power of mathematical statistics and probability theory did not penetrate the applied physical sciences and engineering until about 60 years ago.

The ignorance of statistics and probability is confirmed by the lack of any hint or reference to the two sciences by Professor Frank A. Laws of the Massachusetts Institute of Technology in his internationally recognised and authoritative book, 'Electrical Measurements' (1917 & 1938). This is surprising as the reduction of errors is specifically acknowledged by Laws as of paramount importance in the work of standardising the fundamental electrical quantities. Perhaps the most potent factors in creating an awareness of the significance of probability theory in the fields of engineering and the physical sciences have been the development of Operational Research during the last war (P.M.S. Blackett 1962) and the application of probability concepts to quality control in reliability engineering.

9.7.1 Idealism and realism in probability theory

It is my view that the idealism that permeates the Western Weltanschauung (See Section 8.1) lies at the roots of the intriguing and enigmatic controversy about the nature of probability, that is to say whether it is 'objective', 'subjective' or 'aleatory', the latter associated with the 'frequency theory' (See Glossary). The aleatory concept provides justification for acceptance of the systems approaches currently so much in vogue. Realism favours the commonsense interpretation that expresses the reality of 'The Deed' and suggests that all three theories are true to the extent of the relevance and stability of the data available in a given case. Probability thus enables an engineer to make a good, plausible guess whereby he can escape from the dilemma presented by the gap between certainty and doubt. Moreover, it is a very powerful intellectual tool, relevant to all human activities. Nonetheless, owing to its comparatively recent revival, probability is still, by and large, an unfamiliar concept. Not surprisingly, errors in its use abound, notoriously in certain clinical applications (D.G. Altman 1980).

Ordinary people use qualitative probability judgements all the time with words such as 'might', 'probably', 'likely', 'conceivable', 'one in a million' and their antitheses such as 'improbable', 'unlikely', 'not a chance' and so on. The doubts held by engineers and other scientists concern the quantitative or aleatory uses of probability in the realm of very small risks, a point made by the American Physical Society in their critique (1975) of the 'Safety Study' (N.C. Rasmussen 1975/d). However, serious debate about the justification or otherwise of the predictive value of probability is best left to philosophers and academic mathematicians. An indication of the abstruse and complex nature of the arguments evoked is given by the following excerpt from a work by A.W.F. Edwards of Caius College, Cambridge:

> 'I have been unable to accept any philosophy in which a probability, subjective or not, can be associated with an uncertain proposition. After prolonged consideration of the various schemes advanced, I have been forced to conclude that they ill reflect the true complexity of inductive inference, representing a many-dimensioned substance by its one-dimensional shadow.'
>
> Likelihood: Prologue on Probability,
> Cambridge University Press, 1972. p.xv.

Nevertheless, it is necessary to enter the debate to some peripheral extent. Consequently, the criticism is restricted to the meaning to be attributed to the very small risk numbers that are produced by the analyses, the relevance of data compilations used in them, the logic of the quantitative approach per se and the utility of numerical probability in safety analysis and risk prediction that must of necessity be practised by engineers.

9.7.2 Data collection and risk models

Any efficaceous approach to event prediction, be it of the more mundane expectancies of ordinary life or that of an LPE, will involve some form of sampling, that is the classification and consideration of those prior events that are deemed to be relevant. In their notes on sampling, G. Udny Yule and M.G. Kendall make the following pertinent observation:

> 'The theory of sampling is thus closely bound up with the theory of probability. The many problems which arise in this connection are among the most interesting and at times the most difficult which science and philosophy offer.'
>
> An introduction to the theory of statistics, Charles Griffin, London, 1944, p.10, 0.41.

Some of the most important applications of methodologies of risk assessment and safety analysis, namely the 'Canvey Island' investigation (See Section 7.1) and the 'Reactor Safety Study' (See Section 7.3), have been mentioned earlier. The value of such analyses in a given risk situation can be no more efficaceous than the truth of the model constructed for the purpose and that of the data used in it. The criterion which is called 'Ontological Relativism' (See Glossary) requires that both the model and its data base be assured in terms of adequacy, relevance and validity. D.J. White (1975/b) has named three tests by which these properties may be established. For the safety analysis of a nuclear power reactor system, they may be restated thus:

(i) A priori evaluation -

Confirmation that the model used corresponds in all essential respects with the design or designs that it is supposed to represent;

(ii) Behaviour -

Confirmation that the model is able to simulate all potential fault sequences and that the failure rate data used to quantify the fault trees are both valid and relevant; and

(iii) Implementation -

Comparison of the performance of the model and its output with accessible information about the behaviour of existing plants and systems of similar or analogous design. (This is one of the objectives of the U.S. Licensee Event Reporting scheme outlined in Note 15 and of which specimens are shown in Table III).

It is interesting to note that in the summary of the principal comments concerning the credibility of the Safety Study's methodology (supra) virtually the same conditions for relativism were specified by NASA and the U.S. Department of Defense (N.C. Rasmussen 1975/e). They cover almost the same ground as the criteria set by O.H. Critchley (1976) for the meaningful application of quantitative safety analysis to a nuclear power program (See Document No. 1 in the Annex). These required verification that:

(i) The plant has been or will be constructed strictly in accordance with the design as assessed;

(ii) The materials, components, equipment, sub-assemblies and other elements used or to be used do in fact conform with the design requirements;

(iii) The data about failure rates or time-to-failure used in the safety analysis are of a kind to provide true knowledge about the performance of the actual elements that comprise the plant or will comprise it as designed;

(iv) Where true failure rate data are not available as in the case of a novel or modified system, then the inferential system that created the synthetic data is fully disclosed and any uncertainty factors openly stated;

(v) It should be possible to show that an independent program of safety analysis would arrive at a similar quantitative assessment of the risk; and

(vi) Enough user experience has been acquired with the given system or about similar systems to establish that those significant faults and failures have occurred, or are otherwise known, so that the credible fault sequences that could lead to a major catastrophic event have been, or can be, identified.

U.S. Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) in their approach to securing reliability in military and space hardware appear to have adopted the same principles of 'Ontological Relativism' as enunciated by D.J. White (supra) and their tests as described by U.S. Comptroller General (infra) cover similar ground to the above 6 criteria and, when not the same, are akin by implication and intent. When satisfactory relativism could not be established, NASA adopted a process sometimes called 'burning-in' which W. Bryan (1975) has described as 'design-make-test-fail-fix' (supra).

In the case of the 'Safety Study' (supra), factual failure rates for many of the major components and subsystems were not available. In order to quantify the fault trees, synthetic distributions were constructed to provide the missing data (infra). Inevitably, these distributions contained a large proportion of conjectural elements (N.C. Rasmussen 1975/f).

The Peer Group Review and other critics found the management and presentation of this material less than safisfactory, the former body thought the treatment to be 'inscrutable' (See Section 7.3.1).

In addition to being abstruse in the view of its critics, the data base of the 'Safety Study' fails to meet the last four of the six criteria for ontological relativism given immediately above. These defects impugn the credibility of the risk numbers cast by it. In this connection, in commenting on the 'Study', the U.S. Comptroller General (supra) observed that:

> 'Absolute reliability numbers are misleading and that the time required to develop them is better spent on critical-component reliability analyses.'
>
> Letter to Senator the Hon. Mike Gravel, Reactor Safety Study: Main Report, Attachment 3, WASH-1400, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1975, p. 196.

The Safety Study and other risk analyses using similar methods seem, therefore, to produce prophecy rather than valid predictions of system performance. A major weakness from which they suffer is the paucity and lack of relevance of the basic fault-rate data available for the calculations, but this is an irreparable characteristic of complex industrial innovations like nuclear power. The virtue of analyses of this kind is 'the discipline they can inject into design analysis'.

9.7.3 The fallibility of synthetic data distributions

In order to make good the lack of relevant fault-rate data needed for quantitative risk and reliability analyses (QSA), many systems analysts have constructed synthetic data banks for their calculations. The report of the U.S. Reactor Safety Study makes an open and comprehensive disclosure of the method adopted to compile the required population.

> 'The fault trees ... were developed to an extremely detailed level ... Each fault tree was constructed down to the basic component to determine the basic causes of system failure; relays, wires, wire contacts, and gaskets are examples of the level to which the fault trees were developed. - Major components such as pumps, valves, diesels, etc., were of course also included. A representative fault tree ... consisted of roughly 300 basic component failure causes, 700 higher faults, ... 1,000 fault relations - gates on the tree - and 30,000 combinations of basic component failures that would result in system failure.
>
> The extreme detail in the fault trees made it possible to identify single component failures and single human failures that would cause the entire system to fail.'
>
> N.C. Rasmussen et al.
> Reactor Safety Study: Main Report,
> U.S. Nuclear Regulatory Commission,
> WASH-1400, Washington, D.C.,
> October 1975, pp. 160 - 161.

T. Thedéen (1979) in a review of the problems of quantification described the methods used to create the failure rate data required by safety analysts working in the field of risk evaluation in energy generation. He found that the failure rate figures for the components, sub-systems, sub-assemblies and other parts comprising a nuclear reactor, PWR or BWR (supra), were compiled from the following sources:-

(a) Informed subjective judgements,
(b) Estimates by specialist experts,
(c) Results extrapolated from experiments with models, and
(d) Time-to-failure figures derived from specialised data banks for components, sub-assemblies, sub-systems and so forth with reference to:
  (i) Similar or comparable types and
  (ii) replicates of the components specified.

Of the four of these sources identified, the first two are the results of supposition, the third, though empirical, introduces the uncertainties of extrapolation and the last which is factual is in two parts of which only the second can be used without further assumptions

in the fault trees. The first, source (d)(i) inevitably requires the analyst to infer the relevance of the analogy between the given datum and the actual element to be incorporated in the plant. It is not a very stable one, therefore. Yet, in spite of the lack of fidelity, data of this kind provides the failure rate figures that must be used in many of the key links in the fault chains, namely ducts and other large pipes, pumps, structural parts of the main pressure vessel and its nuclear core and big valves, things that for the most part are purpose built for a given plant or are manufactured on site.

More serious difficulties arise when attempts are made to create data that makes allowance for human error. It is a capricious factor with no respect for circumstances and, except in the most mundane of repetitious tasks, there is no satisfactory way of quantifying it. Furthermore, erratic human behaviour and mistakes have been the prime cause of many disastrous plant incidents, for example those at 'Browns Ferry', 'Three Mile Island' and 'Flixborough' (See Appendix II) and it is estimated that they are the cause of 60% or more of all accidents (M.B. Biles 1969, Glin Bennet 1983). Human error contributions were included in the 'Reactor Safety Study' fault tree computations (supra), but drew some adverse criticisms (See Section 7.3.1.).

Similarly compiled populations of data have been used by the Systems Reliability Service of the UKAEA (S.R.S. 1984) for its safety evaluations of the Authority's nuclear installations and in its commercial work, for example, the risk investigation supporting the Canvey Island/Thurrock petrochemical complex safety study (See Section 7.1 and Note 10). Some years earlier, a very large and extensive assemblage of data was used for the cost-benefit analysis made in support of Mr. Justice Roskill's abortive inquiry (1971) into the siting of a third London airport, an exercise described by Peter Self as 'Nonsense on Stilts' (1970).

Synthetic data distributions would appear to offer the analyst all the assets of one based on a collection of real, stable elements, but where the synthetic material constitutes a major part of the data, such a belief is illusory. The compilation of a synthetic data universe is an intricate and often open-ended task, and it is seldom easy to trace a datum back to its source. In the case of the Reactor Safety Study, the Peer Review Group were very critical of the way in which the failure rate data was managed (Lewis et al. 1978).

From the foregoing, it may be concluded that when the data base for the risk or safety analysis of a system has a major component of synthetic elements, then any quantitative predictions or assessments derived, particularly when LPEs are concerned, will be no more valid than the data used. If the data are insubstantial in quality, then quantitative attempts to assess a system's risks are little more than guessing, and that may be badly informed. Nonetheless, the foregoing criticisms do not derogate from the positive contribution that a well-organised national data bank can make to the quality and reliability of engineering products and major artefacts generally.

9.8 Overview

It has been the aim of the foregoing critical analysis of the development of technology and the consequent experience of accidents in Western society to show that the rare Low Probability Event manifest in the catastrophic failure of an engineering artefact, plant or system, is a singular phenomenon distinguished from the usual run of accidents, and even from those occasional, uncommon but not entirely unfamiliar, happenings of a more abnormal sort referred to in Table II as 'Unusual'. Accordingly, the hazard of the LPE is unique, presenting the community with a 'zero-infinity' risk.

The Section has traced modern methods of risk management through their evolution from the engineering Safety Factor to the present day sophisticated techniques of quantitative safety and reliability analyses of which the U.S. Reactor Safety Study is a prime exemplar. There is no doubt that they have made important contributions to safety and reliability at the stage of design and may well assist in arriving at expedient decisions about nuclear reactor siting. In spite of these advances, they have not displaced the earlier Design Basis and Maximum Credible Accident concepts which are seen as developments of the Safety Factor criterion. It has been noted that, while these attempts to replace a mainly qualitative philosophy of safety engineering by an approach based on quantitative systems analysis have been welcomed by administrative decision makers, some important establishment figures and certain theoretical scientists, they have been coolly received by engineers. This paradox has been cited as an example of the widening disjunction between the cultural domain of administration, finance, law and politics and that of science, technology and engineering depicted in Figure 6b which has grown so markedly since the end of the Second World War.

The widening gulf is also an aspect of the 'Information Explosion' that is bringing about a qualitative change in the nature of administration and management in modern Western society. Whereas previously, a single able administrative brain could readily encompass within its executive fief all the relatively simple features of the industrial and social applications of technology, this is no longer the case because the fields that have to be covered have become so vast and complicated. The effect was foreseen by Auguste Comte more than 150 years ago when he defined the engineer as a scientist of a new type who was placed to bridge the gap. For societal reasons of a profound nature that it is not appropriate to explore in this text, the engineer has not attained the important position envisaged. Instead, decision making methodologies and systems analysis have been developed that appear to offer an alternative to use of the engineer as an intermediary by reducing the nub of a technological problem to quantitative parameters that can be handled by a purely administrative approach.

It is argued that quantitative methods of risk prediction and hazard management in nuclear power are in fact illusory. The fault sequences to which they assign feasible probabilities will be properly designed out in any competent engineering plant construction process, whereas those which they perceive as beyond the credibility fringe are metaphysical and therefore too unlikely to happen. The rare and unusual event that may run to a catastrophic conclusion and is potential in any plant posing a major hazard will be one that has not been foreseen should it occur, as for instance the disastrous accidents at the 'Browns Ferry' and 'Three Mile Island' nuclear power stations. This risk situation is that depicted in Figures 7 and 8. Furthermore, the calculations underlying these quantitative predictions in the case of highly innovatory technologies lack the support of an adequate data base. Deficiencies are made good by failure rate estimates compiled from analogies, engineering inferences and suppositions. While this kind of synthetic data may offer the plant designer with a vade mecum of technical performance estimates and reliability comparisons, it does not necessarily provide a stable foundation for the prediction of LPEs. The construction of synthetic data bases of the kind used in the Reactor Safety Study has been briefly discussed and the validity of the assumptions upon which they rest reviewed against the criterion of ontological relativism. The requirements are not satisfied, a finding

consistent with that of 'inscrutable' which was returned by the Peer Review of the Safety Study.

As the topic of probability has played a major part in the research reported in this thesis, several subsections have been devoted to it. These deal with its history of comparatively recent emergence as a science, the realism of the objectivist concept compared with the idealism of the frequency and subjectivist theories and credibility in the prediction of LPEs. In the case of nuclear power plants, owing to the largely supposititious nature of the data base, the intrusion of unknown factors that may be likened to 'noise' into the processes to which the design is subjected before it is converted into the reality of an operating system and other uncertainties, attempts at prediction in any definitive sense are, therefore, deceptive. Informed guessing per se is an inadequate basis for the management of nuclear power risks.

10. INDUCTION, PROBABILITY, ENGINEERING AND SCIENTIFIC METHOD

> 'Inductive processes have formed, of course, at all times a vital, habitual part of the mind's machinery. Whenever we learn by experience, we are using them. But in the logic of the schools they have taken their proper place slowly. No clear and satisfactory account of them is to be found anywhere. Within and yet beyond the scope of formal logic, on the line, apparently, between mental and natural philosophy, induction has been admitted into the organon of scientific proof, without much help from the logicians, no one quite knows when.'
>
> John Maynard Keynes (Lord),
> 'Induction and Analogy - Chap. 18,
> Treatise on Probability',
> The Collected Writings, Vol. VIII,
> MacMillan for the Royal Economic
> Society, London, 1973, p. 241.

Before proceeding to develop further the style of engineering that plays a major part in the New Treatment, it is appropriate to consider certain philosophical and logical matters that arise which justify the novelty of its approach. Engineering has been defined, not as science per se, but as the science of applying the facts that have been established by scientific inquiry for the benefit of the community (M.I.T. 1956). It is therefore a discipline that lies between the domains of 'The Word' and 'The Deed' as shown in Figure 6b. Before the surge of technological discovery and invention that led to the Industrial Revolution, though its services were valued, the discipline itself was of poor standing in the body politic. It is from this lowly station that engineering is only just emerging. In fact, its practitioners have generally been little more than higher grade mechanics, responding to directions coming from the domain of 'The Word', determined by policy in which they have had no voice (A. Cottrell 1976).

Since the Industrial Revolution engineering has been acquiring a broader purpose and a more significant definition, though the meta-morphosis has been far from one of steady progress. The change has been consequent upon both the advance of science and the concomitant enhanced importance of technology, factors that are rapidly widening the intellectual gulf between the administrative affairs of 'The Word' and the technics of 'The Deed' as described in Section 9.5.1. The need for a new discipline able to bridge the gap was foreseen by August Comte, namely that of the engineer (See Section 8.1.2).

With the recognition of his importance no longer denied, the engineer is becoming able to assert a growing influence on technological policy formulation and decision making, something required for the New Treatment, although his status in society has yet to receive proper recognition (See Appendix III), and, there are those who have foreseen even greater things (Thorstein Veblen 1921).

10.1 Engineering and the ethos of nuclear power technology

From what has been said so far, there are few aspects of the management of the hazards of atomic energy that are not properly germane to the fief of the nuclear engineer. The field is so wide that it has embraced almost every other science, has brought into being a special branch of medicine and toxicology in health physics and drawn upon many disciplines not normally associated with technology. Far reaching new legal concepts have been created and incorporated in statute law and regulations and extended Worldwide through binding international conventions (Street and Frame 1966). Alvin Weinberg (1978) has described the fringe between nuclear science and technology and the liberal arts and politics as the realm of 'trans-science' where thought patterns of a novel kind prevail and scientific method does not apply.

In this milieu, the engineer working in the field of nuclear power has to face the challenge of decision making on matters of an advanced and hazardous technology that have serious economic, political and societal significance. It is particularly true for those engineers employed in the regulatory bodies concerned with nuclear safety, as for example the Nuclear Installations Inspectorate (NII), described in a later section of this thesis and elsewhere by O.H. Critchley (1977) in his study of the history and philosophy of U.K. nuclear regulatory practice. It is important, therefore, to examine certain matters of a logical, philosophical and mathematical kind that are normally taken for granted in engineering practice because their uncritical acceptance can conceal fallacies, illusions and false assumptions and cloud technical judgement. For instance, the popular idea that the Euclidian pattern of mathematical reasoning is transferrable to the area of common sense (See Glossary) is, in fact, false. In particular, the process of thought known as inductive inference on which man relies for a very large part of his day-to-day decision making and which certainly underlies engineering design, technical

safety assessment and risk prediction cannot be justified by formal logic. (To cite K. Popper and D. Miller 1984: see also Document No.2 of the Annex.) Neither does scientific method fall into any simple logical slot. Yet, it is by induction and scientific method that the work of engineering is done, and 'trans-science' must be left to the sociologist and politician.

Owing to the beauty of its symmetry and the satisfaction that can be found in its simple logic, mathematics offers an intellectual attraction that can be specious. This combined with the ideological predominance of the realm of 'The Word' has led to an almost uncritical acceptance of the systems approach as a panacea for the difficulties of decision making under conditions of uncertainty. Moreover, this is aided by an impressive mathematical presentation that suggests scientific precision and authority.

J. Schwartz (1962) warned of this extraordinary ability of mathematics to make a scientific argument look convincing without regard to its validity. It has in consequence exerted 'a pernicious influence on science' because 'it can dress scientific brilliance and scientific absurdity in the impressive uniform of formulae and theorems'. J.M. Keynes (1936) commented some years earlier on this failing as detrimental to economics, describing such regalia as 'concoctions ... ... which allow the author to lose sight of the complexities and inter-dependencies of the real world in a maze of pretentious and unhelpful symbols'.

The process of design which is at the core of engineering is largely a matter of inferential logic. Present facts are assembled in the design to express a potential intent, the concept of some artefact that is a machine, structure or system to be created in the future by realising the image of the design. Design is thus an innately predictive activity. Furthermore, safety assessment and the other techniques of risk analysis, whether qualitative or quantitative, are also attempts to make rational forecasts about the behaviour of a plant or system that it is presumed will be built according to instructions given in the relevant design message. This again is an exercise of the faculty of inductive reasoning which has long been one of the fundamental questions of epistemology. Although he did not use the term, the 'problem of induction' was notably discussed by David Hume (1711 - 1776) in his famous work on causation (1748),

and this is generally accepted as the starting point of the modern debate which continues today. It seems to have little chance of being resolved satisfactorily through the logic of 'The Word', being intractable by the use of 'pure reason'. Despite that, induction is in illimitable, naive daily use, justified by the popular logic of common sense (supra).

10.2 The riddle of inductive inference

The mechanical engineer, Ludwig Wittgenstein (1889 - 1951), who later turned logician, dismissed the feasibility of inference by induction in the following terms:

> '5.135 There is no possible way of making an inference from the existence of one situation to the existence of another, entirely different situation.
>
> 5.136 There is no causal nexus to justify such an inference.
>
> 5.1361 We cannot infer the events of the future from those of the present.
> Superstition is nothing but belief in the causal nexus.'
>
> (He appears to escape from the dilemma of the impossibility of inductive inference on the one hand and its practical necessity on the other with his final proposition.)
>
> '7. What we cannot speak about we must pass over in silence.'
>
> Tractatus Logico-Philosophicus - 1922
> (Trans. D.F. Pears and B.F. McGuinness),
> Routledge & Kegan Paul, London, 1972.

Professor Max Black of Cornell University states the difficulty about induction more explicitly:

> 'An inductive inference from an observed association of attributes (A_n - B_n) can justify inference to another case (A_{n+1} - B_{n+1}) or inference to the corresponding generalisation ('All A are B') only if the association is somehow known to be lawlike, not merely accidental. Yet how can this be known in primary inductions that do not themselves rest upon the assumed truth of other laws? Certainly not by immediate experience, nor a priori, nor, without begging the question, by an appeal to induction.'
>
> 'Problem of Induction',
> The Encyclopedia of Philosophy, Vol. 4
> (Editor Paul Edwards),
> Collier MacMillan, London, 1967, p. 171.

Notwithstanding the philosophical arguments about the validity of inductive inference, it is a matter of common experience that induction is both effective and necessary. Therefore, for the purposes of ordinary daily life, the issue appears to be a non-problem. The practice of engineering and the exercise of engineering judgement are inductive skills par excellence. It would be impossible to design, build and operate a complex plant without an effective means of acquiring foreknowledge about the likely consequences of the interplay of the forces and environmental stresses to which its components, structures and sub-systems will be exposed. Moreover, without induction the management of potential LPEs would be impossible.

Despite some recent dissent (infra), there has been wide agreement that an escape from the logical dilemma of induction can be made by turning to the science of probability. The relevance of such an approach to nuclear power was discussed by O.H. Critchley in his work, 'Aspects of the historical, philosophical and mathematical background to the statutory management of nuclear plant risks in the U.K.' (Document No. 2 of the Annex) from which the excerpt below is taken:

> "Probability and Resolution of the Enigma of Induction
>
> 33. The understanding of induction which is still far from complete has improved with man's grasp of the relatively new discipline of probability. Generalising from the science of statistical mechanics which about a century ago was resolving many of the knotty problems of physics, James Clerk Maxwell was moved to observe that Logic could deal only with certainty, doubt and impossibility, whereas reason went beyond these things. The link was provided by 'the calculus of probabilities' which was 'the true logic' for man and science.
>
> 34. Now that probability has allowed an escape from the impasse of the problem of induction, the debate has moved on to the understanding of probability itself and that may be more difficult and contentious than the former challenge."
>
> Symposium on radiation protection in nuclear power plants and the fuel cycle, British Nuclear Energy Society, London, 1978, pp. 11 - 18.

Despite the confidence of the experimental physicist, James Clerk Maxwell (1831 - 1879), expressed in the quotation above, the case in pure logic still seems to be far from settled as no less an authority than Sir Karl Popper has just announced 'a mathematical proof of the impossibility of inductive probability' (K. Popper and D. Miller 1983).

The safety studies, assessments of design and risk analyses that are now in vogue are exercises in inductive probability of a large scale. Therefore, the quandary about induction is of no little relevance to the anticipation and management of the catastrophic LPEs that have blighted the operation of the advanced plants and the use of those other things that have been counted as the blessings of modern technology, among them nuclear power, oil and its petrochemical products and the new pharmaceuticals. A few decades ago when these hazards did not exist, or perhaps those that did were not recognised, for all practical purposes the problem of induction was ignored and left as a philosophical conundrum. Today's answer to the dilemma may lie in the sphere of scientific culture identified by C.P. Snow (See Section 8.1) and, thus, in recognition of that logically untidy entity, 'scientific method', as the pattern of thought germane to engineering and technology.

10.3 Induction, Scientific Method and the language of technology

In a discourse on problem-solving in the evolution of scientific knowledge, J.R. Ravetz describes the difficulty over induction in its modern aspect in the following words:

> '... there is no formally valid pattern of argument that can establish properties of general classes from the reports of particular experiences. The argument may be partly mathematical and deductive, but (outside purely theoretical fields) it must include inductive, confirmatory, probabilistic, or analogical inferences, which are never capable of carrying certainty from premiss to conclusion.'
>
> Scientific Knowledge and its Social Problems,
> Penguin University Books,
> Harmondsworth, 1973, p. 120
> (Earlier edition, CUP 1971).

Incontestably, there is a well-grounded case in formal logic for the impossibility of induction, whereas the verified efficaciousness of the inductive processes used in everyday human activity is an obvious, though perhaps contrary, fact. As suggested earlier in this text, the philosophical impasse presented by induction may lie in the intellectual system which we have inherited from antiquity and are conditioned to accept as absolute. In the days of the glory of the Roman Empire, the world of creative thought was closed to the slaves and lower orders of freemen concerned with technology (See Section 8.1). As Lucius Annaeus Seneca (4 BC - 65 AD) wrote when commenting on some of the inventions

of his time which included transparent window glass and a form of short-hand:

> 'But the inventing of such things is drudgery for the lowest of slaves; philosophy lies deeper. It is not her office to teach men how to use their hands. The object of her lessons is to form the soul.'
>
> 'Epistolae morales 90',
> Quoted by Alan L. Mackay in
> The Harvest of the Quiet Eye,
> Institute of Physics, London and
> Bristol, 1977, p. 135.

Hence, logic as we know it lies in the realm of 'The Word' and is of that precision of thought and grammar that is part of our cultural heritage which, like the message of Seneca's philosophy, has moulded our processes of cognition. Induction is a thing that works with deeds, useful arts, experiment and observation in a holistic way and, therefore, does not fit into the canons of a received logic.

Human thought processes when used to solve a problem or formulate a particular concept are necessarily peculiar to the discipline in which the activity is set, but the language by which the result is expressed is constrained by the accepted linguistic pattern of the cultural milieu. Language which is the product of a society is formed by 'past generations and centuries of human experience', but is specifically fashioned by the intelligentsia who dominate that society. Before the explosive growth of science and technology that began with the Industrial Revolution, the limitations that the inadequacies of language must have placed upon the full communication of scientific ideas and theories were of no immediate societal consequence. They were comparatively simple and when it was too dangerous or suitable words could not be found to express a concept, it was contained in an allusive phrase meaningful to the informed.

Be that as it may, as the ideas and theories became more complicated and with the widening disjunction between 'The Two Cultures' (C.P. Snow 1959), their presentation and communication in simple terms and hints became fraught with difficulties, not only because they challenged authority, but because they could not be properly explained. Dr. Ohm suffered grievously for this reason (See Section 8.1). Moreover, the storehouse of relevant knowledge available to the

practitioners of 'The Deed' was becoming so large that each discipline began to create its own lexicon and metatechnology as well.

It is not surprising then that conventional linguistics handed down from antiquity and properly slow to change was not able to express readily and in a general way the concepts of emerging science and technology and this view is not without authoritative backing. Recently, H.B. Barlow (1983) claimed that the development of language plays an essential part in the evolution of man's intellect. In addition to its function in the communication of ideas, it has 'a primary task of organising information in the mind'. Barlow then argues that language has not yet acquired the capability to provide a satisfactory definition of intelligence. Professor Bruce Archer (1979) holds that mathematics and logical models are the product of an alien mode of reasoning that is not helpful in the work of creative design. This is overcome by 'a designerly way of thinking and communicating' that is as different from the scholarly ways as it is powerful and productive. It may, then, not be unreasonable to suggest that induction shares a similar linguistic disability.

The foregoing argument seems to have received support from recent research in neurolinguistics (See Section 8.1.1). This work suggests that the activities of 'The Deed' use the right cerebral hemisphere more than those of 'The Word'. Intellectual activities in the latter class are centred in the left hemisphere which is held to be the site of linguistic capability, abstract thought and rationalisation (J.R. Skoyles 1984). On the other hand, engineering and design, though no less dependent on analysis, rational thought and logic are also concerned with the intellectual processing of complex ideograms which has its province in the right hemisphere. Their thought processes might, therefore, be expected to include a dimension absent from the intellectualisations of 'The Word', engineer and designer acquiring their special propensities during their education, professional training and subsequent experience. Support for this case comes from the findings of Howard Gardner (1984) who claims that there is a specific cultural basis for the development of such intellectual faculties, for instance the evocation in the Japanese cultural milieu of musical virtuosity in ordinary children of 7 years of age and under who would be considered prodigies if they exhibited their attainments under different circumstances.

In Europe after the Renaissance and more particularly in its northern states, the prevailing cultural pattern enabled science to make rapid progress and her discoveries were presenting a serious challenge to the established schools of philosophy. The savants necessarily taking an empirical view side-stepped the issue of induction when they began to adapt their thinking to accommodate the new knowledge and concepts. Although science is logical, the canons of formal logic were of little help in their enquiries. The scientific way of thinking began to be defined. The first enunciation of the Scientific Method that is so fundamental to scientific discovery is generally attributed to Francis Bacon (1561 - 1626). A little later, the great experimental physicist, Sir Isaac Newton (1642 - 1724), 'a lad of his hands as well as his head', set down in his famous 'Principia' 42 principles of scientific enquiry of which the fourth defines the nub of what is accepted as Scientific Method, namely:

> 'Rule IV: In experimental philosophy we are to look upon propositions collected by general induction from phenomena as accurately or very nearly true, notwithstanding any contrary hypotheses that may be imagined, till such time as other phenomena occur, by which they may be made more accurate or liable to exceptions.'
>
> 'Rules for reasoning in Philosophy',
> Principia (1687) = Mathematical Principles
> of Natural Philosophy (Trans. Andrew Mott),
> Berkeley University Press, 1934, p. 398.

The principle, although applied in our time in a more dialectic way than Newton might have tolerated, has been central to science and technology for nearly 300 years. It has been restated in more general terms by Professor Peter Caws as:

> 'The method of science is a mixture - the proportions vary from one science to another - of logical construction and empirical observation, these components standing in a roughly dialectical relation.'
>
> 'Scientific Method',
> Encyclopedia of Philosophy, Vol. 7
> (Ed. Paul Edwards),
> Collier-McMillan, London, 1967, p. 343.

In summary, it may be said that inductive reasoning in application to scientific and technical things may be identified with the thought processes that pertain to Scientific Method which, like intelligence, still lacks a definition that would be universally accepted as

satisfactory. Despite that, an approach that is essentially Scientific Method underlies almost every creative act in engineering, not least in design, and it plays a very important part in safety analysis for nuclear power plants.

10.4 Recapitulatory synopsis

This section together with Section 9 that precedes it completes the historical, cultural, mathematical and philosophical background against which the New Treatment will be developed. They considerably extend the research reported by the writer in his 1978 work, reproduced as Document No. 2 in the Annex. The New Treatment has emerged in a situation fraught with societal and political concerns engendered by contemporaneous advanced technology, and particularly by the peculiar 'zero-infinity' risk of nuclear power. To justify the need for a new approach, it has been necessary to study in some depth the causes of the difficulties that its predecessors have failed to overcome. Some of these are intractable and there remains a grave but small residual risk of a devastating nuclear reactor accident. The question of greatest significance concerns the validity of the methods for the safety assessment of nuclear power plants and for the prognosis of those faults that could induce catastrophic failure with a massive release of fission products. Another of a different kind, but not unrelated, is to win public acceptance for the system of safety management adopted..

It can be proved to the satisfaction of formal linguistic logic that inductive reasoning is invalid and, in consequence, all attempts to foresee future happenings in terms of prior circumstances are nugatory. But this conclusion is at variance with human experience and normal expectations because, although such forecasts are by no means certain to be fulfilled, they are an efficaceous and necessary part of the conduct of affairs. Inductive reasoning of this kind is a matter of everyday experience and the planned activities of civilised life would be impossible without it. This is also true for the physical sciences, technology and engineering and induction is inherent in scientific method. The processes of design upon which engineering depends for its achievements are also innately inductive. Probability would seem to offer an obvious escape from the dilemma, but inductive probability can also be shown to be invalid in formal logic. In pursuit of a simpler technology in the past, engineering had neither need nor ability to be concerned with the philosophical conundrums of logic, and the physical

sciences slipped out of the quandary by enunciating the Scientific Method as a special way of problem solving peculiar to scientific discovery.

The very rapid advance of science and the concomitant growth of technological industry has widened the intellectual gap between the culture of the milieu in which science and technology flourish, that is the domain of 'The Deed', and that of 'The Word' which is the culture of the arts and administrative disciplines. It is a disjunction to which C.P. Snow some 30 years ago referred in his controversial Rede Lecture on 'The Two Cultures' and the gulf has widened considerably since then. The difference between the thought processes peculiar to them has been acknowledged in this decade by eminent authorities in scientific fields as disparate as psychology and design.

It is therefore reasonable to suggest that the problem of induction may in reality be one of communication because accepted language is not able to convey ideas that are strange to the thought patterns of the dominant social sphere, one in which science and technology are still alien and suspect.

The difference between the role and outlook of those concerned with administration in business, finance and politics and the savants and their science was perceived by Auguste Comte early in the European industrial revolution who saw the need for a new kind of scientist who could work across the intellectual gulf to foster the exploitation of science by industry and thus promote economic and social progress. The Scientific Method may be seen thus, not as a logical anomaly, but as a special way of inductive reasoning proper to the sciences and engineering. For this purpose a linguistic form is needed that differs from the accepted language of the day, offering a dialectic in which the concepts peculiar to a given science or technology may be more tractably discussed and meaningfully expressed.

Despite the fact that the quantitative methods of reliability analysis have made an important contribution to reliability in engineering design and that safer design has resulted, this achievement does not mean that they have the capability to define those unforeseen circumstances in which catastrophic LPEs may occur. No prior theoretical study of design, however exhaustive, can foresee the situations that may arise on a plant that has been constructed and is operated in another distinct dimension, that of practice. The facts are that of the eventualities envisaged, those that could credibly occur will be properly

designed out, while those at the fringe of incredibility are far too unlikely to happen. Yet, where such a hazard exists, some disastrous event is always possible, but the clues to it will either not have been present in the design or be too ambiguous to have been identified as efficient in the analysis.

In addition to the foregoing commonsense reservations, there are more fundamental disabilities. Within the field of formal logic foresight of this nature is not possible. In the area of scientific method where inductive probability is efficient, the quantitative methodology also fails because it is primarily a tool for reliability analysis of design. Prognosis about things that might happen to a plant under conditions of use requires another technique. Yet, other than for knowledge acquired by continuing experience of replicate plants in use no such thing exists. It is certainly absent in the case of nuclear power owing to the essentially innovatory nature of its technology. Again, the very reliability estimates from which the forecasts about LPEs are made are in themselves unstable, being the result of theoretical studies that lose their validity when extrapolated into the 'noisy' dimensions of reality in which the plant in question must operate. Finally, there is a further disability that the methods of assessment per se lack the basis of adequate and stable failure rate data because of the novelty and inconstant nature of their sources, many of which will be of necessity synthetic.

It follows that the preferred way of assuring adequate safety in the operation of nuclear power plants and, for that matter, in other types of innovatory technology, is to recognise the futility of attempting to attain that end by use of techniques of safety analysis and risk prediction that purport to be definitive. Theoretical investigations of this kind, no matter how exhaustive, cannot disclose the nature and occasion of the odd confluence of unlikely events and human errors that can combine together to initiate a disastrous fault sequence. Instead, success is more likely to be achieved by using design assessment aids such as the MCA concept and QSA to an extent appropriate to their proper purpose, assuring a level of safety perceived to be adequate by pursuit of sound engineering confirmed by independent surveillance. Design would then be seen in its proper place as a pattern for the construction and operation of a given plant, recognising the discontinuity between the 'marks on paper' that constitute it and the hardware of the engineering reality that has to be constructed according to its

instructions. The method to be favoured is essentially that of scientific method epitomised in W. Bryan's heuristic maxim (1974) of 'design-make-test-fail-fix' which characterised the approach to space vehicle reliability in the 'Apollo' Moon-shot program.

The engineer, through his unique position of both design scientist and industrial manager participating in the construction and operation of the plant, is able to offer a direct executive link between the upper echelons of administration, finance and politics and the shop floor, construction site and control room. He is thus placed to draw together all aspects of nuclear power and to achieve an outcome of assured reliability: indeed, one that can be recognised as such by the body politic. An example is set by the confidence that Dutch civil engineers have been able to inspire in the population of Holland by their long and successful control of the perpetual threat of inundation from the sea. However, the problem of safety assurance for modern advanced technology is more complex because many of the restraints of the past on hazardous technical innovation, such as personal responsibility for the installation or process, are no longer as effective as they were in the days when the dykes were built.

A system of monitoring is therefore necessary to define individual and corporate responsibility for those personal errors and managerial deficiencies that lead to serious plant accidents. O.H. Critchley in a paper on the part played by human error in the causation of catastrophic failures in major industrial installations and public transport vehicles published in 1981, which is reproduced as Document No. 4 in the Annex, described the evolution and monitoring role of a special class of engineers dedicated to safety technology and regulatory science. The topic is pursued later in this text.

PART FOUR

FEATURES OF THE NEW TREATMENT: DEFENDED SAFETY, EVENT-NOISE AND CATASTROPHE THEORIES AND THE NEED FOR ENGINEERING INSPECTION

Sections 11 to 13 comprising:

A further exposition of the philosophy of the New Treatment in which 'the plant' is presented as a continuing 'noise' creating phenomenon from design concept to terminal shutdown, being maintained in a regime of engineering that blends the qualitative (MCA/DBA) and quantitative methodologies of design assessment and the strategies for construction and operation of the plant in a pragmatic policy for the defence of 'adequate' safety; observations on the nature of engineering design; the human factors - involvement, unintentional and culpable errors and accountability, in event causation; accidents, faults and incidents as 'Event-noise' (En) flux in which major failures and catastrophes are identified as singularities in the flow; the tautotlogy of formal En analysis; recourse to ideographic means to assist the interpretation and comprehension of safety and reliability problems, the representation of En experience and plant operational strategies by a simple Catastrophe model; the paradox of event precursors, evidence of 'loss of resistance to failure' as a guide to safety defence tactics; and the role of engineering inspection in the defence of safety.

THEMATIC SYNOPSIS

Even though the most advanced methods of safety and reliability analysis of design and best organised of strategies of quality assurance and control in construction and operation may reduce the incidence of accidents, faults and mundane failures in a plant, system or process, they are unable to create a regime of absolute safety where there is a potentiality for catastrophic failure. Indeed, cases are legion where a disastrous accident has occurred in a wholely unsuspected and adventitious mode. There are few of these rare, low probability events that have not been precipitated by some human error or omission, unintended, inadvertent or culpable. It is then to inspection, the age-old process that has evolved to detect, expose and prevent human error and kindred failings that attention is now turned.

11. AN OUTLINE FOR THE NEW TREATMENT OF LOW PROBABILITY EVENTS

'Science is built of facts the way a house is built of bricks; but an accumulation of facts is no more science than a pile of bricks a house.'

Jules Henri Poincaré,
La Science et l'hypothese,
Paris, 1902
(Trans. W.J. Greenstreet, London, 1905).

So far the 'New Treatment' has been alluded to rather than described and at this stage it is appropriate to say more of what it is about. Although it is an administrative as well as a technical course of action, its most important aspect is empirical and largely concerned with the way in which a certain kind of practical engineering is undertaken. This follows from the fact that serious accidents, indeed any incident, cannot occur in the corpus of the design of a plant, process or system per se because that design has no existence other than in the realms of thought, being but a collection of ideas and instructions on paper or otherwise recorded. Actual events, rather than speculations about imaginary happenings, must take place in a system that has physical existence. The 'New Treatment' is thus intimately involved in the whole engineering process from the conception of the artefact and the expression of that idea in the design to the realisation of the latter in a satisfatorily functioning entity, for the purposes of this study a reliable nuclear power station running on full load. In addition it must ensure that important societal criteria have been met. This requires that the whole sequence of actions must not only have achieved a safe and reliable outcome that imposes a negligible risk on the community served, but it must be apparent to the interested and concerned public that this has been the case.

The view that an individual takes of risks, safety and the unexpected occurrence of catastrophic failures in technological artefacts, structures and systems is largely determined by a cultural standpoint unique to him as an observer. Consequently, he who professes to expertise in one of the five great cultural disciplines depicted in Figure 1 may be expected to perceive the phenomena of risks and catastrophic failures, for our purposes here, Low Probability Events (LPEs), in a manner peculiar to his profession. The scientist will, therefore, try to measure and explain them; the administrator thinks in terms of principles, the interpretation of rules and of precedents; the

lawyer will seek to establish culpability for infraction and liability; the entrepreneur sees the situation in terms of profit and loss; the doctor will be concerned with the harm and hurt suffered by those exposed to their destructive forces; but the engineer will aim at enhancing the operational efficiency and resistance to failure of the entity at risk. There will be, of course, some interaction between the disciplines and at times a fertilising interchange of concepts, but the response in each case will in general be conditioned by the habits of the particular profession. As may be expected then, mathematicians and many theoretical scientists will favour the quantitative methods of systems analysis, as for example N.C. Rasmussen and F.R. Farmer, and their approaches have been endorsed by the administrative establishment (Lord Robens 1972/b, Sir Brian Flowers 1976/c). In contrast the engineer's stance is inherently pragmatic. His attention is directed to the site realities of accident causation and prevention, the expediencies of siting, emergency action and post-incident damage control and to those improvements in design, quality assured construction and operational practice and plant maintenance that such considerations show to be necessary.

11.1 The 'trans-scientific' aspects of Engineering

It is perhaps not generally recognised that the engineer's perception of the hazards associated with a technology and, thereby, his attitude to management of its risks is inherently different from those that would be evoked in a scientist, and a physical scientist in particular. Engineering is not an inferior kind of science, but a different, though still scientific, discipline cast in the role foreseen for it by Auguste Comte (supra). More recently, J.R. Ravetz found that:

> '... ... there are certain deep differences between the two sorts of work; so that for the preservation of the health of both they must be kept distinct while yet in contact.'
>
> Scientific Knowledge and its Social Problems, Penguin University Books, Harmondsworth, 1973, p. 329.

It may be that the greatest differences between the two fraternal disciplines lie in the use of measurement. The scientist in his search for truth tries to measure and quantify the phenomena he is called upon to explain. Lord Kelvin put this approach in the following words:

> '... ... I say that when you measure what you are speaking about and express it in humbers, you know something about it: but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind.'
>
> William Thomson,
> Lecture to the Institution
> of Civil Engineers, London, 1883.

And without question this is the proper mode of investigation for physical science. It is certainly not an all embracing way of treating those scientific problems that exist in the fringe where science is in contact with society, the region defined by Alvin Weinberg (1978) as 'trans-science'. While measurement is essential to the engineer's pursuit of scientific method, many of the things he encounters cannot be measured and expressed in numbers, but must be appraised in their qualitative aspects.

The engineer is unable to pursue his art with the quantitative rigour of physical science and he must therefore adopt a more flexible mode. Whereas the scientist can identify, select and restrict the variables presented by his problem, the engineer has no such facility. Instead, he must adapt his course of action to accommodate a variety of factors, variable, some incommensurable, many unexpected and others that are in no way scientific. In these circumstances, measurement and quantification are limited, though invaluable tools and must be supplemented by qualitative means, by that indefinable faculty of 'engineering judgement'.

Oddly, engineering is the only major current discipline without a distinct and unique philosophy to guide and inspire its professionalism. There is a philosophy, indeed philosophies, of science. Law seeks its direction and amour propre in jurisprudence. Medicine has long hallowed precepts and practice dating back to Hippocrates. In all countries, administrators in establishment posts are necessarily imbued with a philosophy appropriate to their duties that maintains consistency in governmental and political policy formulation and decision making. Some attempts have been made to fill the more obvious areas of deficiency and there are signs of a tendency for them to coalesce into an identifiable philosophical theme relevant to engineering.

In the past two decades, 'design' has been recognised as a subject for independent study and research and has been incorporated as a topic in its own right in the syllabuses of many engineering degree

courses (M.C. de Malherbe and P.J.B. Solomon 1963-1964). The importance of engineering design has been given some recognition by the Government. The report of a departmental committee on 'Engineering Design' chaired by G.B.R. Feilden appeared in 1963. It recommended setting up of a 'Design Council'. It was updated in 1976 by a Design Council study of 'Engineering Design Education' directed by Alexander Moulton. The topic is beyond the scope of this text, except to say that the writer has given due cognisance of its importance in his research and critical judgements.

11.2 Attempts to define some basic principles of safety and reliability

Despite there being no coherent philosophy of engineering, a number of important doctrines have appeared ad hoc to guide design and bench, shop floor and site practice. Among them are the Safety Factor, the Design Basis and Maximum Credible Accident concepts in nuclear engineering, the criteria of simplicity and symmetry, 'avoid-a-sudden-change-of-section' and so on. In the specific area of nuclear plant design, a comprehensive set of 'Principles' was issued by the U.K. Nuclear Installations Inspectorate (NII) in 1976. The document has been progressively updated since (R. Gausden 1982 - 2). They are intended 'to apply to all systems of significance to safety in a nuclear power station'. They cover the safety assessment topics shown in Figure 3. Principles with statutory force applying to the operation of nuclear power plants are attached as conditions to U.K. nuclear site licences (R. Gausden 1982). They are a mix of legal obligations that concern site demarcation, record keeping, radiation exposure limits, fissile material and radioactive waste management and engineering safety principles bearing on the operation and maintenance of the plant. The latter are technical provisions of a very general nature that require the licensee to respond by formulating rules and instructions.

11.2.1 Characteristics of the approach to radiological protection

The aim of any serious approach to the management of low probability disastrous technological events should be to prevent them, and this has been the principle underlying nuclear safety engineering since its inception and is expressed in the Design Basis Accident doctrine. On the other hand, in the case of radiological protection generally, the policy is to minimise the risk of deterimental consequences as no lower exposure threshold has, as yet, been found, if indeed there is such a thing, and it is not feasible to create zero dose environments

for either public or workers. Practice throughout the World is largely determined by the prestigious 'Recommendations' of the International Commission for Radiological Protection (ICRP). The Commission assumes that "any exposure to radiation may carry some risk ... (and) ... there is no 'safe' dose ..." and protection aims at establishing 'a dose (which) might be called an acceptable dose' (ICRP Publication 9, 1965). The situation is open-ended, labyrinthine, controversial and fluid. The position is currently that:

> ' The aim of radiation protection should be to prevent detrimental non-stochastic effects and to limit the probability of stochastic effects to levels deemed to be acceptable. An additional aim is to ensure that practices involving radiation exposure are justified.'
>
> 'Recommendations of the International Commission on Radiological Protection'. Radiation Protection, Publication 26, S.9, 1977.

While the above 'Recommendation' is consistent with the ICRP's earlier philosophy, it represents a change in emphasis from qualitative attitudes of limitation in the spirit of 'as low as reasonably achievable' (ALARA) to quantitative concepts of acceptable dose determined by risk mathematics. In practice, Publication 26 may make little difference to the management of industrial exposures as of now and they will continue to be prudently minimized. Nonetheless, it is a trend towards reliance on quantitative criteria which have by no means secured universal acceptance among engineers and members of the international scientific community (Alvin Weinberg 1972, Karl Z. Morgan 1978, Daphne Gloag 1980).

11.2.2 Principles for the New Treatment

The arguments in the preceding parts of this thesis have eroded the main bases of the present approaches to the management of the hazards of nuclear power. They have exposed the inadequacies of the claims made by the several methods of design safety assessment to predict the chances of catastrophic nuclear plant accidents and the further weakness of the quantitative techniques of safety analysis owing to the instability of the data. As observed earlier, the accidents that are revealed by such analyses are either properly designed out or are otherwise of too low a probability to happen. Moreover, their prognostications relate to design and not to the operating plant brought into being after a lead time of perhaps a decade or more.

However, in any given case the chance of a severe radiation accident will not have been eliminated as something beyond the scope of the analysis can happen instead as suggested in Figures 7 and 8.

The New Treatment offers a supplementary approach, accepting the useful and, indeed, necessary features of the achievements of nuclear safety technology, in particular the enhancement of safety and reliability in design. Furthermore, its central theme is engineering by scientific method and is, thereby, directed at the reality of the operating entity of a nuclear power plant rather than at its design. Salient points in its philosophy are:

(i) Engineering proceeds by inductive reasoning. Its envisaged end product and related conclusions are therefore probable rather than certain and any engineering endeavour must be of sufficient flexibility to adapt to the unexpected.

(ii) Safety follows from reliability: a reliable plant is likely to be a safe one. Reliability cannot be achieved by studies of design alone, but is the result of an evolutionary process epitomised by the iterative maxim of 'design-make-try-fail-modify'. Therefore, in the pursuit of safety, novelty must be minimal.

(iii) Potential events of metaphysical probability never happen (Borel's Single Law of Chance), but something else, unforeseen and equally catastrophic, may.

(iv) Human error is ubiquitous, pervasive and capricious and no process of design or work of construction or operation of a plant or system is immune. Its incidence is unexpected, displacing those failings that are foreseen. It is the major cause of accidents of all kinds and a significant contributor to catastrophic failures. It is impossible to eliminate, but it can be minimised by surveillance in the form of inspection.

(v) Nothing happens without precursors which are more often than not perceptible before an accident. Detection of 'evidence of loss of resistance to failure' is an effective means of anticipating and aborting sequences leading to system failures.

(vi) An engineering approach characterised by elegance and simplicity involving no more novelty than the situation demands is most likely to be reliable and safe.

(vii) Life is risk. Nothing is absolutely safe. Humans will tolerate a modicum of risk, but the risk perceived must be so small in the circumstances of benefit that it can be ignored.

(viii) Human life is beyond price, but some valuation may be needed against malevolent chance in the economic management of humanitarian investment in safety (16).

A characteristic of certain important modern advances in technology is the enormity of the continuing societal risk that the associated hazard can impose on the community exposed. Although that hazard may be safely contained within apparently secure protective barriers, technical or administrative, the dangerous potential remains on leash. Success in risk management of this kind, epitomised by that of nuclear power, has two common goals. One is to secure effective and credible control of the threat and the other is to convince the concerned public that, this being so, the benefits derived are worth enduring a residual risk that tends to zero.

There are four principal conditions to be met if these are to be achieved. They are to secure that:

(i) The source of the hazard has been so effectively contained that there is no significant immediate threat (engineering),

(ii) There exists a credible due process for ensuring that the system on which containment of the hazard relies is effectively and lastingly maintained in its proper state (regulation),

(iii) Opinion leaders amongst the public accept that the system of hazard control meets the requirements of condition (ii) supra (political), and

(iv) The public as a whole are satisfied that the benefits that come with continuing exposure to the hazard are worth the risk that it imposes (societal).

If the engineering and regulatory conditions can be efficaceously met, and be seen to be met after democratic challenge, then public satisfaction with the system of hazard control is likely to follow and the risk should be accepted (J.R. Ravetz 1977 - 2, W.D. Rowe 1979).

11.2.3 The quandaries of 'Adequate Safety'

A challenge to be faced by the New Treatment is that of 'Adequate Safety'. Expressions of disquiet about the safety of advanced modern technological innovations are proper in view of the continuing run of catastrophic accidents of which the public are kept aware by the news media. Although significant fears must be investigated, there is a danger in over-anxious concerns about possible, but improbable risks

that are already satisfactorily contained; of adverse, though rare, reactions in a few patients treated by otherwise effective and safe medicines; and of futile pursuits of the chimeras of hypothetical plant accidents. Excessive emphasis on safety can result in the proliferation of regulations and codes and the ratchetting of industrial costs that bring minimal reduction in accident rates and disease incidence. It has become a blight on the drug industry where multiplying safety regulations and testing requirements have not only grossly increased costs, but have diminished the supply of new and much needed remedies (M. Weatherall 1982). It is justifiably claimed that unduly tight controls have already been responsible for shortened life spans of many throughout the World whom the new drugs could have cured, as in the case of beta-blockers in the U.S.A. Even when the opponents of a major technological project have failed to abort the object of their attack, they have often been the cause of lengthy delays in construction programs that have caused electric power utilities heavy financial losses.

Again, in the case of nuclear power, the Sisyphean hearings on the subject of emergency cooling for the core of a PWR in the case of a loss of coolant accident (LOCA) have involved heavy expenditure on research and legal costs by the U.S. atomic energy authorities and the plant constructors. Design changes have been introduced and PWR may be a safer reactor as a result. Whether or not these were justified by the severity of the envisaged failure and the likelihood of the fault that could cause it or whether they will be truly effective in reducing the latter are moot points. Be that as it may, changes made to enhance the safety of a design as a result of debate about hypothetical faults, rather than those which are justified by experience in the field, can often lead into the morass of 'safer-than-safe' when technical safeguarding investment goes beyond the point of diminishing returns. But, experience of some faults is unobtainable because they are the very things safeguarding should prevent.

A balance is hard to strike. The 'Minamata' (1956 to 1968) and the 'Thalidomide' (1958 to 1962) tragedies shocked the world, and the 'Aberfan' (1968) and the 'Flixborough' (1974) disasters were followed by major public inquiries which changed the style of British safety regulation. None of these events could have been feasibly foreseen by prior design studies. The significant point is that in each case there was a 'hiss-before-bang', but the operators and regulators failed

to recognise the telltales or, otherwise, chose to ignore them (See Appendix II).

The New Treatment accepts that nuclear engineering in Britain has attained a standard that can assure safety in the design of power reactors, given that such designs are subjected to comprehensive safety assessment, guided by properly informed engineering judgement and using, as appropriate, the methods of reliability technology now available. There is a proviso that such assessment must be a continuing process through design, construction, commissioning and operation of the plant until it is eventually shut down, conducted in intimate association with monitoring for human errors, 'evidence of loss of resistance to failure' and any suggestion of 'hiss-before-bang'. Despite the fact that the effective operational hazard can be reduced to a near zero risk, there is no treatment that can guarantee absolute safety. There is always a remote chance that some unforeseen event may break through the safeguards to disaster, but so rarely would this be the case that it is a tolerable risk like that of the ever present threat to Holland of a catastrophic inundation from the sea, a disaster that has happened only twice in the thousand year long history of the Netherlands.

11.3 'Defended Safety' - a holistic concept

The dilemma of public aversion to exposure to the unfamiliar, potential hazards of new technologies on the one hand, and the need for continuing technical progress on the other may appear at times to be intractable. In the case of the exemplar, nuclear power, opposition seems to be hardening, rather than being allayed (See Section 5.4.1). Attempts to escape from the dilemma by using risk-benefit analyses that purport to show that a risk is of no consequence because it is numerically very small in comparison with other risks have been less than conspicuously successful. The fact is that quantification of a risk already acknowledged to be minuscule is of little relevance to the basic cause of public unease, attributable in the case of nuclear power to the peculiar nature of the threat.

Risk-benefit theory assumes that people form their attitude to a risk in proportion to their perception of the utility which it is assumed they associate with it and can weigh against the magnitude of the hazard. W. D. Rowe (1979) has suggested that the theory breaks down when the proposition is tested in reverse and the undesired

consequences become the measure. And, this is the case for nuclear power: avoidance of unwanted consequences is equivalent to averting a risk. The detriments of a nuclear power program have been widely publicised, the threat is thus clearly recognised and feared and the benefits still far from obvious. The early promise of limitless, cheap power from the atom has proved to be empty. People see no reason then to accept apparently unnecessary and grave risks which it has yet to be shown can be made negligible.

The novelty of the new technologies rules out any historical bases for risk toleration of the kind established for certain common hazards, mainly those of transportation or the ones that arise in traditional industries and practices, such as deep sea fishing and coal mining and of medical intrusion into the body. Nevertheless, a risk will be accepted if people are convinced that, not only is it very small, but that there is a credible organisation which, 'through due process', is able to hold it to a degree perceived in the circumstances to be tolerable. Such is the case with surgery where the healing knife is used by hands known to be expert and trusted and verifiably guaranteed as such. It is the phenomenon of 'Defended Safety'. The perceived dangers have not been abolished or argued away but are effectively held at bay. This has been achieved in a number of industrial technologies that also place the public at risk, safety being defended through the agencies of air pilots, ship masters and others whose competence is properly licensed.

Attempts to induce the public to think that nuclear power can be made intrinsically safe by ingenious improvements in design or by introduction of a sophisticated system of computer control would be less than honest. Intrinsic safety is unattainable because the danger is inherent in the process, safety being dependent on a dangerous entity being held in check by engineered safeguards. Despite that, the technology should be accepted as adequately safe, if its safety can be seen to be effectively defended.

11.3.1 The relevance of 'human factors' and accountability

Up to this point, the hardware and control systems of nuclear power technology have been treated as its major safety features. Prima facie, this is the case. Notwithstanding that, the human organisations that design, build and run the plants are no less important; they receive scant attention, yet their proper functions are essential to the assurance of safety which is a unitary and holistic state. For instance, the Reator Safety Study makes only brief reference to the effect of 'human error'. Again, in British practice the allusion to

the 'human factor' made by A. Aitken (1977) is typical. Both approaches identify man as a subservient attendant on the machine, but one whose unfortunate errors can upset its normally smooth working. Hence, by greater automation and computer control the 'human factor' may be eliminated.

The reliability of human performance in activities of a routine kind is notoriously uncertain owing to boredom and transient disturbances of mental state. The proper role for automation and the computer is to relieve the human brain of routine tasks and to handle information. But, for it to reduce man as operator to a mere machine minder is to court danger by depriving the system of human intellect as a high-level information processor and decision maker on call in an emergency.

The artefact is more than an assembly of its physical parts and safety cannot be assured through engineered safeguards and automation alone. The reliability of the plant is dependent on the exercise of human skills and ingenuity throughout all its stages of design, construction, commissioning and operation. Defended safety is thus the holistic outcome of all those human efforts aimed at safety and reliability, but inadequacy, ignorance, incompetence or negligence in discharge of these functions can frustrate the most cunning of protective intentions. The concerned public are fully aware of the fact that the required standards of dedication and consistency of behaviour are not innate in human nature. There must, therefore, be clear evidence of a credible function monitored by a trustworthy organisation open to public scrutiny able to establish the accountability of those responsible for nuclear plant safety. The principle has been identified by Talbot Page (1979) as 'Keeping Score' in his actuarial critique of the 'Zero-Infinity Dilemma' that faces the insurance industry (See 8.3.1.). Further, such accountability is neither a self-initiating nor a self-fulfilling function in a corporation responsible for creating a major technological risk. Instead, experience shows that large corporate entities suffer from strong centripetal tendencies, and not least internally, whereby the various units providing specialised services within the body exhibit sectarian trends towards agglomeration into discrete interest nuclei with minimal inter-group contacts. This is the antithesis of unitary corporate functional accountability and, in the case of a body charged with management of a hazardous plant or process, can lead to serious 'loss of resistance to failure'. Verification of the necessary unity, accountability and efficiency of the internal

integration of the corporate functions can only be provided by independent, disinterested, externally directed surveillance which is the proper task of inspection, a topic discussed in some detail by the writer in his paper, 'Technical Progress, Safety and the Guardian Role of Inspection', which is Document No. 4 in the Annex. The question of circularity raised by J. R. Ravetz (1974) may be answered by the ultimate national inspectional authority of a democratic parliament, acting independently of the executive arm of government.

11.3.2. 'Bootstrapping' and 'Defended Safety'

The problem of determining societal and personal risk imposition is not new. Georgius Agricola (1494-1555), metallurgist and minerologist, is quoted from his work, 'De re metallica', published in 1556, by Baruch Fischhoff et alia (1981) as proposing that activities which would create risks greater than those associated with those experienced in some 'pre-existing natural state' should be prohibited. The concept of risk acceptance by reference to past experience is described by the same authors (ibidem) as the technique of evaluating the acceptability of currently proposed risks by comparing them with the level of risk tolerated in the past. The assumption is made that society has been able to reach a nearly optimal balance of risks and benefits for particular technologies and that this experience can be codified into historical standards to be used as comparisons in future risk-involved decisions. It is described as 'Bootstrapping' when used to justify the acceptance or imposition of a new risk attributable to the introduction of an innovatory technology, e.g. nuclear power. B. Fischhoff and his co-authors (ibidem) identify two other main approaches to technological risk management, namely:

> Professional Judgement - employing the expertise of engineers, safety scientists and other informed authorities in decision making about the level of risk that can be imposed or may be accepted as the result of technical innovation. This is a common regulatory approach to the management of the exposure of workers to industrial toxins and other noxious things.
>
> Formal Analysis - theory based procedures for the modelling of risk problems and calculating the best decisions therefrom. Cost-benefit and decision analyses are the best known methods.

In the ultimate all scientific methods of risk management reduce to 'Bootstrapping', because they are attempts to win societal acquiescence to official plans to introduce a new risk. This requires the assessor to

establish that it will not impose one significantly greater than that associated with some already existing comparable risk or risks. Overt approaches of this kind are those of F. R. Farmer and N. C. Rasmussen made in connection with the nuclear power risk (See Section 7.2 and 7.3). The quantitative risk assessments calculated are used for comparison with statistical tables of current causes of mortality among the populations likely to be exposed and in the nuclear case are orders lower (N. C. Rasmussen 1975 - 2, F. R. Farmer 1975). The verity of these results is not in dispute, but they pertain to design and not to the reality of the operational entities. They are, therefore, not 'true' values, a point made in Section 8.4.9 above.

In quantitative terms, it seems that there is general agreement that any hazard bearing a risk threshold of less than 10^{-5} chance of death per year to the individual, unless it provides no discernible benefit or can be easily reduced, is ignored by those exposed. While the 10^{-5} threshold may have a historic basis, it cannot be applied to unquantifiable risks, nor should it form an immutable fiducial value. It is desirable that human life should be made safer and longer and the decision criterion for risk toleration or imposition should not be formally related to some historic standard but should follow a trend to reduce all risks. It is keeping with public expectations and desire for 'a taste of immortality'.

A matter of major political interest in risk management is that humans are concerned not to be unnecessarily or arbitrarily exposed to a risk for which they see no sound or immediate reason to tolerate. The cogent fact is one of assurance that the risk can be maintained below the threshold at which it may be ignored. In the case of exposure to risks from major hazard industries, and in our case nuclear power, this depends upon the establishment of public confidence in the maintenance of the engineering reliability and, thus, safety of the system presenting the hazard.

It is recognised in the insurance industry, and elsewhere in engineering circles, that a risk created by a plant built to a sound and proved design in the hands of competent operators is virtually zero in spite of any grave intrinsic hazard possessed by such an entity. This is the actuarial 'zero-infinity dilemma' (See Section 8.3 et seq.) in which circumstances safety is effectively assured but cannot be made absolute because of a vestigal risk that is intractable. Therefore, in the face of the most detailed provision of engineered safeguards, of

instrumentation and control systems and of managerial arrangements, there remains the possibility of a catastrophic accident of unforeseen causation that can circumvent those defences because of gaps in their continuity due to 'ignorance of mechanism' and, not least, to human fallibility. Inerradicable factors in the potential causation of these disasters set an ultimate limit to the tolerance of technological hazards because no risk which could have genocidal consequences in the event of an extreme accident is acceptable. While devastating losses of life and property about the environment of a hazardous plant could be borne by society, an accident with an outcome that could destroy the major part of its population or property could not. This is the ultimate criterion for technological risk acceptance (17).

It is of little avail to hope to assure a permanent state of virtual-zero-risk in a nuclear power plant by pursuit of excellence in the artefacts of its engineering alone. Assured safety is a unitary combination of the physical system and human factors essential to its creation and use which must continue through design, construction and operation. Therefore, the New Treatment envisages the possibility of a nuclear power program of virtual-zero-risk to the environment and public by establishment of an accountable regime of a continuing, dynamic defence of safety in which any tendency towards loss of resistance of the system to failure can be detected and countered. The plant is thus seen as a vital entity comprising all its parts, physical, organisational and human whose proper interrelations are conducive to a maximum of safety through reliability of function. It is not possible for an entity to sustain such a state in isolation by virtue of its internal efforts alone owing to the drift towards increasing disorder and lethargy caused by its inherent entropy. The continuing assurance of safety is in consequence dependent on external surveillance by a discrete and independent agency which can be identified as inspection. The topic of engineering inspection is central to the theme of the writer's published works offered as Documents No. 3 and No. 4 of the Annex, and is further discussed in Section 14.

11.4 Synoptic Overview

The text so far has attempted to describe the modern techniques of risk management and safety engineering in their historical and cultural settings. Attention has been directed at the catastrophic LPEs that are the consequence of failures in the sophisticated systems of today's innovatory technologies, and in nuclear power plants in particular,

which have become matters of great concern in the advanced Western countries. The existing approaches intended to control these events, traditional, qualitative and quantitative, have been reviewed and the risk theories underlying them examined. Although they have made notable contributions to the safety and reliability of the technology, none of them have provided fully satisfactory evidence of a capability to assure the concerned public that nuclear power is an acceptable risk. It has been to satisfy this desideratum that a new treatment of low probability events has been researched and developed.

The New Treatment is not fundamentally divergent from the leading approaches that currently exist which include the long-standing qualitative design criterion of a maximum accident and the quantitative methodologies of risk evaluation of the kind originated by F. R. Farmer and his associates in Britain and by N. C. Rasmussen in the U.S. Reactor Safety Study. Despite the adverse criticism directed at it, the design concept of limiting fault sequences leading to some postulated, catastrophic system failure, namely a design basis (DBA) and a maximum credible (MCA) accident, has not been discarded. The conflict of choice between these qualitative and quantitative methods has been shown to be illusory and can be dismissed by an approach that embodies them both. In pursuit of this, the reliability and the quantitative safety analyses are seen as essential adjuncts to the qualitative design concept which provides an ultimate engineering decision criterion. Furthermore, the need for identification of those responsible for safety relevant decisions at all levels of management and performance, for the strict accoutability of those who take them and for democratic public scrutiny of any such major safety regime are advocated as essential for the winning of public confidence in the defended safety of nuclear power.

The societal effects of the rapid advance of technology during the second half of the Century and the growing divorce between the 'Two Cultures'; one, the arts, law, politics, the academic philosophies and administrative practice, and the other, science, technology and engineering; on the approaches to safety and reliability have been considered. The cultural disjunction has encouraged recourse by generalist decision makers in the economic and political establishments to quantitative decision methodologies when faced with complex problems in matters technological and, not least, in the affairs of nuclear safety where it has had less than conspicuous success.

The safety of a sophisticated and potentially hazardous plant is a dynamic rather than a static state. It is, therefore, necessary that

it be maintained and 'defended' by the alert and active participation and acceptance of responsibility of all concerned in its design, construction and operation. This state of safety depends upon a continuing, unitary, holistic combination of the relevant physical and human factors that make up the system. Such a condition is not an intrinsic property of any complex artificial system. It will instead exhibit, to a greater or lesser degree, those centripetal and entropic tendencies from which no human social organism is free. These tendencies are inimical to the maintenance of internal cohesion and integration of safety routines. Any drift towards schism, lethargy and disorder reduces safety. To counter such trends, intrusive surveillance by an independent and disinterested authority is required. This corrective which may be identified as inspection is treated in detail in the Annex and later in the text.

An attempt has been made to identify the salient elements that could make for a more credible structure for safety in nuclear power engineering. Among those of direct relevance to the New Treatment are:

1) To use the MCA/DBA concept in association with the powerful methods of safety and reliability analyses that now exist to ensure that nuclear plant design in all respects meets adequate criteria, quantitative where applicable, to establish that the discernible, potential modes of failure of the plant are identified and the overall design modified to ensure that they may be classed as 'incredible'. It is proposed that this be achieved by a design orientated towards intrinsic safety or, where this is not achievable, by failure sequence blocks that employ engineered safeguards, control and instrumentation limiting parameters for alarm and shutdown, redundancy and administrative controls.

2) The failure sequence criterion of 'incredibility' in quantitative terms is defined as the probability of failure for the system in question, e.g. a burst-duct/channel-fire catastrophe given a Magnox reactor. It should be not greater than 10^{-6} per year which is Borel's limit beyond which an event is too rare to happen in human experience.

3) In meeting the two foregoing requirements, the risk of a foreseeable reactor accident is reduced to a virtual zero and the chance of its occurrence, given the inviolability of the assumptions on which the forecast is made, may be ignored. Nevertheless, an LPE that has not been foreseen in the design analysis that has a finite, but indefinable, probability through ignorance of mechanism may still occur. An analogy has been drawn with noise theory in which the occurrence of such a disastrous LPE may be seen as an anomalous spike in the mundane flow of the normal event-stream of faults, failures and occasional minor accidents. It is argued that the event-stream if properly reported, collated and analysed could show divergencies and anomalies giving evidence of the loss of resistance to failure which is a normal precursor of a system failure, 'the hiss before bang'.

4) The information requirement of the immediately preceeding passage suggests that the plant's behaviour should be effectively monitored by its operators reporting all identifiable deviations from normality, namely faults, acts of maintenance, variations in operational program, and changes in the composition and responsibilities of managerial, specialist engineering and senior technician staff and any other such matters that might be of significance to safety. These Licensee Event Reports (LERs) should be agglomerated through a national reporting network and analysed nationally or, preferably, more widely.

5) The inevitable centripetal tendency of a corporate body to form discrete self-centred interest groups should be discouraged by the intrusion of independent, disinterested regulatory inspection applying to the whole system constituted by the plant, being hardware, software and its technical and managerial complements, to confirm the efficiency of operation and function and viability of the state of the organisation.

In application of the foregoing principles, the need for the standard of safety to be adequate, not 'safer than safe' must be kept in mind. The state to be attained is one of adequately defended safety which does not attempt to claim the absolute, but a level which may be recognised as one that reduces the perceived risk to one which may be acknowledged as virtually zero and thus be ignored.

Public confidence in this state of affairs can be secured by demonstrating the accountability of those responsible for its maintenance and by opening the safety mechanism to informed public scrutiny. The criterion of equivalence in 'Bootstrapping' whereby the assessed safety of the given hazard is compared with analogous risks of common experience is accepted as essential in any approach to risk management and, hence, not least, to that of LPEs. However, the Bootstrapping approach on its own is inadequate because there is no assurance that its requirements will be met throughout the 'at hazard' life of the plant. A design criterion of 10^{-5} per year of the chance of death or serious injury to the individual member of the public at risk is too high in the nuclear case. It should be at least an order lower to be compatible with the qualitative criterion of 'incredible'. Moreover, such a criterion is not immutable. It must follow the historic trend in safety which is to reduce all risks and, thereby, to secure for man a safer and longer expectation of life.

12 ENGINEERING DESIGN, 'EVENT-NOISE' AND THE MANAGEMENT OF LPEs

'When any great design thou dost intend,
Think on the means, the manner and the end.'

Sir John Denham (1615 - 1668),
Of Prudence, l. 186.

The feature that distinguishes the 'New Treatment of Low Probability Events' from the more conventional approaches to nuclear power plant hazard control and, indeed, from concepts of risk management for other major-hazard industrial installations is its attempt to be pragmatic in its philosophy. Whereas, the U.S. Reactor Safety Study (See Section 7.3 et seq.) which may be taken as the paradigm for the quantitative probability approach is largely an abstract study of those possible failure modes discernible in representative Boiling Water (BWR) and Pressurised Water (PWR) Reactor designs, the 'New Treatment' is empirical. It is more particularly concerned with the effects that arise in the construction and operation of plant than with contemplation of the design ideal per se.

By placing its emphasis on site phenomena rather than on design office meditations and mathematical studies, the 'New Treatment' is, essentially, an engineering approach and, thus, an attempt to identify and extend the pragmatic methodology that has evolved in the line of the Design Basis (DBA) and Maximum Credible (MCA) Accident concepts of nuclear hazard management. Nevertheless, the 'New Treatment' does not eschew the important contributions to safety engineering attributable to reliability technology. It involves a philosophy of risk management centred on quality in engineering, defended by inspection (a theme developed further in supporting Document No. 4 of the Annex) rather than on the exhaustive and largely mathematical analyses of design. Nonetheless, it accords to design its due place in the theoretical structure of engineering where it is nothing less than the keystone of the art (infra).

The 'New Treatment' is also at variance with a widely canvassed proposal to substitute a computer dominated, rather than assisted, regime for the judgement of control room engineers in a plant accident emergency. The idea is that a software program should override immediate operator actions taken to overcome the fault and contain the damage to the reactor. This view together with some portentous ideas about regulation and inspection has been put more explicitly by an eminent safety scientist and former Director of Nuclear Safety in the U.K. Health and Safety Executive. To quote him:

(On the management of emergencies)

'Emergency procedures start in the control room. As far as the plant is concerned they should be fully automatic for the initial phase of perhaps half an hour and it is sometimes argued that the operator should be physically prevented from intervening during this time.

... ...

(On inspection)

There is a ... ... rather quaint opinion to the effect that inspection is the primary source of safety. ... ... but it is not, I fear entirely true. Certainly, the new look which an inspector can give to a situation which has become over familiar to the operating management enables safety issues to be raised and improvement suggested. But I suspect that these improvements are essentially marginal.

... ...

(On the importance of theory in regulation)

Perhaps, ... the regulatory bodies should be moving away from detailed studies of the safety of individual designs of plant and towards the assessment of the knowledge and understanding of physics, chemistry and engineering of that plant by designers and operators.'

H. J. Dunster, CB,
'Some reactions to the accident
at Three Mile Island',
Nuclear Energy, June, 1980, 19(3),
pp. 139 - 142.

While the foregoing opinions are not in themselves new, having formed the subjects of a long-standing debate on nuclear power plant management, it is only recently that they have been given such explicit expression. The significance of the above pronouncement is to reduce the role of the site engineers and their technicians in favour of stipulated routines at the expense of immediate intellectual involvement in the control of the plant. For instance, Dunster's hint has more recently been given official force by advocacy at the Sizewell PWR inquiry by Central Electricity Generating Board representatives that expert human operational decision functions in a reactor control room during an emergency should be superseded by a computer program (Gittus and Matthews 1984). The strategy for management of a plant emergency could thus become a matter of prescriptions in decision methodology formulated in a design office remote in space and time from the reactor in trouble. His advocacy of theory and rejection of empiricism is

extended to inspection and regulatory practice. It is an example of the profound disjunction that can exist between science per se and engineering (See Sections 8.1, 10 and 10.1).

12.1 On the nature of engineering design

There are few concise and explicity definitions of engineering design, although Lord Kings Norton (H. R. Cox 1973) was not alone in recognising 'the art of design as the pinnacle of the whole structure of engineering'. Despite the approbation, design has received less than due attention in the education of engineers. Professor R.E.D. Bishop (1963) has suggested that there are three discrete processes in industrial design which are:

i) Conception: visualisation of the intended artefact and formulation of possible approaches to its creation, utilising as appropriate those analogies that are known;

ii) Analysis: study of the feasibility of these approaches in the light of scientific knowledge, workshop and other construction technologies, prior experience and cost; and

iii) Synthesis: the process of attaining the design objective, taking the appropriate utility factors into account, such as economics, reliability, ergonomics, siting, safety and aesthetic styling.

The end product of the design activity is a set of plans, drawings, specifications, consisting-of schedules and construction, commissioning, test and operating instructions. At this point none of these things exist in the form of matter, but as information as marks on paper or held in computer data banks. Design is thus differentiated from the other creative activities of engineering in that the work of the designer is separate from its realisation and can remain indefinitely in the realm of ideas. The implementation of a design is to attain correspondence between the concept and the artefact it is intended to create. There is, therefore, a discontinuity through which the action of design and its realisation must pass as it is interpreted in the light of engineering science and empirically established shop floor and construction site practice, a transformation depicted diagrammatically in Figure 8. The design is more than a scientific model as the process of artefact creation is holistic. Nonetheless, it is in essence incomplete because the designer implicitly assumes that lacunae will be made good in the light of the professional competence of the engineers and technicians who will read its prescriptions.

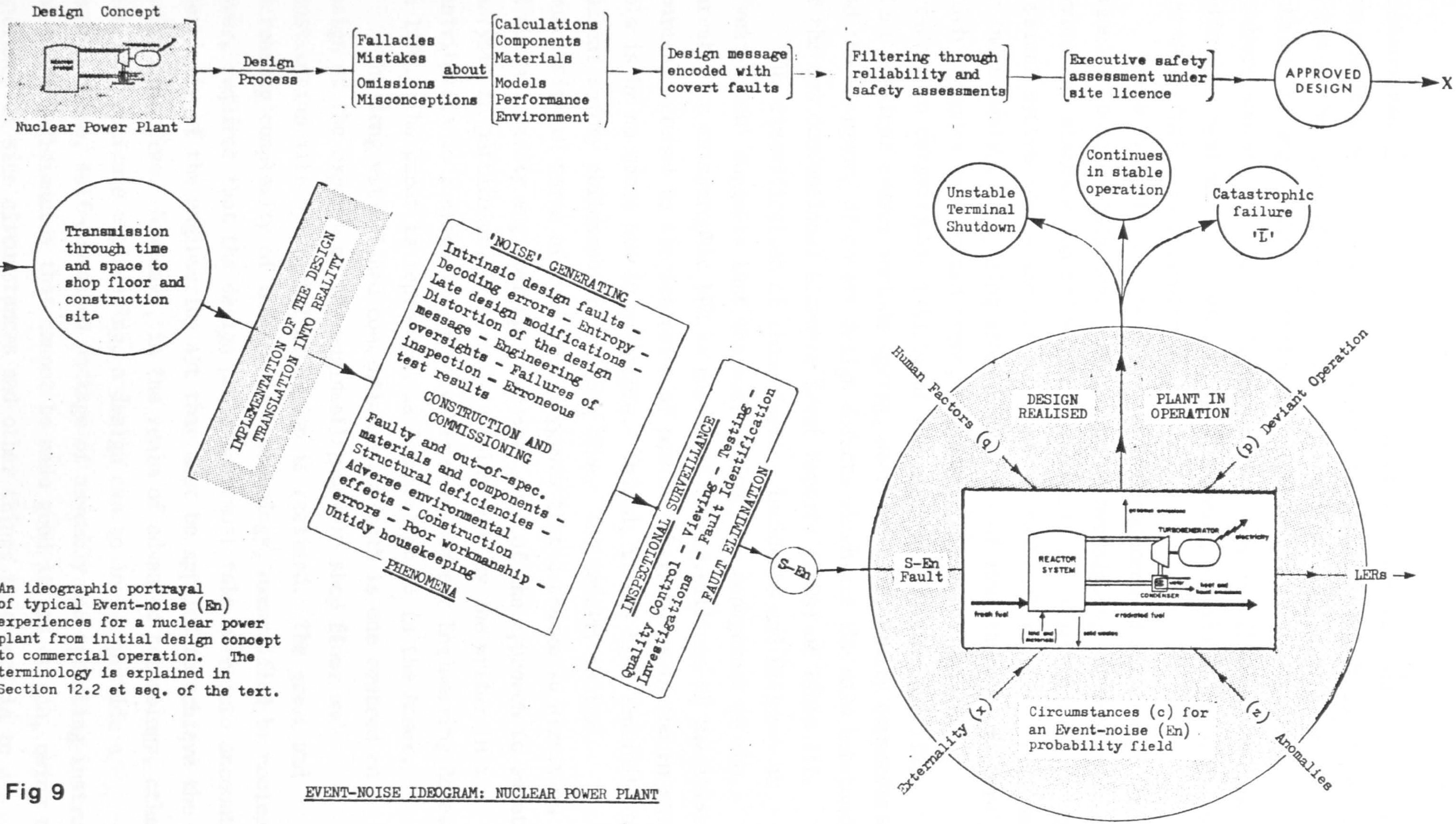
12.1.1 The Design-Hardware Transform and the concept of 'Event-noise'

The information held in the design is of the nature of a message to be transmitted through time and space for realisation as hardware at some point in the future. The construction processes are neither proportional nor reversible and are of the nature of mapping the design concept on to a field of matter, a transform that is both convoluted and non-linear. As for any signal passing through a non-linear channel, modulation and inter-modulation products are formed which add things that were not present in the original message or, conversely, certain details are ablated from the information content or otherwise distorted. The design message suffers further mutilation and accretes extraneous elements in its experience of interpretation on the shop floor and construction site, both environments of engineering assumptions, expertise and practice that may well differ from those taken for granted by the designer. Again, as the message ages during the leadtime, it suffers entropic decay of its meaningful content as some of its constituents lose their clarity or become incongruous in a situation remote from the original design milieu. The construction and commissioning activities that convert the design into an operating plant are shown diagrammatically in Figure 9.

In its transition from the realm of ideas to the reality of hardware, the distortion the design message suffers may be identified with the ubiquitous phenomenon of 'noise', namely those undesired effects that degrade the useful or wanted information in a signal. The plant after commissioning experiences further random effects that derogate from an authentic implementation of the design concept and disturb the steady circumstances of its operation. These latter things are the whole gamut of accidents and 'faults and incidents' to which some reference has already been made in Section 8.6.1 above. Taken together, all these random and unpredictable effects may be classed under a generic title of 'Event-noise'. Their existence is the chief factor that vitiates the assumption of stable distributions of failure rate and design-correspondence data implicit in attempts to make quantitative predictions of nuclear power plant risks, at least within meaningful confidence intervals.

12.2 Philosophy and implications of 'Event-noise' theory

Of salient importance in 'Event-noise' philosophy are its holistic implications. The 'plant', or synonymously the 'installation', is a societal thing that extends beyond the physical bounds of its



An ideographic portrayal of typical Event-noise (En) experiences for a nuclear power plant from initial design concept to commercial operation. The terminology is explained in Section 12.2 et seq. of the text.

Fig 9 EVENT-NOISE IDEOGRAM: NUCLEAR POWER PLANT

hardware and the electronics of instrumentation and control to embrace the people concerned with its creation and use. The plant is, therefore, a system that combines organised human intellect in the necessary echelons of engineering expertise and technical skills with that hardware and its ancilliary elements. 'Event-noise' (En) may thus be defined as systemic phenomena, each event being a disturbance affecting the whole entity to a greater or lesser degree.

These systemic phenomena are the consequences of management and organisational misjudgements, mistakes and oversights; job performance errors and slackness on the part of personnel; specific failures in the physical system itself and the intrusion of external factors. Together or individually, they bring about that 'loss of resistance to failure' which precedes an untoward event, ranging from a minor industrial accident to catastrophic failure of the plant or system. Specific plant physical causes include ageing, wear-and-tear, faulty components and the emergency of covert design defects which are the main substance of the now conventional Licensee Event Reports (LERs) of Table III.

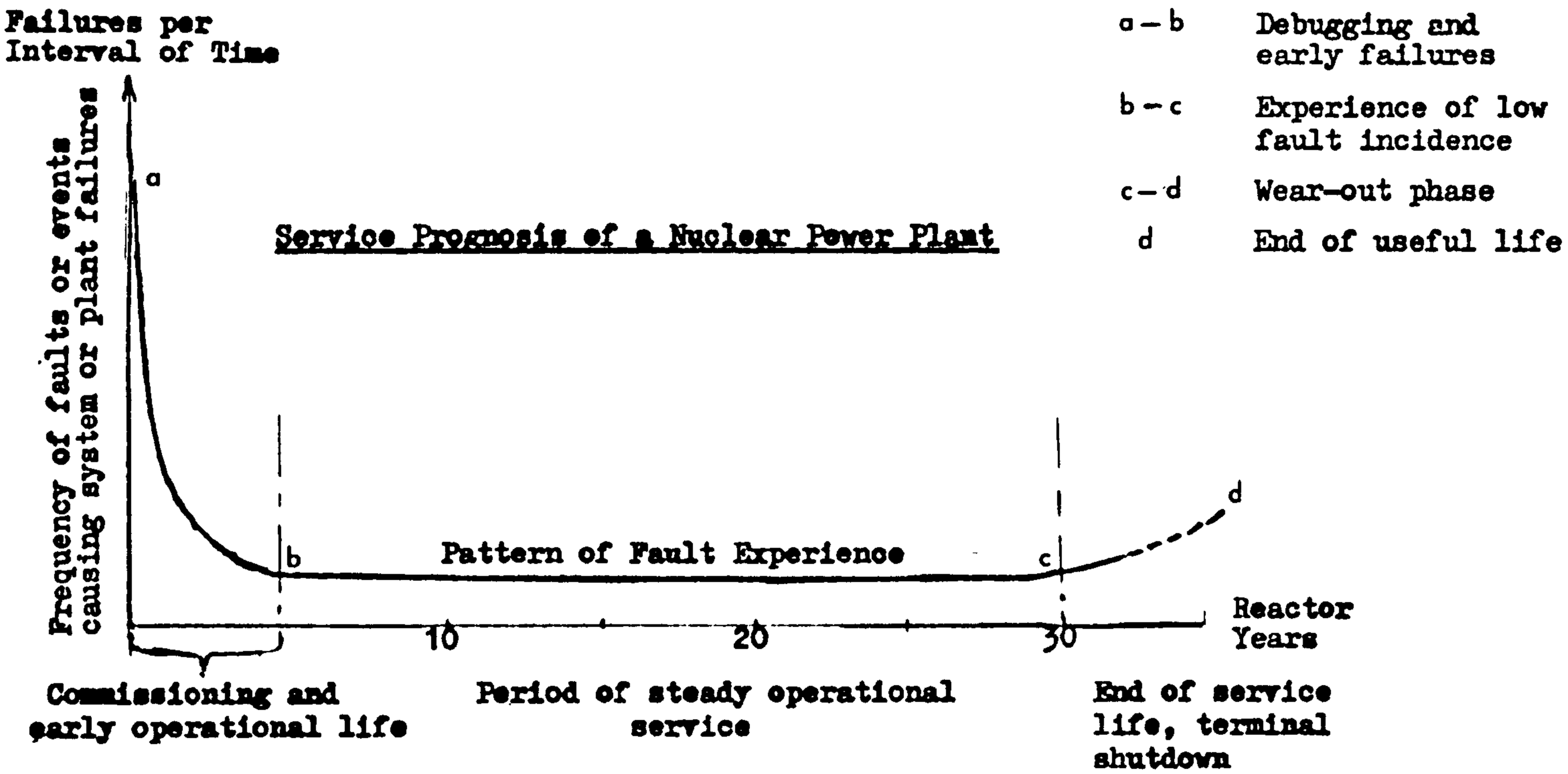
The classification of those faults, incidents and failures as 'Event-noise' suggests that the most efficaceous management of the threat of a catastrophic LPE is one based on surveillance of the noise sources, attuned to the detection of possible harbingers in the En stream. This is by no means new in principle. Indeed, it has been implicit in nuclear safety philosophy for a long time. The novelty is its enunciation in terms of En. This suggests that a change in direction of nuclear safety engineering in general, and of the approach to safety analysis in particular, is needed, a point made by the writer in a contribution to a symposium on 'Directions in Nuclear Engineering Research' in 1980. The paper is reproduced as Document No. 3 in the Annex.

The long established conventional approach is one centred on design at the expense of the engineering on the shop floor and construction site by which that design is realised. The great and increasing complexity of modern high-technology, exemplified by nuclear power, requires that the design philosophy must take more into account the parity of the engineering art that must be applied to achieve the design objective. Nowadays, in the realm of advanced technology, other than for replicate engineering, a design can no longer provide a comprehensive, self-contained package of assembly and operating instructions. There are deficiencies that cannot be made good at its origin, owing to ignorance of site circumstances and other things that pertain to a situation remote in time and immediate technology from it. The design

message is, therefore, incomplete in itself, an insufficiency made worse by the noise processes that mutilate it. The lacunae have to be made good by ad hoc engineering skills during the construction process. This is a further example of the growing disjunction between 'The Word' and 'The Deed' which, as Auguste Comte (1825) opined, is the task of engineers of the scientific class to bridge (See Section 8.1).

12.2.1 Categories of Event-noise

The above organic inadequacies in the design message are noisy per se because they complicate the task of its interpretation. In the phenomenon of Event-noise two kinds may be distinguished, namely 'Static Event-noise' (S-En) and its counterpart of 'Dynamic Event-noise' (D-En). The former, S-En, is seen as static because it originates in the design process itself due to flaws in theory, erroneous conceptions, mutilation by 'noise' during encoding, transmission and decoding and oversights in engineering on site. It is in a sense timeless, describing latent effects that are not brought into physical existence until the design is implemented in the operational plant, but the definition is by no means hard and fast. On the other hand, D-En is constituted mainly by the flow of mundane day-to-day accidents and failures with the occurrence of an occasional disastrous 'spike' in the form of a major incident (See Section 8.2 et seq.). The phases of commissioning and early operation are 'noisy' periods in the life of a nuclear power reactor, being plagued by a host of minor failures that are, for the most part, of S-En origin. The faults that cause them, together with other defects that have become patent, are rectified by a process known as 'debugging', their progressive elimination being responsible for the steep negative gradient of the initial part of the 'Bathtub' reliability curve shown in Figure 10. However, not all the S-En defects appear at such an early stage and, for this reason, fail to be eliminated. The residuum is a most important sub-class of S-En covering many things that remain as covert weaknesses that can long lie dormant in the system. Owing to some odd transient disturbance or tension, one can precipitately emerge and interact with faults or incidents of the dynamic kind to cause a severe failure sequence. The low probability, but disastrous potentiality of the main pressure vessel of a Pressurised Water Reactor (PWR) to fail catastrophically by the sudden progressive propagation of an undetected crack in its steel membrane (A. Cottrell 1980, 1982) may be cited as an example of the precipitate emergency of such a hidden flaw from the cache of residual S-En.



Service Prognosis of a Nuclear Power Plant

a – b	Debugging and early failures
b – c	Experience of low fault incidence
c – d	Wear-out phase
d	End of useful life

Bathtub Curve

Fig 10

The disturbances of the second kind, classed as 'Dynamic Event-noise' (D-En), continue unceasingly throughout the operational life of a nuclear power reactor and, indeed, that of any other major industrial installation. Such failures of components, equipment, structures and systems which may be combined with other accidents, often involving personnel as well as plant, are typical of the 'fault and incident'data returned to nuclear regulatory bodies and collation and analysis centres as 'Licensee Event Reports' (LERs) of which an excerpt is reproduced in Table III and are reviewed in Note 15. LERs for the most part concern things of a mundane nature analogous to the common pattern of electrical circuit noise. This is the characteristic stream of random, weak impulses, occasionally punctuated by irregular, short surges of much greater energy, such noise being an innate feature of communication circuits. These disturbances can mutilate and degrade the message carried by a signal.

The most energetic of the impulses may be compared with the occasional serious events that interrupt operation or damage a plant, harm people on its site or involve combinations of these things. These 'spikes' of Event-noise include the rare Low Probability Events (LPEs) that have precipitated the disastrous accidents summarised in Appendix II. As mentioned above, events of this kind are often caused by a combination of D-En with the latent design or in-built plant defects characteristic of residual S-En. Take, for instance, the serious design error that permitted a confluence of unseggregated essential service and control and instrumentation cables to run together in the Browns Ferry nuclear reactor cable vault. A fire started on the insulating sheath of a cable by a carelessly placed candle used for draft detection spread rapidly through the web in the cable vault, progressively disabling the reactor control circuits. The fire was only brought under control in time to prevent a severe reactor accident and, incidentally, by an operator's initiative in violation of certain plant operating rules.

12.2.2 Event-noise sources

Event-noise (En) in a nuclear power program has some six identifiable and distinct sources. Being no more than potentialities held in a nuclear power plant's design package, En obviously cannot reveal itself before the construction program is underway. Despite that, many of the 'noisy' factors that would make for weaknesses in the

plant and its systems or be sources of potential failures can be eliminated from the design by safety analysis to the extent that the efficient factors are discernible. Yet, the analysis can never be complete and is particularly open in the case of a novel design. A residuum of undetected design flaws can thus pass into the constructional and operational phases of the plant's existence as latent causes of failure, for instance, a part weak because it is made from the wrong material, corrosion because a component is not compatible with its environment and so on.

The common sources of En in nuclear power plants may be identified as:

(i) The Design Process: a potential source of S-En

Fallacious theory, misconceptions, 'ignorance of mechanism', false assumptions about operational and site conditions, paucity or irrelevance of data, calculation errors, omissions in conceptual sequences and defective models. Many of these things can only be recognised by experience in use and become S-En by slipping through the nets of safety and reliability analyses. The design process therefore does not produce En per se, but has the potentiality for the creation of S-En.

(ii) Theatres of design implementation: the main source of S-En

Failure to apprehend fully the design instructions, ablation or distortion of information during transmission and receipt of the design message, inapposite substitutions for lack of material and equipment as specified, inadequate design specifications, construction errors, bad workmanship, poor engineering, supply and material anomalies, consequences of industrial action and mischief.

(iii) Running-in: the early phase of commercial operation

The most prolific theatre of D-En and is characterised by the steep downward slope of the initial part of the 'Bathtub Curve' in which elements of S-En come to light as faults and incidents and are rectified. Reduction of the rate of En to a steady and acceptable level is a sine qua non for normal commercial operation.

(iv) Commercial operation

The En plateau in the 'Bathtub Curve' of Figure 10 characterises the usual run of operational faults, incidents and accidents as described in Licensee Event Reports (LERs), a sequence of mundane events that may be expected to continue throughout the useful life of the plant, except for occasional interruptions for maintenance and overhauls and hiatuses due to the rare incidence of major faults. Commercial operation is, of course, the main theatre of D-En.

(v) Maintenance and modifications

These two procedures aimed at reducing En are not infrequently agencies for introducing potential faults and weaknesses and, as such, are a source of further S-En.

(vi) Externalities, Anomalies and Singularities

These are the unusual, unforeseen and unexpected external events and internal agencies among which are electricity grid failures, severe environmental conditions, catastrophic external circumstances such as earthquakes, falling objects, missiles, maloperation, incompetent engineering and other human errors and capricious mistakes outside the normal ambit of operational experience which can produce 'spikes' in the flux of En of magnitude ranging from a temporary shutdown to a catastrophic failure. Although extraordinary, these events should be classed as D-En.

Event-noise is ubiquitous in industrial plants and processes. Nonetheless it is logical to infer that the quieter a plant, the greater its presumed reliability and safety. Finally, the concept of Event-noise has analogies with that of 'reliability degradation' in conventional reliability engineering (18), identifying broadly the same factors. Consequent upon the grave potential hazard, the standards of safety and reliability in nuclear power engineering have been impressively high from the beginning. Although in no way an acknowledged aim, the result of the endeavours made to attain them has been to reduce that potpourri of detrimental effects here called Event-noise to a minimum. The S-En component of this medley has been managed by various methods of technical design safety assessment that, latterly, have been strongly influenced by quantitative probability philosophies. The D-En fraction has been largely controlled by monitoring the engineering activities on site. Nonetheless, it has not become an integrated engineering approach and has remained largely inchoate.

What guiding philosophy there has been has tended to be scientistic rather than pragmatic in a situation that has more to do with humans and hardware than with speculations about risk theory. Less than due interest has been shown in the realities of day-to-day operational experience, a trend to which attention has been drawn in the introductory passages of this chapter. Furthermore, the writer has identified a co-ordinated approach, which he regards as essential in securing the acceptance of an adequately safe nuclear power program, with efficaceous engineering inspection. That matter is discussed at some length in his

paper on the topic offered as Document No. 4 of the Annex, and the hypothesis made is developed further along quasi-mathematical lines in the passages that follow.

12.3 The Event-noise stream: Characteristics and singularities

The sources of Event-noise (En) have so far been examined descriptively. So to recapitulate briefly, the two principal elements of En are a 'Static' or latent component, S-En, created by the interaction of the design with matter during the processes of construction and commissioning a nuclear power plant, and 'Dynamic' constituents that are mainly created during the course of its commercial operation. In addition to the foregoing, the plant may experience the occasional intrusion of 'Externalities' which are those unusual happenings that occur without the site, but produce marked effects within it, and 'Anomalies' which are events of extraordinary causation often being the result of some uncharacteristic human error. Among the latter contributions to the En flow may be included those rarer 'spikes' or 'Singularities', otherwise Low Probability Events (LPEs), that may be associated with major plant damage, the consequences of which range from a shutdown for repairs to a catastrophic radiation accident.

12.3.1 The Event-noise concept and the Reactor Safety Study

A comparison of the Event-noise approach with that of the U.S. Reactor Safety Study (See Section 7.3) is of interest. In the latter work, representative designs of the Boiling Water (BWR) and Pressurised Water (PWR) Reactors were exhaustively and imaginatively analysed in order to construct 'Event Trees' and 'Fault Trees' from which the probabilities of failure sequences could be deduced. An 'Event Tree' presented the course of events from an initial failure within the plant to its consequences in a postulated radiation accident, ranging from minor to catastrophic. A spectrum of 'Event Trees' for the given reactor type covered all radiation accidents judged to have a feasible mechanism of occurrence. The likelihood of each failure sequence in the 'Event Trees' was then calculated in terms of its numerical probability from the corresponding sequence in a relevant 'Fault Tree', using failure rate records collected in specially maintained and serviced data banks, the required material being synthesised where none existed (See Section 9.7.3). An attempt was made to allow for 'Externalities' and 'Anomalies' (supra) respectively as extraordinary faults and 'human error', but this presented almost intractable

difficulties in quantification owing to the very arbitrary and capricious nature of errant human behaviour and the rarity of the former.

While the approach is rational, the philosophy underlying the Safety Study, differs fundamentally from that of the Event-noise approach, the latter effectively starting where the former ends. The Study is a meta-assessment of representative designs of the BWR and PWR that had already in their prototypes been exposed to that process of incisive safety assessment which has long been established practice in the Western nuclear industries in the preparation of a 'Safety Case' supporting the claim for the reliability and safety of the design (J. F. Ablitt 1960). Therefore, no nuclear reactor design with discernible features that were credibly unsafe or unreliable would have been presented to the Study's analysts. Consequently, those accident sequences revealed by its processes of further exhaustive safety analysis would either be of very low probability or obscure or both or, otherwise, they would have been eliminated by a further refinement of the design. As argued earlier in Section 9.6.1 and in the appraisal of quantitative probability methods in Document No. 1 of the Annex, those unlikely failure sequences that remained after this hierarchy of scrutinies would be so rare that they could not happen in realisable plant experience because the probability is metaphysical. Despite that, there is the reservation that some unpredicted event might happen instead and not in the manner conjectured in the analysis.

The Event-noise approach accepts that a design subject to such searching safety analyses is safe enough per se and, given satisfactory quality assurance during construction and commissioning, can produce a plant that is, prima facie, adequately so. The rare chance of a catastrophic accident cannot be absolutely excluded despite the elaboration of safeguards, for instance an element of S-En not perceived during the processes of design assessment and its implementation in the constructed plant may have escaped detection. The net risk is indeterminately small, but still finite. It can, nonetheless, be made tolerable because verifiable arrangements can be devised that are able to secure the safety bastions, a matter to be dealt with in some detail later and particularly in Section 13.

Although as a result the true risk may be made demonstrably negligible, it is still not zero. There is, moreover, an essential reservation. A design that holds the clear threat of an unacceptable

accident (17), however remote the credible chance of its happening, is not tolerable in Event-noise philosophy. Despite the fact that the assessed quantitative design probability be metaphysical, an unsuspected fault sequence might exist that could bring it about. This does not preclude the possibility of a credible engineered safeguard that could absolutely prevent such an eventuality as suggested in Section 8.4.3 (Kirk and Taylor 1971). The implications for siting policy and choice of reactor system are not dealt with here.

12.3.2 An analytical treatment of the Event-noise concept

An attempt to put Event-noise theory in mathematical form may help to clarify the foregoing verbal descriptions, although it will have little quantitative significance at this stage owing to unresolved mathematical problems, but also because the necessary data is unobtainable by reason of commercial security and lack of collection and collation of certain essential elements. As defined, Event-noise is an ensemble of effects of diverse origin characteristic of a given plant that are indicative of disturbances in its performance, expected or capricious as the case may be. While the argument here will be confined to a notional nuclear power plant, it nonetheless applies to any large, technically complex industrial installation. Giving symbolic representation to the efficient factors and circumstances in the situations in which they take their effect, we can write the conditions leading to the generation of the Event-noise (En) emanating from the plant, thus:

Let e be the general En state of the plant at reactor-time, 't', in the particular circumstances, 'c', 'p' and 'q', owing to the peculiarities of its design, construction and operation, these circumstances being compounded by certain external conditions, 'x', and by certain anomalies, 'z', arising in its internal state, where, more specifically:

'c' relates to any lack of congruence with the design at the completion of the construction and commissioning processes prior to operation;

'p' is associated with the immediate situation on the site as it impinges on the design, its implementation and use of the plant, being such things as mal-operation, faulty maintenance or misconceived modifications as at 'Flixborough';

'q' is the result of 'human factors' and other related unusual conditions arising within the site or otherwise affecting it owing to management, personnel or engineering matters, say a vacancy in a key post as at 'Flixborough';

'x' is an Externality, being some physical factor which affects the state of the plant, but originating outside the site, say failure of the main electricity supply drawn from an assured external source, eg. the 'Grid'; and

'z' is an Anomaly, being a divergence from the normal, internal state of the plant caused by some abnormal intervention in its operation, say a strike or the arbitrary re-programming of the autopilot and change of flight plan imposed by the Air New Zealand administration of which the crew were ignorant that led to the Mount Erebus polar sightseeing flight disaster;

the above symbols being represented ideographically in the latter part of the Event-noise creation sequence shown in Figure 9.

Then, $e = n + s + l$ .....(i),

where 'n', 's' and 'l' are the D-En, S-En and 'spike' components of the given En experience at 't', and

$n = f_n(p,q,t)$ .....(ii),
$s = f_s(c,p,n)$ .....(iii) and
$l = f_l(s,n,x,z)$ .....(iv).

The latter term (iv), the 'spike' function, is the chief component of the Event-noise of interest here. It is designated as 'L', the Catastrophe-function, when it describes the plant's operational history of major En incidents up to the experience of a terminal event at some reactor-time, $t = T$.

If 'δe' is an undifferentiated element in the stream of En, then

$\delta e = \delta n + \delta s + \delta l$ .....(v).

Representationally, these differentials may be seen as derivatives over an instant, 'δt', a time short compared with the normal operational life of the plant, of the respective En generating functions.

Thus, $\delta n = f'_n(p,q,t)\delta t$ .....(vi),
$\delta s = f'_s(c,p,n)\delta t$ .....(vii), and
$\delta l = f'_l(s,n,x,z)\delta t$ .....(viii),

where f'_n, f'_s and f'_l are symbolic of the changing state of the plant with time and the other time dependent circumstances. The differentials, δn, δs and δl are representative respectively of individual En incidents,

namely mundane faults, failures and industrial accidents of D-En; the design associated events of S-En or the occasional 'spikes' of En experience that may, in rare cases, be the terminal events of catastrophic failure. Despite the simplistic representation above, they are very complex, multidimensional functions in design and operational space and cannot be properly represented on any two-dimensional graph. The attempts to do so by the event-trees and fault-trees of quantitative reliability analysis are incomplete because they are portrayals in design space alone. The complexity and multidimensionality of the circumstances in which Event-noise has its origin are illustrated by the combination of the two failure causation triangles, one due to Sir Henry Chilver (1977), namely Figures 14 and 15 which are discussed in the preamble to Appendix II and on page 206.

Summation of the differentials described by the identities (vi), (vii) and (viii) above,

$$\sum_{o}^{t=T}\delta e = \sum_{o}^{t=T}\delta n + \sum_{o}^{t=T}\delta s + \sum_{o}^{t=T}\delta l \quad \ldots\ldots\ldots\text{(ix)},$$

may be written,

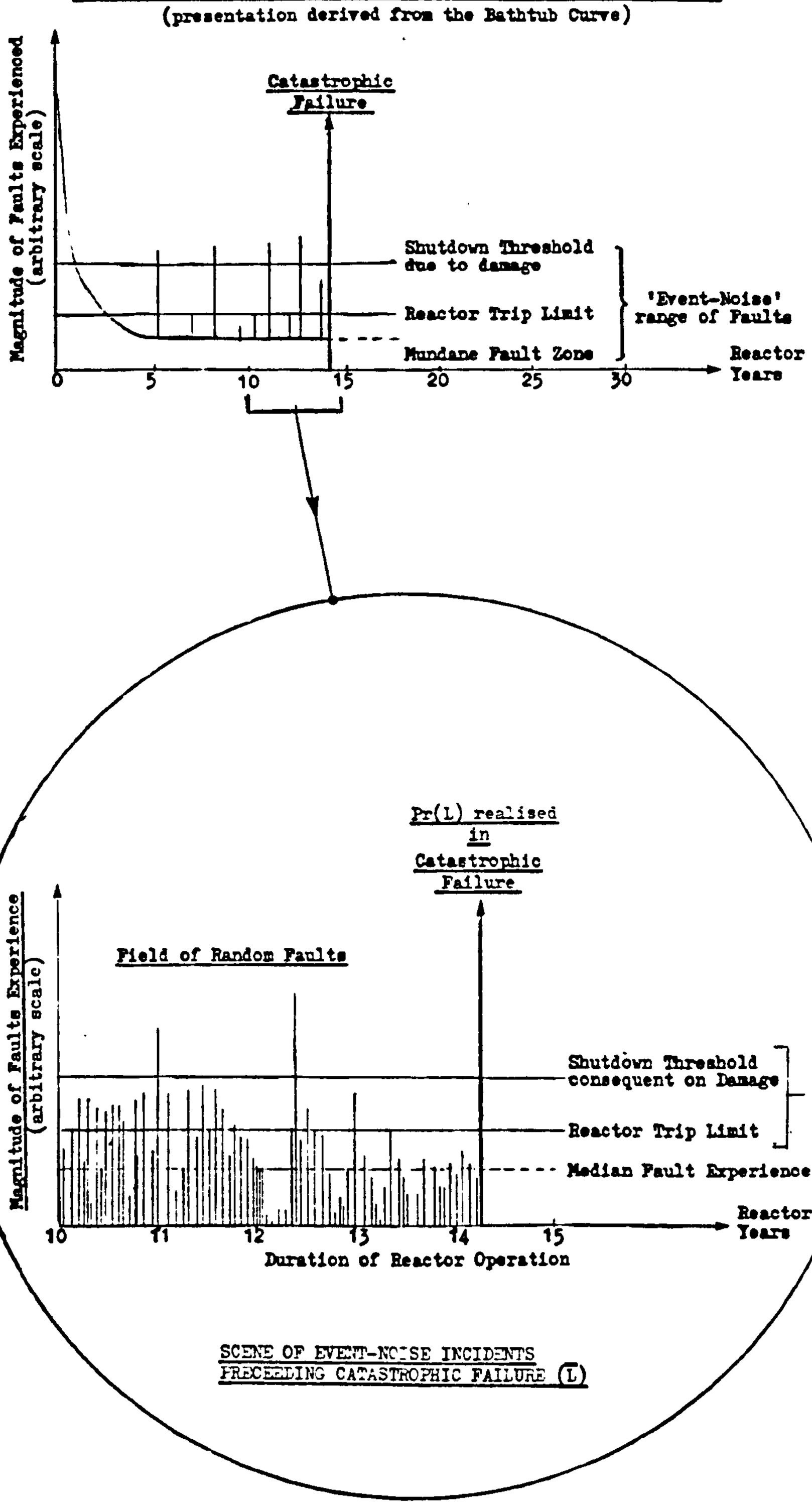
$$E = N + S + L \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(x)},$$

where 'N' and 'S' are respectively the Dynamic and Static contributions to the Event-noise experience of the plant from the beginning of commercial operation until some final time, 'T', when it reaches the point of ultimate shutdown for economic or operational reasons or in the low probability event of catastrophic failure. These are the circumstances depicted in the final stage of the historical Event-noise sequence shown in the ideogram of Figure 9. The Catastrophe-function is represented by 'L' which is associated with those major instabilities of behaviour properly outside the D-En classification that have been called 'spikes'. 'L' also embraces those major plant accidents whose consequences exceed the 'Damage Threshold' depicted in the graphs of Figure 11 derived from the Bathtub Curve of Figure 10 which include severe operational accidents and the ultimate terminator of catastrophic failure, the treatment of which is the avowed aim of this study.

In summary, there is reason to conclude from logical considerations supported by field experience that the mathematics of risk science and its operational research specialities of reliability analysis and quantitative safety analysis (See Section 7) are unable to manage the

SCENARIO OF REACTOR FAULTS TERMINATING IN CATASTROPHIC FAILURE

(presentation derived from the Bathtub Curve)



SCENE OF EVENT-NOISE INCIDENTS PRECEEDING CATASTROPHIC FAILURE $(\overline{L})$

LEGEND

'Spikes' = the more serious Event-noise transients, ie. δl incidents

Pr(L) = the probability (very low) of catastrophic failure, $(\overline{L})$

Event-noise Display

Fig 11

Catastrophe-function, 'L', when manifest as the low probability event of severe plant damage or catastrophic failure. Moreover, the attempt to use Event-noise theory for the latter purpose leads to the tautology of Equation (x) and the intractable expression for 'L' involving the summation of identity (viii).

12.3.3 Engineering and its proper involvement in the defence of safety

The preceding attempts to establish a formal mathematical framework for the treatment of catastrophic LPEs have proved to be nugatory. Furthermore, those familiar approaches, both quantitative and qualitative, that deal in the appraisal of design are inadequate because they are unable to enter the theatre of operational reality where the fault sequences that lead to catastrophic plant failure actually take place. The concept of Event-noise which could join theory and practice has been shown to be beyond conventional mathematics. Moreover, it has to be recognised that nuclear power together with certain other large scale energy industries has become too sophisticated and the penalties for failure too grave for critical technical decisions to be made by ad hoc engineering judgements.

Engineering inspection has already been identified as a most important part of the New Treatment. However inspection is not enough because the loss of resistance to failure which it attempts to detect cannot be properly perceived by the classic approach limited to the assessment of design and shop and site surveying. So far, cognisance has not been given, overtly at least, to the plant as a compound entity of interacting physical systems and human behaviour in their societal setting. Loss of resistance to failure is a common property of engineering systems, but it becomes a threat to safety when it is not recognised or when nothing is done about it. On the other hand, the developments in engineering science have opened the way to a less circumscribed approach. This is necessarily one which can bring together the engineering sciences of materials and structures, the technologies of non-destructive testing, radiological protection and control and instrumentation and other such advances with the newer disciplines of management in engineering, ergonomics, industrial psychology and decision methodology, all of which have effectively utilised operational research (OR). What is needed is a way of orchestrating all these thing so that they can act together in a defence of safety that is not only efficaceous per se, but which can be convincingly presented to the public as such.

In view of the importance that has been placed on OR, and it underlies the quantitative treatment of risk and safety assessment, it is appropriate to distinguish more specifically between the ways in which OR is used. Its application to prophecy in the field of low probability events differs from its use in reliability engineering. The case of prophecy is typified by the Reactor Safety Study (N.C. Rasmussen 1975) and by 'CANVEY' (Locke et al. 1978). These studies and certain other essays of like kind have been the subject of critical appraisal earlier when their claims to define field safety situations have been faulted, a critique summarised in Section 9.8.

On the other hand, the latter use of OR in reliability engineering is seen as a further and important advance in 'safety by hindsight', having little connection with prognostication other than through enhancement of plant safety in design as a consequence of technology transfer. A convenient exemplar is the reliability analysis of pithead winding gear protection that followed the Markham Colliery shaft cage crash of July 30, 1973 (25) in which 18 miners lost their lives (J.W. Calder 1974). Another example of a more distributed nature is the piquant reporting and analysis of mainly minor, but no less serious, plant accidents, failures and process loss incidents and their correction by 'fixes' that has been published by the Petrochemicals and Plastics Division of the Imperial Chemical Industries (T.A. Kletz 1982). An even more sophisticated and powerful approach, dominated by experiment, is that attributed to the National Aeronautics and Space Administration (NASA) in America described as 'burning-in' or 'design-make-test-fail-fix' (W.M. Bryan 1975).

An analogous OR approach is already in use in the engineering of defended safety, the 'fixes' being engineered safeguards, the limit and shutdown functions of control-and-instrumentation and administrative controls. However, as there will be no past experience to justify these 'fixes', anticipation must be used instead. This is a matter for engineering judgement for which neither design assessment nor noise theory give firm and cost effective guidance. Attention has been drawn to the dangers of 'ratchetting' in Section 8.4.2.

The task of organising and maintaining the defensive system thus falls to the engineer. To carry it out he must be able to grasp and interpret information and concepts that, in addition to the societal aspects of management, are presented largely in ideographic ways, namely by engineering drawings, pictorial plans, circuit diagrams and other

graphic symbols. As suggested in Section 8.1.1, the engineer can cope with this peculiar language because, in addition to the logical and analytical powers that are essential to the performance of any responsible intellectual function, he possesses a special mental faculty, acquired during his training and professional experience which enables him to comprehend and use information conveyed in ideographic form.

Having set aside the methodologies of design safety analysis and finding noise theory beyond the scope of any mathematical technique available in the present circumstances, a more tractable approach is needed. It seems that this may be found in Thom's Catastrophe Theory which can offer a simple multidimensional, dynamic model that can combine the principles of the 'fix' with the probability functions of noise theory. His 'General Theory of Models' offers a novel explanation for the sudden changes of form that occur in biological and physical systems (D.H. Fowler 1975) and this is relevant to the LPE.

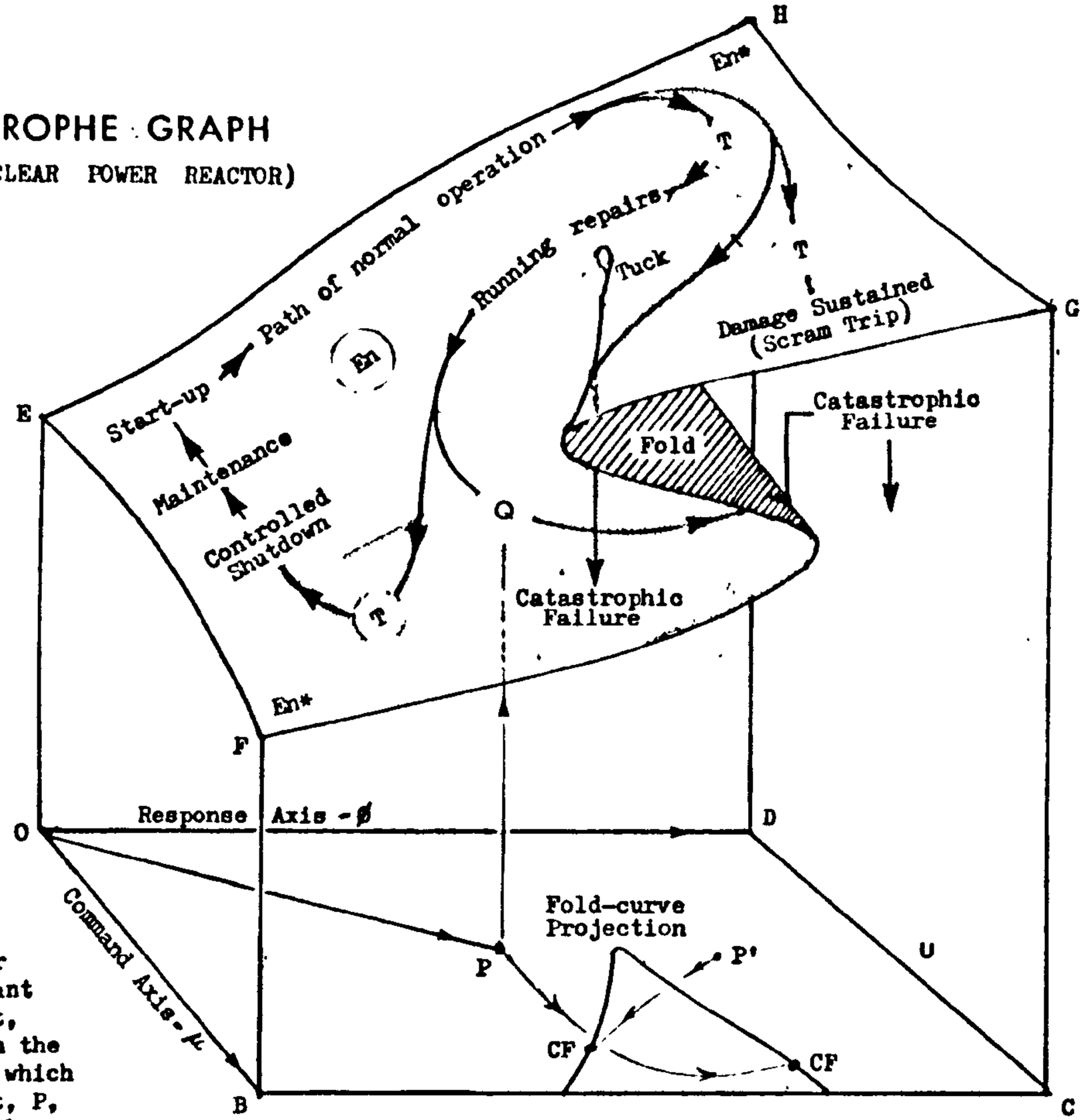
12.4 The relevance of Thom's 'Catastrophe Theory'

The discontinuity problem of an apparently stable system experiencing a sudden change of state to which René Thom (E.C. Zeeman 1977) has provided a novel mathematical solution in what has become known as 'Catastrophe Theory' is relevant to the safety and stability of nuclear power plants. An elementary application of the theory is shown by the cuboid graph of Figure 12. The circumstances in which the Event-noise attributable to the plant is created can be described in terms of the movement of two points, 'P' and 'Q', lying on two roughly parallel surfaces, a lower and horizontal one called the 'Control Plane' (OBCD) and an irregular 'Behaviour Surface' (EFGH) of the nature of a probability field above it.

The intended operational program of the reactor is depicted by the path of the point 'P', plotted on the Control Plane. The instantaneous position of this point describes the actual response of the given nuclear power plant as a holistic system embracing both physical and human aspects to the control imposed upon it, a control which is intended to achieve the particular electricity generation policy of its mangement. The position of 'P' is, then, determined by two orthogonal co-ordinates, 'OB' and 'OD', taken for convenience along the two bounding edges of the rectangular Control Plane, the corner at 'O' forming the origin of the co-ordinate system.

THOM'S CATASTROPHE GRAPH

(BEHAVIOUR OF A NUCLEAR POWER REACTOR)



OBCD = Control Plane

EFGH = Behaviour Sheet

CF = Catastrophic Failure

En = Event-noise, normal field

En* = Event-noise, disturbed field

P = Point indicating reactor state

Q = Image of P on the Behaviour Sheet

T = Reactor Trip - Operational

P' = An alternative path path for P

The envisaged behaviour of an nuclear power plant is displayed by a point, Q, following a path on the Behaviour Sheet (EFGH) which is the image of a point, P, moving in the Control Plane, (OBCD) in a manner determined by the Operational Command and System Response co-ordinates of P, which are 'μ' and 'ϕ' respectively

Note A catastrophic failure results when 'Q' passes over the lip of the Fold-curve

Cuboid Model

Figure 12

The side 'OB' is designated the 'Operational Command Axis' along which the control co-ordinate, 'μ', extends as a function of time, 't', in accordance with management action defined as the 'Command Force'. There is a corresponding extension, 'ϕ', along the side 'OD' which is the 'System Response Axis'. The 'OD' co-ordinate represents the instantaneous state of the reactor system as it responds to the Command Force. The response of the system is not immediate, nor is it directly proportional to the particular instructions presented by the Command Force, 'μ', because the reactor system is a holistic entity of diverse interacting elements, material and human. The material aspects comprise the plant's structure, core, nuclear fuel, instrumentation and control system and ancilliary equipment which are interpenetrant with those that are human, namely the site operational team of engineers, control room staff, service technicians and supporting personnel. The response, 'ϕ', thus lags on the Command Force, 'μ', owing to modulation and delays in this complex system of linkages, that actuates the system. As a result, the path taken by 'P' is a distorted hysteresis loop instead of being a straight line from the origin at 'O'.

(a) The Behaviour Surface

The observed behaviour of the plant is described in terms of Event-noise by the experience of the point, 'Q', and it moves over the Behaviour Surface (EFGH). That point is the image of 'P' and is located where the normal to 'P' meets the latter Surface and, hence, 'Q' also follows the distorted hysteresis loop traced by 'P'.

While the Control Plane (OBCD) is determinate, flat and smooth, the Behaviour Surface (EFGH) is not, its irregularities being characteristic of its probabilistic nature. It is, nonetheless, continuous and, as shown in Figure 12, much of the surface is either bumpy or wrinkled and there may be a fold ('fold-curve'). These asperities, undulations and folds describe the operational vicissitudes the plant may experience in terms of Event-noise.

A map of the Behaviour Surface will, by its very nature, be inconstant, being subject to change as the circumstances of the plant's constitution and environment vary the probabilities of those factors that can create Event-noise and are represented by the irregularities. While the irregularities have magnitude in a qualitative sense, this dimension is not quantifiable in prospect other than in terms of potentialities which are more subjective than objective. This, of course, is the nub of the objection to the validity of the very low probabilities cast for catastrophic LPEs by quantitative methods of safety and

reliability analysis. In these cases the potentialities become ever harder to discern as less and less likely events are identified, becoming insubstantial at the metaphysical fringe shown in Figure 4. Charting of the Behaviour Surface is more a matter for engineering judgement than for computation.

(b) The Stub Vector

The instantaneous state of the plant is represented by the attitude of a short stem or 'Stub Vector' supported by the point, 'Q', which is always normal to the Behaviour Surface itself at the point of contact. It is aligned to the perpendicular where the surface is flat, but the asperities, bumps and folds translate the point as it moves over them into domains of instability where the resistance of the system to failure is lost in measures proportional to the deformity of the surface. The Stub Vector then tilts, its degree of displacement from the vertical indicating the extent by which the plant has been disturbed from its stable state as shown in Table IV.

The duration of the instabilities represented by an encounter of 'Q' with a Behaviour Surface anomaly is, of course, the time for which the Stub Vector remains at the tilt. This is a function of the rate at which 'Q' moves across the particular surface irregularity. Clearly, the speed at which 'P' moves in the Control Plane is not constant, being determined by the operational strategy pursued as varied by exigent system requirements: tending to be stationary when the plant is shutdown, though plant and human factors render demarcation of such periods indeterminate. For example, time is taken to remove after-heat in the core before a planned shutdown can be completed and start-up may be a lengthy and complicated operation. In retrospect, the encounters that 'Q' has with the Behaviour Surface anomalies are otherwise identifiable as elements of Event-noise, 'Dynamic' (D-En), 'Static' (S-En) and the 'spikes' of the Catastrophe-function, 'L', as the case may be. Salient among the latter is the rare and terminal event of catastrophic failure designated as 'Ł', a topic of the following Sub-section 12.4.1.

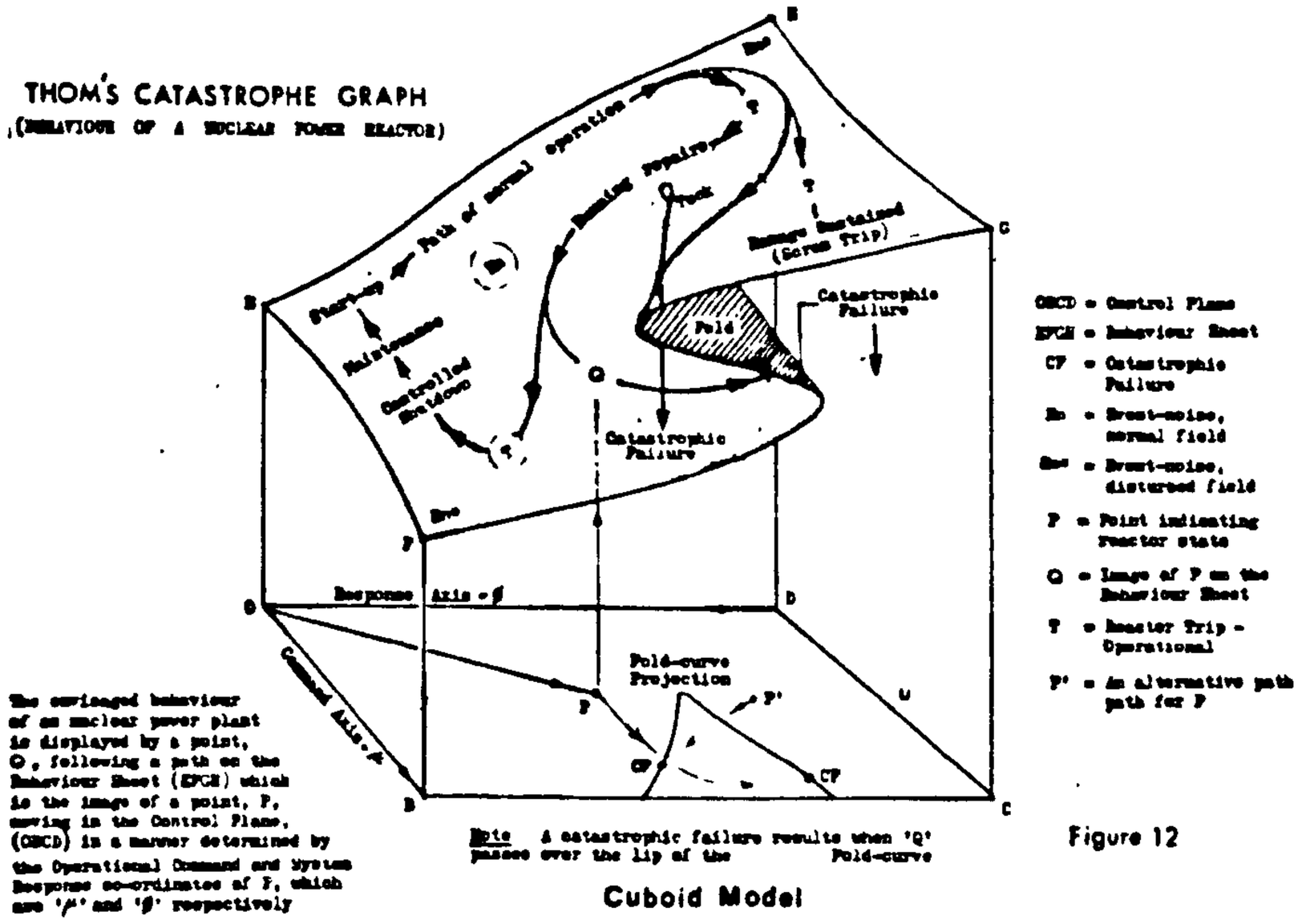
(c) The Behaviour Surface as an Event-noise generator

While the Control Plane is determinate, the Behaviour Surface has been identified as a probability field on which Event-noise characteristic of the operation of the reactor is generated as the point, 'Q', bearing its Stub Vector, passes across the irregularities in that surface, the analogy with a gramophone needle and record groove being strong. The

TABLE IV

Stub Vector Attitudes

Explanatory Note - In discussing the Event-noise (EN) features of the Behaviour Surface (EFGH) of the Cuboid Model, it is appropriate to assign meaning to its upward slope from E-F to G-H. The bumps, creases and folds that form the 'asperities', the 'wrinkles' and the 'fold-curve' which represent the En probabilities then appear as changes of slope with respect to the z-axis. The magnitude of these changes is indicative of the severity of the particular En experience, potential or realised, and is described by the tilt induced in the Stub Vector as 'Q' proceeds around the operational hysteresis loop and encounters the various Behaviour Surface irregularities.



The envisaged behaviour of an nuclear power plant is displayed by a point, Q, following a path on the Behaviour Sheet (EFGH) which is the image of a point, P, moving in the Control Plane, (CBCD) in a manner determined by the Operational Command and System Response co-ordinates of P, which are 'μ' and 'β' respectively

Note A catastrophic failure results when 'Q' passes over the lip of the Fold-curve

Figure 12

Cuboid Model

SLOPE ANOMALY IN THE BEHAVIOUR SURFACE	STUB VECTOR ATTITUDES (surface cross-section and Vector tilt)	EVENT-NOISE EXPERIENCE (in terms of system stability)
System stable	———	Normal operational state with minor Event-noise
Asperity	⟋‾‾‾	Quasi-stable, major industrial accident, fault or incident, i.e. D-En or S-En
Wrinkle	⟋‾‾‾	Unstable, severe fault or incident - En 'spike'
Fold-curve	⟋‾‾‾	Catastrophic failure - severe radiation accident or disruptive fault with terminal shutdown, $Pr(\overline{L})$

instabilities indicated by the orientation of the Vector may be associated with specific Behaviour Surface anomalies which can be described as 'asperities' for minor irregularities, 'wrinkles' and 'folds' in ascending order of magnitude as shown in Table IV. The extreme case is a 'fold-curve' which results in complete inversion of the Stub Vector, turning it through 180°, bringing about the terminal LPE of '$\bar{L}$' (supra). More particularly, the asperities may be associated with industrial accidents and minor component and systemic faults of a casual nature. The wrinkles, symptomatic of more significant disturbances to the system's stability, represent major equipment, sub-assembly, structural and system failures and the occasional reactor trips consequent upon them. Taken together, the asperities and wrinkles symbolise the generality of D-En and S-En as identified by 'n' and 's' in Equation (i).

In conditions of normal, steady operation the reactor will cycle around a loop of start-up, occasional trip, maintenance in service, periodic shutdown for overhaul and return to operational service, being little troubled by the mundane Event-noise arising, a situation depicted in Figure 12.

(d) The Fold-curve and other surface anomalies

More serious events appear in the medley of En when, owing to the unusual circumstances suggested by the factors operating on the term on the RHS of Equation (viii) above, the point 'P' deviates from its expected cyclic path in the Control Plane. As a result, the image point 'Q', following the deviant path taken by 'P', is deflected from its prospective course and may encounter an unanticipated major wrinkle or fold in one of the rougher and uncharted areas of the Behaviour Surface which have been labelled En_*. Such events constitute the 'spikes' of En that mark certain parts of the 'Bathtub Curve' (See Figure 11). Catastrophic failure of the whole system is represented by 'Q' moving over the rare anomaly of a fold-curve when a sudden change of state occurs as the point passes over and down, or up and under, the lip of the fold on to its lower surface where the direction of the stub vector is reversed, indicative of a catastrophe as described in Table IV.

It is reasonable to think that the presence of 'Q' in the region of the fold could result in the appearance in the Event-noise flux of precursors of the impending loss of the system's resistance to failure. The New Treatment will suggest that such warning signals could be detected by alert and percipient observers properly cognisant of the

engineering of the plant and its circumstances of operation. The topic is raised again in the next Section.

In addition to the hysteresis loop traced on the Control Plane by the point, 'P', the projection downward of the 'fold-curve' in the Behaviour Surface appears in the form of the 'bifurcation set' suggestive of a 'cusp' (E.C. Zeeman 1977). Despite that, the probability distribution of the fold-curve is unimodal for any conceivable maximum reactor accident and, although, the lips of the 'fold-curve' may be approached from two directions as shown in Figure 12, only one type of catastrophe is described by the form of the given surface. The representation is, therefore, not that of a 'cusp catastrophe', but one analogous to the capsizing of an ocean-going ship, ie unimodal outcome, but of multiform possibilities of causation. By comparison, salient among those in the case of a nuclear power plant are the LOCA, a reactivity excursion, loss of control and precipitate total rupture of the main coolant pressure vessel.

12.4.1 Some qualitative aspects of the Cuboid Catastrophe Model

In the attempt to combine the Event-noise concept with Catastrophe Theory, it has been necessary to take some liberties with the formal presentation of the latter. René Thom's theory deals with the catastrophe per se which, in the first example used by E.C. Zeeman (1977/a), describes the state of rising tension in the case of an animal facing a threat or provocation. The creature experiences rising fear and aggression, the tension being relieved by a catastrophic change of behaviour into flight or fight. Similar scenarios can be written for the collapse of a strut under increasing load and with appropriate sophistication for systems of increasing complexity.

The case of the animal is a simple 'cusp-catastrophe', but much more complicated catastrophe situations may be treated, some of which involve higher orders of dimensionality such as those concerning problems of space-time as discussed by D. Trotman (E.C. Zeeman 1977/b).

The major simplication made here has been to describe the risk of nuclear power plant failure in terms of the degrees of loss of stability shown in Table IV as represented by the attitude of the 'Stub Vector'. By the embellishment of the Theory it has been possible to combine the Event-noise and Catastrophe concepts in a simple idea whereby the Behaviour Surface (EFGH) of the Cuboid Model of Figure 12 is depicted not only as having the characteristic 'fold-curve' used to describe a simple catastrophe, that is total loss of stability corresponding to

catastrophic failure of a nuclear power plant, but as having surface anomalies as well which represent Event-noise (En) of increasing severity.

To avoid involved descriptions and recourse to the mathematics of Thom's theory, the feature of the 'cusp' has been glossed over because there is only one catastrophic case which is total loss of stability. Doubtless, the multiplicity of forms which that might take, for instance a LOCA, criticality excursion, channel dry-out and so on could be studied in depth, but this is not necessary for the purposes of the New Treatment. To quote E. C. Zeeman on this point when discussing the 'Stability of Ships':

> 'This approach in terms of canonical forms offers a qualitative geometry that is complementary to the classical approach. Whether or not such formulation is of any use remains to be seen, because to make quantitative predictions it is still necessary to use co-ordinates and approximations as in the classical theory. However as a general principle it is always advantageous to retain the dynamics in a conceptually simple form for as long as possible so that the importance of the qualitative features can be kept in the forefront of the mind unobscured by detail, allowing the eventual approximation to be tailored to the job in hand.'
>
> Catastrophe Theory: Selected Papers 1972-1977, pp. 441-442.

Although the simple Catastrophe Theory model given above is 3-dimensional, or 'Cuboid', it has in effect more than three because of the complex linkages involved in the 'Command' (μ) and 'Response' (ϕ) functions acting in the Control Plane and the peculiarities of the Behaviour Surface. This 'Cuboid Model' offers a multi-dimensional concept in contrast to what is essentially the 2-dimensional design regime that characterises quantitative safety and reliability analysis as in the Reactor Safety Study (N.C. Rasmussen 1975). The Cuboid Model through its multi-dimensionality thus helps to blend the reality of plant construction and operation with design theory, bridging the gulf between the two regimes of theory-as-design and practice-in-construction as shown in Figure 8.

The simple exposition of Catastrophe Theory presented here is no more than an introduction in a treatment that is innately qualitative, being concerned with an understanding of the quandaries of LPE management rather than with the underlying mathematical logic of any specific application of the Theory. A study in greater depth might be justified on grounds of rigour but is well beyond the scope of the

present text and would add little to understanding.

The style of modelling used to represent the LPE of catastrophic outcome is associated with the 'fold-curve', an approach that tends to be subjective, and properly so because the Model has to represent the analyst's conception of a multi-dimensional entity, that is the reactor system as a complex grouping of factors that is labile and lacks definitive bounds. The case for the more general class of technological LPEs is illustrated by the combination of the two 'Failure Triangles' of Figures 14 and 15 as discussed in the Preamble to Appendix II. The above use of Catastrophe methodology in the treatment of LPEs may be compared with the exiguous simplicity of the 2-dimensional representation of the Event-trees and Fault-trees on which the analyses in the Reactor Safety Study are based.

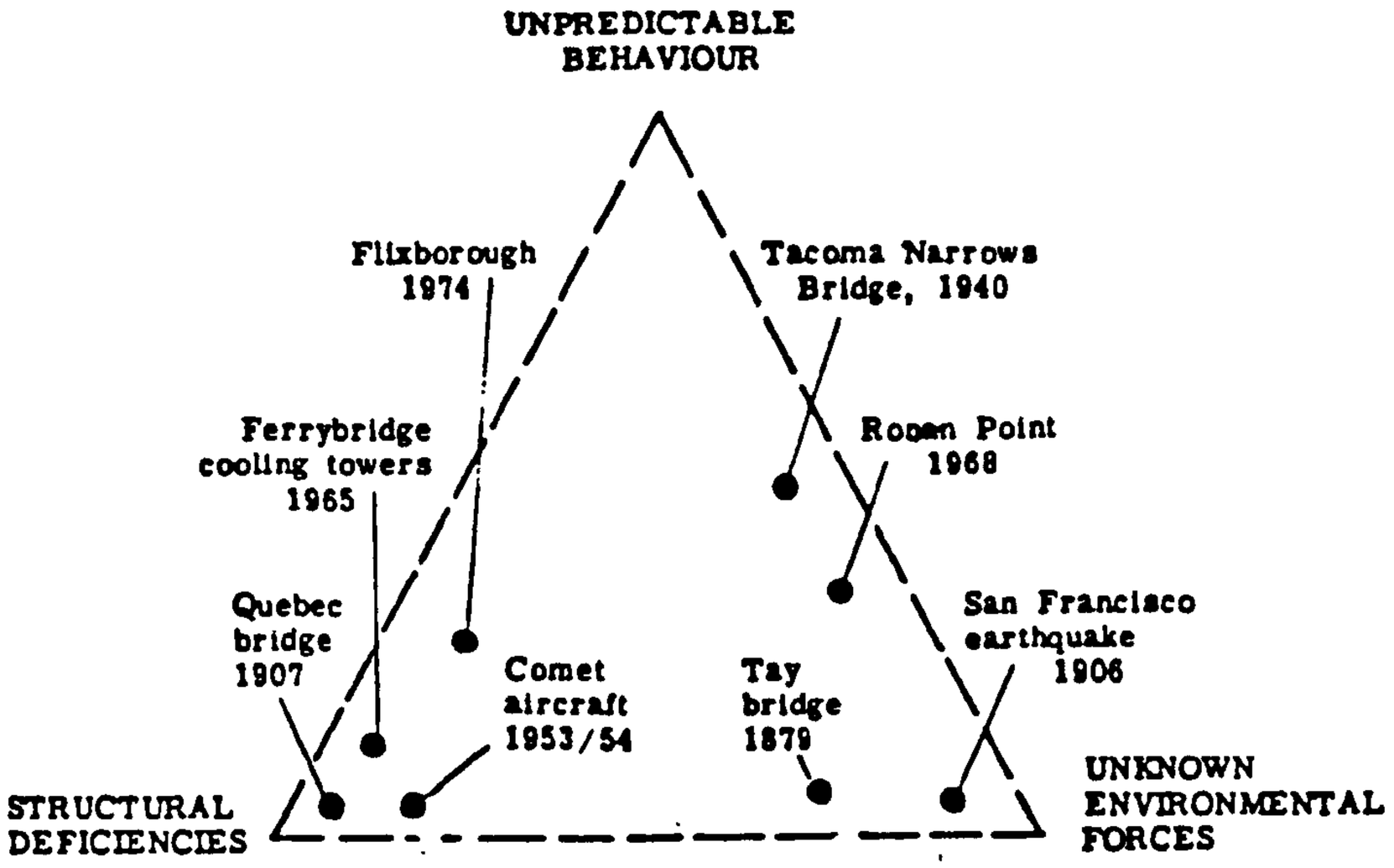
Nonetheless, it is possible to identify some quantifiable elements in the Catastrophe Theory treatment among which are control rod redundancy, the provision of instrumentation sensors and various operational limits, one of these being the provision of fuel element thermocouples in the British Magnox reactors as described in Document No. 5 of the Annex.

In view of the simplicity of the Catastrophe Theory application that has been adopted, the value of the concept in relation to study of LPEs may be questioned. In this connection it is useful to observe the qualitative modelling used in many branches of modern physics and other sciences, not least in Particle Physics. Even some 20 years ago the use of qualitative models was described by Professor A. W. Merrison in 1964 as 'simple, but imaginative modelling, trivial arithmetic and hard thought'.

The New Treatment is, then, using Catastrophe Theory to give a multi-dimensional representation of the causative phenomena that precede and underlie the catastrophic failure of a nuclear power plant. By this means, the steps that must be taken to prevent such an untoward event by defending the safety of the plant at risk may be better understood. Clearly, the outcome is going to be neither one of mathematics and algebra nor specifically quantitative. It is one instead that can assist inspectional policy by keeping the practical features of a nuclear plant risk to the fore, while 'keeping at the back of one's mind the necessary reservations, qualifications and adjustments we shall have to make later on' to paraphrase John Maynard (Lord) Keynes's disparagement of a tendency to place excessive emphasis on mathematical treatments in economics (1936).

A NEW OUTLOOK ON LPE CAUSATION

An ideogram that proportionately ascribes three generic causes for the failures of major engineering artefacts



FITTING FLIXBOROUGH INTO A PATTERN

From an article by Sir Henry Chilver,
Nature, 10 February 1977, Vol. 265, 494

Using the explosion of June 1, 1974 which devastated the petrochemical processing plant at Flixborough as an example, Sir Henry Chilver writing in Nature early in 1977 identified the important issues raised by the event in respect of the safety and reliability of complex installations of the kind. He saw them as the adequacy of the engineering skills available for their design and construction and the effectiveness of the supervision of these engineering activities in practice. He observed that, not only must all engineering disasters be individually explored with a view to discerning the causes, but they must be seen more broadly as matters of concern to engineering science as they may disclose 'some general pattern of engineering failures as a whole'. He attempted to generalise the case by 'fitting Flixborough into a pattern' that could embrace other engineering failures.

He distinguished three main causal factors among a number of notorious failures, namely:

(i) Unknown structural or material deficiencies, for example, the materials used may have been substandard or a vital component have suffered accidental damage, ie. 'Structural Deficiencies'.

(ii) Unknown forces in the environment of the structure, for example a long-span bridge may suffer exceptionally high winds or a building experience an unusually severe earthquake, ie. 'Unknown Environmental Forces'.

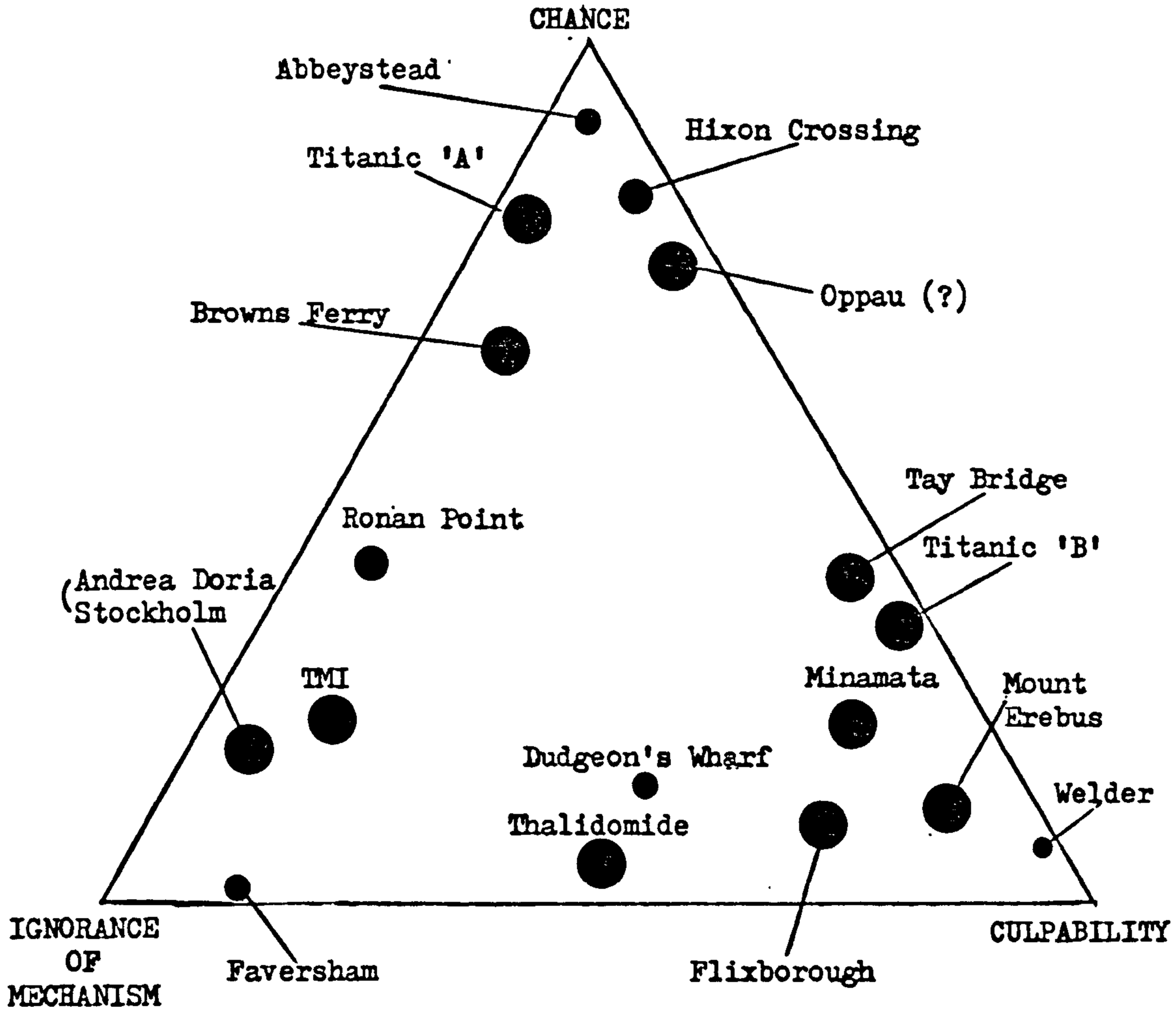
(iii) Unknown forms of behaviour of the structure within its environment, for example a new form of oscillation, or buckling may occur for a new structural form, ie. 'Unpredictable Behaviour'.

Chilver relates these factors to apices of a 'Triangle of Failures' as shown in the figure above. Failures of very different sorts may be located in the Triangle and, where a failure involves mixes of factors, it can be placed nearer to the apex associated with the cause deemed to be dominant.

The representation is not quantitative, but it can assist in forming a qualitative judgement about the main sources of loss of resistance to failure. This can provide a basis on which policy in regard to design and inspection may be formulated.

THE CHILVER FAILURE TRIANGLE (Appendix II refers) FIG 14

CAUSATION TRIANGLE FOR LOW PROBABILITY EVENTS



The size of each dot gives an indication of the scale of the incident in terms of injury to humans and damage to property. In the cases of the Three Mile Island (TMI) and Browns Ferry nuclear power station accidents, though there has been very heavy financial loss, no known harm was done to either workers or the public by leakage of radioactivity from the plant.

The clustering of the dots is in accord with the findings of the Analysis in Appendix II. It show a definite trend towards culpable human error, defined in the diagram as 'Culpability', as the major factor in accident causation, a deduction that has been confirmed by more generalised accident studies. It is, however, one that can be effectively minimised by a regime of inspection of a suitable kind.

TRIANGLE OF INCIDENT CAUSATION

Fig 15
(Appendix II refers)

12.4.2 The nature of the Catastrophe-function 'L'

It seems that none of the present approaches to nuclear hazard management offers any sure guidance for the defence of a plant against those severe system failures of very low, but imponderable probability, that are occasionally realised, a point that may be confirmed by reference to Appendix II.

Nonetheless, Catastrophe theory can assist understanding of the complicated interactions between matter and the human intellect that enable an intricate machine to be designed, constructed and properly used in safety. In this connection, E. C. Zeeman concludes an erudite exposition of 'A catastrophe model for the stability of ships' with the following observation:

> ' ... there is at present a lack in the theory of non-linear coupling. Consequently, there is a lack of mathematical language in which to express and communicate the intuition which experienced pilots possess of how to handle a ship in heavy weather. It is not enough to say that capsizing is probably due to that once-in-a-million freak wave, because capsizings do occur more frequently than we would wish, and it might be that the intuitive knowledge of one experienced pilot could have saved another. A case in point is Lindemann's discovery of how to get out of a flat spin in an aircraft by pushing the stick fully forward and kicking hard on the opposite rudder. What was at one time a situation dreaded by all fliers, is now a routine recovery procedure taught to all beginners. Analogously, in ship stability, the qualitative simplicity of the singularities that we have been discussing might eventually lead to a better understanding of the routine procedures for handling that big wave.'
>
> 'Catastrophe Theory: Selected Papers 1972-1977', Addison-Wesley, Reading, Massachusetts, 1977, p. 492.

It is suggested that the answer may lie, not in more recherché excursions into risk and reliability analyses, but in ascertaining how to anticipate a covert, major wrinkle or latent fold-curve in the Behaviour Surface of a Cuboid Catastrophe Model. The vagaries in the path of 'P' on the Control Plane (OBCD) shown in Figure 12 are due to the 'non-linear coupling' between the 'Operational Command' (μ) of the plant management and the 'Response' (ϕ) of the system. Besides the Response has its own, often capricious, dynamic owing to human initiatives and other factors defined in Section 12.3.2. above, namely 'p' and 'q' and the associated 'Anomalies', 'z'. Moreover, the Behaviour Surface (EFGH) is a probability field owing among other things

to the circumstances of 'c' which is the lack of congruence between the theory of the design and the reality of the plant, of impingeing externalities, 'x', that disturb the system and the internally generated inconsistencies just mentioned. In consequence, the irregularities of the Surface which are its asperities, wrinkles and such folds as may be distinguished are not fixed features and the encounters of 'Q' with them are also influenced by an element of chance. By earlier definition, then, 'δl', the 'spike' of Event-noise, a major instability that is the result of 'Q' passing across a wrinkle or fold-curve in that surface, is represented by an output pulse of the 'Catastrophe-function', 'L' which may be written formally by summation of identity (viii) as

$$L = \int_{o}^{t} f_1'(s,n,x,z)\delta t \quad \ldots\ldots\ldots\ldots \text{(xi)},$$

where 't' is the duration of the passage.

As written, the function, 'L', depicts all 'spikes' in the Event-noise flux as major, impulsive fluctuations in the stability of the plant's system, but that associated with catastrophic failure is terminal. The latter is, therefore, in a separate class and is designated as '$\bar{L}$'.

The last term, 'l', in the earlier Event-noise equation,

$$e = n + s + l \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(i)}$$

now becomes $$l \simeq L + Pr(\bar{L}) \ldots\ldots\ldots\ldots\ldots \text{(xii)}$$

for t = T when the plant has reached the end of its useful life. $Pr(\bar{L})$ which is the objective probability of the system experiencing a catastrophic terminal event is very small and tends to zero. The term may be associated with the 'zero' concept in the 'Zero-Infinity Dilemma' facing the insurance industry actuary when assessing nuclear and certain other modern technological risks.

The movement of 'P' on the Control Plane is, of course, the result of the operational intention represented by the 'Command' co-ordinate, 'μ' and the expected 'System Response','ϕ'(supra). The point is 'steerable', but its course exhibits an unpredictability owing to the non-linear couplings between the interactive human and physical linkages. This uncertainty added to the stochastic nature of the Behaviour Surface makes the experience of 'Q' unforeseeable in a definitive quantitative sense. Besides, the confidence limits are too

wide to give values to the risk parameters that are meaningful in anything but a qualitative connotation for the plant as an operating physical entity, a conclusion arrived at by more tortuous mathematical and engineering arguments earlier in the text.

12.5 An interpretation of the Catastrophe/Event-noise approach

By combining the Event-noise and Catastrophe Theories, a model of the plant as a working entity of interacting physical and human parts may be constructed. It can then be presented as a holistic system in an engineering aspect and an escape made from the inhibiting formality of the quantification logic of reliability analysis which then falls into place as a valuable intellectual tool in the exercise of performance assessment. Thus, the New Treatment gives scope for functional analysis in depth of a nuclear power plant along the lines pioneered by René Thom and others. As E. C. Zeeman (supra) also remarks:

> 'Firstly, the geometry of elementary catastrophes may be used to describe phenomena, particularly those in which gradually changing forces produce sudden effects. The philosophical justification ... is that mathematically they are higher dimensional analogues of the simple concepts of maxima, minima and thresholds. ... such a model may be scientific in the sense of reducing the arbitrariness of a description, by providing a coherent synthesis of otherwise unrelated observations. Secondly, it may be possible to explain a model by deducing it from more fundamental hypotheses. ... ... Thirdly, ... models (may be used) ... to design experiments and predict new results.'
>
> Catastrophe Theory: Selected Papers 1972 - 1977, Preface. Addison-Wesley, Reading, Mass., 1977, pp. ix - x.

The elementary Catastrophe theory model of Figure 12 is a static slice taken from a multidimensional system progressing in time. Without allowance for updating, it would rapidly fail to represent the system. However, Event-noise theory provides for continuity by introducing a dynamical aspect that enables the changing physical and human linkages to be recognised and the consequences of their interactions described. In the case of nuclear power plants, this wider knowledge of the system as a whole may be used to emend safety and reliability engineering strategies and to re-orientate engineering investment in safeguards, physical and administrative, on a more effective basis. The risk may be thus assessed in circumstances that obtain beyond the realm of the design office.

12.5.1 Some 'Catastrophe' representations of Event-noise elements

Further examination of the RHS of Equations (i) to (iv) yields some more information relevant to a better understanding of the problems of nuclear power hazard control.

(a) Dynamic Event-noise - D-En

The complex term for 'n' on the RHS of Equation (ii) represents the D-En experience of an operating nuclear power plant. It describes the random occurrence of minor equipment, components and structural faults, process interruptions and industrial accidents typical of any large engineering installation, an experience also portrayed by the asperities of the Behaviour Surface of the model in Figure 12. Owing to the high level of safety and reliability awareness that pervades such industrial entities, as for example in factories handling explosives, the rate of D-En flux may be expected to be substantially lower than for the generality of industry. This has been confirmed by the rate reported from the U.S. nuclear industry over the first 15 years of operation which was only one-third of the national figure (M. B. Biles 1969) and a similar pattern prevails in the U.K. It also suggests that the safety and reliability problems inherent in D-En are being efficaceously managed by the U.S. Nuclear Regulatory Commission (NRC) and the British Nuclear Installations Inspectorate (NII).

(b) Static Event-noise - S-En

Interpretation of the term for 's' on the RHS of Equation (iii) is more profound. S-En as defined in Sections 12.2 and 12.2.1 above is a phenomenon of the design and construction processes that introduces largely covert defects into the whole fabric of the entity. The more significant of them are represented by the wrinkles in the Behaviour Surface of the cuboid model. Most of the elements of S-En not eliminated during commissioning emerge as copious En in the initial phases of operation to constitute the typically large, but rapidly decreasing number of 'early failures' characteristic of the 'Bathtub Curve' shown in Figure 10. Residuals remain and can appear fortuitously later in the history of the plant, occasionally combining with other elements of En in propitious systemic circumstances to make paths for fault sequences that can run to catastrophic failure of the system, that is to produce a fold-curve in the Behaviour Surface. An example of the late emergency of covert, residual S-En was the casual discovery of break-away corrosion of vital steel bolts in the graphite

core restraint bands in the British 'Magnox' reactors in 1968 (Daily Telegraph 1973, David Fishlock 1975), the consequent 'behavioural' instability being so serious as to require a drastic reduction in output of these stations and later shutdown for major repairs. However, this 'event' may be seen as a major 'spike' of En and may be grouped with effects of the Catastrophe-function, 'L'.

(c) Event-noise 'spikes' and the Catastrophe-function 'L'

The En element represented by the term, '1', in Equation (i) comprises 'noise' events of a more serious kind than those of 'n' and 's', being identified with the 'spikes' discussed in the text above. These events of low probability, and for the most part threats to the stability of the system but not envisaged in its design, are of diverse causations acting in unanticipated situations. The 'spike' generating function, described by the expression on the RHS of Equation (iv) is complex, convoluted and enigmatic and its meaning cannot be fully understood in any mechanistic sense prior to the event with which it is identified. Its action is almost invariably systemic, if not in its origin, then in its consequences, and the 'spike' itself is the result of interaction among the multifarious factors identified on the RHS of Equation (iv). The occurrence of such incidents usually involves the late emergence of covert S-En, although seldom without human fallibility making an important contribution. In Catastrophe Theory, 'L' is represented by wrinkles and major irregularities on the Behaviour Surface of the cuboid model of Figure 12 which 'Q', the image of the Control point, 'P', may encounter as it moves in response to the directions of the system control program. The wrinkles are illustrative of situations in which the stability of the system is disturbed sufficiently to create 'spikes' in the Event-noise flux.

Typical examples of low probability 'spike' events due to major surface anomalies include the ingress of sea water into the nuclear core of one of the Hunterston AGR reactors and the cracks found in the fabric of the main coolant ducts of the Dungeness 'A' power station No. 2 reactor in August 1978 during a routine shutdown for overhaul (David Fishlock 1979, Anthony Tucker 1980). Inspection disclosed covert S-En in the presence of cracks in the membranes of the expansion bellows assemblies. The system suffered an extended shutdown for repairs. Catastrophic crack propagation leading to precipitate failure of a duct in operational circumstances and explosive decompression of

the reactor coolant pressure circuit would result in the archetypal Maximum Credible (MCA) or Design Basis (DBA) Accident for a 'Magnox' system. More seriously, passage of 'Q' over a fold-curve represents terminal destabilisation of the system. This terminal low probability event symbolised by $Pr(\bar{L})$ in Equation (xii), although strictly a 'spike', is discussed separately infra.

(d) The Low Probability Event $Pr(\bar{L})$- the Terminal Catastrophe

In the Event-noise stream coming from a nuclear power plant, catastrophic failure symbolised by $\bar{L}$ in Equation (xii), stands out from the generality of 'spikes', being singular in consequences rather than in nature despite the fact that it terminates the flow. The very low probability of this unlikely happening is depicted by the operator, 'Pr' that has been introduced into the Equation. The resulting term, $Pr(\bar{L})$, is also indicative of the asymptotic zero risk identified actuarially as the 'Zero-Infinity Dilemma' of the insurance industry discussed earlier in Section 8.4. Notwithstanding the vestigal probability of occurrence, the fact that a damaged nuclear power reactor can release very large quantities of radioactivity to the environment capable of putting a whole community at risk makes $Pr(\bar{L})$ an issue of transcendent importance in both the engineering and politics of nuclear power. The event, $\bar{L}$, is represented in the cuboid catastrophe model of Figure 12 by an encounter of the point, 'Q', with the lip of the fold-curve. The ensuing inversion of the stub-vector indicates a total loss of the system's stability as described in Table IV. The probability and scale of such an event and the quest for ways by which it may be averted has been, and continues to be, the central theme of all approaches to safety in the management of nuclear power.

An example of an $\bar{L}$ event is provided by the Three Mile Island catastrophe. The failure sequence was initiated by tripping of the main feedwater pumps due to an S-En element introduced during maintenance. The system reacted correctly, but owing to a design weakness (S-En) the emergency feedwater valves were set in the closed position. The steam generators boiled dry, depriving the reactor of a heat sink (a destabilising 'spike'). As a result of inadequate design, a pilot operated relief valve on the pressuriser (S-En) did not close when the reactor pressure surge relaxed which mislead the operators as to the true state of the plant. In consequence, a series of operational errors (D-En) followed. Nuclear fuel in the core overheated with some melting and release of fission products and generation of hydrogen from

the reaction between steam and zircalloy contributed major 'spikes' to the now chaotic En flux. The catastrophe culminated in a massive escape of radioactivity to the containment where a hydrogen bubble was also formed which later exploded. There was general confusion in the control room and for a time the system was totally destabilised. Viewed systemically, a plant experience which might have been no more than a minor 'spike' instability, became a catastrophic failure because of defects in the human links in the response system. The plant was, in effect, steered across the Control Plane (OBCD) of the cuboid model into catastrophe, represented on the Behaviour Surface (EFGH) by the operational state image point, 'Q', passing over the lip of an unenvisaged fold-curve. Among the many factors of human S-En was the obese somatype of a senior control room engineer that inhibited his proper perception of the instrument panel displays (Barbara Culliton et al. 1979). A further, enigmatic feature of the incident was that the fold-curve encountered was conceptually anomalous because the catastrophe was beyond the DBA (P. Halliday 1982).

A similar analysis can be applied to the sequence of events that led to the 'Flixborough' petrochemical plant disaster of 1974. It was initiated by cracking of the membrane of one of 6 large cyclohexane reactors, owing to inadequate metallurgical design (S-En). The defective unit was properly bypassed for repairs and after tests the plant returned to the production of caprolactam. As the vacant post of plant engineering manager had not been filled (S-En), responsibility for site engineering was in the hands of a maintenance foreman (S-En). The technology of the repair was beyond his competence and his design faulty, though the workmanship was excellent (S-En). Some 4 weeks later, the bypass failed in service (D-En) and the site was blanketed by a cloud of cyclohexane vapour. It was ignited by an open flame (D-En) and the consequent explosion (fold-curve catastrophe) wrecked the plant, killing 28 workers and causing extensive damage in the nearby villages. The actual direct cause of the incident was a matter of dispute at the subsequent inquiry, but the official view prevailed. Like 'TMI' the accident was beyond the DBA (Christopher Simon 1975), being the result of inadequate human linkages in the mechanism that determined the Response (ϕ) of the system to the Operational Commands (μ) of management. The catastrophic rush over the fold-curve which happened in minutes rather than hours may be attributed to the sudden, consecutive realisation of the chain of S-En elements.

12.5.2 An evaluation of Event-noise/Catastrophe Theory

As concluded in the earlier comments on the expression $Pr(\bar{L})$ of Equation (xii) the potpourri of interacting factors that determine the response, 'ϕ', of the plant to the command parameter, 'μ', are intractable and defy analysis by any known rigorous logical or mathematical device. Hence, the consequent experience of the system depicted by its progress in the probability field of the Behaviour Surface (EFGH) of the model (Figure 12) cannot be forecast in any meaningful quantitative sense for low probability events beyond mundane industrial experience. As posited in Section 9.6.1, quantitative prophecies of very low risks, especially when made from design concepts, are metaphysical and describe hypothetical events that are too rare to happen in the manner foreseen. The system is no more reliable thereby because something not conceived in the analysis may happen instead, a conclusion justified by the experience of technological failures (See Appendix II).

Although Event-noise and the Catastrophe theories give no more in the way of direct guidance towards the desired goal of absolute safety than any of the other methods of treating the nuclear risk, the combined approach offers an advance by identifying $\bar{L}$ as part of the En flux, being the last of an otherwise continuing sequence of 'spikes' and exceptional only in that it becomes the terminator. This gives the method a conceptual continuity that is absent from the DBA or the equivalent MCA approaches which have their focus on major catastrophic events to the apparent exclusion of the smaller ones, although these still have serious consequences. Although this has long been recognised by nuclear engineers as a weakness, the criticism of the MCA was first voiced by F. R. Farmer (1967) to justify his criterion of distributed radiation accident probabilities known as the 'Farmer Line'.

Both the DBA/MCA and the quantitative probability methods of the 'Farmer Line' type are engrossed in theoretical matters of design at the expense of practice in engineering site and operational realities. By comparison, the New Treatment by combining the Event-noise and Catastrophe theories takes due account of the importance of practice by including engineering realities of construction and operation in the En stream while continuing to recognise the basic role of the design theory. Moreover, the assimilation of En elements into the catastrophe model completes the representation of the plant's operational behaviour by the inclusion of human factors in both the decision function (μ) and

the system response (ϕ). The overall behaviour of the plant is thus depicted as a system experiencing a consistent succession of disparate events that possesses the ergodic continuity characteristic of noise. The outcome of the approach is not predictive but explanatory, thereby enabling steps to be taken to abort the drift of an apparently safe system into catastrophe.

A nuclear power plant would be dead and useless without the human motivation and direction provided by its operating team, recognised by Event-noise theory as an integral part of the plant's holistic constitution. That there are few catastrophic failures in major technological systems which have not been primarily due to human error establishes the truth and importance of this fact. Therefore, assurance of the integrity and stability of the plant's system of human factors is essential to its safety and reliability. An inference from Goedel's theorem justified by field experience implies that the vital concord, consistency and efficiency cannot be wholly protected against entropic deterioration by efforts from within the system itself. Action by an external agency is needed and that is the principal duty of inspection, a topic discussed in the next main Section and in Document No. 4 of the Annex. A further inspectional task would be to distinguish the potential precursors of a fold-curve encounter which the continuity of Catastrophe theory suggests are always present in the En flux, though not necessarily either overt or immediate, being usually emergent S-En or a sudden human lapse. In fact, attempts to ascertain such loss of resistance to failure have already been made in the American Licensee Event Reporting (LER) scheme (15) from which an excerpt is shown in Table III. The scheme has been orientated towards faults and incidents arising in the physical realm rather than towards evidence of human failings.

Catastrophe theory has not been uncritically received. Zahler and Sussmann (1977) among others claim that it has 'no advantage over better established mathematical tools' quoting its failure to produce 'true testable predictions'. Brian Goodman (Open University), reviewing a critique of the theory by the Russian mathematician, V. I. Arnold (1984), describes it as the 'most extraordinary mathematical development of the Century'. However, its use in this thesis has been, not to predict, but to explain the nature of the relationships between those disparate factors that are able to cause a nuclear power plant accident, and that is a very different matter. Thus, elementary Catastrophe theory

has been used to build the Cuboid Model ideogram of Figure 12 to assist conceptualisation of the vicissitudes that accompany the operational behaviour of a nuclear power plant.

12.6 Overview

The 'Two Cultures' disjunction has long consigned the field aspects of engineering to limbo compared with the attention given to theory, design and administration. While this position was tenable in a world of the relatively simple technologies of wireless, uniselectors, permanent way and 'Ocean Queens', it is certainly not so for the advanced technologies of today, the pace setter among which has been nuclear power. Full recognition and understanding of the field accomplishments required of engineering have now become essential for both the continuation of technical progress and for the defence of safety in the more hazardous applications of science, the latter having become a major issue of social concern.

Event-noise theory is an attempt to move beyond the formalism of quantitative systems methods which are preoccupied with analyses of design into an objective regime where due weight is given to the realities of engineering experience as these relate to the safety and reliability in technology and particularly nuclear power. While the paramount importance of design and theory must be acknowledged as the themes which determine all practice, a design is seen by New Treatment as a packet of instructions to be transmitted from the design authority through time for implementation on a remote shop floor, construction site or control room. As for all signals, the design message suffers distortion, mutilation and loss of information during transmission, that is it experiences the phenomenon of 'noise'. Event-noise theory extends the concept to embrace all effects which impoverish, modify or corrupt the design intent. Two main classes of 'noise' are distinguished. The first, of latent effect, is 'Static Event-noise' (S-En) which describes flaws in the design as hidden defects introduced into the plant during construction or through later modifications or maintenance, its elements emerging unexpectedly from time to time. The second, 'Dynamic Event-noise' (D-En), is an active component embracing the sequence of accidents, failures, faults, errors and multifarious incidents of an immediate nature which disturb, or otherwise destabilise, the plant in its proper function. D-En combined with emergent S-En together constitute the Event-noise stream which characterises the operational experience of a plant from commissioning to terminal shutdown.

In reliability science, this is described by the 'Bathtub Curve' of failure rates plotted against plant operating time.

Attempts to express the Event-noise characteristic of a nuclear power plant in mathematical terms have been shown to produce intractable expressions, particularly that for the transcendent probability of catastrophic failure, a very low probability event identified as the terminal 'spike' of Event-noise represented by the term $Pr(\bar{L})$. Recognising the futility of this effort, attention was turned to representation of the behaviour of the reactor system by an adaption of Catastrophe theory. This enables the stream of Event-noise to be described in terms of the experience of a point moving in a probability field called the Behaviour Surface that forms the upper sheet of a cuboid catastrophe model. Deformities in the Surface represent potential disturbances to the stability of the plant which, if realised, produce Event-noise ranging in scale from minor incidents to catastrophic failure. The degree of stability is depicted by the attitude of a stub vector located at the point, the vector being normal to the Surface and thus becomes tilted as it passes over protuberances. Its inversion at lip of the fold-curve symbolises catastrophic failure, represented by the terminal event, $\bar{L}$, in the Event-noise flux. The point bearing the stub vector is the image of another moving in the lower sheet of the model called the Control Plane which is parallel in aspect to the upper surface. Its instantaneous position is determined by two orthogonal co-ordinates, one representing the operational decisions of management and the other, the overall response of the plant as a system of interacting, synergistic physical and human factors. The path it takes on the Control Plane is a hysteresis loop owing to the lack of proportionality in the response linkages. Safe and reliable operation of the plant requires an engineering strategy that must reduce the probability of exposure of the system to effects caused by encounters of the image point and stub vector with major abnormalities of the Behaviour Surface and, particularly, that of the maximum accident of catastrophic failure should it pass across a fold-curve.

Three important conclusions may be drawn from the foregoing first-order adaption of Catastrophe theory to the Event-noise concept. First, it is descriptive and explanatory and in no way predictive in any quantitative sense. Second, the plant's operational policy must be related to its existence as a holistic entity of interacting physical and human components which may give indications that can

supercede historical considerations based on analyses of design. That is to say, the fold-curve encountered may represent a catastrophe beyond the DBA or outside the predictions of a quantitative risk analysis, two examples of which have been cited. The third is that a presumption of continuity made from Catastrophe theory predicates the existence of precursors in the Event-noise sequence preceding a major disturbance of plant stability. Assurance of safety, therefore, lies in their perception and consequent change of operational policy so that an encounter with a major protuberance or fold-curve in the Behaviour Surface may be avoided. Efforts to detect such harbingers have already been made in U.S. nuclear industry, but the reporting schemes are more concerned with failures and failure rates for physical components and sub-systems than with the equally important matter of quality in the human aspects of plant management.

13 EVENT-NOISE: CAUSATION, SIGNIFICANCE AND PRECURSORS

> 'Hinton (Sir Christopher) wrote that engineering is an art rather than a science because in the arts there are no single answers to problems: engineers are faced with many possible answers, each one a compromise between conflicting advantages and disadvantages. ... ... the previously unknown hazards of nuclear power presented a new challenge (paraphrased for brevity) ... ... In the event - a lack of precedent in matters of health and safety - the atomic energy industry set a notable example as the first through rigorous scientific control of its hazards before, not after, evidence of damage had enforced action.'
>
> Margaret Gowing,
> Independence and Deterence: Britain and Atomic Energy, Vol. II,
> MacMillan, London, 1974, p.101.

The study of the phenomenon of plant Event-noise (En) has so far been mainly one of classification concerned with the macro-aspects of the total En experienced by a nuclear power plant over its useful life cycle. Little attention has been paid to the micro-aspects of the particular causations of these flux elements per se. They are, nonetheless, important because in the En experienced may lie clues that the system is moving towards a fold-curve and possible catastrophe as described in Section 12.4 et seq.

Any approach to absolute safety in nuclear power is either illusory or asymptotic, but confident attainment of the latter is feasible and can be achieved by good engineering through evolved reliability in design, construction, operation and maintenance as, for instance, in the case of the civil engineering works that are the Dutch dykes or in the space vehicles launched by the U.S. National Aeronautics and Space Administration. In its development, the New Treatment advocates this line and has attempted to show how interdependent it is on the above functions. In particular, it cannot be achieved through design studies alone because of the 'noise' that mutilates the design message in the process of conversion from ideas to reality.

The construct of the Event-noise/Catastrophe theory in the cuboid model of Figure 12 symbolises the risk situation as it is in reality for a nuclear power plant. The roughness of the Behaviour Surface with its asperities, bumps and fold-curves could be represented by probability density functions for the various En elements, but, though this might be more satisfying mathematically, it would not

be very helpful in a qualitative study such as this one and the topic is not pursued further here.

13.1 Some further deductions from En-Catastrophe theory

The mechanism whereby the En flux produces significant disturbances to the plant's stability, represented by 'spikes', and the realisation of catastrophic failure by an encounter with a fold-curve on the Behaviour Surface of the En-Catastrophe model have already been discussed. A point to note is that the Behaviour Surface is a probability field and not static. Not only can the Surface abnormalities change their positions in that field, but new ones may appear. The 'Three Mile Island' catastrophe is such a case because that disastrous incident was beyond the Design Basis Accident (DBA), representing an encounter with a fold-curve immediately created by management default and operational errors. The attitude of the stub-vector represents the instantaneous state of the plant and, therefore, the history of its attitudes up to the point of a major instability can expose the precursors that led to that instability. While these obviously have no predictive value because the event has already occurred, they provide valuable data for 'fixes'. Furthermore, they can reveal operational paths to be avoided in similar plants, but more significantly, they disclose management and organisational frailties that can reduce reliability and safety. For instance in the case of the 'Three Mile Island' incident of 1979, a notable weakness was the lack of proper technical understanding of the plant shown by its operators and certain technical advisors who arrived later on the scene. A conclusion may be drawn from the probabilistic nature of the Behaviour Surface is that, while the provision of sophisticated information technology can be of assistance to the proximate plant operators by giving the knowledge that may be otherwise lacking, it cannot replace satisfactorily the decision functions of the human operator. The program written for the purpose of overriding independent operator decisions must be based on the assumption that events following an incident will take a predetermined course, but in the event that course may not be followed by the system or even exist in the future state. As Ludwig Wittgenstein contended:

> '5.1362 The freedom of will consists in the impossibility of knowing actions that still lie in the future.'
>
> Tractatus-Logico Philosophicus
> (Trans. Pears and McGuinness)
> Routledge and Kegan Paul, London, 1972.

In fact, the arrangement suggested above in Section 12 could be dangerous, as for example the incident of the Air New Zealand Mount Erebus disaster of 1979 (See Appendix II). Awareness of the approximate behavioural position of a fold-curve distinguished as a potential MCA provides no reason for assuming that there are no other unsuspected fold-curves on that surface.

The constructs of the probability field of the Behaviour Surface and the decision field of the Control Plane of the cuboid model of Figure 12 depict the inherent pervading presence of human intellect, actions and skills in the reality of the operating system. The state of the probability field itself and the operational path taken by 'Q', the image of the instantaneous control position, indicated by 'P', are the outcomes of managerial and technical decisions and the responses of the holistic system thereto. The control path is taken purposively to avoid situations of significant risk to the plant represented by major surface anomalies and an identified fold-curve. The human factor thus plays a dominant part in every aspect of the creation and operation of the system and all faults and failures in the ultimate derive therefrom. The certain attainment of nuclear power plant safety and reliability is therefore tantamount to the successful management of the immanent human factors, and this theme will be dominant in this text from now on. Although this may seem patently obvious, it has received less than due acknowledgement and attention has been concentrated on matters of theory and design at the expense of practice in their realisation in the field. The situation is characteristic of Western society today, being the result of the 'Two Cultures' disjunction which still separates the administrative, legal and literary intelligensia from the engineers and technologists (See Section 8.1), and that formalism also evinced by certain applications of systems analysis as noted in Sections 8.1, 9.6 and 12 above.

A safety conscious management aims in its engineering to steer a smooth and safe path through the hazards of the Behaviour Surface as far as these have been identified. Such a tactic was adopted for the U.K. Magnox nuclear plants to avoid a break-away fuel element fire in the graphite core following a burst duct LOCA. The operational decision situation involving a 'fire risk criterion' (Dale and Harrison, 1971) is discussed in 'Thermal Control of the Magnox Nuclear Heat Engine' (Document No. 5 of the Annex), particular attention being directed to its Figures 1, 3, 5 and 7. Despite the most careful plans, any such

safety strategy will be inevitably plagued by unknowns which can be eliminated only through their realisation in operational experience or by the artifice of virtual operational experience as through the 'design-make-test-fail-fix' method of NASA which was used to establish confidence in the reliability of the 'Apollo Moonshot' vehicles (W. M. Bryan 1975). The flow of Event-noise created in the passage of 'Q' over the Behaviour Surface described in Section 12.4 et seq. will contain precursors of its approach to a cause of major instability, that is to a 'spike' or a fold-curve, owing to the continuity of that Surface. In other words the event is the consequence of a chain of causes, although the links in that chain would not have been discerned by the proximate observers before it occurred, otherwise the sequence could have been arrested. Indeed, the tragedy of October 21, 1966 at Aberfan was notorious for the gross lack of perception by those responsible for the safety of the No. 7 spoil tip.

13.2 The enigmatic nature of event precursors

Precursors deny themselves because if they are perceived and action taken, the event does not occur and they are precursors only in a virtual sense. Despite the fact precursors to major En phenomena may be known with certainty after the event but not beforehand, it has been argued in the preceding Section 12 that analysis of the En elements emitted by a plant can reveal things about the state of the system, thereby identifying weaknesses that could presage failure if not corrected. However, these elements which might be called 'virtual precursors', are seldom discernible by observers within the system, as for 'Aberfan' (supra), 'Three Mile Island' and the other catastrophes that are legion.

13.2.1 A role for technical intuition or engineering judgement

As there are no certain logical processes by which the future may be foretold, man's need for reliable harbingers of things to come has brought forth legions of soothsayers from the Stone Age witchdoctors to modern systems analysts. Nature through evolution has, however, not been unresponsive to this demand and the human brain over some two million years of necessity has acquired a remarkable faculty called 'intuition' (See Glossary) which is the power of immediate intelligent insight and is less mysterious than may appear at first sight. Man can hold in the unfathomable depths of his memory a vast store of information.

A feature of this data base is the penetrating associative property of the access facility which can recognise faint analogies and similarities, a problem that has yet to be solved for artificial intelligence. Intuition coupled with the faculty of reason underlies most creative human endeavours, as for example its exercise by successful entrepreneurs and politicians. In the field of science, intuition enabled Max Planck to resolve the dilemma of the 'Ultraviolet catastrophe' by correcting the radiation formula (Werner Braunbeck 1974). This faculty of perception appears in technology as 'engineering judgement' and when highly developed, as in the case of experienced engineers, has led the way to great technological advances, not least, the electric telegraph, telephone, radio, radar, the jet engine and atomic energy itself. In the actuarial field, it is the necessary forte of the successful assessor of the more exotic risks.

A solution to the problem of discerning such ephemeral potential precursors in the En flow from a nuclear power plant may lie in using the intuitive faculty. A difficulty is that in technology it is a specialised rather than a generalised talent and it would have to be applied to a particular type of plant by an engineer with detailed knowledge of its constitution and management. Attainment of credible ability in it depends therefore on long practical experience in the field supported by ample theoretical and technical knowledge and the ability to exercise a particular intuitive skill with penetration and perception. Such individuals are scarce owing to the tendency to specialism in engineering, but are to be found in the community of engineering inspectors who have to acquire an interdisciplinary approach. Moreover, it appears to be measurable by psychophysical methods, a point to be made in the next Section.

13.3 Loss of resistance to failure, a harbinger of major system faults

Experience in the aeronautical industry and particularly in air transport has established a concept of 'perception of that loss of resistance to failure' which generally heralds the advent of an accident or mishap. It was initially developed in Latin American airlines to improve the efficiency of maintenance and to reduce costs. Its reported success attracted the attention of established air transport operators in the U.S.A. and formally constituted debriefings of aircrews along similar lines are now customary. Pilots and engineers fresh from experience with a machine are able to report on perceptible changes in

performance suggestive of deterioration in function. Maintenance is then directed towards correction of the identified weaknesses rather than invested in blanket routine schedules which can often introduce faults per se (M.A. Laceby 1976).

The Licensee Event Reporting (LER) scheme that covers selected Event-noise elements as developed of recent years in the U.S. nuclear industry (15) is analogous to the management of aircrew debriefing data. While no such scheme of intuitive analysis of nuclear plant event reports could give an assurance of absolute effectiveness because even the most perceptive of analysts may miss a clue, a comprehensive one could, nevertheless, reduce still further what is already a very small risk. For instance, it is doubtful if the pre-accident situation at 'Flixborough' in May of 1974 would have escaped perception of its hazardous instability if it had been exposed to scrutiny of the foregoing kind, when the catastrophic sequence would have been aborted.

13.4 The problem of lethargy and centripetal tendencies

The organisation of a nuclear power station including the higher levels of management in the controlling utility is a closed system of directors, managers, operators and technicians, exchanging instructions downwards and passing information upwards in vertical hierarchical channels which acquire centripetal propensities that inhibit horizontal flows among departments. This is a wellknown weakness in large corporate bodies which justifies recourse to management consultants. A serious consequence of this departmental egocentricity is that it can conceal lethargy and discourages internal criticism of weaknesses. These tendencies are inimical to safety and reliability. The intrusion of the disinterested, independent inspection imposed by a statutory body like the Aeronautical Inspection Directorate in the field of supply for the armed forced or by the Nuclear Installations Inspectorate and the Nuclear Regulatory Commission in the U.S.A. can exercise a potent corrective effect, breaking down psychological barriers between departments and encouraging internal self-criticism otherwise lacking (A. K. Nuttall 1946, T. Griffiths 1966). The nature and application of inspection are treated more fully in Documents 3 and 4 of the Annex and in the following Section with particular application to the management of low probability events.

13.5 The assurance of safety and reliability by stability of form

Early experience in use with new types of plant or variants of an established type is invariably 'noisy'. It is impossible to foresee and eliminate in advance all the faults and failures that will arise when a nuclear power plant of this kind is put into service. The initial or 'early failures' slope of the 'Bathtub' reliability curve of Figure 10 depicts the occurrence of these failures and likewise for the experience on the Behaviour Surface of the cuboid En-Catastrophe model of Figure 12 as the image point, 'Q', proceeds around the operational hysteresis loop. As the faults emerge and are eliminated by 'fixes' taken to prevent their re-occurrence, being designed-out, contained by effective administrative controls or otherwise treated, the system acquires an improved reliability in an asymptotic approach towards the highest feasible standard. Such is the case of the Rolls-Royce automobile for which it is claimed changes in engineering and styling are imperceptible over less than a decade (Daily Telegraph 1976, Edward Eves 1979), the manufacturer's aim being to maintain the quality and reliability of a product of known excellence. The phenomenon is well-known in nature as the principle of the survival of the fittest that ensures the continuance of the best and most reliable of forms that survive by their stability and resistance to failure under stress (Roberts and Tregonning 1980) which is exhibited in 'the robustness of natural systems'.

As interpreted in the development of nuclear power, the occurrence of certain Event-noise elements of permanent system significance (S-En) in a generic reactor type, say the appearance of cracks in the membranes of the main coolant gas ducts of certain British reactors, tends to diminish and approach zero as the system moves towards greater safety and reliability. This implies that reactor designs should be standardised as reliability evolves in use. Ad hoc design improvements should therefore be resisted, except as the need for change is shown to be desirable by experience because of the proven superiority of established, stable forms over novelty (John Maddox 1984), despite any attractions of the latter scientistically.

13.6 Overview

En-Catastrophe theory offers an approach to the management of the hazard of catastrophic failure of a nuclear power plant that is pragmatic rather than theoretical. Assuming that the design has been subjected to a comprehensive and penetrating safety analysis and has

been constructed according to that safety assured design, then the plant will not suffer the DBA or MCA or other envisaged unlikely accident as their probabilities are metaphysical. Despite that, something unforeseen, and no less catastrophic could happen instead. But, such an event cannot occur without prior links in its failure sequence and, if these precursors could be discerned before the prospective event, then it could be averted. However, such precursors are usually 'virtual' in that their identification is enigmatic and their status as such can never be confirmed as efficient with certainty unless the untoward incident occurs.

The history of incidents, faults and failures experienced by a nuclear power reactor, or other industrial plant, has been described in terms of Event-noise. The process of creation of an En flux has been depicted in terms of the cuboid model construct of Figure 12 for which the operating strategy is one of steering the plant in safety through the instabilities of a Behaviour Surface which is an incommensurable, though objective, probability field. En-Catastrophe theory thus presents a likelihood scenario that describes the current state of the plant as a holistic system in a human dimension rather than in terms of some prior safety assessment of its design. Then, given a plant of verifiable sound design and construction, reliability and safety thereby depend upon competent engineering in achieving that end. The state of this complex plant-entity can be monitored by analysis of the En flux emanating from it and evidence of loss of resistance to failure detected. However, this requires an exercise of human judgement attuned to the given technical situation which must be aided by a linked examination of the system in operation so that any entropic deterioration in its efficiency may be apprehended.

Success in technological analyses of the foregoing kind requires an intuitive faculty of penetrating intellect supported by relevant theoretical knowledge and pertinent practical experience, in other words good engineering judgement. When the safety of a nuclear power plant is defended in this way, the probability of a disastrous accident becomes very small indeed and may be properly presented as a tolerable risk in view of the accompanying energy amenity.

Despite the foregoing precautions there remains a risk, though asymptotic to zero, that in some rare and unusual circumstances a previously unperceived threat of catastrophe may be realised: the 'Zero-Infinity' potentiality. Nonetheless, further confidence in safety may be assured through stability of form as the system's reliability is proved

by experience in use for a set of like plants. This requires that changes in an established design of proved worth must be resisted except where there is an unchallengeable case for modification on cogent safety grounds.

PART FIVE

INSPECTION: FEATURES, FALLACIES AND FACTS, AND A SYNOPSIS OF THE NEW TREATMENT OF LOW PROBABILITY EVENTS

Sections 14 and 15 comprising:

A critical review of inspection, the societal regulatory agency of ancient antecedents that has evolved to meet the need of modern technological civilisation for a wide range of checking, investigatory, monitoring and police functions which are, in the main, those which it is incumbent on the State to provide; some fallacious ideas about inspection that are held in certain scientific and establishment circles: the hierarchy of functions that characterise engineering inspection, namely 'Viewing', 'Examining' and 'Executive Inspection'; Quality Assurance and Quality Control and their inspectional identities; the innate inability of an inspectional organisation to appraise its own performance (Goedel's theorem); the need for accountability and Signal Detection Theory as a means of appraising the efficiency and reliability of risk assessors and safety inspectors engaged in regulatory activities.

A synoptic and recapitulatory survey of the case made in justification of the New Treatment of Low Probability Events and of the style of regulatory inspection central to it for which the U.K. Nuclear Installations Inspectorate has been taken as a representative example.

THEMATIC SUMMARY

Throughout this study an attempt has been made to describe and justify a new approach to the management of those low probability events that can end in the catastrophic failure of a technological innovation, and of those incidents that concern nuclear power plants in particular. This New Treatment, while embracing the scientific advances, engineered safeguards and other things that have made nuclear power, despite its grave potential hazards, an innovation which experience has shown can be contained in effective safety, emphasises that this state is inherently unstable. It depends absolutely upon the integrity of the engineering involved for which the new style of inspection has proved to be the guarantor. It is further suggested that inspection according to the New Treatment could offer the assurance of safety in the maintenance of that recognised state of negligible risk needed to inspire the public trust necessary if the hazard of nuclear power is to be accepted as tolerable.

14 PROBLEMS OF INSPECTION IN THE DEFENCE OF SAFETY

'In any formal system adequate for number theory there exists an undecidable formula - that is, a formula that is not provable and whose negation is not provable, the undecidable formula being true. It therefore follows that it is impossible to prove the consistency of a formal system of this kind within the system itself.' - Goedel's Theorem.

Anthony Quinton,
Trinity College, Oxford,
Excerpt from The Fontana Dictionary
of Modern Thought,
Fontana/Collins, London, 1971, p.267.

In 1931, Kurt Goedel published a paper setting out his famous theorem which is paraphrased in the above quotation. Its immediate result was to bring to an end attempts with which Bertrand Russell was associated to formalise mathematics in one complete and consistent system. Professor J. van Heijenoort described its far-reaching effects thus:

'Goedel's theorem shattered the Aristotelian ideal of perfect deduction from first principles. The bounds of mathematics cannot be those of one formal system. Since mathematics has often been regarded as the standard of rational knowledge to which other sciences should attain, Goedel's theorem seems to acquire significance for the whole body of human knowledge ... ... However, all sciences other than mathematics are so remote from a complete formalisation that this conclusion remains of little consequence outside mathematics.'

'Goedel's Theorem: Epistemological Significance',
The Encyclopedia of Philosophy, Vol. 3,
Collier MacMillan Publishers,
London, 1967, p. 356.

In spite of the caution of conservative logicians like Heijenoort, the generalisations of Goedel's theorem and its corollaries are still making their mark on modern thought. One of the wider inferences is 'the falsity of any theory which takes human mind to be a mechanical, deterministic system' (Anthony Quinton - ibidem).

If the human mind is not mechanical and deterministic , then neither are the disciplines that it creates and they are stultified when attempts are made to so constrain them. This principle applies to engineering science and its practice and, not least, to engineering inspection which it has been argued by the writer, here and in his fourth paper of the Annex, is the key to safety in nuclear power and an essential factor in securing popular acceptance of that state.

14.1 The nature of 'inspection'

The activities embraced by the term 'inspection' are very wide and varied and are in no way confined to engineering. Neither are the dictionary definitions restrictive, for example:

> 'To examine closely, especially for faults and errors',
>
> Collins (New English) 1979,
>
> and
>
> 'Looking carefully into, viewing closely and critically, examining something with a view to find out its character and condition',
>
> OED, Edition 1901.

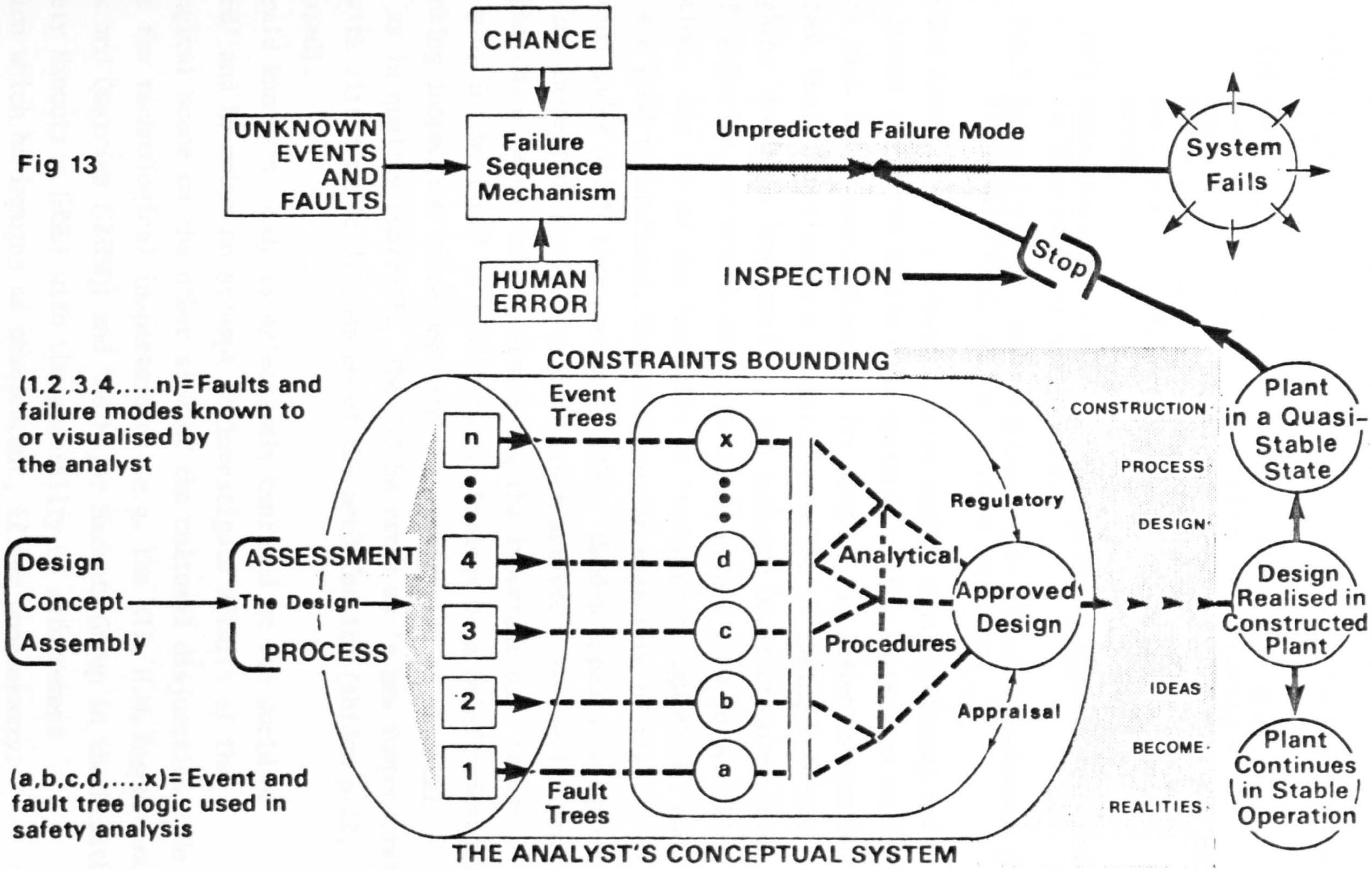
Inspection is an activity of great antiquity used by governments to back the authority of the state. Today, it has many varied and specialised functions and is largely concerned to protect the health and welfare of citizen and community. Over the past century, it has assumed important engineering and scientific dimensions to meet the regulatory and safety needs of technological advances in industry, medicine, power generation and transport among other things. Of particular interest is the part it can play in the management of the risks of catastrophic low probability events (LPEs) stemming from the peculiarly hazardous processes and substances used in the exploitation of advanced technologies, not least in the case of a nuclear power plant as illustrated in Figure 13.

Inspection is largely, but by no means exclusively, concerned with the task of detecting, anticipating and investigating all manner of human errors, i.e. lack of foresight, omissions, mistakes and malfeasance, with a view to preventing or correcting them and, thereby, aborting their consequences from tax evasion to radiation accidents. Among the few substantial studies of inspection is the profound research by Gerald Rhodes (1981/a) into 'Inspectorates in British Government'. He distinguishes seven varieties of official inspection, namely:

(i) Enforcement - to ensure compliance with duties and obligations imposed by statute or ordnance. In this group Rhodes lists 34 inspectorates that include H.M. Factory Inspectorate, Cruelty to Animals, Wages, Drugs, Gaming and the Nuclear Installations Inspectorate (NII) among others equally diverse.

DESIGN SAFETY ANALYSIS, IGNORANCE OF MECHANISM AND INSPECTION

Fig 13



(ii) Efficiency - monitoring the performance of bodies which receive and disburse government grants, among which Rhodes names some six bodies concerned with education, the police and fire services.

(iii) Internal Management - surveillance of numbers and quality of staff in Government departments.

(iv) Revenue Collecting - collection of taxes, customs duties and other imposts.

(v) Checking - in this group Rhodes mixes H.M. Quality Assurance Directorate (QAD) which is concerned with engineering inspection in the supervision of Ministry of Defence procurement contracts with the surveillance of such things as the proper use of regional development grants.

(vi) Quasi-judicial - hearings into planning appeals referred to Department of Environment.

(vii) Investigatory - investigations into aircraft accidents and financial frauds in the field of commerce.

Rhodes categories are administrative rather than functional and he pays little attention to the modi operandi of the inspectors at the practical task interfaces. However, for most of the inspectorates he has listed, their function is a formalised matter of taking evidence and weighing its legal implications, for instance dereliction of duty, abuse of authority, or breach of regulations, with a view to possible prosecution. The job of the inspector is 'to enforce regulations and, if they are good regulations, they achieve the objective of the legislation under which they are made' (19). Rhodes appears to ignore engineering inspection (infra) as a distinct activity, seeing it merely as a mechanism of enforcement, dismissing the important part it has come to play in the field of industrial technology by a brief reference to 'checking inspection concerned with the examination of physical objects as in quality control'. The NII he rates as 'a new inspectorate set up with little or no discussion of the need for it' (ibidem p.22, paraphrased).

Gerald Rhodes's study is effectively confined to the world of 'The Word' and he makes no attempt to investigate affairs of the technological scene on the other side of the cultural disjunction. He brackets the technological inspectorates, e.g. the NII, H.M. Inspectorate of Mines and Quarries (HMIMQ) and the Major Hazards Group in the Health and Safety Executive (HSE) with the generality of enforcement inspection which he impugns as obsolescent, if not unnecessary.

To quote him:

> 'It can be said therefore that in the 1970s enforcement inspection continues to flourish largely because nobody has seriously explored - and certainly not in any systematic way - either the limits or alternatives to inspection.'
>
> Gerald Rhodes,
> Inspectorates in British Government,
> Allen & Unwin, London, 1981, p. 226.

Committed to the above position, it would have been difficult for him to admit to the existence of another kind of inspection lying ouside his administrative categories, being one that was perceptive, consultative and participative and of a form accessible to accountability. Nonetheless, engineering inspection undeniably exists as a necessary, emergent and evolving discipline, though one as yet lacking recognised formal integration and currently receiving less than due attention in spite of its importance in the management of LPEs.

14.2 Aspects of 'engineering inspection'

Until the end of the 19th Century, engineering inspection was an informal task falling to foremen or one of self-appraisal by craftsmen and finishers. As the products of industry were for the most part unique structures or simple artifacts and machines, it was little more than 'checking inspection', Rhodes's fifth category (supra). However, the invention of heavier-than-air flight by the Wright brothers in 1903 proved to be a turning point in its evolution. Their invention of the flying machine was followed by the rapid development of military aviation and the mass production of warplanes.

By 1911, the number of these machines lost in crashes had become a matter of official concern. Dr. R.T. Glazebrook (1913) was commissioned to hold an inquiry into the cause. He reported that the failures were due to manufacturing defects which could be remedied by properly organised inspection. His report was accepted and in January 1914 the Army Council authorised the formation of an Inspection Department. This became the AID (Aeronautical Inspection Directorate) which continued under that title for nearly 70 years when, quite recently in a major Ministry of Defence re-organisation to meet the call for better integration of procurement within NATO, it became the Aeronautical Quality Assurance Directorate (AQD). Until that change, its basic approach to engineering inspection remained relatively unaltered. In the U.K. it has been the antecedent of all similar engineering bodies

and, latterly, of the NII as described in the Appendix to Document No. 4 of the Annex. Indeed, it may be truly said to be the antecedent of all systems of manufacturing inspection, notably those of quality control by statistical methods (infra).

Rhodes' failure to deal adequately with the engineering aspects of inspection may be attributed to lack of a real perception of the sophistication of the technical entities that are the creations of modern technology in its commercial applications, but probably more to the fact that engineering is an activity of 'The Deed'. Judged from the viewpoint of the other culture across the technological disjunction, it would be deemed to be a subordinate function, being merely an adjunct to the executive duty of the inspectorate concerned. On the contrary, in the technological field, engineering inspection is far from being a lesser complement to a given regulatory process, but is rather the process per se. It differs from the seven categories of inspection named by Rhodes (supra) in that it has the peculiarity of an extra dimension in technology. This extends far beyond the simple mechanics and metrology of the checking in the view-room or go-no-go inspection bay to the very frontiers of modern science itself, for example as practiced by the National Aeronautics and Space Administration (NASA) in assuring the reliability performance of the U.S. 'Apollo' Moonshot project space vehicles.

By virtue of its extra degree of freedom, the faculties of engineering inspection range from the skill exercised by a mechanic scrutinising pieceparts to the challenging intellectual task of decision making during the on-going processes of inspection of, say, a nuclear power plant during its construction, commissioning and initial operation. In such a process, inferences drawn from the technical assessment of design must be combined with information acquired by direct inspection and testing of the multitudinous facets of the entity in question.

14.2.1 Orders of Engineering Inspection

The writer has distinguished four levels of engineering inspection in ascending order of technological complexity and managerial responsibility (O.H. Critchley 1981), although the fourth, 'Inquiry', merges again into the administrative scene and is not discussed further here, except to notethat it may require both scientific eminence and great political acumen. The three truly engineering degrees are:

(i) Viewing - the most fundamental and commonly identified aspect involving direct scrutiny of a piece-part or basic element of a system to enjoin its conformity with plan, drawing or specification or to confirm compliance with detailed procedural instructions or regulations determining a technical process. Its exercise requires little or no discretion, although a high order of skill may be needed. It is comparable with Rhodes's fifth category of 'checking' and among these other things is used to provide sampling data in quality control schemes.

(ii) Examining - a higher tier function of a discretionary nature used to assess the attainment of a design intent by examination and by testing of completed products or parts of such products, structures, equipment or systems of work, often depending on sampling and analyses of the results of viewing. It includes technical safety assessment of design, but not managerial decisions based thereon.

(iii) Executive Inspection - a managerial activity concerned with the extent to which the design intent is achieved in compliance with drawings, plans and specifications and with assurance of the attainment of that intent during manufacture, construction, commissioning and operation of the given plant or system. More particularly, it is interpretative and involves decision making about deviations from the foregoing directions owing to design errors, omissions, equipment faults, material shortages and other defects. Besides, it is participative in that defect remedies involve negotiation with the designer or his client. Furthermore, it is the level at which sanctions may be imposed to secure the correction of flaws, faults and weaknesses in the artefact or its performance, and is concerned with policy formulation in respect of the purposes of its inspectional role.

The three tier structure of Engineering Inspection was reflected ab initio in the organisation of the AID with a staff of 'Viewers', 'Examiners' and 'Inspectors'. The latter was the managerial grade (Flight 1915).

The third and executive aspect of engineering inspection as defined above is couched in terms appropriate to the work of a regulatory body, like the NII, USNRC or H.M. Factory Inspectorate's specialist branches. Of course, it applies more widely in industry and is carried out by inspection groups maintained by insurance companies, for instance Lloyd's of London, or by independents working on a consultancy basis. Often, it is internalised as a safety and reliability department in a large corporation. The (then) British Aircraft Corporation at Filton near Bristol used a highly qualified engineering inspection team during the Concorde program who worked closely with their 'French

counterpart in Toulouse and the U.K. Civil Aviation Authority's (CAA) safety branch.

Every feature of the Concorde design was analysed for safety and prospective reliability in service and assessed by powerful statistical methods with qualitative oversight. The requirements of constructional quality control (QC), ie. Viewing, were carried out by lower tier teams (M.A. Laceby 1976). While Executive Inspection cannot entirely prevent the rare, catastrophic LPE, it can eliminate or reduce the likelihood of foreseeable major faults and accidents to a minimum that in most circumstances should be socially and politically acceptable.

14.2.2 The characteristics of Executive Inspection

It may be asked on what authority do the terse definitions of 'Executive Inspection' and its subordinate functions given in the preceding sub-section rest. The answer is that there are few quotable sources and much of the relevant confirmatory information remains undivulged and currently inaccessible in classified files and papers. As a result the topic of Engineering Inspection has been litte researched and the definition is mainly drawn from the writer's personal familiarity with evolved practice and the lore of the engineering inspectors who have been his colleagues. It has been the objective of a private study over some 20 years from which this thesis and the supporting papers have emerged. Considerations of military and official secrecy are not the only reasons for the lack of authoritative references. Another important limitation has been the interdisciplinary nature of the field that might have been allied to management studies in engineering, but that topic has only been accepted by university engineering faculties as scientific in the past decade or so.

There are, however, a few references that reveal at least the framework of the discipline. Between the wars, Lt Col. H.W.S. Outram, then head of the AID, finally secured publication of an article on engineering inspection in the supply of aeroplanes for both civil and military use. An abstract of the passages relevant to Executive Inspection is given below:

> Inspection starts at the design stage when the designer defines the materials and mode of construction. It is the task of the inspector to see that all the design requirements and intents are met in respect of material, dimensions, handling during manufacture, assembly and final testing. This is an unbroken chain from raw material to flying machine and it is the responsibility of inspection to see that it remains unbroken until the complete aircraft is ready for trial flight.
>
> If any Government or other body of independent inspectors were to carry the whole responsibility, that organisation would become so large as to be unmanageable and, aside from consideration of cost to public funds, would have the undesirable effect of taking responsibility from existing efficient internal inspection departments that exist in most firms and their subcontractors. The British system of aeronautical inspection is, therefore, based on each firm carrying out its own inspection in a manner approved and supervised by the AID on behalf of the Air Ministry. It is thus possible to extend inspection back to the primary raw materials, continuing to the complete aircraft and all its ancilliary equipment.
>
> British Aeronautical Inspection,
> The Air Annual of the British
> Empire, Vol. II,
> Gale and Polden, London, 1930, pp. 226-250.

The links in Outram's 'unbroken chain' included applications of the most advanced technologies of the time and necessitated the support of a large and well-equipped Test House with elaborate facilities and a staff of specialist engineers and scientists. His concept continues to be characteristic of Executive Inspection in the industrial exploitation of advanced innovatory technologies and, not least, of nuclear power (K.J. Meekcoms 1980 and supra). The American approach has been described under the title of 'Quality assurance program evaluation' in a book by L. Marvin Johnson (1970) among a plethora of works on the topic. Although orientated towards private enterprise involvement in matters of the inspection of government defence contracts with a tendency to be more prescriptive, the principles are substantially those defined by Outram. Johnson's treatment of 'evaluation' is of a general nature, being little more than a survery of the administration of the process from which only the tip of an immense submerged mass of complex engineering detail is visible, to which he makes little reference. On the other hand, there has been much activity in the ancillary fields of Quality Assurance (QA) and

Quality Control (QC), but interest has been directed toward specific techniques of application (infra) rather than to the nature of the functions per se.

Owing to the lack of research and few reports or substantial publications on the discipline of Engineering Inspection, its span of ancillary technologies and formerly acknowledged identity seem to have become diffused among a number of supplementary scientific specialities. These include materials testing, industrial radiography and other non-destructive methods of defect detection, stress analysis and reliability technology, among other applied sciences. Neither the sophistication of the technologies nor the requirements of military and commercial secrecy have helped integration. As a result these inspectional arts have yet to be formally drawn together once more under the title of Engineering Inspection, although they are practised in a unified manner by the major engineering inspectorates, e.g. the NII, and other groups such as those maintained by the insurance industry.

To sum up, Engineering Inspection in its three domains of Viewing, Examining and Executive remains the arbiter of the degree of excellence attained in the products of the engineering and manufacturing industries and other, often unique, technological innovations, for instance nuclear power plants and the 'Apollo Moon-shot' program in the U.S.A.

14.2.3 Quality Assurance, Quality Control and Engineering Inspection

During the post-War decades there have been great increases in the quantity, range and complexity of the products of industry. Moreover, the processes of manufacture have become less labour intensive and more and more automated. It would, therefore, have been uneconomic to maintain consistent standards of conformity with specifications, of quality and of durability under modern factory conditions by the older practices of engineering inspection. To meet the need for control of quality, sophisticated methods of statistical sampling were developed to replace such operations as detailed piece-part scrutiny and the proportion of items viewed was reduced in step with optimisation of track and shop floor production costs. The risk of occasional unit failures or customer rejection of substandard or defective items is set at a level judged to be acceptable to the majority of consumers. These methods are known as Quality Engineering (QE) and more specifically as Quality Control (QC) or Quality Assurance (QA) or both.

After all, QE may be equated with many aspects of Executive Inspection.

The confusion between the higher brackets of inspection and Quality Engineering is illusory, being a matter of semantics. In practice, the terms QA and QC are used interchangeably and are usually associated with batch production of military supplies procured for defence and of commercial articles like TV sets, motor vehicles, automated domestic machinery and packaged prepared foods. In this text Quality Assurance (QA) is taken as the administrative framework in which a Quality Control (QC) scheme aimed at ensuring a uniformly high standard of quality in manufacture is executed.

In the case of weapons and other defence materièl, manufacture has to conform to elaborate QA clauses in supply contracts, as for example those laid down by the U.K.'Ministry of Defence Quality Control Systems Requirements', Series 502-21 to 502-26, or to currently updated versions. Quality Assurance and Control schemes also play an essential part in maintaining health and safety standards in manufactured products by enjoining compliance with statutory regulations and codes. Quality Control is an offshoot of Engineering Inspection and corresponds to Viewing and QA to the higher tier activity of Examining, functions described in Section 14.2.1 above.

The definitions are important because of the obtrusion of an augmented concept of QA into nuclear safety and particularly into the management of the potentially catastrophic low probability events that are identified with nuclear power. M.J. Milner (1983) in a review of QA in the nuclear industry describes it as 'an integrated management system with the task of efficaceously ensuring that company legal and contractual obligations to its customer and the community are met', a definition in accord with that of British Standard BS 5882:80 for a 'Total quality assurance programme for nuclear power plants'. Both ignore QC as an independent subordinate activity, subsuming it under works and site inspection and testing as a substrate in a hierarchial QA methodology. In the case of nuclear safety, Milner advocates a Quality Assurance Manager to work in parallel with the Works Manager and Chief Engineer to direct QA arrangements, the QA Manager having equivalent status, professional attainments and monetary rewards. On the other hand, BS 5882:80 rejects the centralist approach and recommends that the organisation of QA 'must not be the sole domain of a single group'.

In the case of undertakings with internal QA departments, it is desirable, and in the case of those awarded defence procurement contracts usually obligatory, for the QA function to be evaluated by independent appraisal. Such investigations fail to be convincingly objective when made internally as the evaluators in such circumstances are known to be blind to all butthe most obvious of their organisation's faults and weaknesses (L. Marvin Johnson 1970). The observation confirms an earlier inference from Goedel's theorem that a system of the QA type cannot be self-checking throughout its structure. This caveat is not trivial, but has profound administrative and political implications. J.R. Ravetz (1974) drew attention to it in his 'Who guards the guardians?' criticism of the NII. Moreover, it is of particular significance in the appraisal of schemes designed for the treatment of potential catastrophic LPEs in the case of nuclear power plants.

The semantic confusion about QA and QC disappears if the former practice of including all these inspectional arts and faculties, managerial and technical, under the general title of Engineering Inspection, to which they properly belong, were to be followed. This is not to derogate the importance of QA, but to recognise it as an essential adjunct to modern technology, particularly in the area of mass production. However, inspection at its Executive level lies deeper, being concerned with the interpretations and decision making that are required to resolve the problems caused by variations in the supply of materials and by obscurities in a design. They often involve baffling enigmas which do more to frustrate progress in design implementation than do difficulties in compliance with the minutia of specifications and codes. The latter are, nonetheless, the proper concern of inspection, but one that falls to its lower tiers of Examining and Viewing, already identified with QA and QC respectively.

In the case of nuclear power plants, QA and QC duties are the responsibility of staff of the utility and its principal contractors and suppliers, in Britain as a condition of the licence, for example in assaying material and in the non-destructive testing of reactor pressure circuit components. The wider role of Executive Inspection in the work of the NII in assuring the safety of the U.K. nuclear power program has been reviewed by Gronow and Gausden(1975/b) and again by Gausden (1982), the latter in a comparison with similar practices in Western Germany, France and the U.S.A.

There are other differences. For instance, in nuclear power owing to the high standards of quality and reliability that are essential in its engineering, safety inspection is a necessarily participative function, whereas in their formal philosophies both QA and Quantitative Safety Analysis (See Sections 7.2 and 7.3) appear to stand apart from activities in the domain of engineering. Finally, for brevity from now on the term 'inspection' will be used to mean 'Engineering Inspection', unless the context implies otherwise. Furthermore, it will also refer to 'Executive Inspection' except when the subordinate operations of Viewing and Examining are indicated.

14.3 Some misconceived ideas about inspection

The concept of inspection generally held by the administrative and political establishments and certain of their scientific advisers seems to be one clouded by increasing incomprehension. For example, despite the fact that Gerald Rhodes in his study of 'Inspectorates in British Government ' (1981) shows that inspection is a more complex activity than the mere exercise of quasi-police powers, he argues that:

> 'The original conception and ideal model of inspection was that of a means of checking that what Parliament intended should happen was in fact happening. It still has validity. This role symbolised by the traditional weights and measures inspector is in essentials a very narrow one. That alongside it there can exist a wider conception of the aim of inspection, one which seeks to relate inspection not simply to specified requirements but to the underlying purpose for which the legislation was evolved ...'
>
> Ibidem (G. Rhodes) - 173-174.

And, he goes on to treat what in his view is an odd fact as 'a matter of major interest'.

Moreover, Rhodes fails to discern the existence of the discipline of Engineering Inspection and makes only a passing allusion to the important functions of QA and QC. Yet, he proceeds to made the following comment on the NII;

'The Nuclear Installations Inspectorate was established with a dual function. It was the body which was to provide the Minister with the necessary scientific and technical appraisal of proposals to instal and operate nuclear plant from the safety aspect as a preliminary to the granting of a licence; and it was subsequently to inspect installations, specifically to ensure that they complied with the conditions on which the licences had been granted. That these two functions are really part of a wider role, essentially that of taking care of the central government's concern with the safety of nuclear installations has been clear from the beginning.'

Ibidem, p. 172.

Nonetheless, elsewhere he perversely concludes that such a remit is beyond the scope of inspection. In fact, his idea of inspection does not extend beyond Viewing, to quote him:

'In drawing attention to this phenomenon of inspectors who do more than inspection we are in effect going beyond the aims of inspection. The distinction which has been made, in examining this question, between inspecting for specific statutory requirements and inspecting directed more generally to the underlying purpose of legislation is also relevant to the discussion of other functions which inspectors may perform. For it is in concerning himself with the underlying aims of legislation that the inspector may cease simply to be an inspector, and may pursue other activities which promote those aims - even though they be activities which have little connection with inspecting and do not need to be performed by officials possessing the special powers which are the mark of an inspector.'

Ibidem, p. 172.

Rhodes thus poses a conundrum. On the one hand, he admits that a nuclear inspector is committed to a dual role, one technological and the other regulatory. On the other, because this is not Viewing, he must say that the former is not inspection, inferring that it is a task proper to officials who are not inspectors, if it should be done at all. He attempts to escape from his dilemma by the quaere:

'But once this wider role is acknowledged and accepted, at what point does the inspector cease to be an inspector and become a man who 'de facto' if not 'de jure' is assuming some responsibility for the standard of safety?'

Ibidem, p. 163.

The answer comes when the inspector extends his purview from Viewing to Executive Inspection, but Rhodes does not recognise the latter activity as inspection.

14.3.1 Involvement of the inspector and shared responsibility

Actually, Gerald Rhodes (1981) has exposed the nub of the matter and the full response is that the engineering inspector is inevitably drawn into the executive role of technical decision making about the safety of the entities in his regulatory fief. In this he assumes a responsibility for the standard of safety. The novelty, complexity and mutability of design of modern advanced technological industry and its installations admit of no other course. The things to be inspected are seldom ones that can be made to conform to rigid standards, but involve interpretation of principles which themselves can only be enunciated in imprecise terms.

Consider the 'enforcement' of a typical condition of a U.K. licence for a nuclear power plant, 'the licensee shall make appropriate arrangements to be approved by the Minister for the safe storage of nuclear fuel' (i.e. fissile material). Acceptable provisions must be tailor-made for the given plant and 'approval' will rest on the outcome of imformed technical discussions with the licensee's engineers and safety officers. Whether the inspector formally acknowledges his agreement by advising 'The Minister' (or the Health and Safety Executive) to 'approve' the result, is passive by failing to 'disapprove' or otherwise signifies his acquiescence, say, by lifting a 'Notice' issued under the Health and Safety at Work Act 1974, he has become a participant, ethically if not legally. Only if a specification or regulation can be inspected to its letter in a Viewing approach of 'GO, NO-GO' is the inspector able to eschew responsibility. Technical involvement is an inseparable part of the higher orders of Engineering Inspection and the capability to elicit the necessary information owes its existence to 'the special powers that are the mark of an inspector' (supra).

14.3.2 'Meta-inspection' - the need for an inspection of inspection

The fact is that Rhodes's study is a voice from the realm of 'The Word'. He is a political scientist, no engineering inspector sat on his working party and there is no record of any member of an engineering inspectorate being consulted (20). Though his work may be a contribution to political science and the theories of 'pure administration' (24), it is of little significance in the world of

'The Deed' in which nuclear safety engineering and inspection have their seat. Its relevance to the treatment of potential catastrophic LPEs in nuclear power plants is miniscule, except to expose some of the deficiencies in the administrative approach.

Nevertheless, a valid query is raised. Over the past few decades there has been a great increase in the number of inspectors and of those administering them. Is this proliferation at the public expense giving value for money? Is inspection properly directed and efficaceous? Little attention has been paid to these things and 'the question of accountability has been blurred'. There is no guard for the guardians: is a meta-inspectorate of inspectorates required? In truth, the inspectional system is open at the top and a means of closing it to enhance the safety of nuclear power is suggested later in this text.

14.4 Some further fallacies of the scientistic approaches

Of recent years, certain engineering bodies with statutory responsibilities for the safety of nuclear power plants, and especially for defence against possible catastrophic radiation accidents, have been under increasing attack for their reluctance to abandon a long established modus operandi that uses a postulated 'credible' maximum accident (MCA) as the basis for design assessment and inspection in favour of one centred on quantitative probability analysis. Both the former and the synonymous Design Basis Accident (DBA) are embraced by 'the doctrine of limiting accidents' that was discussed in Section 9.1 and 9.2 et seq. In the U.K., the censure has been directed at the NII as the statutory authority for regulating the safety of nuclear installations by licensing. Exemplars of the alternative methodology that has been recommended are the U.S.A. 'Reactor Safety Study', described in Section 7.3 et seq., and a similar approach advocated by F.R. Farmer.

The first hint of criticism came from the 'Inquiry into Safety and Health at Work' (Robens 1972/b). Four years later, it was voiced more strongly by Sir Brian (now Lord) Flowers, to quote:

> '276. ... ... There seems no doubt, however, that the technique (probabilistic) is the best available to achieve safety in design.
>
> ... ...
>
> 282. We do not doubt the technical competence of the Inspectorate or the thoroughness with which they carry out their work. However, the discussions we have had on reactor safety with several authorities have left us with some doubt as to whether the criteria adopted by the NII in establishing reactor safety are soundly based and whether their functions are correctly defined.'
>
> Sixth Report of the Royal Commission on Environmental Pollution: Nuclear Power and the Environment, HMSO, London, Cmnd 6618, Sept. 1976.

This criticism was echoed later by the Hon. Mr Justice Parker (1978) at the Inquiry into a proposal to expand the thermal oxide reprocessing plant (THORP) on the UKAEA Windscale site.

The foregoing strictures are oblique. Reference to the literature shows that, rather than overlooking probabilistic methods, reliability analysis and other quantitative applications of probability theory, these techniques had been long and extensively used, especially by the NII. Examples abound, as, for example, their use by T. Coxon (1971) in a discourse on the role of the Maximum Credible Accident (MCA) in British nuclear power reactor design, in operational research style approaches to the management of fuel can operating temperatures in Magnox systems (Dale and Harrison 1971 and see Document No. 5 of the Annex) and in the policy of the NII for the selection of reactor sites (Charlesworth and Gronow 1967).

Some years in advance of the above criticism, Gronow and Gausden had described the application of quantitative probability methods of the type referred to by Flowers (supra) in the approach of the NII to the safety assessment of power reactor design in the following terms:

> 'The design basis accident is still used to define the range of faults for which automatic shut-down and emergency cooling must be provided, but the fault analysis has been extended to cover a wider range of accidents. The object of this further analysis is to ensure that there is no step change in the consequences of accidents and, if necessary, to reduce the risk or consequences of such accidents by changes in the design. Where appropriate use is also made of the technique of probability analysis in a safety assessment of reactor components and systems and, for later designs, this technique has been extended to include a range of possible accidents and their consequences. This exercise has proved to be of limited value, not least because of the lack of reliable data on which failure rates of components which make up the complete reactor system.'
>
> 'Licensing and Regulatory Control of Thermal Power Reactors in the United Kingdom', Symposium on the Principles and Standards of Reactor Safety, IAEA, Vienna, 1973, p. 528.

More recently, Professor A. Birkhofer (1979) of the West German Reactor Safety Institute gave further endorsement to the validity of the DBA/MCA philosophy:

> 'Experiences so far have shown that this safety concept has proven its worth.'
>
> Ibidem: excerpt from Section 7.4 above.

The durability of the doctrine of limiting credible accidents that characterises the MCA and the associated DBA approach lies in the fact that it is appropriate to the actualities of engineering on the construction site and in the control room which are beyond theory in the design office. The utility, advantages and disadvantages of the MCA were discussed at length in Section 9. It remains to iterate that the New Treatment favours an approach according to that doctrine in which probability concepts and the methods of reliability technology and quantitative safety analysis take their proper place as useful adjuncts.

14.4.1 The fallacy of the dependence of inspection on equal expertise

A further criticism levelled at inspection during the Windscale THORP inquiry (supra) concerned the nature of inspection and its capability to appraise the work of experts, namely:

'11.24 It was suggested that NII were not sufficiently involved in all stages of design to ensure ultimate safety and that they were in any event not equipped with sufficient scientific expertise to check the designs. The former suggestion I reject. ... ... The second is one to which attention should be given. I make no finding that NII are inadequately equipped. ... ... Their task is to pass judgement on plants which are designed by very highly qualified experts and they must, if they are to perform their function, have, or have access to, at least equal expertise. It was not established to my satisfaction that this is the position.'

Hon. Mr Justice Parker, ibidem, p. 67.

Of course, an engineering inspector must have ready access to the most expert and authoritative scientific expertise, and be able to interpret such advice. This has never been otherwise. However, Parker's belittlement of the competence of the NII to discharge its higher order inspectorial functions is an expression of a fallacy that is commonly held about the identity, indeed the very existence, of the upper brackets of engineering inspection.

Truly, as seen from the dominant half of the 'Two Cultures' (C. P. Snow 1959), that is to say from the viewpoint of 'The Word', engineering inspection to Mr Justice Parker, sitting in the Inquiry's chair as a senior member of the legal and administrative establishment, would not appear to be properly capable of achieving much more than verifying that a nuclear reactor and its design confirmed with specifications, operating rules and statutory requirements. Thus, according to his lights, its purview would not reach beyond Viewing. This is what Gerald Rhodes (supra) had in mind for his category of 'Checking inspectorates' whose 'characteristic is to check standards' as in quality control, inferring that certain inspectorates, eg. the NII, had assumed a position that exceeded their remit.

In practice, the higher orders of inspectional activity go far beyond mere checking and inevitably bring in the purposes for which the inspection was instituted and to the observer in the superior culture do, in fact, exceed their remit. Therefore, Rhodes is forced to the conclusion that such activities have little to do with inspection or could be performed by persons other than inspectors (supra). Likewise, both Flowers and Parker (ibidem)

from their very cursory examinations of the wider role of the NII concur with Rhodes, inferring that the formulation of nuclear safety policies for siting, design criteria, plant operating limits and so on are things that would be better performed elsewhere than in an inspectorate. The short answer is that they would not.

The threat of a major radiation accident in a nuclear power plant is not presented by the 'marks on paper' and other information which constitute its design but from the operating plant that is its physical realisation. Moreover, it is only an engineer 'possessing the special powers that are the mark of an inspector' (G. Rhodes ibidem) and experienced in their use who can elicit and integrate the information about the given plant, or like plants, that is needed for a truly efficaceous assessment of its design and subsequent operational performance on which safety decisions may be properly and economically made. Successful realisation of that state is another matter.

Parker's stricture as it concerns lack of equal expertise is due to a further misconception about the true role of inspection. This is not so much to pass judgement on the work of the 'highly qualified experts' as to confirm that the design is in fact the work of appropriate 'highly qualified experts' properly applied in the solution of the given safety problem. An inspectorate in its monitoring role must study a licensee's safety submissions, not so much exhaustively, as in sufficient detail to verify that the case presented is in fact valid and properly supported by arguments that can be shown to be scientifically sound. Much of the evidence given in a safety report will stand by the engineering consensus on its own merits. The proper foci of inspectional attention are those aspects of the design of dubious safety status or which have become matters of scientific controversy, as for example the integrity of the pressure vessel in the case of the PWR (Sir A. Cottrell 1980).

It is unnecessary, therefore, that every safety relevant detail be meticulously scrutinised. Rather, effective engineering inspection requires an integrated appraisal over the widest achievable technical span so that the area assessed can be seen as a whole rather than in its parts. Moreover, no engineer, let alone an inspector, could attain to the depth of knowledge necessary to

check with equal expertise the work of the 'very highly qualified experts' identified by Parker over any major portion of the design of a nuclear power plant. For the proper discharge of his duties, an inspector need not, indeed should not be 'a very highly qualified expert' confined thereby to a related group of specialisms. Instead, he must be a competent and experienced engineer who can apply his knowledge of the several generic scientific disciplines that are his fortes in a broadly imaginative manner. He must thereby be able to engage in constructive dialogue with the given design authority and to consult other experts on the matters in question. The inspector's task is managerial as he is seeking to confirm the integrity of the design of the plant rather than to become involved in punctilious disputations about minutia. This is the arena of the savants from whom the inspector must confirm that the issues are properly resolved.

Owing to the breadth and impartiality of his surveillance, the inspector can see beyond immediate concerns and special interests of the design office to perceive potential failure sequences overlooked in the formal safety case. In this exercise, members of an inspectorate are aided by the cross-fertilisation that is a result of the close association and interchange of personnel between design assessment and site inspection teams. This was characteristic of the NII's modus operandi (O. H. Critchley 1977).

A further fallacy about inspection lies in the imputation that it claims to be a source of safety. It is not a source of safety, nor could it be. While inspection may confirm that a certain situation is safe, this is an observation and not an assertion of truth. In nuclear engineering, the true source is a safety conscious licensee with an adequate understanding of the science and technology embodied in the reactor whose operators are thoroughly familiar with the plant in their charge.

14.5 A role for inspection: a quasi-cultural aspect of safety

Notwithstanding the impossibility of preventing all reactor incidents of serious import, commercial nuclear power has so far escaped a truly calamitous accident because of the effectiveness of its policy of safety defence in depth. Even 'Three Mile Island', the worst accident so far, caused no known radiological casualties.

Nonetheless, there have been happenings which have smacked of incompetent management, neglect and shoddy engineering. Moreover, the botched or blown attempts to cover up embarrassing operational failures have not lessened the adverse public impact of such events.

Often highlighted by the media in a sensational and sometimes derogatory way, these things have tended to give nuclear power a poor image. Against such a backdrop, a severe reactor accident involving a significant number of fatalities and extensive environmental and economic damage could halt the progress of the nuclear industry for a generation or more. An incident of this scale is indicated by the point on Figure 2 at which the 'Public Reaction' vector cuts the boundary curve that indicates the level at which the incident's consequences in terms of casualties would evoke serious public disquiet. Its position suggests a catastrophic event involving some thousand or more disastrous experiences of fatalities, malignant illnesses, civil disruption, consequential property losses and environmental damage.

Unfortunately, it is not possible to devise any feasible scheme of safety management or of regulation that can do more than reduce the threat of such an event in a large and complex technological artefact like a nuclear power reactor which contains an intractable residual hazard. Although the hazard cannot be eliminated, it can be held at a level that may be regarded as negligible, defence against the danger being secured by engineering safeguards in the maintenance of which inspection plays an essential part. Its role is to assist in sustaining the safety ethos that has become a cultural feature of nuclear engineering. In this it has to encourage, indeed enjoin, management in the industry to establish and maintain a standard of engineering that will ensure an adequate defence of safety in each installation at risk.

Inspection itself is not necessarily free from error and meta-inspection, that is the surveillance of inspection, is a topic to be developed in the passages that follow. One source of error comes through obsessive attention to the letter rather than the spirit of a regulatory duty. An intrusion by inspectors that has the effect of validating a presumed state of safety on the basis of overt compliance with statutory regulations and codes of practice while being blind to more subtle frailties, may create false

confidence that can conceal incipient danger. Some think that this was the case at 'Flixborough' (G. Atherley and R. Booth 1975) and a similar charge has been levelled against the U.S. Nuclear Regulatory Commission (NRC) in respect of the 'Three Mile Island' incident (See Section 5.3.1).

In a societal environment of increasingly stringent factory safety laws, product health and safety regulations and new concepts of liability, the continuing pursuit of the mirage of unquestionable safety for nuclear power has been one of rising costs not commensurate with the public confidence so inspired. Progress in industrial health and safety is reaching an impasse. Nonetheless, the achievements in protection of workers, public and environment cannot be diminished and some continuing escalation in costs is inevitable, but ways of making such investment more economical must be sought.

In the case of nuclear power, the burden suffered by the industry was described in evidence given to the Commons Select Committee on Energy by Charles Komanoff, an eminent American energy cost consultant:

> 'Costs are being ratchetted up by late safety requirements. Estimates consistently fail to anticipate the cost of efforts to reduce the hazards of nuclear plants ... (and) ... putative, intangible reductions in accident possibilities have been introduced which are now belied by the TMI affair. Fossil fuel stations do not suffer this handicap, ... (but) ... nuclear plant, often delayed during construction or overtaken by new safety requirements, suffers cost escalations which are much larger than those for conventional systems.'
>
> Cost escalation at U.S. nuclear power stations,
> Minutes of Evidence,
> House of Commons Paper HC 397-V,
> HMSO, London, 12 March 1980.

In addition to the costly changes that have been forced upon the design, often in a technical morass of 'safer than safe', must be added the expense of the many inquiries, the cost of supporting research and the fees of expert witnesses required for debating the pros and cons, which in the case of the current Sizewell PWR inquiry has exceeded £10 million (David Mellor 1982). Not least is the financial penalty owing to the delay in bringing the project to a useful state which, in the case of an electric power station, may involve very large sums to pay for lost output.

Nonetheless, the issue of societal risk assessment for which nuclear power has been the focus continues to be a matter of prolific research and vigorous debate. The open ended nature of the topic has been described by J.R. Ravetz in a report to the Council for Science and Society:

> 'The problem of risk management should not be seen statically as if it could be solved satisfactorily once and for all by scientific analysis or administrative procedure. Rather, the social dynamics of risk extend to perceptions and evaluations of risks themselves. Risk management should evolve through an interaction of all the diverse interests concerned in each case.'
>
> The Acceptability of Risks,
> Conclusion 8,
> Barry Rose (Publishers),
> London, 1977.

The scientistic path of design safety enhancement has reached a point of diminishing returns, having failed to win public confidence. Progress lies in securing public belief in the safety achievements of nuclear engineering, the standards of which can be assured by inspection, but an inspection that not only is, but can be demonstrably shown, to be efficaceous. The required philosophy and organs for such inspection have, in fact, emerged to meet such a need, though this has yet to receive proper acknowledgement.

14.5.1 The new style of engineering safety regulation

The association between technological progress, the concomitant threats to man and his environment and the development of engineering inspection has been discussed earlier in this text and in document No. 4 of the Annex. The point of interest here is the change in the inspectional function that has reflected the growing sophistication of modern industrial technologies, a change that has been most pronounced in the special style of regulatory inspection that has evolved to meet the unusual and severe hazards created by the exploitation of atomic energy and nuclear power in particular. Inspection is the central feature in a group of related activities of sufficient consequence to be called 'Regulatory Science'.

Two regulatory bodies that have exhibited the characteristics of the new style are the Nuclear Regulatory Commission (NRC) in the U.S.A. and the Nuclear Installations Inspectorate (NII) in Britain. The antecedents of the latter have been discussed in the writer's paper,

'Technological progress, safety and the guardian role of inspection' which is presented as Document No. 4 of the Annex.

In America this initiative in regulatory inspection was moulded according to the national pattern of civil administration and the NRC tended to acquire a legalistic formalism that landed it is disarray when faced with the exigencies of the Three Mile Island incident of 1979. In a characteristic British way, growth of the NII took place in that certain ambience of informality and flexibility and so was able to adapt itself to the unfamiliar field in which it had to shape its policy. Thus, what was, by necessity, a predominantly engineering body acquired a freedom to develop a new kind of safety regulation.

Of the two inspectorates, the NII has been chosen as the exemplar, because, although it falls short of the requirements of the New Treatment, it has provided a base on which the theory has been developed. However, the NII was a house of many mansions and the writer as an erstwhile member of the senior staff from 1964 to 1978 has to some extent drawn upon his own practice in the interpretation of its regulatory procedures.

To iterate, plant accidents do not occur in the design of a nuclear reactor per se, but only when the paperwork etc. of that design have been converted into an operating installation. Moreover, although a design weakness may enable a fault sequence to run to catastrophic failure, the experience of reactor accidents has been that they are precipitated by human error. In consequence, a singularly important part of the NII's function lay deeper than safety assessment of design and the division of effort between assessment and site inspection had to be made accordingly; for while sound design of high integrity is paramount, it is the realisation of that design in the form of a properly operating plant that is the true mark of safety. The design assessments of nuclear power stations in construction have, therefore, been wide-ranging, resourceful and forward-looking studies in which proper regard has been paid to the effect of site circumstances in each case.

While appropriate use had been made of probability based operational research techniques, the formalism of the systems approach was not permitted to constrain creative enterprise (Gronow and Gausden 1975/b). The work of assessment thus integrated with the flow of Event-noise (En) combined with relevant experience derived from site inspections may be

called Forward Safety Analysis (FSA), though this aspect of the Inspectorate's activities has received far from due recognition and has been ignored by the august inquiries (supra).

Forward Safety Analysis has been used by the NII to direct emphasis in its program of design safety assessment and to justify calls for fault studies and for specific probability assessments of certain design features such as those that arise in control and instrumentation problems, although FSA has not formally been recognised as an inspectional discipline.

14.5.2 The question of appraisal of inspection and accountability

Central to the case for the New Treatment is the postulate that catastophic low probability events (LPEs) very rarely occur otherwise than through human errors in the processes of physical realisation of design or because of unforeseen, and at times unforeseeable, inadequacies in the design itself. The initiating events do not appear until the design is realised in an operating plant. Risk and safety assessments, neither qualitative nor quantitative, can provide any reliable prior knowledge of the likelihood of very low probability catastrophic events. In reality those that they do foresee, are either designed out or otherwise reduced to a level of probability so low as to be metaphysical. Such LPEs never happen in human experience, at least in the manner predicted. Protection against the catastrophic LPE occurring in a nuclear power plant therefore lies with inspection and that particular variety of the art which has evolved in the industry to meet the need, Figure 13 showing the way in which inspection plays its part. Its methodology is largely that which has been practised in America by the NRC and in Britain by the NII.

The demanding nature of the work of a nuclear inspector has been commented upon earlier under the generic title of 'Executive Inspection' in Sections 14.2.2 and 14.2.3 and also in the writer's paper, 'Technological progress, safety and the guardian role of inspection', included as Document No. 4 of the Annex. The professional requirements seen as necessary for the working grade of Senior Inspector in the then Inspectorate of Nuclear Installations (now the NII) were specified some 25 years ago by Major General S.W. Joslin, the first Chief Inspector, as high academic qualifications in an appropriate branch of science or engineering together with long and responsible experience of the design, research or inspection of large scale plants (21).

However, these attainments are not enough in themselves and must be coupled with that penetrating capacity of technical intuition needed for the effective pursuit of Forward Safety Analysis: an intuition that gives a profound appreciation of the likely future event field, that is of a plant's path on the Behaviour Surface as depicted by the cuboid catastophe model of Figure 12. This conceptual field is a construct based on an intimate knowledge of the engineering aspects of its design as displayed in Figure 3. To this perception must be added direct experience of the given plant in its existence as an entity on site, together with a comprehensive Gestalt of the relevant faults and incidents discernible in the total En flux gathered from the industry. Paths leading to catastrophic failure sequences and anomalies that may give evidence of loss of resistance to failure are thus perceived as likely points of instability on the Behaviour Surface and can be dealt with by inspectional intervention in the processes of design, construction and operation as appropriate.

The effectiveness of 'executive' inspection of this kind depends critically on the sensitivity of the inspectional body to perceive in the way just described those pertinent singularities, instabilities and anomolies in the event fields to which it has access. This faculty when coupled with the collective engineering intuition of that body gives an awareness of the existence or imminent emergence of those efficient situations that could initiate a failure sequence. The necessary prognostic propensity, the faculty that is the sine qua non of efficaceous nuclear safety inspection, is a personal endowment of members of the team. But, its exercise is that of participation in a group where these propensities should combine holistically to give the inspectorate its necessary power of Forward Safety Analysis (FSA). However, in the present organisation of statutory inspection such a capability is incommensurable as noted by Gerald Rhodes (1981).

Lester and Rothman (1977) have, however, shown that Signal Detection Theory (SDT) can be used to give a quantitative index of success for certain well-knownprognosticators who over the past half century have attempted to predict the course of future events in the field of technological progress. Such prognostications are analogous to those which are required of a nuclear inspector in his exercise of foresight in FSA and, therefore, SDT may be used to assess success in pursuit of FSA and provide a means of dealing with the ultimate gap in the heirarchy of inspectional accountability identified by J.R. Ravetz (1974). While

the use of SDT to assess the performance of individual inspectors could well be counterproductive and be taken as an intrusion on the proper responsibilities of management, an organisation such as the NII could be subjected to independent, disinterested appraisal in a manner akin to the method of 'Keeping Score' suggested by Talbot Page (1979) as a means of assessing the performance of risk assessors employed by government agencies.

14.6 The assessment of inspectorial competence by Signal Detection Theory (SDT)

To recapitulate, in view of the central role engineering inspection plays in the New Treatment, verification and maintenance of the quality and competence of the inspectional body which performs the executive function in the nuclear regulatory hierarchy are paramount. However, as inferred earlier in this Section from Goedel's theorem, an inspectorate cannot effectively inspect itself and can offer no convincing evidence by introspection that it is fully effective, efficient and economic in its work.

The human faculties of perception, discrimination and use of acquired knowledge in making sensitive judgements underlie all inspectional activities from the GO:NO-GO routines of viewing in industrial quality control with increasing intellectual involvement to the fine decision making required for nuclear safety inspection. While much of the simpler work of industrial inspection has been taken over by computers, those that involve the exercise of critical judgements are unlikely to be displaced by machines in the foreseeable future. Inspection, therefore, remains as a significant element in manufacturing costs. Ergonomists in seeking ways of assessing the efficiency of this element have had recourse to SDT because of the analogy between defect recognition in a flow of manufactured items and the detection of radar and other signals at the threshold of identification on a horizon of noise.

It seems that W.P. Colquhoun in 1960 was among the first to study the use of SDT in the appraisal of industrial inspection and the topic has since attracted much attention because of the labour-intensive nature of inspection. David E. Embrey (1976) used SDT to assess the effectiveness of methods for training piece-part inspectors. Lester and Rothman (1977) were the first to make an empirically supported study of the extension of SDT to more sophisticated intellectual activities in an

appraisal of predictions about the future made by Professor J.D. Bernals and certain other forecasters of technological progress.

There is an analogy between technological forecasting and nuclear safety inspection in its discipline of forward safety analysis (FSA). As explained elsewhere in this text, the practice of FSA involves the use of engineering judgement based on studies of design in association with empirical data from the field. It is exercised in the prescription of modifications to that design as it has been, or will be, realised in the plant in question, or to require changes in the way in which the latter may be operated. In terms of Catastrophe Theory, the process may be seen as steering the system along a path on the Behaviour Surface of the Cuboid Model of Figure 12 so that the dangers foreseen by FSA and depicted by major irregularities on the Surface may be avoided or surmounted.

An executive inspectorate like the NII in pursuing FSA receives a comprehensive flow of Event-noise composed of elements of safety related data, among which are the reports from design assessors and field inspectors, LERs and other information from various sources such as the fault and incident data banks maintained by the Safety and Reliability Directorate of the UKAEA (S.R.S. 1984). Its proper task is to detect in this stream of information (which has been defined as 'noise') those things perceived as signals that give evidence of loss of resistance to failure or other indications that the plant may suffer a loss of stability.

Acting upon its interpretation of these signals with a view to restoring safety and reliability, the Inspectorate may use delegated authority under the Nuclear Installations Acts to require the operator of the plant deemed to present the hazard to take some appropriate action to reduce the potential danger. To this end, the NII works through licence conditions (R. Gausden 1979) in the manner described in Section 14.3.1, being able to shut the plant down if necessary. Alternatively, as in the case of non-nuclear industrial hazards, an inspector can use his powers under the Health and Safety at Work Act 1974 to lay a 'Notice' instructing the operator of the plant to eliminate the danger or stop the process.

14.6.1 An alternative to the test of market forces in nuclear risk assessment

Unlike the prognostic safety analysts of NII and NRC and their auxiliaries, actuarial risk assessors in the insurance industry are subject to the test of market forces. Errors in risk appraisal incur economic penalties. If insurance rates are set too high, clients seek cheaper cover: if they are set too low, the underwriters face financial loss. Indeed, failure is a phenomenon not uncommon in motor insurance.

Nonetheless, a regulatory body has a protective role and the nuclear inspectorates were established to ensure that major radiation accidents would not occur. There is no direct way in which the competence of such a body may be proved as no experience of failure can be allowed. However, if it does fail, then it suffers the débâcle of loss of public confidence, that is its very raison d'être. Moreover, it is illusory to attempt to prove its competence in terms of events that have yet to happen or that might have happened but did not, unless there is a clear nexus between the envisaged approach to failure and the steps to prevent it.

In many cases the required nexus could be established on the basis of material drawn from the studies of design which are carried out by, or on behalf of, the regulatory bodies charged with the safety surveillance of the so-called 'major hazard installations'. In Section 8.4.7 attention was drawn to Talbot Page's proposal (1979) for 'Keeping Score' of the performance of government and agency risk assessors engaged in hazard evaluation in the field of atomic energy and other advanced technologies. His idea was that the serious event scenarios and the fault sequences leading to them as treated in their assessments contained numerous lesser sequences that would not run to major system catastrophes. Among the mass of information so assembled, there would be certain fault sequences that could be matched against the actualities of site and control room experience. The required synthetic data would come from the official assessments, while the empirical material is available in the form of Licensee Event Reports (See Note 15 and Table III) and elsewhere in inspectors' visit and other reports.

In this way the skill of the official assessors in identifying the mechanisms of causation of lower tier accidents, faults and incidents could provide evidence of their likely success in predicting those major

potential LPEs which are the precursors of catastrophic accidents. Such validation of the prognostic efficiency of the inspectorates and the risk assessment agencies associated with them would enhance public confidence in the protection they are supposed to offer. Moreover, it is a form of validation of their abilities that could be progressively updated as well as imposing a measure of accountability.

14.6.2 SDT and the psychophysics of Forward Safety Analysis

Signal Detection Theory (SDT) is a sophisticated decision methodology that can be applied to a very wide range of situations where a decision has to be made on equivocal evidence and, more particularly, it can be used to assess the performance of the decision maker. The evidence for the decision, that is the 'signal', must be elicited from a background of 'noise', comprising irrelevant information and events that tend to confound the decision process. The analogy with the communications problem of detecting weak signals in electrical circuit noise is obvious. The application of SDT to psychophysics began some 20 years ago, progressing from the field of sensory perception to the study of intellectual task performances of increasing complexity, such as medical diagnostics. A thorough and authoritative introduction to SDT is 'Signal Detection Theory and Psychophysics' by Green and Swets (1974).

The following application of SDT to Forward Safety Analysis is elementary, using the basic 'Yes-No' method, as reference to any of the more sophisticated techniques would involve profundities beyond the scope of this research. The Forward Safety Analyst looks for evidence in the stream of Event-noise, or in other information made available to him about the plant and its condition, of design weaknesses or other signs of loss of resistance to failure. He responds to that which he discerns as a signal by proposing a safeguard which it is assumed will be incorporated in the given plant or system. Four states of response may be distinguished which, using the standard terminology, are a:

(i) 'Hit' (S/s) - a danger signal has been properly perceived and a correct response made to avert the pending failure.

(ii) 'Miss' (N/s) - the signal has not been recognised and no action taken. In consequence a failure occurs unless the sequence is otherwise aborted.

(iii) 'False Alarm' (S/n) - an element of 'noise' has been incorrectly identified as a signal and safeguarding action taken which proves to be futile.

(iv) 'Correct rejection' (N/n) - an obtrusive element of 'noise' has been correctly identified as devoid of safety significance and no action taken.

By collating the analyst's behaviour for a number of cases, a table of his conditional response probabilities may be compiled, thus:

Safeguarding Response

Stimulus	S	N
Signal = s	'Hit' P(S/s)	'Miss' P(N/s)
'Noise' = n	'False Alarm' P(S/n)	'Correct Rejection' P(N/n)

The above stimulus-response matrix may be represented graphically with P(S/n) as the abscissa and P(S/s) as ordinate, noting that P(N/s) can be obtained from 1 - P(S/s) and, if the 'False Alarm' rate is known (not always the case), P(N/n) is given by 1 - P(S/n). The points on the graph representing P(S/s) against P(S/n) when joined give a curve called the 'Receiver Operating Characteristic' or ROC curve which describes the safety assessor's performance. Two important parameters may be deduced, namely, his 'sensitivity' and 'bias'. The former indicates how well he is able to make correct judgements and avoid incorrect ones. 'Bias' is the extent to which the assessor is influenced by preconceived views in his interpretation of the evidence available to him. For a fuller description of the SDT technique reference may be made to the very clear and readable treatment given by D. McNicol (1972). The method can be readily adapted for the purposes of 'Keeping Score' of the performance of official and agency risk assessors as proposed by Talbot Page (supra). In this application, the synthetic situations envisaged by the assessors would be matched against analogous real events in the En stream.

14.6.3 A macroscale, synthetic exemplar

Despite the fact that the data for a convincing demonstration of the foregoing SDT methodology exists, it is inaccessible on grounds of commercial and official confidentiality and lack of authorisation 'to know'. Besides it would be both invidious and impolitic to use the NII as a paradigm in such circumstances without formal consent. Therefore, a suppositional regulatory body with universal authority is used as a model. This so-called International Technological Health and Safety Commission (ITHSC) would set targets and impose those limitations and

requirements deemed necessary to defend health and safety, acting in response to its perception of harbingers in the Event-noise it might be envisaged as receiving.

By definition, the ITHSC would have no access to such microscale data. Despite that, it is possible to depict how this synthetic commission might be held to operate on the macroscale because the information necessary for such an exercise is largely available in post-disaster reports and in those from official commissions of inquiry. An example of how this data might be arranged for an SDT study is given below.

A 'Hit' - 'Cockcroft's Folly'

At a late stage in the construction of the UKAEA plutonium piles at Windscale in Cumbria, particulate filters were built into the tall exhaust gas chimneys. These proved their worth by acting effectively to remove radioactive dust from the fumes emitted to the atmosphere when No. 1 Pile went out of control in a massive core fire on October 10, 1957. Had it not been for this act of foresight attributed to Sir John Cockcroft, the Windscale accident would have had much more serious consequences.

A 'Miss' - Three Examples as described in Appendix II

In the cases of the tragic accident at 'Aberfan' when a colliery spoil tip adjacent to a Welsh mining village engulfed its school and part of the town with heavy loss of life; when the tranquiliser, Thalidomide, caused hundreds of severely deformed children to be born; and in the case of mass poisoning by methyl-mercury when the wastes from a Japanese plastics factory contaminated the waters of the fishing ground of Minimata estuary, strong signals of impending disaster were ignored by those who had a major responsibility for health and safety.

'False Alarm'

The U.S. Food and Drug Administration in a misconceived action prevented the medicinal use of beta-blockers in cardiovascular illness for a number of years, causing the premature deaths of thousands of people. European experience was giving clear evidence of their safe use.

'Correct Rejection'

Information in this category is held in the files of the regulatory bodies and is, otherwise, inaccessible, but there are many cases in which chimerical proposals for safeguards are rejected. One case based on equivocal evidence was the 'Ozone layer depletion' hypothesis calling for restraints on the use of fluorocarbon propellants was properly dismissed.

A study, somewhat along the above lines though not involving SDT, provided an empirical basis for the report of the Council for Science

and Society's working party on 'Superstar Technologies' (J.R. Ravetz 1976) which recommended a national Technology Control Commission to exercise surveillance over the innovation and operation of advanced technology plants and processes.

The microscale appraisal of inspectorial performance offers an objective criterion because the safety investment specified for the given minor fault sequence assessed has been made or recommended and the loss due to failure or the potential loss that might have been incurred can be costed (D. McNicol 1972). Furthermore, extrapolation of an appraisal of task competence made at the microscale to the macroscale is common in human experience, being the basis of licence to practice in many areas of human skills, particularly in the awarding of higher professional qualifications, eg. for commercial air pilots and surgeons. The efficient transfer of higher order intellectual skills is a well-known phenomenon.

Finally, the SDT method of assessing prognosticators described by Lester and Rothman (1977) in 'Signals of the Future' could be readily adapted to Talbot Page's scheme (supra) for appraisal of the capability of official safety assessors and risk analysts by 'Keeping Score'. Unfortunately, although most germane to the New Treatment, there is neither time nor space to accord the topic more than the brief outline given above and the topic must be pursued elsewhere.

14.7 Advantages of the MCA/SDT philosophy of nuclear risk management

A distasteful aspect of the quantitative risk-benefit approaches to safety management in nuclear power is their detriment orientation in terms of fatal casualties. For instance, the abscissa in the 'Farmer Line' graph discussed in Section 9.4 is fundamentally scaled in lethalities, despite its presentation in terms of fission product releases. On the other hand, the New Treatment escapes from the dilemma by retaining the concept of design that had evolved in nuclear engineering which is based on a credible limit for a radiation accident known as the MCA (See Section 9.2). Such an event would not insult an exposed child's thyroid with a dose greater than 25 rems within the bounds of the siting policy (See Section 9.3) for the scales of failure that could befall the plant; 'incredibility' being a synonym for the realm of metaphysical probabilities where events lie beyond human experience (See Section 9.6.1).

The state of 'incredibility' is to be maintained by implementation of a design of attested reliability in a construction and operation of sound engineering assured by inspection. That assurance can be confirmed by SDT whereby the competence of management throughout the whole inspectional chain is appraised by disinterested third party action. This meets the criticisms of the impossibility of effective self-inspection, lack of accountability and open-endedness in its higher echelons which were referred to earlier in this Section.

Although the probability of an accident on the threshold of incredibility is metaphysical and will never happen in the way envisaged, some other unforeseen low probability event may occur instead, there being an almost infinite spectrum of such possibilities when human frailties are taken into account. No objective probability can be attached to such an occurrence except to say that it is exceedingly unlikely, but there is an upper qualitative level at which the remote chance of a very severe disaster presents an intolerable threat to the community (17). This eventuality bears on the very widsom of exploiting a technology that presents such a dire threat and certainly espouses a remote siting policy until proper experience has been acquired in its management. The use of certain potent drugs in medicine comes into this class and, perhaps, even that of poison gas in warfare as being too dangerous for either side to use. Indeed, it is the rationale for deterrence in present day military strategies.

14.8 Overview

The end of the first decade of this century saw the emergence of a new kind of engineering inspection devised to control the unusual and grave hazards of certain of the leading advanced technologies, namely aeronautics and, later, nuclear power. These new methods of inspection with supporting disciplines of non-destructive testing, stress analysis, forward safety analysis (FSA) and reliability analysis grew rapidly. This was mainly under the stimulus of military exigencies in the approach to and experience of two world wars and the subsequent reaction to major geo-political threats, particularly after World War Two. Associated with these more pragmatic developments has been the application of operational research methods, chiefly as quantitative systems analysis, to administrative decision making in a wide range of situations. However, these attempts have been less than conspicuously successful because they have tended to ignore engineering as the true arbiter of

safety and the necessary bridge between the administrative, commercial, legal and political realm of 'The Word' and the pragmatic and empiric domain of 'The Deed' that embraces the practical skills and useful arts by which the discoveries of science find their societal applications.

The inspectorates that came into being to regulate the new technologies with their unexpected dangers, owing to their technical and organisational sophistication, could no longer be effectively managed by the traditional higher tier administrative organs. Further, as may be inferred from Goedel's theorem, neither can such bodies effectively regulate themselves. They can thus proliferate and extend their influence in ways that neither maximise attainment of their objectives nor inspire the necessary confidence of society. A situation thus exists that appears to be open-ended on the one hand and beyond effective political control on the other.

Despite the foregoing doubts, recent developments in psychophysics can offer some of the necessary answers. The salient feature of the new form of inspection that has developed around nuclear power is its prognostic philosophy of safety by foresight or FSA. Signal Detection Theory (SDT) can be used both to confirm the efficacy of the inspection process itself and as a measure of the effectiveness of the associated assessment function as well as the bias with which it may be exercised. SDT, therefore, would offer a means of closing the accountability gaps that exist at the top of the official inspectional hierarchies as well as subjecting their performances to appraisal analogous to that attributable to the market forces which bear upon actuarial assessors in the insurance industry.

However, in view of the novelty of the concept and the nuances of interference with existing organisational forms, the suggested application of SDT has been confined to a notional, universal inspectorate, an International Technological Health and Safety Commission (ITHSC). A few imputed successes and failures of FSA have been attributed to this ITHSC, and its suppositional management of the new technological risks has been briefly examined by a simplistic application of the SDT methodology.

15 CONCLUDING OVERVIEW AND CONSTITUTION OF THE NEW TREATMENT

'There is no subject so old that something
new cannot be said about it.'

Fyodor Mikhailovich Dostoevsky,
'A diary of a writer' (1876) -
3, July and August.

The New Treatment of Low Probability Events is the outcome of a critical evaluation of the achievements in safety engineering and reliability theory and practice that have had their culmination in the nuclear industry over the past 40 odd years. These advances, like most things in science and engineering, have, in the main, been the result of re-appraisal and reconstitution of long established methods to meet the new and unique dangers presented by the large-scale exploitation of atomic energy and especially those of nuclear power. It has been appropriate therefore to describe the New Treatment against the historical and societal background of growing concern about the darker aspects of the technological advances that began with the Industrial Revolution.

The new and rapid industrial developments were doing serious harm to the health and safety of workers, public and environment. Life and limb were cheap. The risks that workers faced were no more than a natural consequence of their employment and there was little more regard for member of the higher social orders. Industrial pollution and loss of amenity were accepted as the unfortunate consequences of work activities compounded by national economic policies, e.g. deforestation, enclosures and the dumping of spoil. Even so, the growing prosperity of the community as a whole in the countries that were becoming industrialised, and in Britain in particular, was making life a happier experience for all classes and something to be valued and extended. Government intervention in the interests of health, hygiene, safety and a clean environment was seen to be necessary and steps began to be taken to control pollution and abate the rising toll of industrial accidents and diseases. Legislation was conduced by public opinion and intelligent economic self-interest and important health and safety laws were enacted, but, perhaps most effective of all the contributing factors, was the creation of an economic base to meet the costs they imposed on the community.

By the end of the first quarter of the Twentieth Century, the toll of factory and mine accidents had been greatly reduced and the worst of industrial pollution had been brought under control. There followed a period of consolidation, but the advanced countries were now suffering a sensational series of catastrophic failures of technological systems, notably in the field of mass transportation of which the 'Titanic', 'R-101', 'Hindenburg' and 'Morro Castle' are examples. After the Second World War, the pace of technical progress accelerated and brought with it a new dimension of danger with the development of mass air travel, new and potent pharmaceuticals and nuclear power.

Public awareness of these hazards and anxiety about safety and the state of the environment have become acute and the measures being taken to allay these fears now pose a threat to essential progress, and not only in the case of nuclear power. It has become part of a rising trend of hostility towards technology which is a matter for serious concern per se. On the one hand, the World's population is rapidly growing and billions of deprived people are yearning for a better quality of life. On the other, the Earth's balance of natural resources against demand is not static and the available reserves of energy are particularly limited. The only escape from an eventual catastrophe is by continuing technical progress and nuclear power offers both an essential and available avenue . Besides, resolution of the problems that are hindering its progress may soon become urgent.

A constructive outcome of the state of public concern about technological hazards, inspired by doubts about atomic energy, has been the emergence of risk science which has adopted the systems approach that reached a pinnacle in the U.S. Reactor Safety Study and parallel initiatives in Britain inspired by F.R. Farmer. While these methods have contributed to the technical safety assessment of engineering design, they seem to have done little to reduce the incidence of rare, catastrophic failures like the Three Mile Island disaster of 1979.

15.1 The essential nature of the New Treatment

Largely on grounds that evolved systems tend to be more reliable than those of ad hoc novelty however cleverly contrived, the New Treatment proposes that the practices that have long been successful in hazard control in the atomic energy industry should be substantially retained. From this vantage point, it has taken an engineering

initiative and shows a way of striking a societal balance between the acknowledged very small but grave and finite risks that arise in the commercial exploitation of some of today's advanced technologies and the benefits they offer. Yet, its particular application is to power generation by nuclear fission.

In the welter of controversy, inquiries, reports and studies aimed at presenting those risks as vanishingly small, there is a danger that the expenditure on safety may continue to escalate into a region of safer than safe, rendering nuclear power hopelessly uneconomic. And, the burden is already heavy. The New Treatment differs radically from that of quantitative risk analysis currently being promoted in the industry. Safety is not defined as a static parameter than can be accurately measured and, thereby, judged as adequate or otherwise, but as a defended state that has to be actively maintained by human effort and vigilence. Such is the proper task of inspection. It is engineering that follows a course of action that uses rather than depends on the mathematics of quantitative safety analysis. The risks are recognised and assessed and appropriate technical action taken to contain them, but this must be a continuing and sustained effort, confirmed by inspectional monitoring.

The New Treatment then suggests that plants built to good and properly assessed designs, well engineered and operated, very rarely fail catastrophically owing to known plant or equipment faults. They fail instead because of 'Ignorance of Mechanism' has obscured a fault mode; because of some act of human fallibility, culpable or inadvertent; or because of an unforeseen change confluence of circumstances. The pattern of these fundamental factors in the causation of failure is shown in Figures 14 and 15 and is briefly reviewed in the Preamble to Appendix II.

The remedy does not lie in the achievement of better risk mathematics or in attempts to enhance engineered safeguards which already provide for a satisfactory defence of safety, but by an industry characterised by engineering of demonstrable excellence. That this is so can be confirmed and maintained by an accountable inspectional regime open to public verification. Within such a regime, it should be possible to secure assenting compliance with the necessary statutory regulations, licence conditions and other requirements of good engineering practice.

This is substantially the state of affairs that exists in the nuclear power industries in Britain and, to a lesser extent, in the U.S.A., having been fostered by the responsible regulatory bodies in each of the two countries, respectively the Nuclear Installations Inspectorate (NII) and the Nuclear Regulatory Commission (NRC). A feature of the British regime has been its involvement in the formulation of safety policy and its participation with licensees in decision making in matters of nuclear plant design and operational safety in the manner described in Section 14.3.1.

While the NII and NRC have been taken as exemplars, neither inspectorate fully meets the terms of the New Treatment. The regulatory body it envisages would have to be subject to appraisal of its efficiency and modus operandi by and, moreover, be accountable for the outcome of its work, to an independent public body or commission on the lines proposed in Sections 14.5.2 et seq. However, developments along these lines might meet some formidable obstacles owing to the 'Two Cultures' divide that separates administrators and politicians on the one side from the engineers on the other. The former group, acting in accordance with what has become constitutional practice, holds the primary responsibility for creating the agency which would be charged with carrying out the foregoing inspectional functions and, what is more, with the formulation of the policies which would determine the way in which that work is to be done.

It is obvious then that enhancement of the powers accorded to engineering inspectors acting as an autonomous body must diminish the administrative prerogative, a trend that has been manifest in the NII and certain other advanced technology groupings since the advent of commercial atomic energy (Margaret Gowing 1974/a). It may well be that failure to recognise the effective shift in the centre of technological policy formulation and decision making has led to much of the misconceived criticism of the advances in engineering inspection that has been discussed in Section 14.3 et seq. Furthermore, regulation of those technological hazards of innovation that have characterised the second half of this century, and among which nuclear has been salient and a pace setter, demands an inspectional approach which, as previously observed, is one of participation and shared responsibility. This is in contrast with the traditional detached approach concentrated on enforcment of regulations enjoined by prosecution. Clearly, any further errosion of administrative tier authority may be expected to meet opposition.

Despite the fact that this radical new approach to safety in the exploitation of advanced technology had its origin in the U.S. nuclear industry, the Nuclear Installations Inspectorate (NII) has been chosen as the exemplar in preference to the U.S. Nuclear Regulatory Commission (NRC). No doubt there has been substantial transfer of theory and practice, but the further development of the latter has been constrained by the dominant legalism of American government administration. On the other hand, the NII, by virtue of its emergence in the exceptional and novel circumstances that arose in Britain owing to the conjunction of a pressing need to regulate the commercial development of nuclear technology and the repercussions of the Windscale plutonium pile accident, was given scope to evolve a unique and effective system of participative statutory safety surveillance of non-government nuclear installations and, primarily, power reactors. An important factor was that the development of the NII fell almost entirely into the hands of some eminent and experienced nuclear engineers. Moreover, the NII had become the admitted leader in nuclear safety regulation in the Western World as, for instance, is inferred in the report made by Rogovin and Frampton (1980) to the U.S. Nuclear Regulatory Commission.

Efficaceous safety inspection depends, not only on appraisal of the design of the reactor plant, but on the subsequent circumstances of the construction and operation of the power station on site, the latter factor in many respects transcending the former in importance. The assurances as to the quality and reliability of design remain as bookwork, but the reality of the plant is in the practical engineering of building, operating and maintaining it in situ, matters being realised in America with the débâcle of 'Marble Hill' (22).

Therefore, catastrophic low probability events take place in the latter regime and not in the plans and specifications which are the formalised conceptions of the design office. While this has been the guiding principle of the New Treatment and the reason for its emphasis on inspection, it must be recognised that in the absence of a design, there would be no plant to inspect. Moreover, both relevant theory and a proper safety appraisal of design are essential for the effective pursuit of that inspection. To meet this need, New Treatment has attempted to develop a consistent theory about the causation of those low probability events that lead to catastrophic plant and system failures. Without such direction an ad hoc approach to safety is

inevitable, but inadequate as, indeed, was that of those National Coal Board officials who failed to perceive that the mine spoil tip poised above the village of Aberfan was dangerously unstable.

The New Treatment suggests an analogy between the experience of industrial incidents and noise theory in which the flow of mundane faults, failures and accidents may be likened to the casual disturbances that are a feature of communications channels. In this background of 'noise' there are larger impulses or 'spikes' which are analogous to the occasional major events that disrupt the normal operation of the plant, even to the extent of a catastrophic failure. Accident records show that such events are usually preceded by lesser ones as precursors. These give evidence of the loss of resistance of the system to failure, but the harbingers are inevitably disregarded for if they were not, the accident would not occur. Owing to the fact that the true risks of nuclear power are incommensurables in any precise, mathematical, predictive sense, the nuclear safety inspector must seek qualitative guides to his decision making. His task is to apprehend both objective and hidden precursors of failure in the constitution and behaviour of the plant and to guide its management accordingly. Catastrophe theory has been used in an elementary manner to construct a simple behaviour model to depict the operational scenario of a nuclear power plant. It is thus possible to give an overall portrayal of the operational risk situation through which the plant's management must pilot it, the fault and failure hazards being represented as irregularities in a probability field, namely the model's Behaviour Surface. Encounters with anomalies in this Surface represent destabilisation of the plant's normal performance from minor faults to catastophic accidents. The disturbances may be associated with Event-noise and a panoramic risk scenario created in which potential accident precursors are more likely to be identified and safety investment and efforts more logically and effectively apportioned.

In a review of the state of risk science now orientated to quantitative methods, it has been argued that the failure modes foreseen by reliability analysis of design will never happen in a properly built and operated plant. The factors so identified in their causation will have either been designed out by prudent engineering or will be related to unlikely happenings for which the computed chance of their occurrence is too small for eventuation. On the other hand, low probability events not foreseen in such analyses can and do occur.

Nevertheless the existence of a sound design, free of identifiable faults is an essential precondition for safety and reliability.

To escape from this impasse, the New Treatment suggests that potential accident precursors may be identified by an inspection that is perceptive and forward-looking. In such an endeavour an approach combining the powerful quantitative methods of design assessment with the qualitative analytic logic of Event-noise-Catastrophe theory can offer an effective aid, potential fault sequences being arrested before they are able to run to catastrophic failure. This must even now be the case for near-miss accidents. However, it is difficult, if not impossible, to establish with any certainty that such a catastrophe would have occurred had not the preventive measures been taken. Nonetheless, a 'noisy' plant is inspectionally suspect as failure prone and measures taken to 'quieten' it should reduce that risk. Reports of work-accidents, faults, other incidents, and especially those of management difficulties made by regulatory site-inspectors and operators in Licensee Event Reports (LERs), provide a flow of 'noise' for inspectional analysis and discernment of potential precursors.

15.2 Some matters concerning the public acceptance of nuclear power

A major argument advanced against nuclear power by its opponents is that there can be no absolute assurance against catastrophic radiation accidents. While this is true, at least for current designs of nuclear power reactors, it is also the case that, if a regime of safety assurance could convince the intelligent, rational, opinion-forming section of the public that it had reduced the realisable likelihood of a possible severe radiation accident to one that was truly negligible, then the threat posed by nuclear power would be likely to be ignored. That threat would then be seen as the very unlikely chance of a low probability event against which all reasonably practical steps had been taken. It is further argued that, if this could be presented in a truly convincing way, it would be conducive to a state of confidence in management of the nuclear risk in which the properly informed and unprejudiced public would be willing to tolerate the minuscule residual hazard.

This has been achieved in the realm of air transport where the personal risk to the prospective passenger is accepted as insignificant, but in this it is relevant that the keepers of safety are the pilots and air-traffic-control whose competence and efficiency are properly

subject to continuing surveillance and attestation. Catastrophic accidents may be attributed to failure of inspection of the latter kind, seldom being due to equipment or structural faults.

But why has not this state of affairs been established for nuclear power, given its enviable record of safety? The answer has an unavoidable political flavour that limits discussion here. Nonetheless, two points may be made. First, those serious attempts that have been made to win public support have turned on bland assertions about almost unquestionable safety from committed public figures and certain eminent scientists, some of the latter truly out of their field, backed by tenuous excursions into risk mathematics. Second , the relevant arguments lie in the realm of engineering as in the case of air transport.

In the case of nuclear power, the official guarantors of the engineering and operations, and especially the NII in Britain, have been under continuous disparaging attack, not likely to enhance public confidence in the efficacious surveillance of safety. Besides, the circumstances are bedevilled by the complex and enigmatic political factors hinted at above that have been treated more fully in Document No. 4 of the Annex.

15.2.1 The new style inspectorates and public trust

The point has been made earlier that the raison d'être for the NII and other new style inspectorial bodies like the NRC was that they were needed to provide a defence against the envisaged disastrous human and financial consequences of a major nuclear mediated radiation accident, ie the 'infinite' aspect of the actuarial risk. The task was not given to the existing organisations responsible for industrial safety, eg H.M. Factory Inspectorate, because their post-event strategy of prosecution for observed breaches of regulations, usually after an accident, was unacceptable in the circumstances. In common with other statutory bodies with regulatory functions, the NII and its compeers lack public accountability and there appears to be no means whereby their competence may be openly verified. These are matters of importance if inspection is to be seen as the guardian of safety. Indeed, the accepted view is that such things are 'incommensurables' (Douglas Wass 1983) and the officials who manage the inspectorates owe allegiance to the upper echelons of the bureaucracy, rather than to the public in any direct sense. Moreover, public confidence in the defences against the unfamiliar and far

reaching hazards of nuclear power is not likely to reside in faith in the capability of faceless public officials, but in the conviction that the defence of safety is verifiably effective, efficient and well managed.

Engineering which, unlike mathematics and physical science, has a societal role is the proper source of this trust, but, whereas the material achievements of engineering are tangible, inspection has been impalpable. Despite that, recent developments in psychophysics have shown that the performance of inspectors can be measured by Signal Detection Theory (SDT) and, not only can the technique be applied to Viewing operations, but to the more sophisticated arts of forecasting technical outcomes, the relevance to design assessment and Forward Safety Analysis being obvious.

An attempt has been made to show that SDT can be used to assess the performance of an engineering inspectorate like the NII on a scientific basis, justifying the claim to assure safety by foresight, namely that of the effectiveness of its faculty of Forward Safety Analysis and of an ability to discern the harbingers of failure. In the foregoing applications SDT also has a disciplinary use as a test of the effectiveness of the performance of inspectional work. It can thus, not only provide a check on the efficiency of inspection, but offers a means of securing accountability as well.

15.3 Synthesis of the New Treatment of Low Probability Events

The New Treatment is an approach rather than a prescription which sets down those principles on which an efficacious and convincing model of a system for statutory safety assurance of the reactors in a commercial nuclear power program can be built. It is therefore the gathering together of the themes developed during the discourses on the several topics examined in the preceding passages in this thesis, namely:

(i) The historical background from which the modern attitudes to industrial hazards emerged;

(ii) The necessity of the advance of technology, risks and benefits;

(iii) Catastrophic failures in technical systems and their causation;

(iv) The state of the art in risk science;

(v) The emergence of probability and its relevance to hazard management;

(vi) The idea that very low probabilities are metaphysical in open systems and that the specific hypothetical events to which they are ascribed never happen (14);

(vii) The analogy between the actuarial 'Zero-Infinity Dilemma' and the quandary of safeguarding-investment economy in nuclear design safety assessment;

(viii) The analogy between the actuarial admission of 'Ignorance of Mechanism' and the inability of quantitative safety analysis to identify true low probability plant failure sequences rather than hypotheticalities;

(ix) The discontinuity between the design concept and its realisation in an operational plant;

(x) The growing disjunction between the 'Two Cultures' and the alienation of realm of administration and politics from the domain of science and technology;

(xi) The concept of plant accidents, faults and failures as an 'Event-noise' flux;

(xii) Representation of the possible operational experience of the plant as its movement on the probabilistic Behaviour Surface of a simple Catastrophe theory model;

(xiii) The discernment of harbingers of major plant failures in terms of 'loss of resistance to failure' from evidence in the accidents, faults and incidents gleaned from Event-noise and other operational sources;

(xiv) The central role of engineering inspection in nuclear power plant risk management and safeguarding;

(xv) Signal Detection Theory and the appraisal of efficiency of inspection and safety assessment functions;

(xvi) Accountable engineering inspection and public trust; and

(xvii) Acceptance of nuclear power as the preferred energy option and toleration by the public of the minuscule residual risk.

Although the above schema for hazard management has been discussed with nuclear power in mind, it may be readily adapted to other dangerous technologies.

The foregoing principles provide a framework for a policy that could win rational public toleration of a technology of great and essential benefit to the community, but one that also brings with it a dire potential hazard. They underlie the arrangements that have made the grave risks of mass air transportation acceptable with little demur, although one yet to be achieved for nuclear power.

In essence they meet the criteria held by W.D. Rowe (1979), Talbot Page (1979) and other eminent authorities to be necessary for public acceptance of a major technological risk, namely that:

(a) it is generally accepted that the risk has been reduced by a system of efficient and stable control to a level so small that it may be ignored for the practical purposes of daily life;

(b) the efficient system of control is exercised by a credible organisation with statutory responsibility for health and safety;

(c) the credible organisation is accountable to the public for its activities; and that

(d) the competence of the organisation and the efficiency with which it can perform its functions are verified by a disinterested, independent agency.

However, the opposition to nuclear power is not due to concerns about its technological dangers alone as the opposition gains support from fears of a general political nature, matters discussed in Section 5.2 et seq. These latter factors will sink to insignificance with the approach of the energy crisis that will inevitably accompany exhaustion of the World's oil reserves. This has already happened in France which has suffered from an energy dearth for generations that would become a major economic embarrassment in an oil famine. Nonetheless, there remains a very real hazard in the case of nuclear energy that must be kept under effective control and similar problems may have to be faced as other potent new technologies are introduced.

15.4 A concluding comment with some reservations

A historical background to the New Treatment has been provided from the Industrial Revolution to the scene today when a rapidly advancing technology is imposing new hazards on the public and environment as a concomitant to the benefits. The societal reaction in Western society has been examined in the light of the changes in government administration and corporate management that have taken place to meet the new technological situation.

The leading innovation so far has been the exploitation of atomic energy in the generation of electricity. In view of its intrinsic hazard of a devastating radiation accident, nuclear power has not only brought into being safety technologies of a new kind, but it has been properly subjected to a special regime of statutory regulation. Nonetheless, widespread unease about its safety and certain other aspects is hindering further progress in exploitation of the nuclear energy option.

The present regulatory scene is unsettled, although the underlying reasons for this do not reach the level of public debate. One of the more subtle of them is the divergence between the pragmatism of the engineers and promotion by the scientists and those favourable to their cause of frequency theories of probability and allied systems mathematics as panaceas for all problems of practical risk management. An attempt has been made in the New Treatment to re-establish a balanced perspective in which the relevant scientific and mathematical advances may be properly seen as tools, appropriate in some situations, but inappropriate in others.

Engineering is not science, but the scientific utilisation of science to meet the needs of society and, more particularly, a given society. It has, therefore, a greater dimensionality. This divorce between the two disciplines has long been known, but it has been customary to describe it in a manner derogatory to engineering. In the days of simple technology, of flying machines, wireless, permanent way and rhumb line navigation, any serious attempt to reject this inferior status would have been futile. Except for the occasional genius like Edison, Watson-Watt, Blumlein and Whittle, engineering in the first part of this Century had an image of drawing office, foundary, fabrication, boiler suit and oil can.

Today there is a new situation. The complexity and sophistication of modern technology has extended the horizons of the engineer to computer software and information science, aerospace, communications and the intricacies of micro-electronics to name but a few, let alone atomic energy. If a country is to compete effectively with others in the Western orbit, then engineering must be accorded the status of a creative intellectual activity on a par with the other great branches of culture identified in Figure 1. And, the management of technological risk is part of that culture.

Much of the New Treatment is a restatement of engineering pragmatism in this modern setting. Another has been the creation of a rationale in which the challenges and quandaries of the new engineering science can be properly presented in the existing economic and social milieu. In consequence, certain aims of the New Treatment have political and constitutional overtones. Perhaps the most far reaching of them is the suggestion that the efficiency with which many engineering activities, and particularly those of a managerial and administrative kind, are

performed is determinable and, in consequence, those who are responsible for them can be appraised and held accountable.

Introduction of the New Treatment would bring about substantial changes in the administration of the regulatory organisations and the complementary safety echelons in the utilities and other industrial managements as they exist today. As in the case of all such organisational change, constitutional obstacles as well as the inertia of the existing hierarchies would have to be overcome. It might well be that without the sanction of some major accident, no doubt nuclear, the New Treatment could not be introduced in the face of obdurate opposition. For these reasons, it might be more readily acceptable in a situation where a regulatory system for nuclear power was being considered, say in a country about to embark on a national program.

A word on the philosophical tone of this study is in order. The arguments on which the New Treatment has been advanced lie principally in the arena of philosophy, logic and ethics, but in an engineering aspect. The problems of management of very low probability technological risks are now societal rather than technical. The achievements of reliability and risk science are not in dispute, but their intrusion into the former area as major determinants is.

Finally, there is an ethical reservation of some profundity. A retrospective Fatal Accident Frequency Rate (FAFR) is an objective statistic, but the New Treatment implicitly rejects the prospective use of the FAFR as a design parameter. Of course, absolute accident prevention is impossible and there will be fatal industrial accidents, but an ethical safety philosophy should be centred on the protection of human life, not on acquiescence in death. The writer expressed this in relation to nuclear power plant design thus:

> 'To bridge the innate discontinuity in a logic which sums the products of events which may be reasonably expected to happen with those which must not, there is an implicit postulation of the inevitability of occurrence of the untoward and forbidden. While no plant, however well built and managed, can be expected to run absolutely risk free, this philosophy of accepting disasters so as to make prophecies about the harm which may be attributed to a nuclear power programme is questionable. Nuclear plant designers must be guided by an aim which secures that major plant disasters do not occur. Their designs and precautions must make them 'incredible'. Of course, experience in safety has shown that there is very little which is impossible. For this reason, the worst consequences of a plant accident must be known, not as a basis for a safety philosophy, but as a guide for siting, emergency planning and damage control needs. If such an untoward catastophic event occurs, it should be in spite of human endeavours and not because of a failure which could be attributed to a permitted weakness in design.'
>
> O.H. Critchley,
> 'Risk prediction, safety analysis and quantitative probability methods - a caveat',
> J. Br. Nuclear Energy Society,
> Jan. 1976, 15(1), p. 19.
> (See Document No. 1 of the Annex.)

The New Treatment is open to the criticism that it is strong on philosophy, but weak on prescription. True, but to make substantial changes in the engineering and safety structures in the nuclear power industry, the commission charged with the task would have to be given statutory authority to inquire deeply into the administration and organisation of the electrical power utilities and their contractors and of the inspectorates that regulate them. It would also need a remit to prescribe staffing policies for these bodies so that their key managerial posts would be filled by engineers of the proper calibre. It would also need to direct the engineering towards standardisation of plant design to be enjoined by strict quality control during construction and operation. A mandate from the public that was endorsed by the political establishment would be required to secure passage of the enabling legislation. This essential support could not be won in absence of a cogently argued case, justified by reasons of polity, science, economics and ethics. This thesis is an attempt to outline a philosophy and suggest a methodology on which such a case could be made.

PART SIX

MISCELLANEOUS MATERIAL AND SUPPORTING PAPERS

Sections 16 to 23 consisting of:

16 Epilogue

17 Acknowledgements

18 Notes - Numbers 1 to 26

19 Appendices I, II and III

20 Figures 1 to 21

21 Tables I, II, III and IV

22 References

23 Annex - Documents Numbers 1 to 5

16 EPILOGUE

The thoughts marshalled in this thesis have been punctuated by three disastrous Low Probability Events: initiated by 'Flixborough', sustained by 'TMI' and concluded by 'Abbeystead', each in its way emphsising the theme. There is no absolute safety, even in circumstances seemingly innocuous, but a proper treatment of an overtly dangerous technology can maintain a state of safety asymptotic to the absolute. From each an important lesson may be drawn: from 'Flixborough', dependence on the quality of engineering in management; from 'TMI', the sine qua non of competent and properly trained technicians; and from 'Abbeystead' that there is no defence against 'Ignorance of Mechanism', being another tragedy of incredible causation like 'Moorgate'. But, the defences against these things do not take care of themselves, owing to the lethargy, tendency towards centripetal conceits and over-confidence that can afflict even the best of managements. To overcome their baneful effects, a continuing and intrusive, but disinterested inspection is necessary, though it must be an inspection of the proper kind that is itself accountable to the people for whose benefit it was instituted.

Some of the most important advances in safety have been made by the use of operational research (OR). Salient among them has been the application of reliability technology to design safety assessment which, together with other developments in safety and regulatory science, have been studied here in the light of the growing disjunction between theory and practice that characterises present day Western civilisation. That the promotion of OR methods of risk assessment in nuclear power over the past two decades has been paralleled by a more general exploitation of systems techniques as the decision maker's panacea is not without relevance.

The enhancement of safety of a nuclear power plant or other major hazard installation by improved reliability in design is unquestionable: that reliability per se can virtually eliminate the threat of a very low probability catastrophic failure is not. On the other hand, engineering inspection which has lacked due recognition of late can ensure the compliance of a complex technological artefact with its design, and this is a sine qua non of operational safety, though by no means a guarantee of it. Moreover, it can reveal evidence of that loss of resistance to failure that almost invariably precedes a catastrophic

fault sequence, such tell-tales being more often disregarded than recognised even by alert managements.

Inspection, aided by reliability analysis, can thus offer an efficaceous way, not only of preventing mundane accidents, faults and incidents, but of reducing the chance of catastrophic failure to a virtual zero. Presented as a verifiable and accountable system of safety management, it could inspire public confidence that the risk accompanying the nuclear energy option, though real, was effectively negligible.

In so wide a field, it has been possible to do not more than outline a framework for the New Treatment. Its methodologies have, for the most part, been only sketchily described and some passed over with little more than a hint. Among the areas of specific interest deserving further study in the construction of a more complete schema are:

1. Licensee Event Reports (LERs)

   Development of effective means whereby LERs can be analysed to identify trends towards 'loss of resistance to failure' in nuclear power plants under surveillance in both their individuality and generality, using noise theory as the means of identifying 'signals of weakness', not only from components, equipment and structures, but from their organisations and managements as well.

2. Engineering Inspection

   An interdisciplinary research into the objectives, organisation, methods and philosophy of the higher orders of engineering inspection, recognising it as a discipline in its own right, embracing such supporting techniques as non-destructive testing, modelling, quality control and quality assurance.

3. Signal Detection Theory (SDT)

   The use of SDT in the appraisal of inspectional functions and, in particular, the technical safety assessment of design; of executive inspection both internal to the plant and regulatory and the relationship between the two with a view to rendering the system accountable to the body politic; and of inspectors as individuals and teams in respect of their prognostic skills in assessing the likelihood of catastrophic failure sequences as a determinant in the management of plant safeguarding investment.

4. The causation of Low Probability Events (LPEs)

   An interdisciplinary investigation oriented towards the personal and managerial aspects of LPE causation, namely oversights, behavioural aberrations, centripetal organisation tendencies, barriers to the flow of safety and reliability information both internally and externally and failures of inspection.

5. Amalgamation of the Event-noise and Catastrophe Theories

A more rigorous justification of the attempt to combine the Event-noise concept with Catastrophe Theory with a view to defining the Behaviour Surface of the Cuboid Model more objectively as a probability field.

17 ACKNOWLEDGEMENTS

The author wishes to thank Professor D.C. Leslie for accepting this interdisciplinary study as a topic suitable for research in the Department of Nuclear Engineering. In particular, he wishes to acknowledge the sustained help, encouragement and guidance he has had from his supervisor, Dr. John Shaw, and, not least, to thank him for his agreement in the beginning to undertake its supervision. He is also very grateful for the patience Dr. Shaw has shown by maintaining a stimulating interest in a study that had to be pursued as a sideline during the author's period of employment as a Superintending Inspector of Nuclear Installations, an occupation that left little time for resolution of the difficulties in its direction that arose during the early stages of the work.

Mention must be made of Messrs. T. Griffiths, E.C. Williams (deceased) and R. Gausden, all erstwhile Chief Inspectors of Nuclear Installations, and of Mr. Brian Harvey who at the relevant time before his retirement was HM Chief Inspector of Factories and one of the three directing members of the Health and Safety Executive for without their sponsorship the study would have been impossible. The author is also grateful for the support he received from the Training Section of the HSE until his retirement from the Civil Service.

The research findings and opinions expressed are solely those of the author for which he takes full responsibility. They are in no way attributable to any member of the Department of Nuclear Engineering nor to any former colleague, associate or principal, though the body of the work has been enhanced by discussion and debate with these people and, not least, by their often trenchant criticism.

Finally, it is his pleasure to express his appreciation for the support and generous assistance he has had from his sons, Julian and Lester, his daughters, Hilary and Philippa, and especially from his wife, Peggy, who has given invaluable help in collating the references and in proofreading the fair copy typescript. Moreover, he thanks Julian for the useful advice and positive criticism he has given during the research and drafting of the text.

18 NOTES

Number	Title	Section*
1	Natural disasters	1
2	Life expectancy and GNP	1
3	Toll on the roads	1
4	Luddites	2.1
5	Pollution control in ancient times	2.1
6	Exaggeration of nuclear power hazards	3
7	Panic and the management of emergencies	3.5.1
8	Human error	4.1
9	'Safest industry in the World'	4.2
10	Canvey Island/Thurrock risk assessment	7.1
11	The persisting influence of Aristotle on Western thought	8.1
12	Closed and Open Stochastic Systems	8.2.1
13	Estimated cost of the Sizewell PWR inquiry	8.4.9
14	Metaphysical probability	9.6.1
15	Safety Data reporting schemes for nuclear power	9.7.2
16	The value of human life	11.2.2
17	Accidents of unacceptable dimensions	11.3.2
18	Reliability Degradation	12.2.2
19	Enforcement inspection philosophy	14.1
20	Engineering inspectors ignored	14.3.1
21	Profile of a nuclear safety inspector (INI)	14.5.2
22	Marble Hill debacle	15.4
23	Peculiarity of the written languages of Japan	8.1.1
24	Pure Administration	9.5.2
25	Markham Colliery Overwind	12.3.3
26	Quantitative Risk and Safety Analysis in the U.K.	9.5

* Explanatory Note

The Section number cited refers to the place in the text where the given note first appears

(1) Natural Disasters - There is a comprehensive list in the 'Guinness Book of Records' published by Guinness Superlatives, London, 30th Edition, 1984. The worst known to the World was the 'Black Death' from 1347-1350 A.D. when some 75,000,000 died, The influenza epidemic of 1918 killed 21,640,000. In the China famine of 1969-1971 an estimated 20,000,000 starved to death. In the Hwang-ho River flood of August 1931 3,700,000 Chinese drowned. 830,000 were lost in the Shensi earthquake of 1556.

Tidal waves are not tsunami. The latter are caused volcanic and earthquake forces. Tsunami 220 ft from trough to crest have been recorded. The biggest tidal wave observed was 112 ft from trough to crest. The most violent volcanic erruption of modern times was that of Krakatoa Island on August 27, 1883 which created 4.3 cubic miles of ejecta. The resulting tsunami killed 36,380 people.

(2) Life expectancy and GNP - Indirect losses in life expectancy . resulting from a general decrease in the gross national product (GNP) have been investigated recently. The effect is hard to quantify. In their study of 'Risk and Culture' Mary Douglas and Aaron Wildavsky (1982) have identified it as a positive factor in reducing life expectancy. In an attempt to scale radiation risks against those due to other societal causes, mainly employment, J. Reissland and W. Harries of the National Radiological Protection Board (1979) note that there is a definite relationship between the GNP and the expectation of life.

(3) Toll on the roads - Deaths attributable to motor traffic run at some 8,000 per year in Britain and are proportionate higher in the USA. Fatalities from all causes in the nuclear industry have not exceeded 12 per year.

(4) Luddites - The introduction of power looms brought ruin to the skilled textile workers of Northern Britian who were unable to compete with the new machines. Through the years of 1811 to 1816, they turned their fury for the loss of livelihood and distress to riot and the breaking of the machinery in mills. It is not known whether their action was spontaneous or organised, but it was attributed at the time to a legendary Nedd Ludd. The movement was put down with great savagery and machine breaking made punishable by death. Sporadic violence continued until as late as 1840.

(5) Pollution control in ancient times - The tanning of hides was a major industry in Biblical times, leather being used for footwear, shields, helmets, girdles, etc. and parchment was prepared for writing. Owing to the unpleasant smells and noxious effluxes, 'tanners were compelled to find quarters outside towns and near water' - 'a tanner by the seaside', Acts 10:32. Excerpt from Black's New Bible Dictionary, 8th Ed., London, 1973, p. 726.

(6) Exaggeration of nuclear power hazards - In addition to the virulently anti-nuclear books like 'Poisoned Power' (Gofman and Tamplin 1973) and the more recent 'Power Corrupts' (Bacon and Valentine 1981), there have been more subtle and credible attacks in the media. One such is 'The China Syndrome', a film in which Joan Fonda stars. It describes a hypothetical nuclear power plant accident that results in the heavy contamination of a large area of land by radioactivity.

(7) Panic and the management of emergencies - The lesson to be learnt from the appalling disaster that was the outcome of the 'Cromarty'-'La Bourgogne' collision is that in the operation of a system that can fail in a catastrophic mode emergency planning is essential. The principle applies no matter how remote the probability of the event is. With no assured leadership and officers probably unaware of what to do in the sudden emergency of a vessel sinking fast under their feet, the crew's discipline broke and they descended into mindless, animal panic. The comparison with the disciplined behaviour of the officers and men of the 'Titanic' is striking, although the emergency planning was pitifully inadequate. This answers the criticism that in emergency exercises the envisaged accident will differ from the real one and therefore the drill is irrelevant. The comparison between the two above incidents shows that it is preferable to have a crew, or team of plant operators, trained to behave in a disciplined way, even if that way is not wholly appropriate than to have disarray and possible panic.

(8) Human error - Strictly, all failures in artefacts and systems are due to human error, ranging from design mistakes and oversights, imperfect planning, equipment and components faults to inadvertent operator mistakes and negligent mal-operation. In this text, the concept of human error is confined to untypical aberrant behaviour, oblivious, mistaken, ill-informed or negligent that results or could result in system failure. However, the commonplace operational mistakes are classed with equipment failures rather than human error per se. These mundane mistakes occur with sufficient regularity to present stable patterns from which meaningful failure rate data can be extracted. In contrast, the former aberrations are wholly random and unpredictable.

(9) 'Safest industry in the World' was how Lord Peter Ritchie-Calder (1969) described the nuclear industry in the West with radiation doses to the public well below natural background. There has been some recent evidence to the contrary in the special case of the Windscale plutonium pile fire of 1957. A National Radiological Protection Board (NRPB) now estimates that some 260 case of thyroid cancer resulted with a possible 13 deaths (Crick and Linsley 1983). However, the work did not include a previously unreported concurrent release of 150 curies of Polonium-210 to which another 20 to 50 deaths may be attributed (Nature, 7 April, 1983, p. 470).

(10) The Canvey Island/Thurrock risk assessment - The report of an exploratory public inquiry into the desirability of revoking planning permission for an extension of the oil refining facilities on Canvey Island on the North bank of the Thames near its mouth contained a recommendation that a safety study was desirable. The study was carried out by the Safety and Reliability Directorate of the UKAEA who reported to the Health and Safety Executive. A summary was published by the Executive in May 1978 (Locke, Dunster and Pittom). The work was not so much an assessment of the probable risk of the Canvey Island/Thurrock installation as a whole, but of the added risk due to the extension. It found that while the extension would only increase the calculated risk by a small amount, the existing risk to an individual resident in the area at hazard being estimated at 1 fatality in 10,000 years of exposure which appears to be somewhat less than that of being killed in a motoring accident, ie. 1.3 in the same period of exposure.

(11) The persisting influence of Aristotle on Western thought - The importance of ancient Greek philosophy upon the emerging civilisation of the West and its subsequent development is hard to overrate. It is the substrate of our culture and the names of those outstanding Greek thinkers have become almost household words, among whom one may cite Heraclitus, Pythagoras, Archimedes, Euclid, Socrates, Plato, Aristotle and Galen. The noted French historian of science, Arnold Reymond (1927), wrote:

> 'Compared with the empirical and fragmentary knowledge which the people of the East laboriously gathered during long centuries, Greek science constituted a veritable miracle. Here the human mind for the first time conceived the possibility of establishing a limited number of principles, and of deducing from these a number of truths which were of rigorous consequence.'
>
> Science in Greco-Roman Antiquity
> (Trans. Ruth Gheury de Bray),
> Methuen, London, 1927.

Of all these thinkers, Aristotle's influence has been paramount.

Logic and rationality which are indicative of educated behaviour in European civilisation today were not recognised as the most propitious ways of thinking before their identification as such by the philosophers, writers and lawyers of ancient Greece and Rome. Today, whenever there is a debate or serious discussion an appeal to logic is made. Aristotle of Stagira (384-322 BC) founded the science of logic and for many centuries logic, either overtly or implicity, has been a central part of further education in Europe and has left a deep and lasting mark on the languages and outlook of her cultured people. Emanating from them, logical thought has become part of the thought processes of both navvy and university don. But it is a particular logic, for logic of a kind is common to all mankind, and that of Europe is characteristic of the Greco-Roman civilisation from whence it came. It is one, excluding the domain of experimental science where the Scientific Method rules, that is more concerned with words, ideals and mathematics than the pragmatic realities of the world. Undeniably, it has been the central force in the evolution of European civilisation, yet in certain respects its influence has been pernicious.

Galileo's thesis in support of Copernicus was published in Florence in 1632 under ecclesiastical licence. As soon as it was realised that it presented a serious challenge to the Aristotlean moral and philosophical basis of society, all Christian Europe both Catholic and Protestant was outraged at the heresy. Galileo was condemned by the Inquisition, silenced, and sentenced to life imprisonment. His book stayed on the Index until 1835. Two hundred years later, the European scientific community dealt with Dr. Georg Ohm in a somewhat similar way, debarring him from academic preferment. Nicolas L. Sadi Carnot refrained from publishing his conversion to the kinetic theory of heat and much of his work remained as manuscript until many years after his death in 1832. Traces of this regressive influence persist today. Prof. J. Schwartz (1962) has argued cogently that mathematical formalism receives an undue deference which is detrimental to science.

(12) Open and Closed Stochastic Systems - In a closed system of random events, the probability distribution is inherently stable. The 'Ernie' Premium Bond Prize allocating computer program is an example. The manager of the weekly draw looking inward sees a closed system. Every properly recorded Bond number has an equal chance of about 1 in 1.4×10^9 of drawing the top prize. This very low probability is not metaphysical because a winning number must be drawn. The probability associated with very long half-life radioactive decay is analogous, for instance that of uranium-238 in which each atom has a 1-in-2 chance of decaying to thorium-234 over a time span of 1.5×10^9 years. A well-planned scientific experiment is an attempt to establish a closed system.

On the other hand, the Premium Bond financial controller looking outward instructed to pay the winner may see an open system. There is a chance that the winner cannot be located. Some millions of Pounds of unclaimed prize money has accumulated. Another 'open' case arises with the very low probability of a catastrophic nuclear power plant incident. A quantitative safety assessment of the design is based on an assumed closed universe of known or allowable factors, but the system is, in truth, open in the case of the plant constructed to that design. There is an inevitable intrusion of unknown and unanticipated elements.

(13) Estimated cost of the Sizewell PWR inquiry

Reports on the cost to the Central Electricity Generating Board to support its case for a Pressurised Water Reactor (PWR) to be built at Sizewell, near Leiston in Suffolk, say that 125 kg of reading matter has been produced. This consists of the safety report, reference design and supporting scientific papers which together with fees to counsel will involve an outlay of between £5 to £10 million (Brian George 1982, J. Edwards 1982). In comparison, the U.S. Reactor Safety Study weighs about 10 kg.

(14) Metaphysical probability - Very rare events in open systems never happen in any realisable span of normal human experience. Either the conditions of the probability situation change or some other event occurs instead. This is an intuitive conclusion reached by many eminent thinkers from antiquity to modern times.

Marcus Tullius Cicero (106 - 43 BC) in his critical dialogue on prophecy had the following to say about chance:

> 'Four dice are cast and a Venus Throw results -that is chance; but do you think it would be chance, too, if in one hundred casts you made one hundred Venus Throws?'
>
> De divinatione (circa 40 BC),
> Book I, Chapter xiii, para. 23
> (Trans. W. A. Falconer, 1923),
> Heinemann, London, 1930.

In the same strain, Jean le Rond d'Alembert (1717 - 1783) observed:

> 'It is metaphysically possible to throw two sixes with two dice a hundred times running; but it is physically impossible because it has never happened and never will.'
>
> Quoted by L. E. Maistrov in
> Probability Theory: a historical sketch.
> (Trans. and Ed. by Samuel Klotz),
> Academic Press, New York and London,
> 1974, p. 125.

More recently, the French mathematician Emile Borel defined the very low probability enigma in terms of an empirical law which he regarded as certain. He called it 'The Single Law of Chance':

> 'Events whose probability is extremely small never occur.'
>
> Elements of the theory of probability
> (Trans. John E. Freund),
> Prentice-Hall, New Jersey, 1950.

However, he hedged this around with certain reservations, noting that if there were enough exact repetitions of the chance situation, then the event could happen. Further, he defined probability bounds in terms of perspectives, namely the:

'Human' as one chance in less than 1 in 10^6,
'Terrestrial' ditto 1 in 10^{15}, and
'Cosmic' " 1 in 10^{200}.

Put in practical terms, he liken the human scale to the chance of an expert typist producing 500 sheets of text without making a single mistake. The cosmic scale he compared with the chance of observing a reversal of the 2nd Law of Thermodynamics.

The very long half-lives in the case of radioactive decay are examples of many exact repetitions of the chance situation in the circumstances of a closed situation.

(15) Safety Data reporting schemes for nuclear power - In addition to those incidents on nuclear power plants that have involved serious damage to the installation or harm to people or otherwise are subject to statutory notification, happenings in certain other categories considered to be of safety relevance are reported. A number of schemes are in operation. In Britain one is managed by the Central Electricity Generating Board (CEGB) and another by the Systems and Reliability Service of the UKAEA. In the USA more information is available to the public. The Nuclear Regulatory Commission (NRC) and the Advisory Committee on Reactor Safeguards (ACRS) in association with the Nuclear Safety Information Centre (NSIC) at the Oak Ridge National Laboratory (ORNL) maintain a data base for'the collection, storage, evaluation and dissemination of safety information to aid those concerned with the analysis, design and operation of nuclear facilities'. Periodical documents and other occasional papers are issued which collate,summarise and review the information made available to the NSIC. Reports, known as Licensee Event Reports (LERs) are supplied by U.S. nuclear site licensees to meet the requirements of the NRC Regulatory Guide 1.16, Appendix A. The Swedish Nuclear Power Inspectorate maintain a similar scheme. Authorised users in the USA and Western Europe can obtain by a computer link access to a data base of nuclear safety information maintained by the Nuclear Safety Advisory Centre of the Electric Power Research Institute, the service being called 'Notepad'.

(16) The value of human life - Attempts to evaluate the worth of a human life are legion, but have mainly concerned judgements for damages for loss of life in an industrial accident. A comprehensive scheme was introduced in Britain in 1897 for industrial accident compensation. Until the 1948 Act, the maximum liability of an employer for the death of a workman with dependents was £700. Damages in legal actions varied widely, and could be much higher, depending on the judge's estimate of economic worth of the deceased. More recent valuations have been made for use in cost benefit analysis. J. E. Hayzelden (1968) found that a life was worth between £10,000 and £30,000, estimated on the basis of the actual, notional or potential earnings of the victim over what might have been the rest of his working life. This comes to a current £117,000 at the top of the range using an inflation index of 3.9. Joanne Linnerooth (1981) in a review of various models quotes a value of around $200,000 (£117,000 approx.) for an average useful life. She observed that 'life value estimates are rough. For this reason, cost-benefit calculations,especially in the area of public health and safety, should continue to be regarded only as an aid to public decision processes'. Black, Niehaus and Simpson (1979) suggest that an employee's death could be quantified in terms of loss of years of life and a fatality can thus be equated with 'a loss of 6,000 man days'.

(17) Accidents of unacceptable dimensions - In considering the propriety of an imposed risk, there is a reservation. If the consequences of a catastrophic failure, however unlikely, were to be one of intolerable devastation and mortality, say the extinction of a populous city, then that innovation is inadmissible. The criterion has profound implications in the choice of a reactor type for a nuclear power program and in siting policy, for instance as between the PWR and AGR systems. In the latter case, owing to the re-inforced concrete pressure vessel and restricted flow-area of the penetrations, it is inconceivable that in any LOCA more than a relatively small fraction of the fission product contents of the core.could be released to the environment. On the other hand, total failure of the PWR steel pressure vessel is not inconceivable and that could result in a massive release.

The personal or group norm of absolute unacceptability for a mortal risk is 10^{-1}, a fact used by the Romans in their policy of decimation to discipline mutinous or cowardly legionaries. Airmen on active service have reacted unfavourably to a loss rate of 5×10^{-2}, whereas a risk of 10^{-2} seems to have been accepted. Most people will tolerate a risk of 10^{-3} of fatality on occasions judged favourable to their purpose, whereas a mortality of 10^{-5} seems to be tolerated with equanimity, provided it does not come into the category of a 'dread risk', that is one personally identified as unendurable.

(18) Reliability degradation - Event-noise theory has an analogy with conventional reliability technology in the concept of 'reliability degradation'. Reliability engineers distinguish three agents that can degrade the inherent reliability of a product or system (Ronald T. Anderson et al. 1982). They are:

Manufacturing - process induced defects, failures of inspection and of quality control arrangements and latent defects (compare Static Event-noise) resulting in failure in service, particularly when the system is under stress.

Operation - degradation of the system in use through wear-out with ageing, though dominant failure mechanisms are rough treatment and incompetent handling.

Maintenance - a prime cause of degradation of inherent reliability is due to the maintenance technician inadvertently causing damage, faults or weaknesses by negligence or inept workmanship.

(19) Enforcement inspection philosophy - The view that the task of the inspector is solely that of ensuring compliance with regulations, etc. is widely, and properly, held by those concerned with the lowest tier of inspection, ie. Viewing. The remark was made to the writer by a 'main grade inspector' during his association with H.M. Factory Inspectorate from 1976 to 1979.

(20) Engineering inspectors ignored - The working group that assisted Gerald Rhodes in his study of'Inspectorates in British Government' consisted of a policeman, 4 senior administrators, 2 political scientists from academia, a managing director concerned with engineering and a general duties member of H.M. Factory Inspectorate, then serving as an administrator in the Health and Safety Executive Corporate Services Division. There is no indication that any professional member of an engineering inspectorate was officially consulted (G. Rhodes 1981).

(21) Profile of a nuclear safety inspector (INI) - In an early Civil Service Commission public advertisement for engineers to join the newly formed Inspectorate of Nuclear Installations, later the NII, the Chief Inspector, Major-General W. S. Joslin, called for experienced chartered mechanical, electrical and certain specialised (eg. metallurgists, physicists) engineers, being graduates with good honours degrees of not less than 37 years of age. While experience in the nuclear industry was desirable, evidence of responsibility in management of a major plant engineering project would be taken in lieu (Civil Service Commission 1959).

(22) The Marble Hill débâcle

The magazine 'TIME' of 30 January, 1984 (p. 44) reported the 100th nuclear power plant construction contract cancellation since 1974 with abandonment of the Marble Hill project by the Indiana Public Service Co. A capital loss of $2.4 bn has been reported, but the completion cost would have been $7.7 bn and probably more on a revised estimate. Marble Hill and other failures have been attributed to 'trouble over quality-control', in other words, failures of inspection.

(23) Peculiarities of the written languages of Japan - The inhabitants of the Japanese islands acquired their written language in toto from the more advanced society on the Chinese mainland about the 4th Century. Initially, all writing was pure Chinese, but the two languages were linguistically dissimilar. Not surprisingly, the Chinese characters failed to represent the spoken Japanese tongue. Owing the immense prestige of the superior Chinese civilisation and culture, the Chinese form was retained for erudite and refined correspondence. But, this did not meet the needs of commerce and popular communications and a semi-colloquial script evolved known as Kana which was largely phonetic, though the formal Kanji (Katakana) is still retained for official purposes. Consequently, the literate Japanese can read and write fluently in lexicals of two kinds, one largely phonetic and the other consisting mainly of ideograms. Nonetheless, it seems that the colloquial script is more suited to modern needs and is continuing to develop.

(24) Pure Administration - The Earl of Iddesleigh (1956) has described the 'Pure Administrator' as a gifted person who need know nothing about the details of his assignment, be it concerned with oil or crankshafts. He justifies this view by quoting from Earl Bertrand Russell:

> 'A man who has a position of power in a great organisation requires a definite type of ability, namely, that which is called executive or administrative: it makes very little difference what the matter is that the organisation handles, the kind of skill required at the top will always be the same. A man who can organise successfully, let us say, the Lancashire cotton trade will also be successful if he tackles the air defences of London, the exploration of central Asia, or the transport of timber from British Columbia to England. For these various undertakings he will require no knowledge of cotton, no knowledge of aerial warfare and no acqdaintance with forestry or navigation. His helpers in subordinate positions will, in several cases, require these several kinds of skill, but his skill is, in a sense, abstract, and does not depend upon specialised knowledge. It thus happens, as organisations increase in size, that the important positions of power tend, more and more, to be in the hands of men who have no intimate familiarity with the purposes of the work that they organise.'
>
> Education and the Social Order,
> Allen and Unwin,
> London, 1932 (new impression,
> 1951), p. 240.

This was not so much true as it was possible when Bertrand Russell wrote more than 50 years ago in the still simple technical world of the time, but his general conclusion is a non sequitur. A Manchester cotton magnate might then have been successful in organising a city's air defences. The necessary mastery of those aspects of the technology which were not general knowledge among the educated classes could be readily acquired by job contact. This is no longer the case because anti-aircraft weapons in common with all other major technologies have become so much more sophisticated that the 'pure administrator' is now totally dependent upon his specialist subordinates. Disquiet about the quality of innovatory technical decision making being widely voiced may well be a consequence of this lacuna.

Something insignificant in those earlier times is becoming an essential asset for those at the top in a large modern industrial complex. Its chief executive now needs empathy with the thought processes of his specialist subordinates and, more particularly, to be able to assist, inspire and lead them in their technical endeavours. This faculty is vocationally specific and is not attainable without career experience in the given intellectual field or in one that is analogous to it. Hence, a chemical engineer could administer a project of major national importance in the nuclear power industry which had to escape from the stultifying hand of 'pure administrators'. The case is not without supporting evidence, for instance, the late Sir Christopher Hinton (latterly enobled) was by vocation an able industrial engineer, but he soon proved himself an outstandingly effective administrator. He began as a craft apprentice in a large railway workshop, 'the best they ever had', going on to Cambridge to graduate with the highest honours in Mechanical Engineering. He then joined Imperial Chemical Industries, progressing rapidly to senior management level. His record as chief executive and principal engineer in the building of Britain's first nuclear power plants was in every respect outstanding.

Compared with Hinton's success, the record in innovatory technical decision making and in engineering management of the 'pure administrators' has been notable for lack of wisdom and paucity of achievement. Among the latter may be listed the tower block housing program of Ronan Point odium, 'Concorde' and the Dungeness 'B' AGR nuclear power plant. They are tales of partial or total failure from which, as Sir Alan Cottrell (1976) observed, 'the voices of the engineers' were either muted or ignored.

If there is such a thing as 'pure administration', then the reality of its practice is confined to the level of princes, prime ministers and presidents and their most senior functionaries and not in the organisation of major technological projects of much novelty. Indeed, the performance by these illustrious administrators has, more often than not, been far from outstandingly favourable.

To sum up, a prerequisite of effective management at any level is that 'definite type of ability' to handle people and situations 'which is called executive or administrative'. 'As organisations increase in size', so the measure of 'that kind of skill' needed grows in step. But today, a previously insignificant factor has become one of major importance. It is that for efficaceous management of a large high-technology project, the chief executive must be able to command with understanding and competence its scientific and technical features as well, and that is what engineering is about.

(25) Markham Colliery Overwind - A disastrous overwind occurred at the Markham Colliery in Derbyshire on July 30, 1974. Owing to a mechanical fault, braking control of the downcast winding drum was lost when the two cages were mid-shaft in the 1,400 ft. pit. The immediate cause was fatigue failure of a single steel rod, 2 in. in diameter and 9 ft. long that linked a nest of powerful springs to the brake bands, the rod having a safety factor of about 7 in tension. Normally, cage movement would only be possible while the brake bands were held off by a comprehensively safety-interlocked hydraulic system under manual control by the engineman. The catastrophic fatigue failure was due to long standing action of an unforeseen bending stress induced by inadequate lubrication of a pivot joint to which the steel rod was attached. As a result of the failure, the two tier cage carrying 29 men for the incoming morning shift continued to descend under regenerative braking of the Ward Leonard mechanism. The engineman, not recognising the nature of the fault, in prudence operated a safety trip that cut the 11 kV electricity supply, thereby disabling the regenerative braking circuit. The unrestrained cage then plunged to shaft bottom and the impact on landing killed 18 men and severely injured another 11.

Whether the loss of lubrication was due to poor design of the pivot bearing, inadequate maintenance or congealed oil preventing ingress of the lubricant or all of these things is not clear, although the official inquiry report (J. W. Calder 1974) was at pains to attribute it to the first. The incident was the subject of an exhaustive safety assessment (Thomas and Burgess 1976) with a view to enhancing the reliability of the design of modern winders. As empirical failure rate records were sparse, synthetic data was derived as required, but with heavy reliance on engineering judgements. An interim quantified estimate of a major failure of cage braking was put at 6 X 10^{-7} per year.

The accident was beyond the scenarios envisaged for the original design, one that had been subjected to exhaustive safety scrutinies by NCB and HM Inspectorate. Moreover, the above probability is metaphysical and, given compliance with the new design, the accident will never re-occur. But, conceivable failure modalities remain, for instance those associated with the single-line arragements for the cage suspension, eg. the rope, its capels and the pulley.

(26) Quantitative Risk and Safety Analysis in the U.K.

Despite the impressive developments that have taken place in the U.S.A. of which the 'Reactor Safety Study' is a prime example, the United Kingdom has made a major contribution to reliability technology and the use of quantification in risk and safety analysis, particularly in the field of atomic energy. The main seat of this activity has been the Safety and Reliability Directorate (SRD) of the UKAEA at Risley, Warrington, firstly in the Authority Health and Safety Branch which later became the National Centre of Systems Reliability (S.R.S. 1984) now sited at nearby Culcheth.

In addition to the massive technical support given to the Canvey Island/ Thurrock petrochemical installation risk study (Locke, Dunster and Pittom 1978), F. R. Farmer (now retired) and his erstwhile staff in the Directorate have contributed prolifically to all aspects of the technology. In addition to those already referred to in this text, among their many works of open publication the following may help to identify the theme underlying their approach:

Reactor safety analysis as related to reactor siting (1964)

Advocacy of quantitative methods of reactor safey analysis in which the Maximum Credible Accident approach is disparaged. To quote, it 'may be a yardstick of limited value in comparing reactors of the same type, but its use to compare the safety of reactor systems of different types is meaningless'.

Quantitative Safety Analysis (1970)

A long, comprehensive and authoritative exposition of the technology of quantitative reliability analysis and its application to safety assessment.

Today's Risks: thinking the unthinkable (1977)

After noting that a major technological accident might kill up to 10,000 people, though this would be an extremely unlikely event, but not an unknown calamity in terms of natural disasters, Farmer concludes, 'The public should recognise the need for wise and balanced judgement in situations where absolute safety can no longer exist'. They should look to experts to find ways of reducing the risk and expect them to be applied. The answer would seem thus to lie in securing a better informed public able to appreciate these matters and in further development of the techniques of technology risk assessment.

What is acceptable risk? (1978)

The case for a wider application of quantitative methods of risk and safety assessment in industry. After a comparison of fatal accident rates among workers, people at home, on the roads and those due to natural causes, he notes that it is 'the unusual accident affecting many people in one place at one time' that evokes a large public reaction. Special attention must, therefore, be paid to the possibility of a major hazard in order the minimise the chance of its occurrence.

Nuclear Decisions (1979)

One of three letters to 'Nature', the other two were from J.H. Dunster, Director of Nuclear Safety on the Health and Safety Executive, and M.J. Gaines of the National Radiological Protection Board. In his, Farmer calls for greater use of SRD for nuclear power plant design assessment and consequent decision making, observing that 'the need to obtain data and analyse quantitatively wonderfully sharpens the mind and illuminates the problem, even if to show up difficulties'.

19 APPENDICES

APPENDIX	TITLE	Page Number
I	A synopsis of statutory health and safety regulation in Britain	298 & 299
II	Selected Low Probability Events	300-309

Preamble

A selection of typical LPEs resulting in catastrophic failures

1. Aberfan
2. Abbeystead
3. Andrea Doria
4. Browns Ferry
5. Dudgeons Wharf
6. Faversham
7. Flixborough
8. Hixon Level Crossing (Fig. 18)
9. Minamata
10. Mount Erebus
11. Oppau
12. Ronan Point (Fig. 17)
13. Tay Bridge (Fig. 16)
14. Titanic
15. Thalidomide
16. Three Mile Island
17. Welder's radiation burns (Fig. 19-21)

Weightings of causal factors collated

Failure and its consequences

Concluding remarks

III	On Engineering	310-312

Two letters to the press (clippings)

APPENDIX I

A SYNOPSIS OF STATUTORY HEALTH AND SAFETY REGULATION IN BRITAIN

Action by the State to protect workers and the environment is by no means new and even in Biblical times a safety standard for those employed in building operations was prescribed (Deuteronomy 22:8) and, owing to their stench and foul effluents, tanneries were located by the sea (Acts 10:32). Britain has, so far, led the field in matters of industrial and maritime safety, not only from considerations of altruism, but of economics and public health as well. Admiralty sponsorship by offer of a £20,000 prize for an accurate means of determining longitude at sea encouraged the invention by John Harrison of his famous chronometer in 1760 which transformed the safety of navigation on the high seas.

Following the Industrial Revolution and the introduction of power driven machinery, the conditions in factories and particularly in textile mills, already bad, became worse, children suffering the most. Eventually the Government intervened and the first Factory Act became law in 1802. Although a notable political advance, it was largely ineffectual because enforcement lay in the hands of Justices of the Peace who were often beholden to factory and mill owners. A series of Acts followed in 1819, in 1825 and in 1831 in a climate of deteriorating working conditions, but, although they attempted to re-inforce the controls already intended by the earlier legislation, they still lacked effective means of enforcement. The turning point came with the Act of 1833 which authorised the appointment of inspectors who could make rules, regulations and orders appropriate to the circumstances and institute prosecutions for infractions.

After 1833 in a milieu of growing social conscience, health and safety laws of increasing effectiveness and stringency were enacted and by 1867 legal protection had been extended to most factories. The legislation was consolidated in the Factories and Workshops Act 1878 and an Employer's Liability Act in 1880 put worker's compensation on a reasonably satisfactory basis. Further consolidation was effected by the Act of 1901 and from then on there was little change until the Factories Act 1961 which brought together and clarified a large body of disparate laws and regulations.

There were important parallel developments, particularly in mining where there had been a heavy toll of life and limb through fire damp and dust explosions, falls of ground and flooding. The decade average centred on 1878 was 1,037 fatalities per year at a rate of 2.57 per thousand miners and figures for previous decades were tragically higher. Once again, the failure to provide for inspection rendered early legislation effectual. The nettle was grasped by the Act of 1843 when the first Inspectors of Mines were appointed. Very comprehensive safety provisions are now administered by H.M. Inspectorate of Mines and Quarries under the Act of 1954 and over the past several decades the rate of fatalities has fallen dramatically to less than 50 annually in 1979 and is still falling. Effective steps to control industrial pollution were taken with legislation that enabled the Government to appoint an Alkali Inspector in 1863.

Further important steps in the statutory protection of workers' health and safety were regulation of the manufacture of explosives in 1875, of the conditions of employment of shop assistants 1886, measures to prevent accidents to railwaymen in 1900, regulation of the petroleum industry in 1928 and of off-shore mineral and oil recovery installations in 1971. The aeronautical industry almost from its inception was in a special class, aircrew protection being secured through assurance of reliability in the manufacture and maintenance of aeroplanes for which purposes an Aeronautical Inspection Department was established in 1912. This unusual government initiative in safety has had an influence on safety regulation in the nuclear industry through assimulation of the philosophy rather than by imitation.

Until 1974 the regulation of health and safety was the concern of the Department responsible for the industry, for example the relevant safety legislation for mines and quarries and nuclear installations was administered by the Department of Energy. A large number of specialist inspectorates had been created for the purpose and there was some overlapping of responsibilities. In that year, the Health and Safety at Work Act 1974 which aimed at unifying the legislation and regulations and establishing a unitary regime of inspection became law. Despite that, the aim has been far from achieved and, for instance, in the important area of the handling, keeping, custody and disposal of radioactive substances there is separate administration by the Department of the Environment with an independent Radiochemical Inspectorate, an arrangement that has already given rise to conflicts of interest and in the identification of responsibility. Furthermore, regulation of health and safety on off-shore petroleum production installations is executed by an inspectorate in the Department of Energy.

The lesson to be drawn the experience of government intervention in matter of health and safety is that it is ineffectual unless backed by inspection and by an inspection that is not only able to impose legal sanctions for breaches of codified regulations, but must be able to use discretion in enforcement and must also be able to prescribe conditions adapted to the circumstances of the hazard. Powers of this kind have been given to H.M. Factory Inspectors by the Health and Safety at Work Act 1974 and to H.M. Nuclear Installations Inspectors in the system of control by licence conditions instituted by the Nuclear Installations Acts of 1959 and 1965.

APPENDIX II

SELECTED LOW PROBABILITY EVENTS

(A review of some representative low probability events - LPEs - of disastrous outcome for the artefacts, people and systems involved)

PREAMBLE

The incidents discussed here have been chosen from a wide range of totally unexpected low probability events that ended in catastrophic failure of the system involved, all of which were confidently thought to be adequately safe. An attempt has been made to classify them using a pattern suggested by Sir Henry Chilver (1977) which he described as a 'Triangle of Failures'. Sir Henry's concept which is shown in Figure 14 relates to failures in engineering structures whereas the approach adopted here and shown in Figure 15 is concerned with failures in a wider range of artefacts and systems, though also seeking to identify common patterns of causation.

Neither approach is quantitative, but rather ideographic, the aim in both cases being to offer a way of presenting such untoward happenings in a manner that could lead to a better understanding of the engineering deficiencies that played a part in their causation.

In the pattern shown in Figure 15 the events are arranged in a field of causation enclosed by an equilateral triangle, the vertices representing 'Ignorance of Mechanism' as defined in Sections 8.3.1(i) and 8.4.1 of the main text; 'Culpable Human Error' which is not an inadvertent mistake or omission, but a blameworthy act or dereliction; and 'Chance', being some wholly undesigned or unexpected occurrence or circumstance and includes inadvertent human error. The position of the event in this causal field depicts the relative contribution made by each of the factors in its causation, the importance of the contribution being indicated by the proximity of the point representing the event to the relevant vertex.

Thus, the points representing the selected incidents have been disposed on a qualitative criterion according to a notional assessment of the weight to be attached to each of the three above factors in the causation of the given incident. The selected events have been assessed according to a 9 point scale and are listed in the table that follows.

No doubt the placements of the points representing the events could have been made by a mathematical decision rule, giving a better measure of the effect of the factors, but the theory has not been pursued beyond Chilver's descriptive attempt. And, this is adequate for the purposes of the present study.

A brief description of the circumstances of each incident follows, though rather more attention has been paid to some than to others when the event has been thought to be particularly relevant to the theme of the research.

A SELECTION OF TYPICAL LPEs RESULTING IN CATASTROPHIC FAILURES

EVENT (Described in terms of date of occurrence, nature, causal factors and consequences)	CAUSATION (Ignorance of Mechanism, Culpability and Chance scored on a 9 point aggregate scale)

1. ABERFAN (21 October 1966) Liability 1 7 2

A large coal mine spoil tip overlooking a small Welsh village turned into an avalanche of slurry. It had been built on ground containing springs and had been allowed to grow in size without proper engineering consideration. Local warnings about its danger made to Coal Board officials had been ignored. The forces created by the slip burst a water main and created the slurry. A school and several nearby houses were engulfed and destroyed. 116 children and 28 adults were killed and 40 houses demolished.

2. ABBEYSTEAD (23 May 1984) Liability 1 0 8

A violent explosion occurred in the underground control room of a remote show place river flood control pumping system valve room during an official visit. A heavy roof of concrete slabs was blown off. Methane gas from an unknown source appears to have filled the control room and ignited when the explosive concentration was reached, ignition being caused by a casual spark. 9 people were killed instantly and another 6 died later of burns.

3. ANDREA DORIA (25 July 1956) Liability 6 1 2

The Andrea Doria, a large, up-to-date and prestigious Italian passenger liner, fitted with every navigational aid and safety feature, was rammed amidships by the Stockholm, a similar Norwegian vessel. The Andrea Doria's stabilising system failed and the vessel listed heavily, finally capsizing. The collision was 'radar assisted' owing to lack of understanding of certain ambiguities in the PPI presentation. Out of a complement of 1709, 59 lives were lost and the ship a total loss.

4. BROWNS FERRY (22 March 1975) Liability 2 1 6

A fire in the control and safety cable marshalling vault of the Browns Ferry nuclear power station could not be brought under control by normal methods of handling electrical equipment fires. The station was operating at full power, but control was progressively lost. The fire was started by a technician who, in disobedience of instructions,had been using a candle to check the air tightness of the vault sealing. He set the plastic sheathed cables alight. The fire was eventually brought under control by water sprays, but extensive damage was done to the plant in an incident that could have led to a major nuclear accident.

5. DUDGEONS WHARF (17 July 1969) Liability 3 4 2

The accident, an explosion of hydrocarbon vapour in a disused oil storage tank undergoing demolition, is described in Section 3.1. Six members of the London Fire Brigade on site to ensure compliance with the regulations were killed. The site was also under the surveillance of H.M. Factory Inspectorate as a potential danger.

The Dudgeons Wharf incident is cited in the Report of the Committee on Safety and Health at Work (Robens 1972) as an example of the confusions that can arise owing to overlapping regulatory responsibilities. The Home Office conducted an inquiry into the incident (Cmnd 4470/1970).

6. FAVERSHAM (14 July 1847) Liability 8 1 0

The incident, an explosion that demolished a plant engaged in the manufacture of gun cotton, is described in Section 3.1. It resulted in the death of 21 people.

7. FLIXBOROUGH (1 June 1974) Liability 2 6 1

A petrochemical plant explosion caused by ignition of a large cloud of cyclohexane vapour discharged on to the site from a breach in a modification to the process flow. A by-pass that had been installed by a foreman without adequate engineering supervision failed in service. The energy release of between 14 and 45 tons of TNT wrecked the plant, killing 28 workers and injuring 36 others. Widespread damage was done in the nearby town with some 53 casualties, though most were not serious. The post of mechanical engineer was vacant on the plant management board. The event has been extensively discussed and there is a Department of Employment report (Roger J. Parker 1975).

8. HIXON LEVEL CROSSING (6 January 1968) Liability 0 1 8

A collision between an express passenger train and a 120 ton electrical transformer inadvertently placed in front of it by a slowly moving road haulage rig. 11 people were killed and 45 injured. The accident is described in Section 3.3.

9. MINAMATA (April 1956 - May 1973) Liability 2 6 1

The incident is a story of poisoning of a city by an industrial effluent at first thought to be harmless. The progressive Japanese Chisso Corporation was established in the town of Minamata in 1907. In 1932, Chisso began to produce acetaldehyde, an industrial chemical used in the production of plastics. Production boomed in the post-war years, but in 1950 dead fish started to float in Minamata Bay, but this was not attributed to the new processes. In 1956, a new disease was treated in Minamata hospital and was so named. Cases became increasingly numerous with florid neurological symptoms and deformities in children. Research suggested a heavy metal, but mercury was not suspected. Attention turned to manganese, selenium and thalium detected in autopsied patients. Chisso used metallic mercury and had provision for removing it from the effluent. By chance a British paper of 1940 gave a link with methyl mercury, a far more potent poison than the metal itself. Methyl mercury was found in the Chisso effluent and the poisoning shown to be due to organic mercury entering the food chain through fish. Though the cause was proved to be due to acetaldehyde manufacture in 1962, Chisso refused to stop production until compelled to do so by the Japanese authorities in 1972. By that time some 10,000 people had be adversely affected, 103 were dead and 700 seriously damaged and the firm had to pay out billions of Yen in compensation. The story is told in detail in 'Minamata', a illustrated report by W. Eugene Smith and Aileen M. Smith (Holt, Reinhart and Winston, New York, 1975).

10. MOUNT EREBUS (28 November 1979) Liability 0 8 1

An Air New Zealand DC-10 crashed into the side of the Antarctic volcano, Mount Erebus, during a sight-seeing flight. All 257 persons aboard were killed. The accident involving a reliable and well maintained aeroplane was piloted by an experienced crew assisted by adequate navigational aids. At the time the accident was attributed to a pilot's error, but a Royal Commission of inquiry under Mr Justice Mahon found that the flight path program in the DC-10 computer had been modified without the knowledge of the pilots who were thus taken over an unfamiliar route during the most hazardous part of the flight by the automatic control. Blinded by Polar light, the pilot had no time to correct his course before crashing into the mountain. The Air New Zealand executive have denied responsibility and have been supported by the New Zealand Goverrment. Mr Justice Mahon has been forced to resign his post.

11. OPPAU (21 September 1921) Liability 8 x 1

The violent explosion of some 200 tons of ammonium sulphate at works of Badische AnilinFabrik at Oppau near Mannheim on the Rhine demolished the plant and destroyed the village. Between 1,000 and 1,500 were killed and nearly 2,000 injured. The cause of the explosion has never been properly explained. Explosive properties are not normally associated with ammonium sulphate and the plant management had a reputation for safety. A French Army detachment was on duty to see that there was no production of explosives, banned under the Armistice agreement of 1918. It is not impossible that illegal nitrates were being produced for the German Army. An incident in such a clandestine process could have triggered a bigger explosion. (New York Times, Sept. 22, 1921, p. 1)

12. RONAN POINT (16 May 1968) Liability 4 1 3

Ronan Point was a high-rise tower block of residential flats built to the Neilsen-Larsen system which had become well established elsewhere in Europe. The plans for the 22 storey block had been subjected to a scrupulously thorough safety assessment and met the statutory building regulations. The design may be likened to a 'House of Cards', but of massive interlocking, reinforced concrete slabs. Flat 90 on the 18th floor was occupied by a single lady of middle age. She opted for a gas cooker, but there was a defective brass union nut in the flexible pipe to the wall gas outlet. No smell of gas was reported during the relevant night, but when she awoke early the next morning and attempted to light the gas to boil a kettle, there was an explosion. The slabs forming the outer walls of the flat were blown out. Support was removed from the floor of the flat above, causing a pattern of collapse that continued upward to the top. The unsupported floors crashed down on the floor of Flat 90. It collapsed, a disastrous progress that continued downwards. 4 people were killed and 17 injured, remarkably few in the circumstances. (Vide V. Bignell, G. Peters and C. Pymm 1977.)

13. TAY BRIDGE (28 December 1879) Liability 1 7 1

At the time of its construction, the railway bridge over the Firth of Tay was a vaunted triumph of British civil engineering. Sir Thomas Bouch, an eminent engineer, was in charge of the project which was completed and went into service on 31 May 1878, after tests and inspections. All went well until Sunday, 28 December, 1879 when a central span collapsed in a high gale under the load of a train said to be going too fast. 75 lives were lost among whom were many children. There was a great scandal. An official inquiry, chaired by Mr Justice Rothery (1880), found that

the design was inadequate, materials of less than the specified strength had been used, necessary test and experimental results had not been analysed, there had been no proper stress analysis and no competent expert had been consulted about wind loadings. The inquiry found that Bouch had been seriously remiss in his duties.

14. TITANIC (14 April 1912) N.B. Treated as two accidents *

Event 'A' - Collision with iceberg Liability 1 1 7

The White Star liner, Titanic, was one of the most remarkable ships for size, luxury, speed and safety ever built. She was of watertight construction with a double bottom and 16 watertight compartments. She could withstand a head-on or amidships collision and was considered 'unsinkable', anything worse than one at the conjuncture of two compartment being 'incredible'. She was on her maiden voyage to New York and some 1250 miles East of her destination. The Captain was aware of the iceberg danger and had ordered a special watch. However, a wireless message from another company vessel advising that she was hove to owing to ice failed to reach him. The huge ship brushed a giant iceberg before the proper avoiding action could be taken by the bridge and contact below the waterline holed six compartments. She could float with four compartments holed, but not six. It took her two and a half hours to founder.

Event 'B' - Loss of life Liability 1 7 1

The Titanic foundered in a sea that was almost dead calm, though icy cold. The lack of waves, wind or swell eased the filling and lowering of lifeboats, but hundreds of lives were unnecessarily lost. There were 2,206 souls aboard in toto of whom 703 were saved and 1,503 perished, of these 156 were women and children. Although the lifeboat capacity was inadequate, there were seats for 1,178. In the event the boats pulled away with several hundred empty seats. The crew behaved with exemplary discipline in the face of certain death, but the management of the emergency was chaotic. They had not been instructed in how to marshal the passengers. The oddest fact was that the Californian was only 10 miles away from the sinking Titanic, saw that she was stopped and firing rockets. Her captain did not ask his wireless operator to make contact and did nothing to help. Had he done so, few lives would have been lost.

15. THALIDOMIDE (1958 - 1962) Liability 5 4 0

The drug Thalidomide was promoted as an effective and innocuous tranquiliser which had survived extensive safety testing. It was being widely prescribed in Europe. Concurrently, a sudden and considerable increase in the number of cases of amelia and other deformities in neonates was reported. Suspicion soon fell on Thalidomide and evidence of its involvement mounted. The manufacturers continued to promote it, ignoring the warnings. Ultimately it was withdrawn, but hundreds of deformed, though otherwise healthy, children were born to face life seriously crippled.

---

* Walter Lord (1976) in 'A night to remember' has written a well-illustrated, graphic, moving and factual account of the loss of the 'Titanic'.

16. THREE MILE ISLAND — Liability 6 1 2

The reports, summaries and analyses of the Three Mile Island (TMI) PWR incident are legion and the conclusions about it diverse. TMI Reactor No. 2 was operating at full power when a feed water pump failed. Pressure rose in the primary circuit. The control room instrument display indicated that the reactor relief valves had properly closed, whereas, in fact, they had remained open. Dry-out in the steam generators ensued. In response to the loss of pressure in the primary circuit, emergency cooling water (ECW) injection began automatically. The operators, now confused about the state of the plant, first shut off one ECW pump and then the other. Deprived of adequate coolant, the core started to over-heat. Not properly understanding what was happening to the plant, the operators took further inappropriate actions which led to melting of the fuel and discharge of a large volume of highly radioactive coolant into the containment, some of which was pumped into the auxiliary building (L. Myrddin Davies 1979).

After some 3 to 4 hours when the operators realised that there had been severe overheating of the fuel and a massive escape of active coolant, the plant was effectively shutdown, though there was great confusion about what had in fact gone wrong and fears for the continuing stability of the core. The confusion extended far beyond the control room and 3 days after the incident, the head of the U.S. Nuclear Regulatory Commission told the Pennsylvania State Governor, 'We are totally blind, your information is ambiguous, mine is non-existent.' (The Guardian, p.4, Sat., April 14, 1979)

As the outcome of TMI, no one has suffered a significant dose of radiation, though there may have been psychological damage to some members of the public, owing the the atmosphere of panic that ensued. On the other hand, the financial loss has been enormous, running into many billions of Dollars. Technological shock-waves from the event have gone around the World, causing the basis of nuclear safety philosophies and management to be questioned. Two divergent lessons have been drawn that concern this study. One is that the operating staff should be selected for engineering ability and aptitude for the work, being thoroughly trained both technically and practically. The other is that the reactor should come under fully automatic control for the first 30 minutes of an incident, during which time the operators should be prevented from interfering while expert assistance is being obtained. The writer holds to the former view.

17. WELDER'S RADIATION BURNS — Liability 0 7 2

In the morning of May 3rd, 1967, a welder working on an Argentinian petroleum distillery site picked up a bright metal 'bolt' and put it in his right overall pocket. Next day he transferred it to the left. That evening he felt 'rheumatic pains in his thigh'. On the 5th, they had become so severe that he was taken into hospital. As severe erythema was observed, he was treated for chemical burns of an unknown nature. He did not respond to treatment. On May 27th, loss of a 13 Curie, Cs-137 radiography source was reported. It was found in his overalls, and radiation burns were diagnosed. His condition continued to deteriorate over the next six months. In November, his left leg had to be amputated and by March 1969 both legs had been amputated at the hip (Benison et al. 1969). It was subsequently reported that he died of cancer in 1971.

WEIGHTINGS OF THE CAUSAL FACTORS COLLATED

	Event	Ignorance of Mechanism	Culpability	Chance
1	Aberfan	1	7	2
2	Abbeystead	1	0	8
3	Andrea Doria	6	1	2
4	Browns Ferry	2	1	6
5	Dudgeons Wharf	3	4	2
6	Faversham	8	1	0
7	Flixborough	2	6	1
8	Hixon Level Crossing	0	1	8
9	Minamata	2	6	1
10	Mount Erebus	0	8	1
11	Oppau	8	x	1
12	Ronan Point	4	1	3
13	Tay Bridge	1	7	1
14	Titanic 'A'	1	1	7
	Titanic 'B'	1	7	1
15	Thalidomide	5	4	0
16	Three Mile Island	6	1	2
17	Welder's radiation burns	0	7	2
	Weighting totals	51	63	48
	Percentages	31%	39%	30%

ANALYSIS

The percentages calculated from the aggregates of the weightings of three causal factors tabulated above for the 18 selected events provide some experimental support for the conclusions in the study about the treatment of catastrophic low probability events (LPEs). Suggestions of bias because the weightings as quoted rest on the writer's judgement may be set aside in view of the obvious nature of the weights given in each case. While it would have been better to have obtained the percentages from questionnaire data, there has been neither time nor opportunity to do so, nor has it been necessary for the present purpose. For example, the tragedy of Aberfan was unequivocally the fault of officials blind to the danger presented by the tip. The radar assisted collision between the Andrea Doria and the Stockholm was clearly due to Ignorance

of Mechanism, while the incompetence of Bouch's civil engineering led to the Tay Bridge disaster. The personal bias of an assessor might make a point or two difference one way or the other from case to case, but such differences would be expected to balance out as between individuals. Anyway, a trend rather than a precise result is adequate for the purpose.

The analysis shows no great difference in the generality of causation among the three factors, though Culpability, ie. negligence, failure to follow instructions, etc., at 39% presents as the one of major weight. This underlines the importance to be attached to inspection of the appropriate kind. Ignorance of Mechanism and Chance tie in second place. The first emphasises the role of engineering competence and, it is now generally agreed in the industry, that, had the operators in the Control Room at TMI been better informed, the incident could have been averted. Chance is generally a contributory element, but by no means a major factor, though in exceptional cases being the principal cause, indeed of the LPE by definition for the regime of defended safety that is maintained in nuclear power plants, eg. at Browns Ferry. Chance determined the Titanic's encounter with the iceberg and the extraordinary event at the Hixon Level Crossing.

To sum up, better engineering and effective regimes of inspection can greatly reduce the probability of a catastrophic LPE, but can never give absolute protection against a potential hazard. It is a fact that must be taken into account in siting policy and before a risk held to be intolerable is imposed on workers, public or environment.

NOTE

Where explicit references to publications, reports, etc. dealing with the above events have not been provided, recourse should be made to the press, in particular the London or New York 'Times' or 'Lloyds Register of Shipping' for which journals comprehensive indexes are published annually.

FAILURE AND ITS CONSEQUENCES

The two ideographic event triangles of Figures 14 and 15 when taken together suggest a figure of 6 apices in hyper-dimensional conceptual space in which most technological events ending in catastrophic failure may be positioned. Broadly, two contiguous volumes representing the principal aspects of engineering can be envisaged; one, a physical domain of 'Chilver-space', and, the other, a domain of 'Managerial-space', illustrated by Figures 14 and 15 respectively. A given failure mode then becomes articulated when the point representing the doomed system arrives at the place in the hyper-volume where all the factors necessary to precipitate the catastrophe are appropriately linked. Usually, one of them is dominant as indicated by the bias in the positioning of the points in the two figures.

It is the proper task of engineering in its roles of design, construction and operation of plant to steer these complex artefacts away from zones of danger as suggested in the application of Event-noise/Catastrophe theory described in the text and depicted in Figure 12. Owing to the inability of an integrated system to be self-checking, an inference from Goedel's theory, the external intervention of engineering inspection is necessary to discern and deflect or stop an incipient fault process from running to catastrophic failure as suggested in Figure 13. Failure to achieve these ends when combined with the caprice of chance opens the door to catastrophe. The horrific consequences that can be the result are displayed in Figures 16 to 21.

Tay Bridge - Event 13 - Figure 16

The collapse of the bridge was a classic failure due to inadequate design (Structural Deficiencies) under the exceptional stress of a Chance confluence of Unknown Environmental Forces. The designer, civil engineer Bourch was guilty of grossly Culpable Human Error, ie. Culpability, that obscured monumentally pathetic Ignorance of Mechanism.

Ronan Point - Event 12 - Figure 17

As is often the case, chance circumstances; namely, occupancy, the fact that all the tenants were in bed, except for the early morning old lady who struck the match, and the relatively fortunate location of the explosion in Flat 90 on the 17th Floor of a 22 storey tower block, minimised the consequences of the accident. As can be seen from Figure 12, had the event occurred in the middle of the structure, the whole front face of the affected side of the building would have fallen out or been crushed with appalling loss of life. The incident was the result of Ignorance of Mechanism in the process of design and malevolent Chance of the combination of an elderly woman who must have had an easily saturated sense of smell with a defective gas pipe union joint, the latter permitting a massive leak into the ill-ventilated flat of which she was the sole occupant.

Hixon Level Crossing - Event 8 - Figure 18

This incredible happening involving the placement of a massive block of metal (120 tons) directly across the immediate path of an express passenger train only seconds before the impact was an odd freak of Chance. Nonetheless, Ignorance of Mechanism and Culpability also played a significant part. Experience of the type of unmanned crossing was limited in British conditions of road traffic behaviour. The administrator who sanctioned its introduction was Culpable of a common human error in that he did not appreciate his lack of understanding of the subtleties of technology, road traffic engineering in the case. An executive system that requires that technical decisions are made by 'pure administrators' on the advice of technologists was at fault, although the element of Chance predominated. Despite that, it was an accident waiting to happen.

Argentine Welder - Event 17 - Figures 19 to 21

This poor man was the victim of a gross Culpable Human Error in which Chance again was an important factor. Also guilty with the radiographer who 'lost' the 13 curie iridium source were the managements of the petroleum refinery and its radiological protection organisation, if there were one, and the local and national regulatory officials. It was their duty to ensure that all persons on such a site were properly instructed in the nature and dangers of radiography and to enforce effectively the custodial regulations. Clearly, this was not the case. The three figures show the course of the accident, Figure 19 in which its tragic history is epitomised, Figure 20 which shows the overdose profiles and Figure 21, a photograph of his somatic injuries at a late stage in the course of his radiation illness.

CONCLUDING REMARKS

The ideographic representation of the factors that can precipitate a catastrophic failure given by conceptual combination of the models of Figures 14 and 15 provides a global and comprehensive way of describing the complex processes that lead to these low probability events. Despite having no direct conventional quantitative utility, indeed it explains the intractability of Identity (viii) and its summation in Equation (xi), the compound model has positive value in its ability to reveal those risk features most prone to failure in the system it represents. In comparison, the quantitative approach of which the U.S. Reactor Safety Study is an exemplar tends to direct attention obsessively towards design, something manifest in the current debates on the safety of nuclear power. Moreover, the model shows that attempts to quantify overall plant failure sequences, as in the case of nuclear power, are illusory owing to the impossibility of constructing a stable data base. It is precluded by the complex and inconstant nature of the linkages that transiently connect the diverse factors which articulate a major failure sequence.

APPENDIX III

ON ENGINEERING

An activity that makes industrial technology possible and the enigma of the persisting lowly status of the Engineer

The two letters to the press appended hereto were inspired by Auguste Comte's (1825) vision of the role of the engineer, emergent as a scienist of a new kind to be the link between the scientist-savant and the commercial exploiters of scientific discoveries, namely the entrepreneurial class of industrialists and investors. Thus, engineering is not science as such, but the art of understanding science so that it may be used in the interests of society. In performance of this office, it has become one of the main pillars of contemporary technological civilisation as illustrated in Figure 1.

Attention is drawn to the odd editorial deletion from the letter to the 'Financial Times' which was written in response to public concern at the dearth of engineers in Britain. The passage deleted read:

> 'While good engineers are in short supply, able administrators, accountants, entertainers, politicians and writers abound. But, in spite of their commendable contributions to the public weal, there has been a continuing downward drift in national prosperity and prestige. May not this be linked to the reluctance of the talented young to choose engineering as a profession or vocation? The hard fact is that a career in engineering today does not offer rewards commensurate with the ability demanded of those who might aspire to enter it.'

This failure to recognise the central role that engineering must now play was also exposed in a 'Guardian' editorial of June 1, 1977 to which the second letter attempted to give answer. The 'Guardian' had failed to attach due importance to Alan D. Blumlein's outstanding achievements as an electronic engineer. It was his technical genius that made that indispensible contribution to TV and, later, radar which gave our Forces an extended vision that could penetrate darkness, fog or storm and which could peer around the curvature of the earth. Without impugning the gallantry of the fighting men, it is to the effectively then unchallenged lead in radar that can be attributed the defeat of the German air offensive against Britain in 1940, the destruction of the formidible Italian fleet of Cape Matapan, the shattering of the Japanese naval arm in the battle of the Midway Islands and the success in countering the U-boat threat to Atlantic shipping. In all these actions the enemy was either tactically blind or had comparatively limited vision in dealing with the attacking force.

Throughout history, the essential contribution of the engineer has either been ignored or his calling denigrated. To quote the famous Greek general and statesman, Xenophon (ca 444 - 354 BC):

> 'What are called the mechanical arts carry a social stigma and are rightly dishonoured in our cities. ... Their practice causes a physical degeneration that results in a deterioration of the soul. ... Those who engage in them have not got the time to perform the offices of friendship and citizenship. Consequently, they are looked upon as bad friends and and bad patriots.'

Despite the fact that engineering is held in far greater esteem today, having risen from a sub-culture of slave and lowly 'mechanical' to become in itself a major discipline of head and hand with its managerial stratum recognised as a learned profession, it still is of inferior standing in the body politic.

The present circumstances of the engineer at the professional level have been described by Eric (Lord) Ashby (1966), thus:

> 'Technology is of the earth ... susceptible to pressure from industry and government ... under obligation to deliver the goods ... ... And so the crude engineers, the mere technologists, are tolerated in the universities because the State and industry are willing to finance them. Tolerated, but not assimilated, for the traditional don is not yet willing to admit that technologists may have anything intrinsic to contribute to academic life.'
>
> Technology and the Academics, MacMillan, London, 1966, p. 66.

Though apparently irrational, this inveterate attitude has its rationale.

As the Western state has become ever more dependent on technology, so has the part played by the engineer become increasingly important and central to the public weal in national economic performance, defence and geo-political prestige. Then, to accord the engineer his due and proper recognition would bring about major structural changes in the traditional social pyramid, in particular near its top. There can be only so many chiefs, and for those who would go up, some would have to come down. For instance, there is no engineer in the top echelon of the Civil Service, ie. at Permanent Secretary level and, but few, in the highest managerial brackets of industry. Moreover, as Thorstein Veblen (1921) claimed the engineers, as a conscious social group aware of their proper status and power, could exert a tranquil, but nonetheless potent, industrial pressure that could bend any democratic government to their rational desires.

Well-known examples of influential professional associations are those of the doctors in Britain and the U.S.A. The source of the prestige and influence they have in society lies in their existence as cohesive groups, cognisant of the interests of the profession and ready on occasion to speak out in order to secure them. One might then suspect that that among certain incumbent sections of the Establishment and upper executive classes there is cognition, though perhaps subliminal, of an incipient threat and of a natural reaction to it. Accordingly, the engineer must be kept on tap and any move to the top frustrated. This might explain the unusual politics associated with the creation of the Engineering Council that has brought about the demise of the Council of Engineering Institutions which had a governing board on which half the members were elected by an enthusiastically supported franchise. On the other hand, the Engineering Council is managed by a Director-General and an executive of Ministerial appointees on which the engineers have no direct voice.

TWO LETTERS TO THE PRESS

On the major contribution engineering has made to the United Kingdom's prosperity - a waning asset

'Financial Times'
3 April 1976

Engineering

From Mr. O. Critchley.

Sir,—A century of progressively enhanced educational opportunities in Britain has coincided with falling status for engineering, both as trade and profession; perhaps because of its dependence on manual skills, though many of our great engineers began as craftsmen. The professionalism of our engineers is not in question; indeed, their past achievements have been unexcelled. More successes like those of Watt, Bramah, Brunel, Whitworth, Crompton and Hinton are needed. Are they so depressingly rare nowadays because so few people of such high calibre enter the vocation and those with the potential often lack opportunities or leave, an exodus abetted by Fultonism?

What is to be done? Professional engineers need a better image, as that of backroom designer, struggling inventor, tough site manager or second-string functionary, worthy and most necessary roles, is too limited an ultimate prospect. Neither higher salaries alone nor altered titles are likely to give it, nor can it be won by empty publicity, elitism, byzantine manoeuvres in learned institutions or by industrial union pressures. Bearing on the schools to guide some of their more outstanding pupils into engineering will not be of much avail as the policy cannot work upwards to be self-reinforcing, time being too short for something which would take generations to realise.

The way of engineering when seen from the desk of the gifted and ambitious child must be as likely as any other discipline to bring fame. Evidence of this could be given by appointing able and deserving engineers still in the course of their profession to those top administrative posts to which their specialities are broadly relevant. Here the Civil Service could help by setting a pattern, but only one or two practising engineers have reached as high as Deputy Secretary so far. A change of style, widely publicised, would show that not only has the need to accord higher status to engineering been acknowledged but that something is being done about it. Nothing less is likely to have the required impact on country and schools.

Octavius H. Critchley,
Department of Liberal Studies in Science,
The University,
Manchester.

---

* Editorial deletion of passage here. See remarks in the text of Appendix

'The Guardian'
7 June 1977

Bias against the rude mechanical

Sir,—Your interesting article on the remarkable achievements of Alan Dower Blumlein (June 1) needs correction.

Yes, Blumlein was indeed a scientist, but more than that he was an engineer. Unfortunately, the profession still carries the ancient stigma attaching to the useful arts and, particularly, the mechanical ones. Old Seneca drew attention to this when noting that in his time there had been the development of central heating, transparent glass windows and shorthand, but in his view "the invention of such things is drudgery for the lowest slaves."

Engineering is not science, but an art which includes science. It is an organising function of the highest order which aims at meeting the needs of society by applying the findings of science. It covers a range of talent from highly skilled craftsmen to managerial engineers, whose achievements in their day have been the wonders of the world and have left a lasting mark upon it. Among them are names which are now household words, such as Stevenson, Brunel, Edison and Whittle.

It is almost as if there is a conspiracy to maintain the ancient curse and the very word "engineer" seems to conjure up some irrational, unpleasant image. In spite of publicity to the contrary it was engineers and supporting technicians who developed radar, television and computers and put a man on the moon and, more recently, sent the Viking probes to Mars and beyond. One must give due recognition to the building blocks provided by the scientists, but the achievements are those of engineering. Blumlein should therefore be acclaimed as a great engineer and not miscast as a scientist.

This country is desperately in need of more Blumleins, Whittles and their kind to enrich and enlighten our industrial potential and so make Britain once again pre-eminent. To this end, more scientists should metamorphose into engineers, entering industry to lead, inspire and create as Blumlein did.

O. H. Critchley,
Hounslow, Middlesex.

20 FIGURES

Number	Title	Location in Text Page
1	The Five Interacting Branches of Culture	86
2	Incident Frequencies, Consequences and Public Reaction to Hazard	109
3	Vistas and Horizons of Technical Design Safety Assessment for a Nuclear Power Reactor	113
4	Perceptions of Chance	117
5	Probability of the Worst Consequences of a US Nuclear Power Station Accident	123
6	'a' - A conventional vector representation of the relationship between the driving voltage (V) and the current (i) in an alternating current circuit with a reactive load	127
	'b' - An attempt at a multi-dimensional portrayal of the relationships that involve administration, science, design, management-and-practice and technician and artisan skills through engineering ...	128
7	Prediction and Pattern of Behaviour in Plant and System in the Realm of Very Small Event Probabilities	134
8	Realisation of Engineering Design	135
9	Event-Noise Ideogram: Nuclear Power Plant	183
10	Bathtub Curve	186
11	Event-noise Display	195
12	Cuboid Model	199
13	Design Safety Analysis, Ignorance of Mechanism and Inspection	233
14	A new outlook on LPE causation - The Chilver Failure Triangle	207
15	Causation Triangle for Low Probability Events	208
16	Tay Bridge Collapse of 28 December 1879	-
17	Ronan Point Tower Block Collapse of 16 May 1968	-
18	Hixon Automatic Level Crossing Crash of 6 January 1968	-
19	Welder - Over-exposure, Dismemberment - Death	-
20	Welder - Ionising Radiation Dose Profiles of Exposure of Thighs	-
21	Welder - Radiation Burns - Degenerative Course	-

THE FIVE INTERACTING BRANCHES OF CULTURE:
THE HUMANITIES SCIENCE MEDICAL SCIENCES ENGINEERING COMMERCE
WITH THEIR SATELITE ASPECTS AND SOCIETAL FIELDS

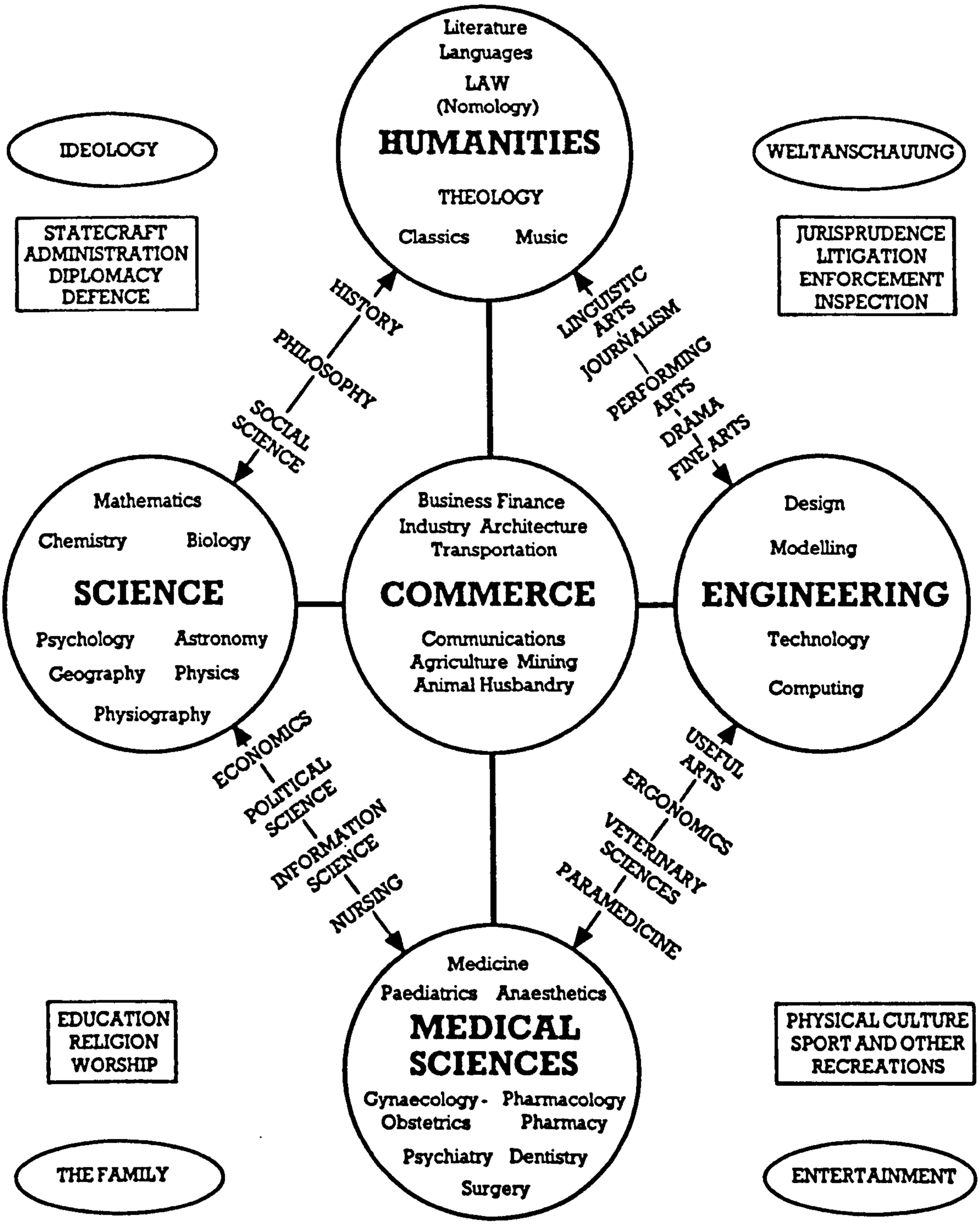


Fig 1

INCIDENT FREQUENCIES, CONSEQUENCES AND PUBLIC REACTION TO HAZARD

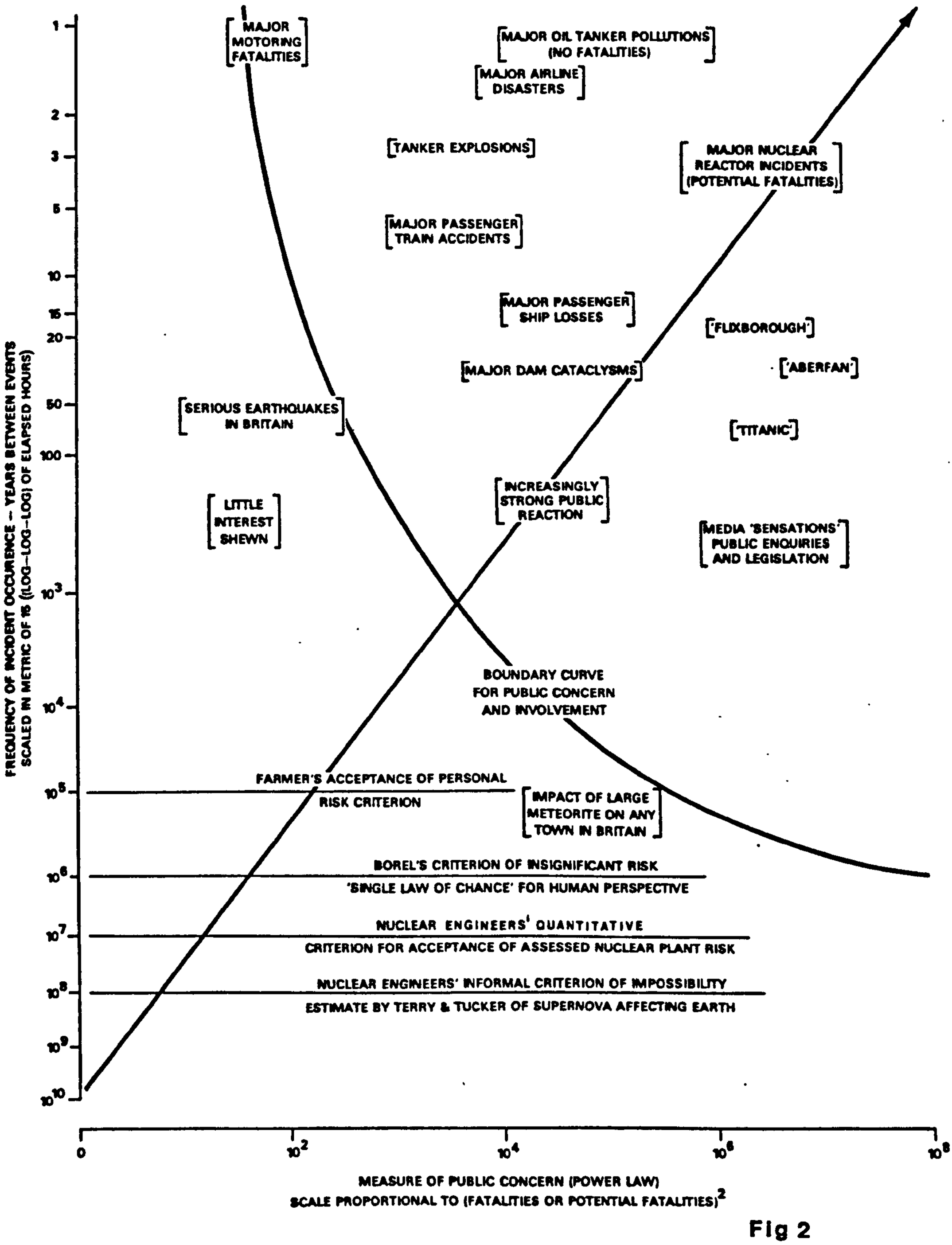


Fig 2

VISTAS AND HORIZONS OF TECHNICAL DESIGN SAFETY ASSESSMENT FOR A NUCLEAR POWER REACTOR: MAGNOX–AGR–PWR

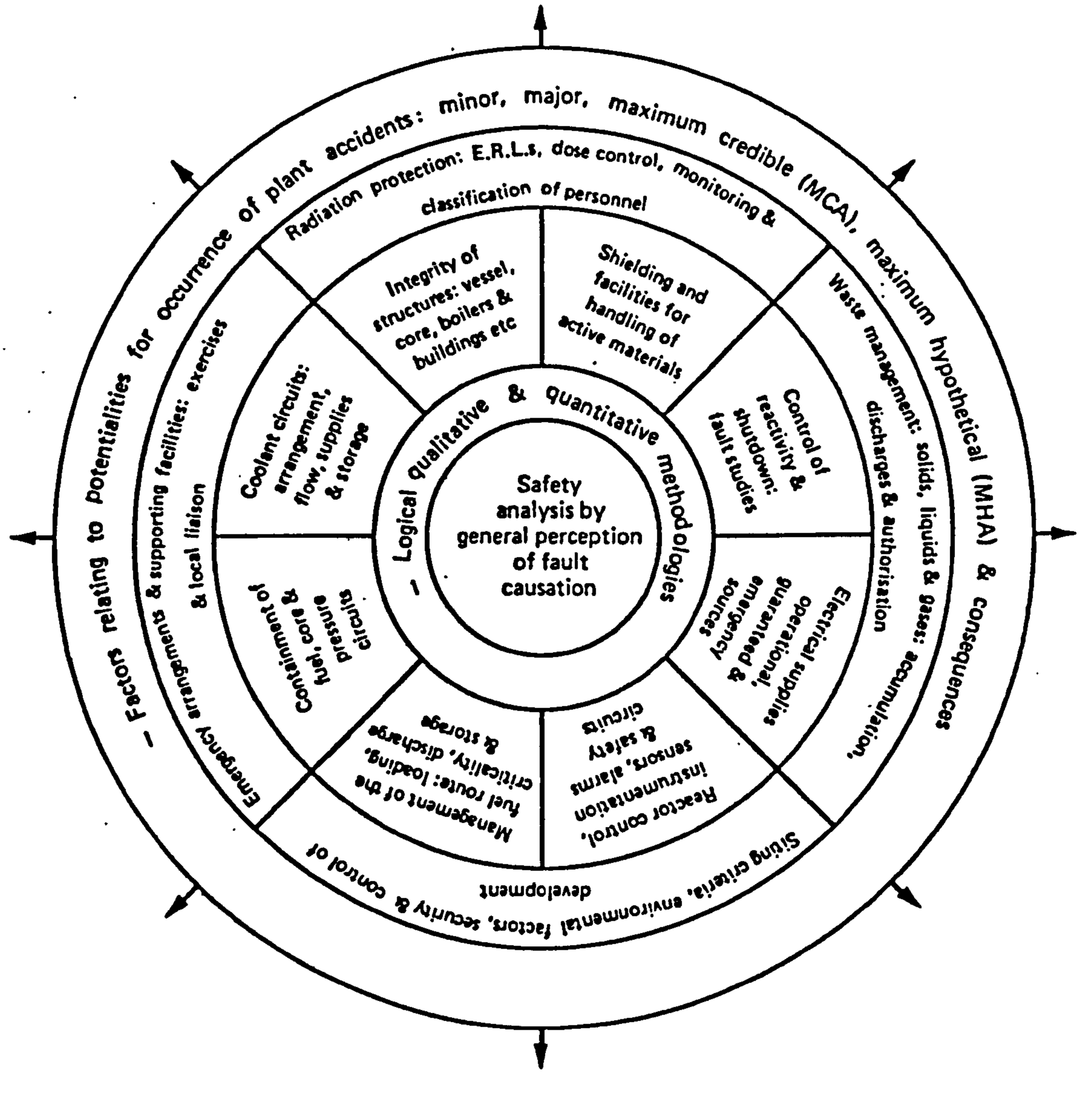
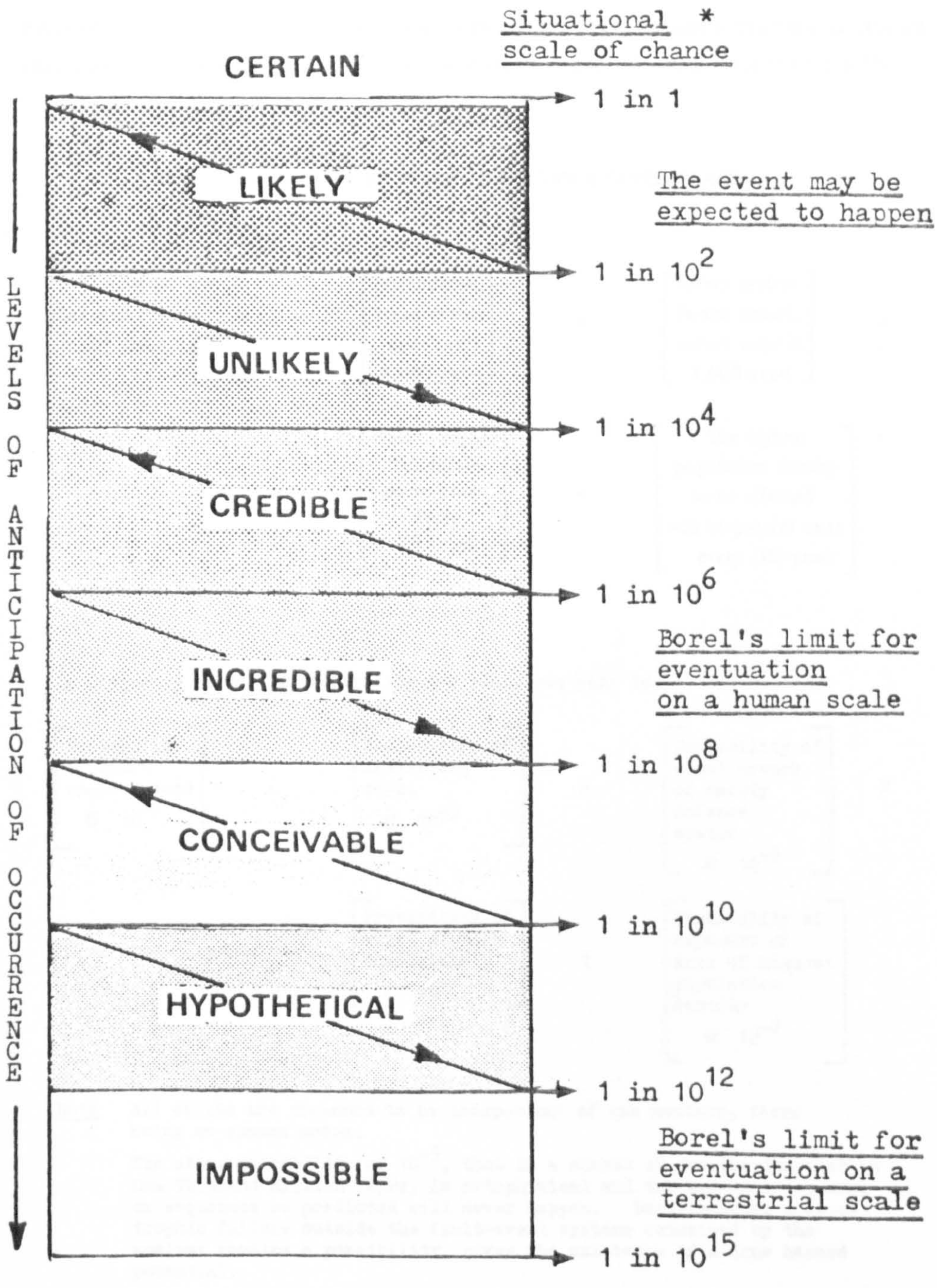


Fig 3

PERCEPTIONS OF CHANCE



Borel's probability limits

Metaphysical probabilities - See Section 9.6.1 and Note 14.

* Situational chance - nuclear

The chance that a specific event will occur during the operational lifetime of a nuclear power plant.

FIG 4

PROBABILITY OF THE WORST CONSEQUENCES OF A US NUCLEAR POWER STATION ACCIDENT

(Rasmussen – Bülletin of the Atomic Scientists 'The Safety Study and its Feedback' Vol 31 1975 p 28)

TIME INTERVAL BETWEEN EVENTS IN A GIVEN PLANT

$$\left[\begin{array}{c}\text{Time span}\\ \text{between events}\\ 10^{9}\text{ years}\end{array}\right] = \left[\begin{array}{c}\text{Precipitating}\\ \text{event occurs}\\ \text{once every}\\ \text{1,000 years}\end{array}\right] \times \left[\begin{array}{c}\text{Safety system}\\ \text{(worst breach)}\\ \text{occurs once in}\\ \text{1,000 years}\end{array}\right] \times$$

$$\left[\begin{array}{c}\text{Worst weather}\\ \text{conditions}\\ \text{occur once}\\ \text{every}\\ \text{10 years}\end{array}\right] \times \left[\begin{array}{c}\text{The highest}\\ \text{population density}\\ \text{to be affected}\\ \text{will be present once}\\ \text{every 100 years}\end{array}\right]$$

In frequency terms the probability per plant per year is:

$$\left[\begin{array}{c}\text{Probability}\\ \text{of worst}\\ \text{consequences}\\ @\ 10^{-9}\end{array}\right] = \left[\begin{array}{c}\text{Probability of}\\ \text{initiating}\\ \text{event}\\ @\ 10^{-3}\end{array}\right] \times \left[\begin{array}{c}\text{Probability of}\\ \text{worst breach}\\ \text{of safety}\\ \text{defence}\\ \text{system}\\ @\ 10^{-3}\end{array}\right] \times$$

$$\left[\begin{array}{c}\text{Probability of}\\ \text{worst weather}\\ \text{conditions}\\ @\ 10^{-1}\end{array}\right] \times \left[\begin{array}{c}\text{Probability of}\\ \text{exposure of}\\ \text{area of highest}\\ \text{population}\\ \text{density}\\ @\ 10^{-2}\end{array}\right]$$

Note All events are presumed to be independent of one another, there being no common modes.

The above probability of 10^{-9}, that is a chance of eventuation once in One Thousand Million Years, is metaphysical and the accident sequence or sequences so predicted will never happen. Nevertheless, a catastrophic failure outside the fault-event systems conceived by the analyst remains a possibility, given the existence of a true hazard potential.

Fig 5

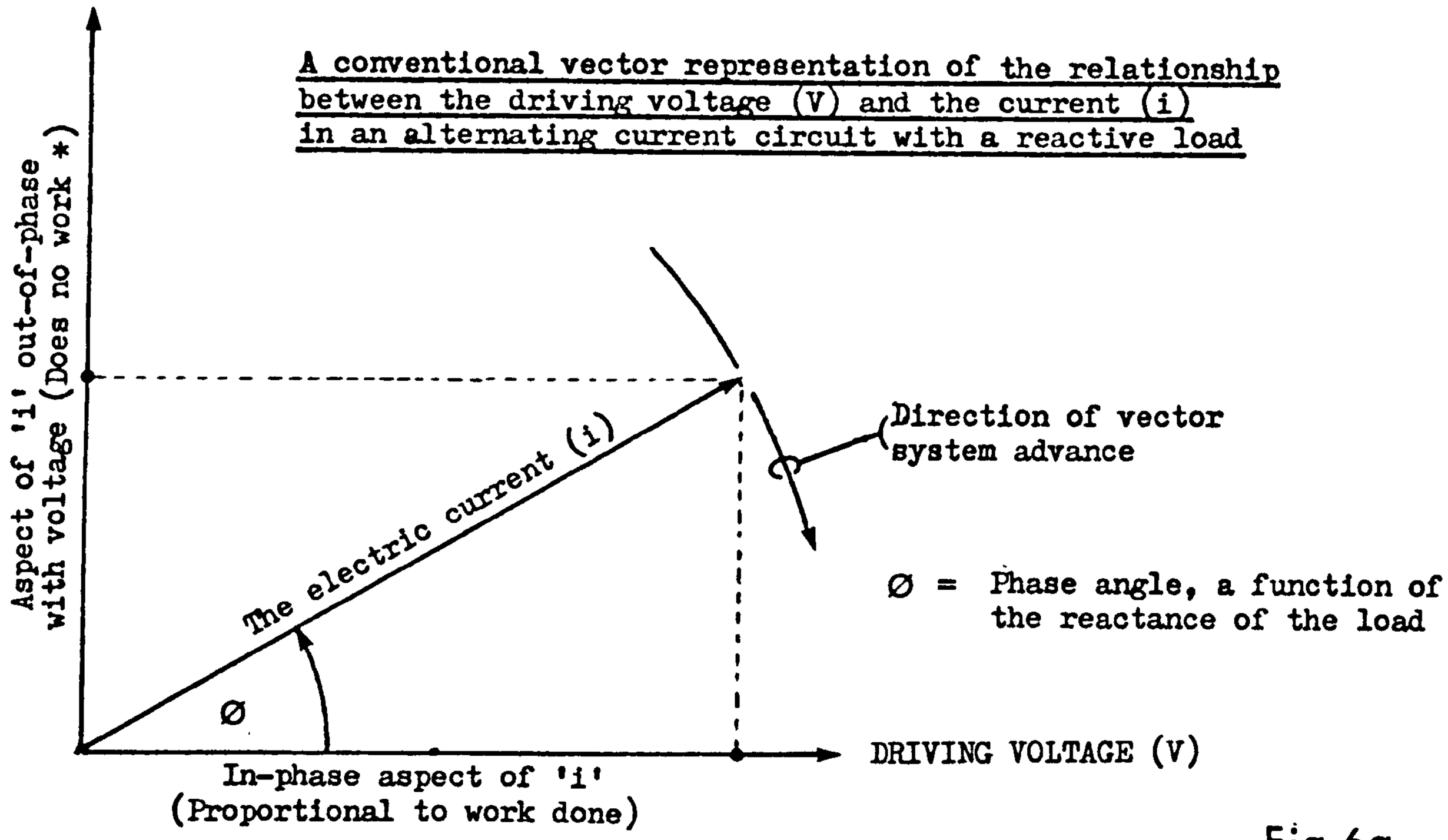
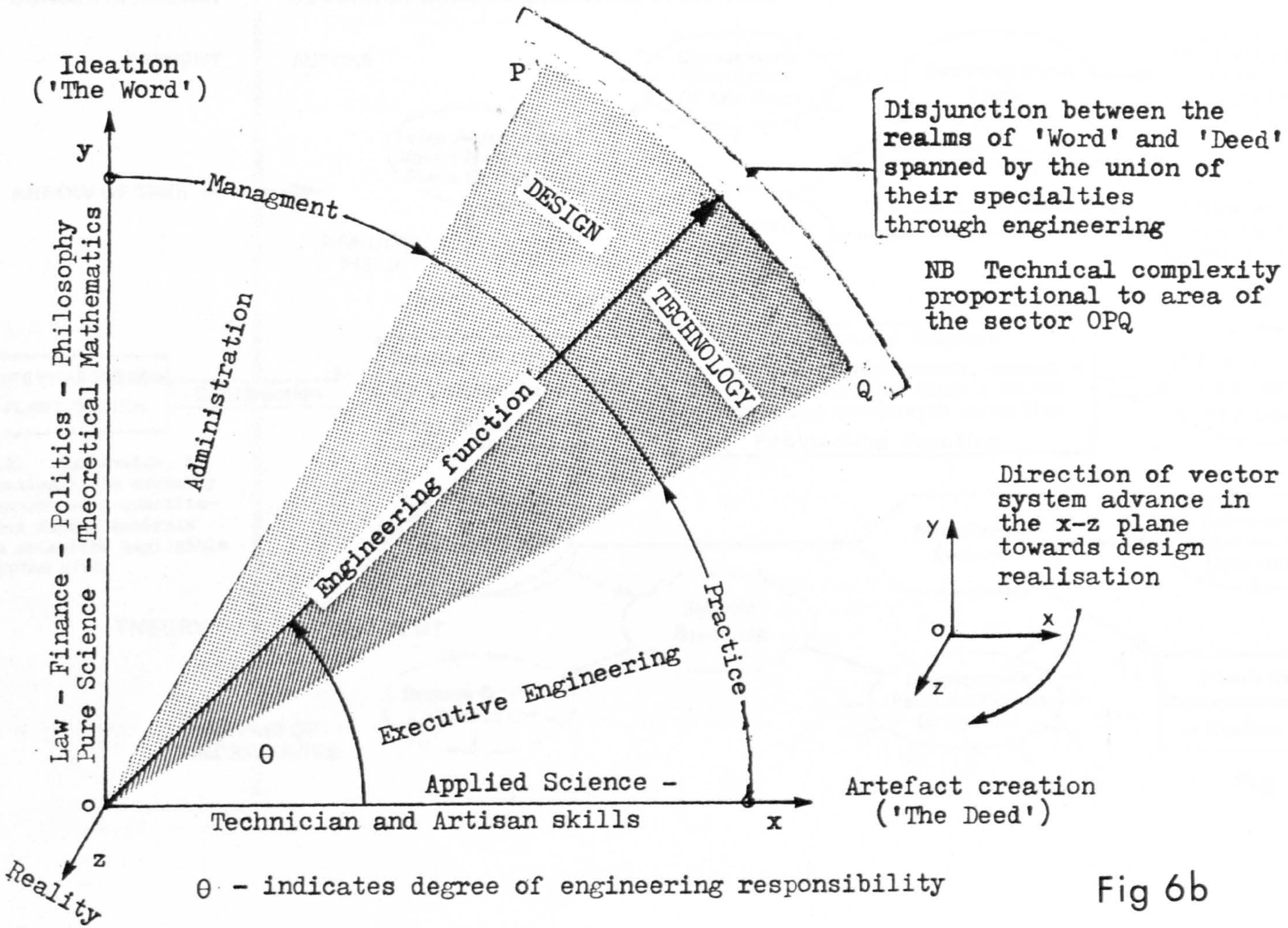


Fig 6a

* - a consequence of a loss-less energy exchange due to the reactance which the load presents to 'V'

The vector representation given above of the flow of an alternating electric current in a circuit containing reactance is an example of an engineering ideogram that enables an abstract technical situation to be presented as a manageable intellectual concept. Such pictograms abound in the language of technology, indeed communication and reasoning in engineering would be very difficult, if not impossible, without them.

An attempt at a multi-dimensional portrayal of the relationships that involve administration, science, design, management-and-practice, and technician and artisan skills through engineering in the creation of a technological artifact



θ - indicates degree of engineering responsibility

Fig 6b

PREDICTION AND PATTERN OF BEHAVIOUR IN PLANT AND SYSTEM IN THE REALM OF VERY SMALL EVENT PROBABILITIES

TWO DIMENSIONAL REPRESENTATION OF AN N DIMENSIONAL EVENT SPACE

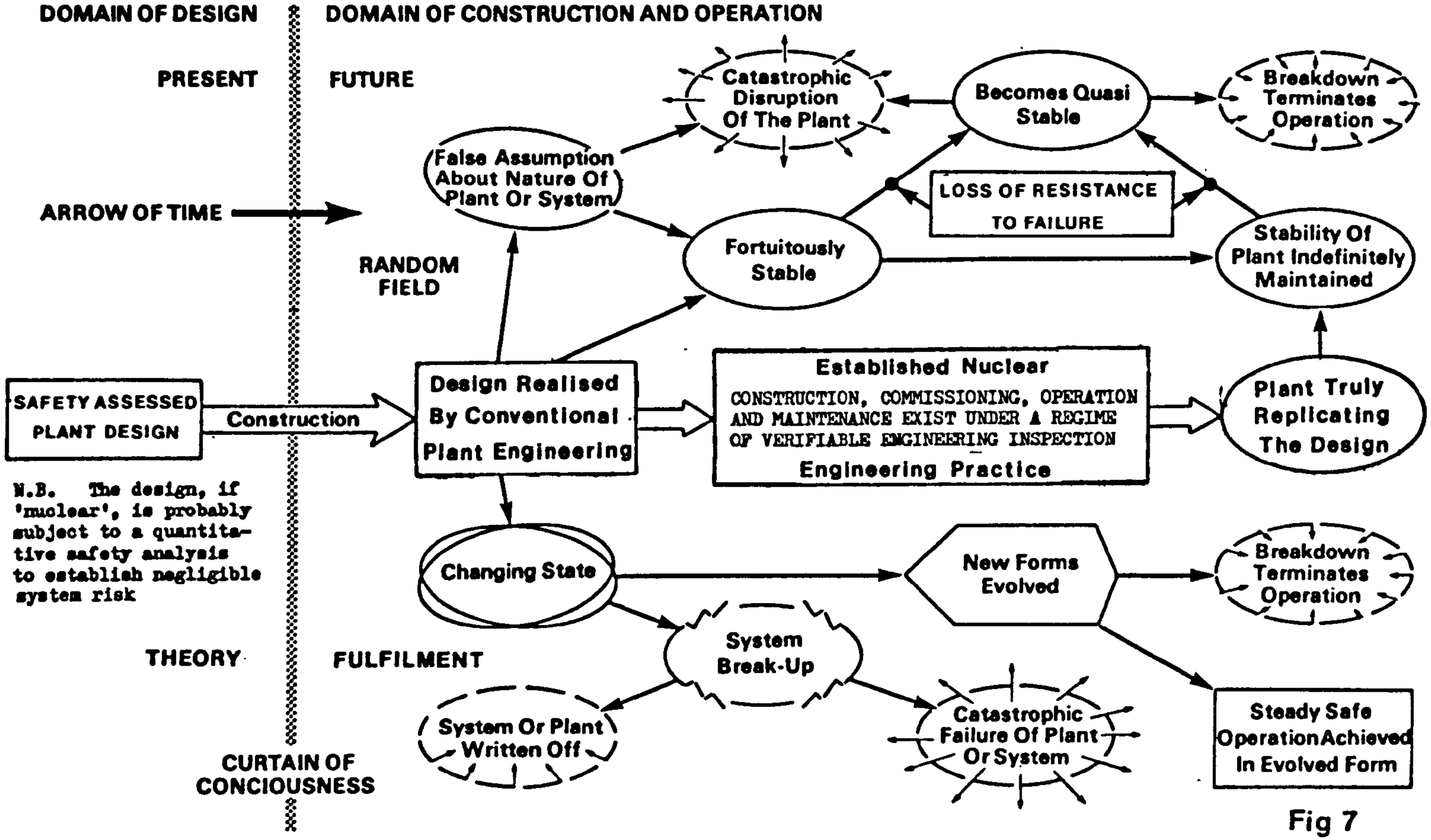


Fig 7

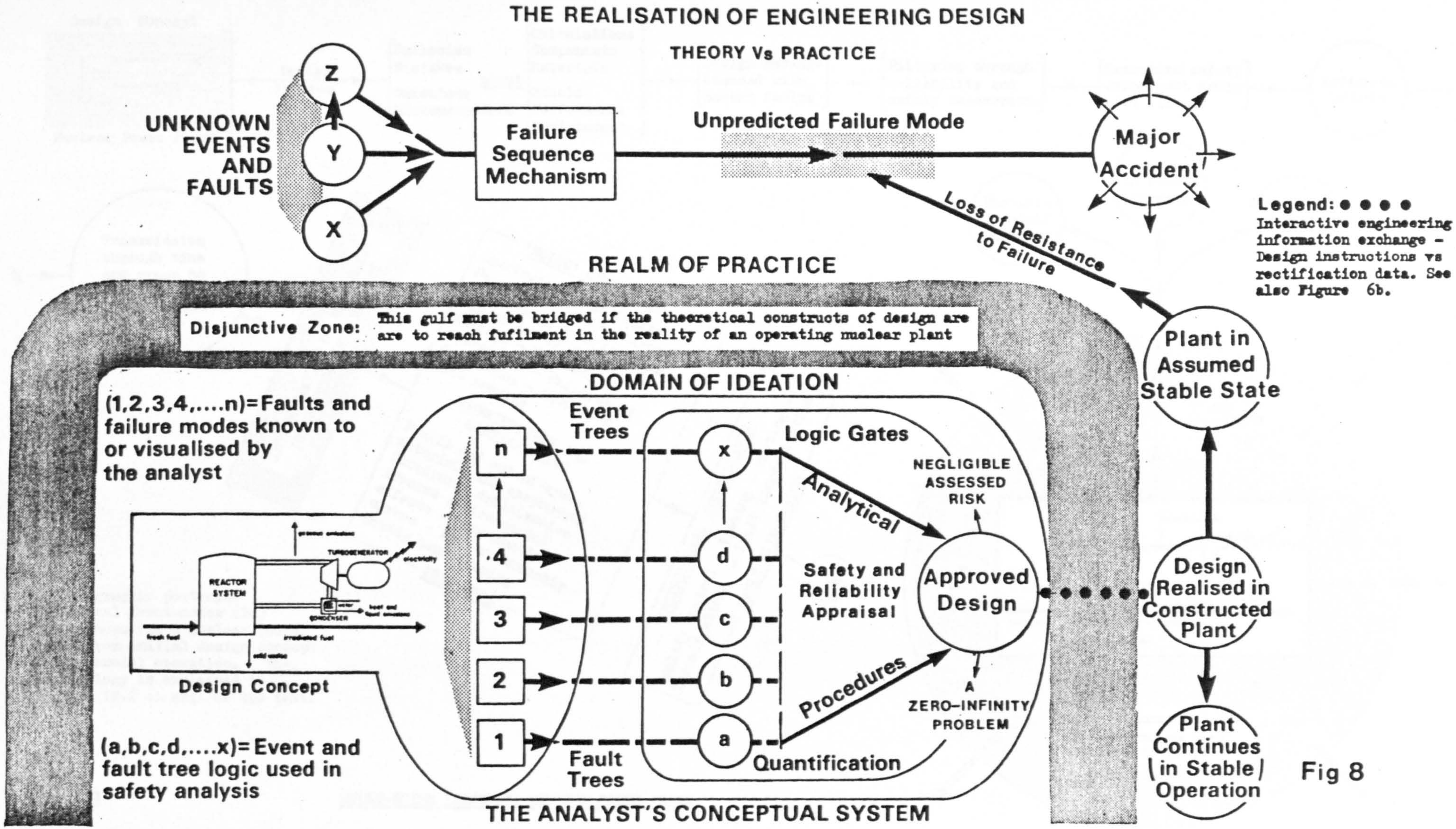
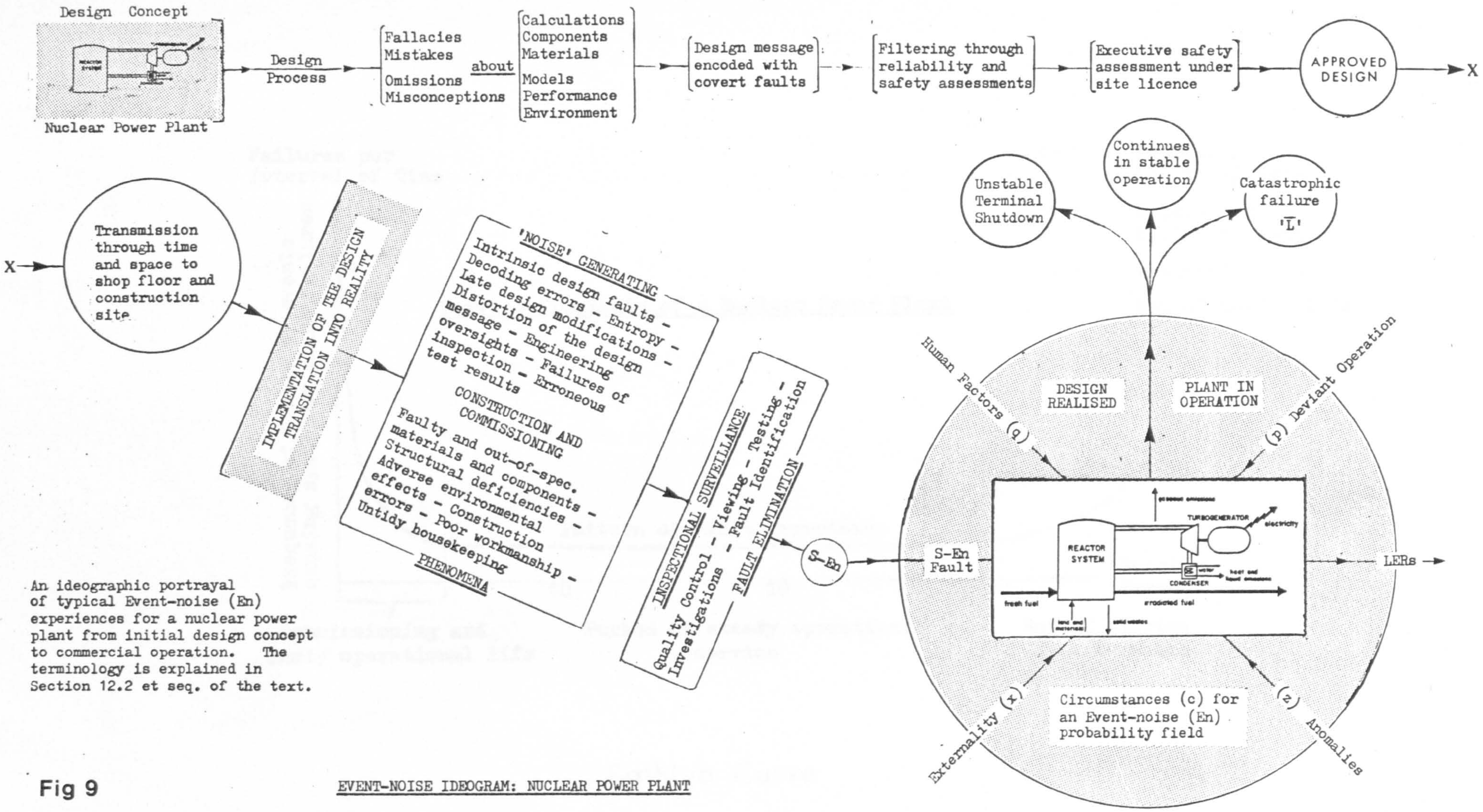

THE REALISATION OF ENGINEERING DESIGN
THEORY Vs PRACTICE
UNKNOWN EVENTS AND FAULTS
Z
Y
X
Failure Sequence Mechanism
Unpredicted Failure Mode
Major Accident
Loss of Resistance to Failure
Legend: ● ● ● ● Interactive engineering information exchange - Design instructions vs rectification data. See also Figure 6b.
REALM OF PRACTICE
Disjunctive Zone: This gulf must be bridged if the theoretical constructs of design are are to reach fufilment in the reality of an operating nuclear plant
Plant in Assumed Stable State
DOMAIN OF IDEATION
(1,2,3,4,....n)=Faults and failure modes known to or visualised by the analyst
Event Trees
Logic Gates
n
4
3
2
1
x
d
c
b
a
NEGLIGIBLE ASSESSED RISK
Analytical
Safety and Reliability Appraisal
Approved Design
Procedures
A ZERO–INFINITY PROBLEM
Quantification
Fault Trees
Design Concept
REACTOR SYSTEM
TURBOGENERATOR
CONDENSER
fresh fuel
irradiated fuel
(a,b,c,d,....x)= Event and fault tree logic used in safety analysis
Design Realised in Constructed Plant
Plant Continues in Stable Operation
THE ANALYST'S CONCEPTUAL SYSTEM

Fig 8



An ideographic portrayal of typical Event-noise (En) experiences for a nuclear power plant from initial design concept to commercial operation. The terminology is explained in Section 12.2 et seq. of the text.

Fig 9 EVENT-NOISE IDEOGRAM: NUCLEAR POWER PLANT

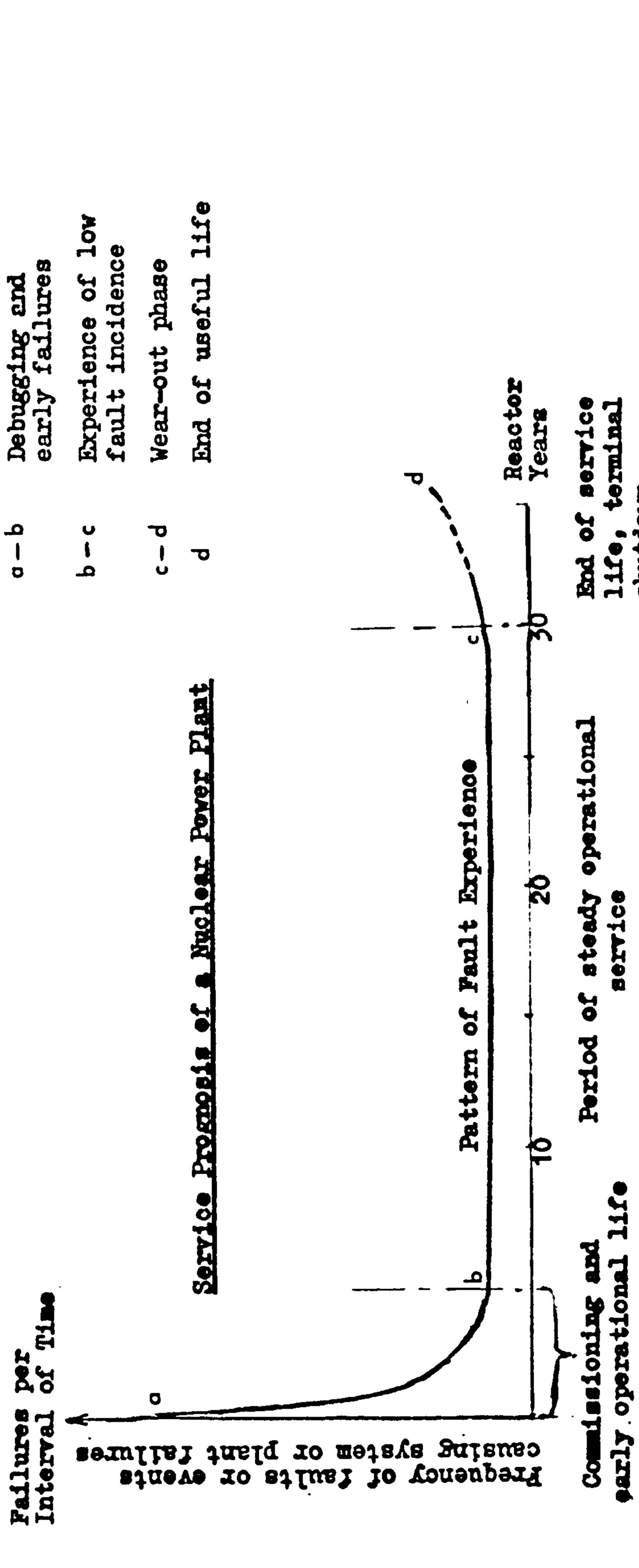
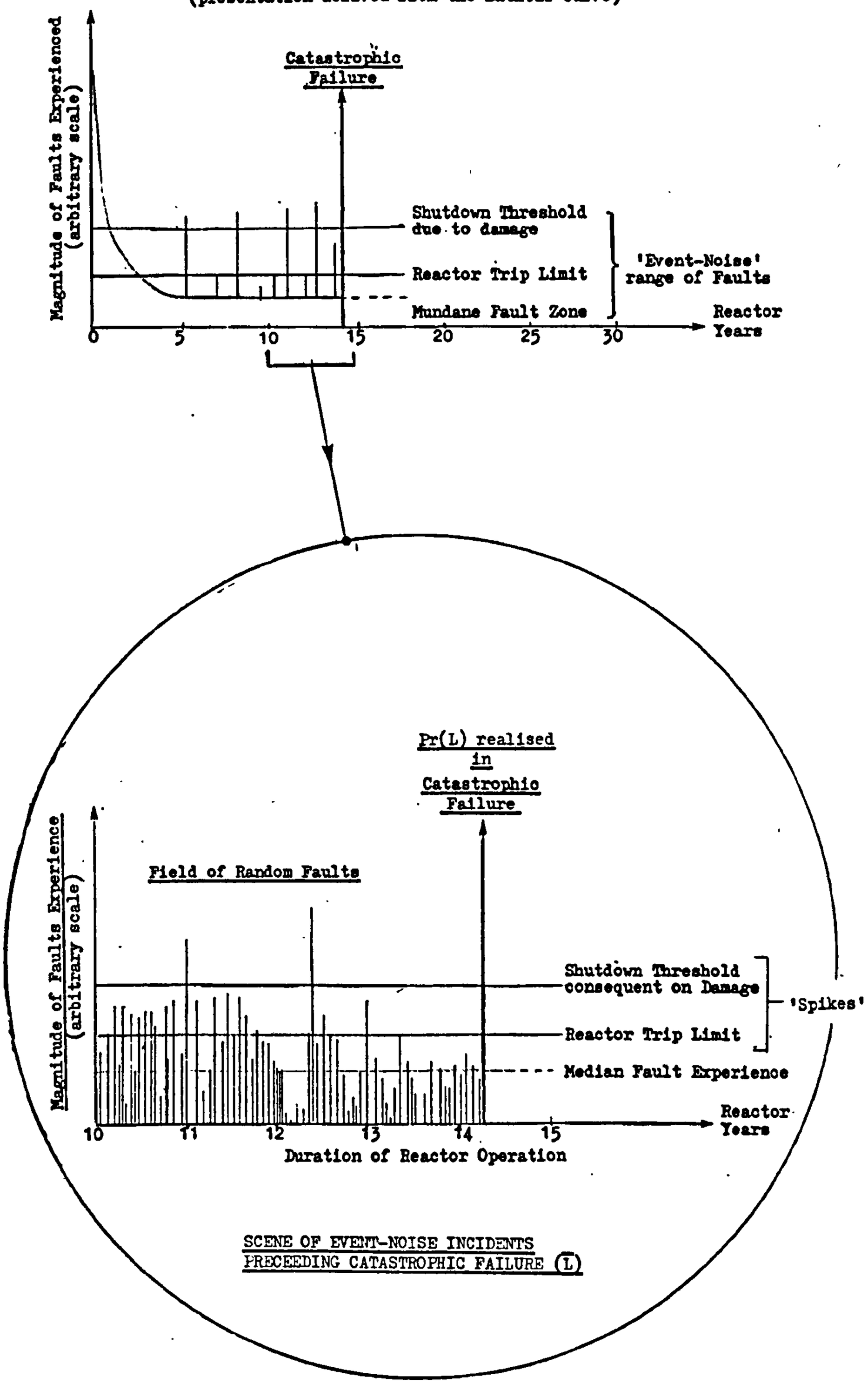


Fig 10

Bathtub Curve

SCENARIO OF REACTOR FAULTS TERMINATING IN CATASTROPHIC FAILURE

(presentation derived from the Bathtub Curve)



SCENE OF EVENT-NOISE INCIDENTS
PRECEEDING CATASTROPHIC FAILURE $(\overline{L})$

LEGEND

'Spikes' = the more serious Event-noise transients, ie. δl incidents

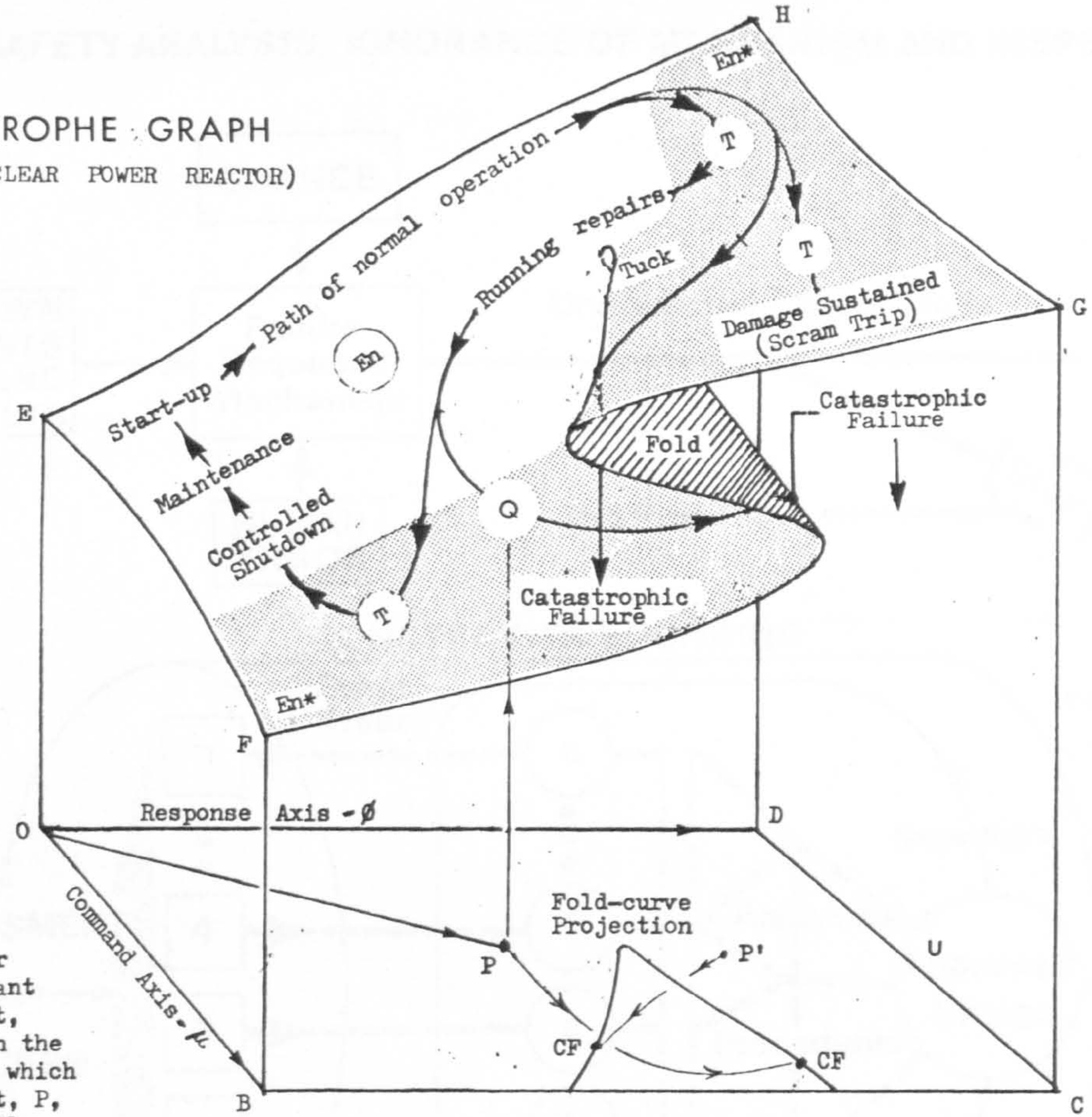
Pr(L) = the probability (very low) of catastrophic failure, $(\overline{L})$

Event-noise Display

Fig 11

THOM'S CATASTROPHE GRAPH

(BEHAVIOUR OF A NUCLEAR POWER REACTOR)



The envisaged behaviour of an nuclear power plant is displayed by a point, Q , following a path on the Behaviour Sheet (EFGH) which is the image of a point, P, moving in the Control Plane, (OBCD) in a manner determined by the Operational Command and System Response co-ordinates of P, which are 'μ' and 'ϕ' respectively

OBCD = Control Plane

EFGH = Behaviour Sheet

CF = Catastrophic Failure

En = Event-noise, normal field

En* = Event-noise, disturbed field

P = Point indicating reactor state

Q = Image of P on the Behaviour Sheet

T = Reactor Trip - Operational

P' = An alternative path path for P

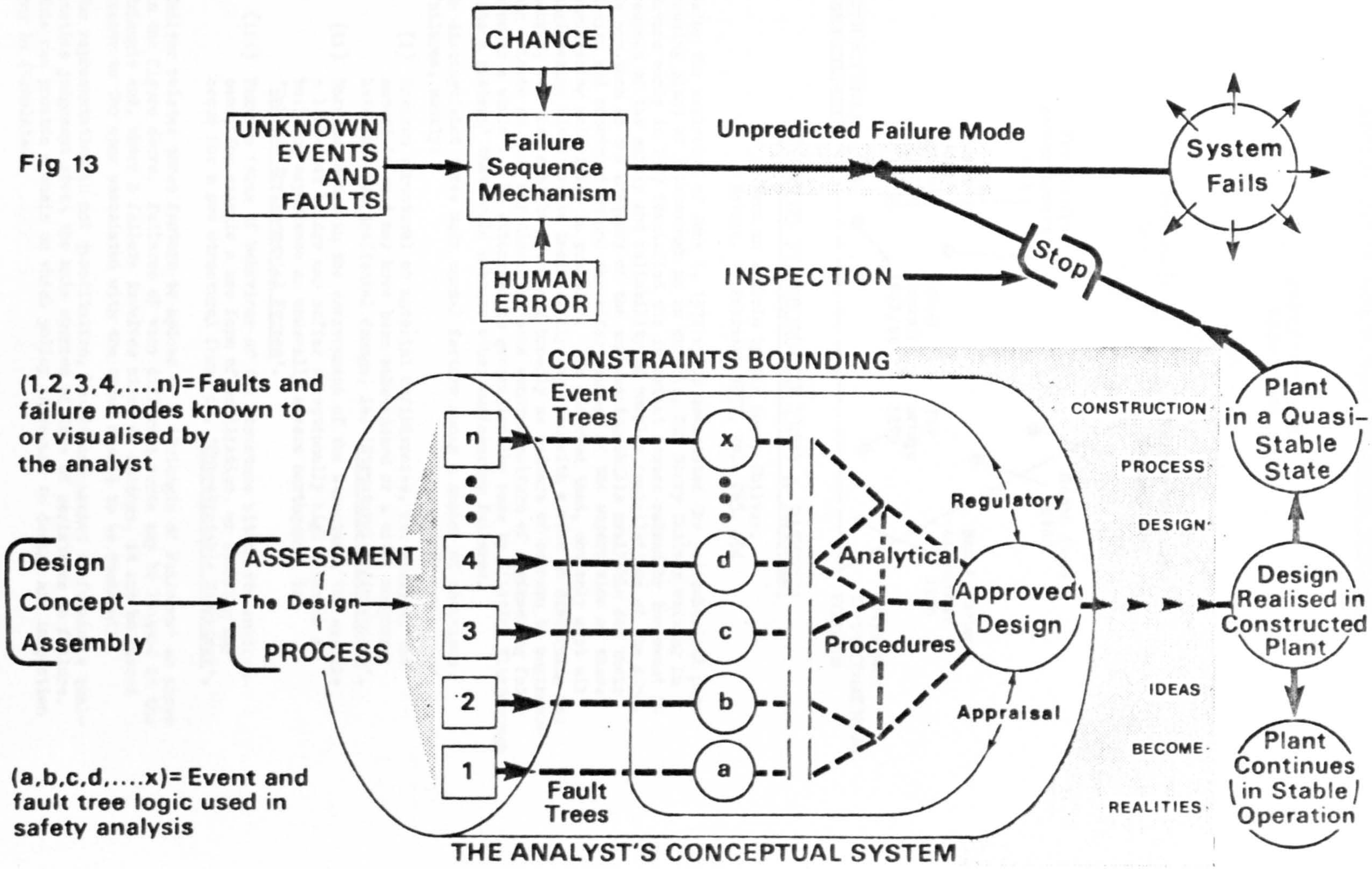
Note A catastrophic failure results when 'Q' passes over the lip of the Fold-curve

Cuboid Model

Figure 12

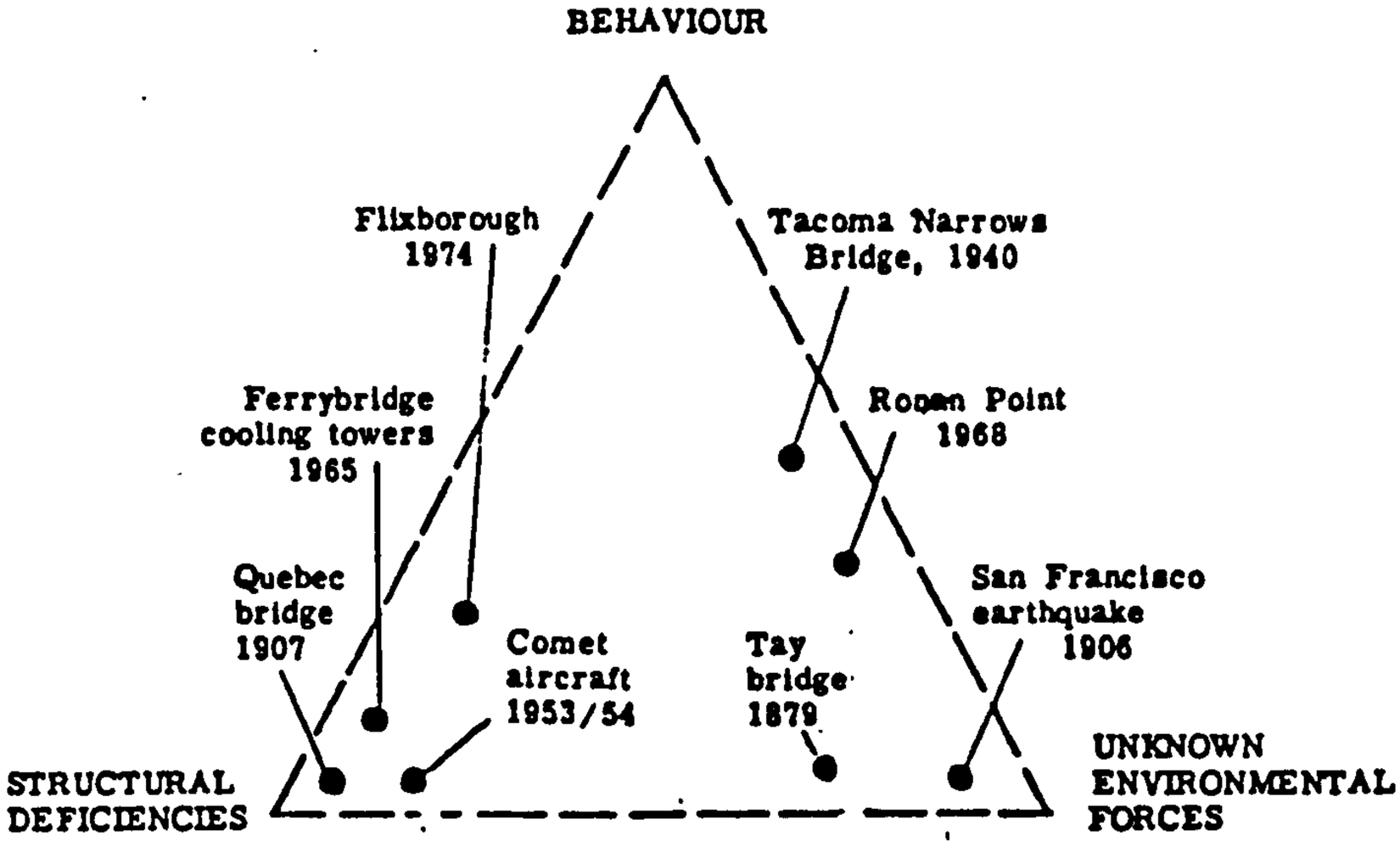
DESIGN SAFETY ANALYSIS, IGNORANCE OF MECHANISM AND INSPECTION

Fig 13



A NEW OUTLOOK ON LPE CAUSATION

An ideogram that proportionately ascribes three generic causes for the failures of major engineering artefacts



FITTING FLIXBOROUGH INTO A PATTERN

From an article by Sir Henry Chilver, Nature, 10 February 1977, Vol. 265, 494

Using the explosion of June 1, 1974 which devastated the petrochemical processing plant at Flixborough as an example, Sir Henry Chilver writing in Nature early in 1977 identified the important issues raised by the event in respect of the safety and reliability of complex installations of the kind. He saw them as the adequacy of the engineering skills available for their design and construction and the effectiveness of the supervision of these engineering activities in practice. He observed that, not only must all engineering disasters be individually explored with a view to discerning the causes, but they must be seen more broadly as matters of concern to engineering science as they may disclose 'some general pattern of engineering failures as a whole'. He attempted to generalise the case by 'fitting Flixborough into a pattern' that could embrace other engineering failures.

He distinguished three main causal factors among a number of notorious failures, namely:

(i) Unknown structural or material deficiencies, for example, the materials used may have been substandard or a vital component have suffered accidental damage, ie. 'Structural Deficiencies'.

(ii) Unknown forces in the environment of the structure, for example a long-span bridge may suffer exceptionally high winds or a building experience an unusually severe earthquake, ie. 'Unknown Environmental Forces'.

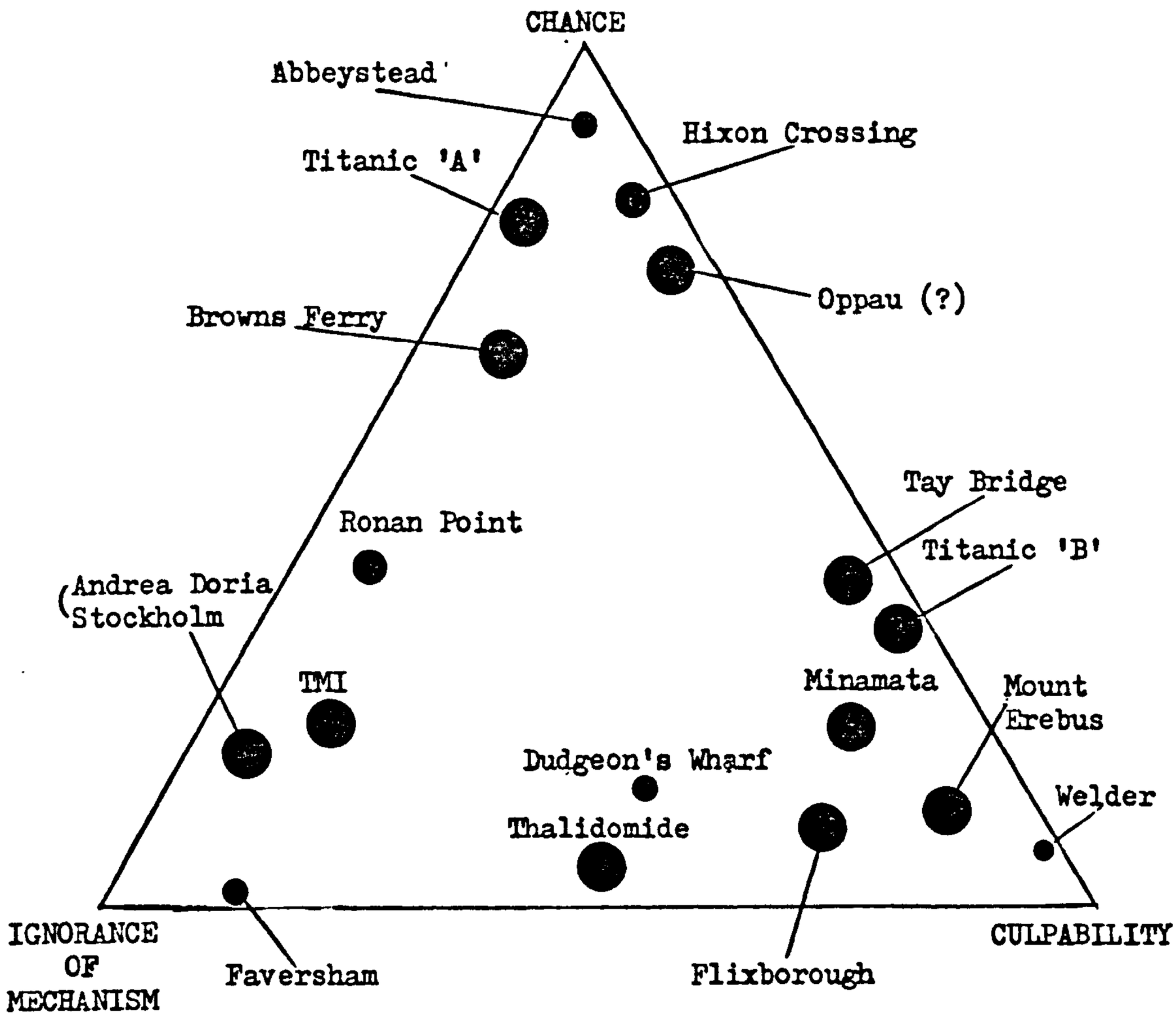
(iii) Unknown forms of behaviour of the structure within its environment, for example a new form of oscillation, or buckling may occur for a new structural form, ie. 'Unpredictable Behaviour'.

Chilver relates these factors to apices of a 'Triangle of Failures' as shown in the figure above. Failures of very different sorts may be located in the Triangle and, where a failure involves mixes of factors, it can be placed nearer to the apex associated with the cause deemed to be dominant.

The representation is not quantitative, but it can assist in forming a qualitative judgement about the main sources of loss of resistance to failure. This can provide a basis on which policy in regard to design and inspection may be formulated.

THE CHILVER FAILURE TRIANGLE (Appendix II refers) FIG 14

CAUSATION TRIANGLE FOR LOW PROBABILITY EVENTS



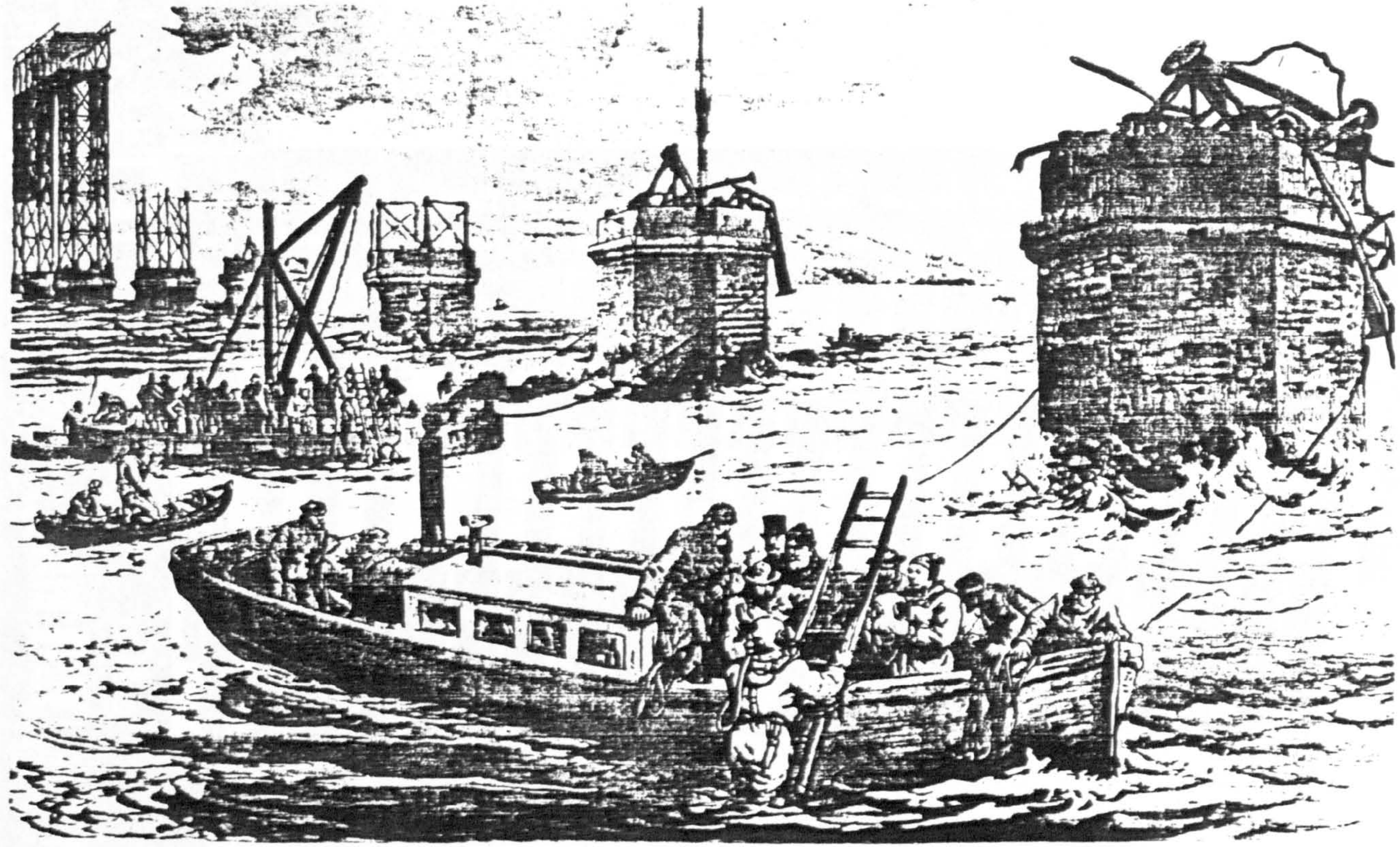
The size of each dot gives an indication of the scale of the incident in terms of injury to humans and damage to property. In the cases of the Three Mile Island (TMI) and Browns Ferry nuclear power station accidents, though there has been very heavy financial loss, no known harm was done to either workers or the public by leakage of radioactivity from the plant.

The clustering of the dots is in accord with the findings of the Analysis in Appendix II. It show a definite trend towards culpable human error, defined in the diagram as 'Culpability', as the major factor in accident causation, a deduction that has been confirmed by more generalised accident studies. It is, however, one that can be effectively minimised by a regime of inspection of a suitable kind.

TRIANGLE OF INCIDENT CAUSATION

Fig 15
(Appendix II refers)

TAY BRIDGE COLLAPSE OF 28th DECEMBER 1879



Divers searching for the wreck of railway train

TAY BRIDGE DISASTER

Fig 16

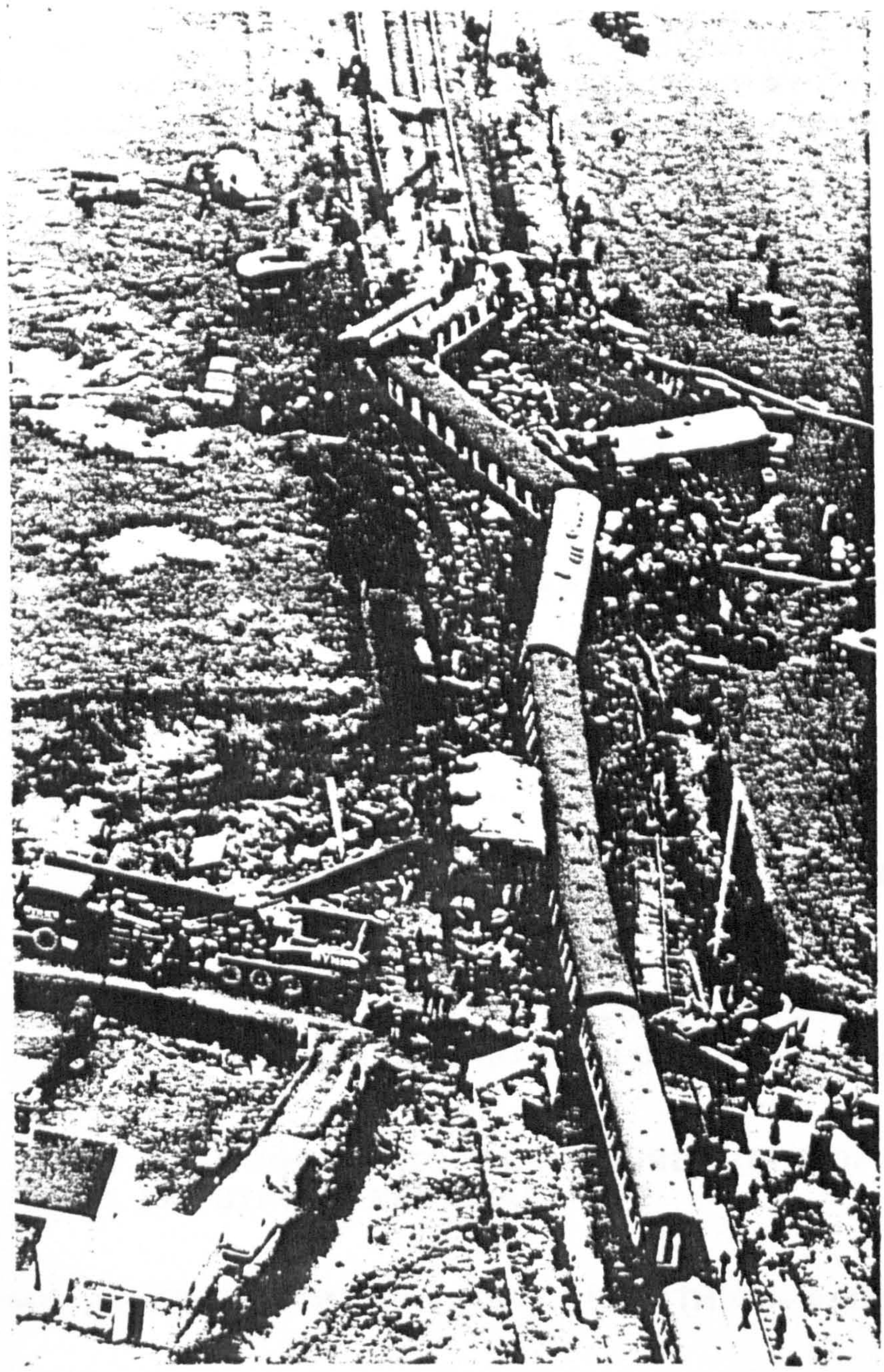
(Appendix II refers)

RONAN POINT TOWER BLOCK COLLAPSE OF 16 MAY 1968

A gas explosion in Flat 90 on the 18th floor of the 22-storey Ronan Point Tower Block blew out the re-inforced concrete slabs which formed its front walls. A 'house-of-cards' collapse followed involving the whole tier of flats above and below from roof to podium.

Fig 17

AUTOMATIC LEVEL CROSSING CRASH OF 6 JANUARY 1968



Aerial view of wrecked train.

The 120 ton electricity transformer, in effect a block of iron, can be seen near the middle of the picture thrust from its platform on the transporter and turned through 90° to lie against two carriages

HIXON LEVEL CROSSING DISASTER

Fig 18

(Appendix II refers)

WELDER

OVER-EXPOSURE–DISMEMBERMENT–DEATH

CONSEQUENCES OF ACCIDENTAL EXPOSURE TO A 13 CURIES Cs-137 WELDING RADIOGRAPHY SOURCE PICKED UP BY AN ARGENTINIAN WELDER (VIENNA,IAEA SYMPOSIUM ON HANDLING OF RADIATION ACCIDENTS–MAY 1969)

COURSE OF SUBSEQUENT TISSUE DETERIORATION

1. SOURCE CARRIED IN POCKETS AT WORK

2. EVENING 4 MAY– PAINS IN THIGHS ATTRIBUTED TO RHEUMATISM

3. MORNING 5 MAY– BURNS OF UNKNOWN ORIGIN DIAGNOSED

4. DAY 27 MAY– LOSS OF RADIATION SOURCE NOTIFIED. INJURIES DIAGNOSED AS RADIATION BURNS

5. INTERREGNUM– SLOW AND PROGRESSIVE EXTENSION OF LESIONS AND ATROPHY IN HEAVILY IRRADIATED AREAS. >500 REMS REGIONS

6. 14 NOV.– HAEMORRHAGES FROM INJURED ZONE OF LEFT THIGH. AMPUTATION NECESSARY

7. MID JAN.1969– SIMILAR EVENTS RIGHT THIGH– AMPUTATED

8. MARCH 1969– BOTH LEGS AMPUTATATED AT HIPS. HEAVY DAMAGE TO ABDOMINAL WALL (SKIN). REPAIR BY GRAFTS. DAMAGE TO GENITAL ORGANS.LEFT ARM PARALYSED.PROGNOSIS–CANCER.NOW DEAD.

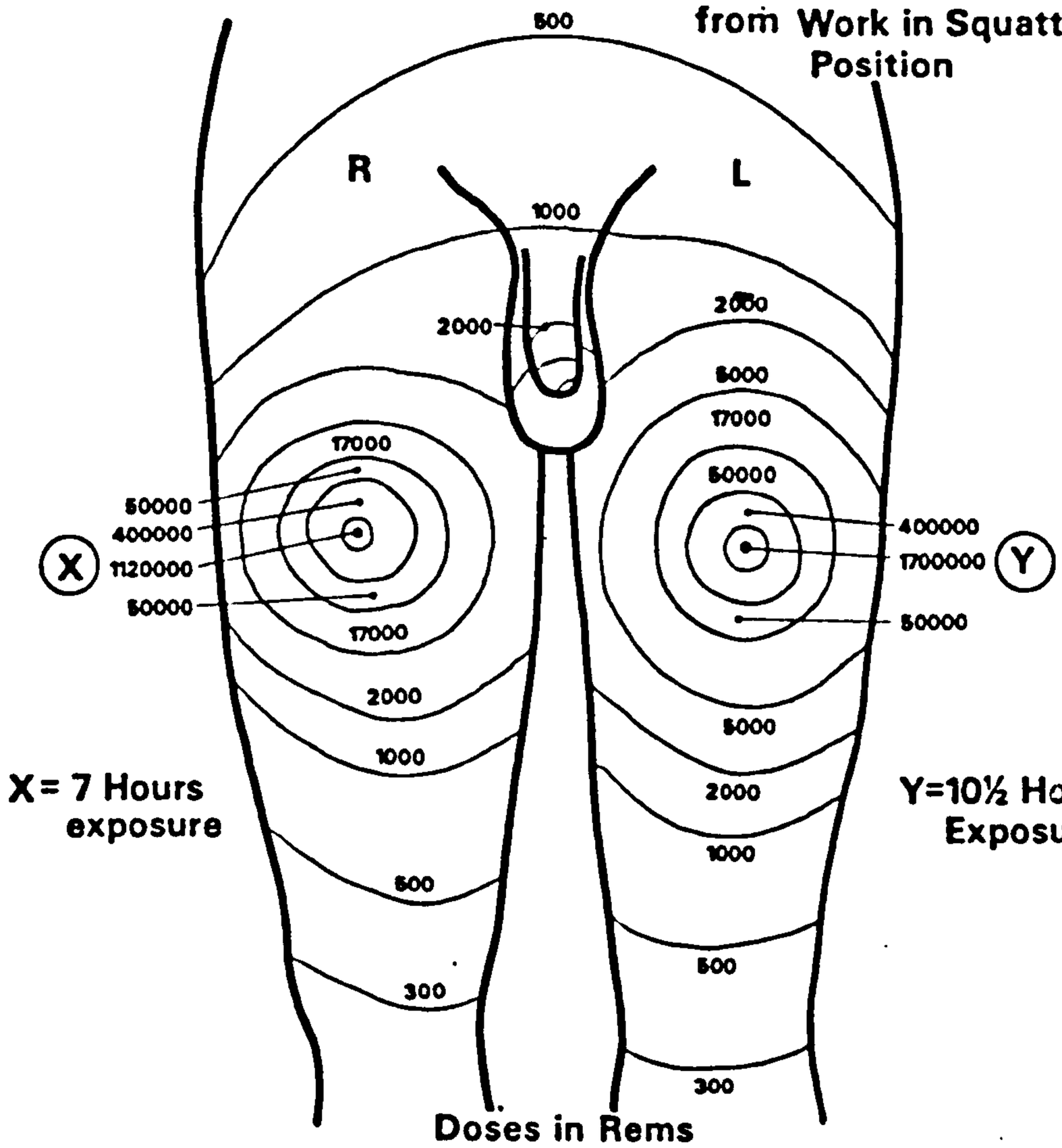
Fig 19

(Appendix II refers)

IONISING RADIATION DOSE PROFILES EXPOSURE OF THIGHS OF AN ARGENTINA REFINERY WELDER

Incident on
3&4 May 1968

(Z) Unquantified Dose to Left Abdominal Wall from Work in Squatting Position



X = 7 Hours exposure

Y = 10½ Hours Exposure

Doses in Rems

The man picked up and carried in his overall pockets at his work a 13 curies CS–137 radiography source which had not been returned to its lead container after use

WELDER

FIG 20
(Appendix II refers)

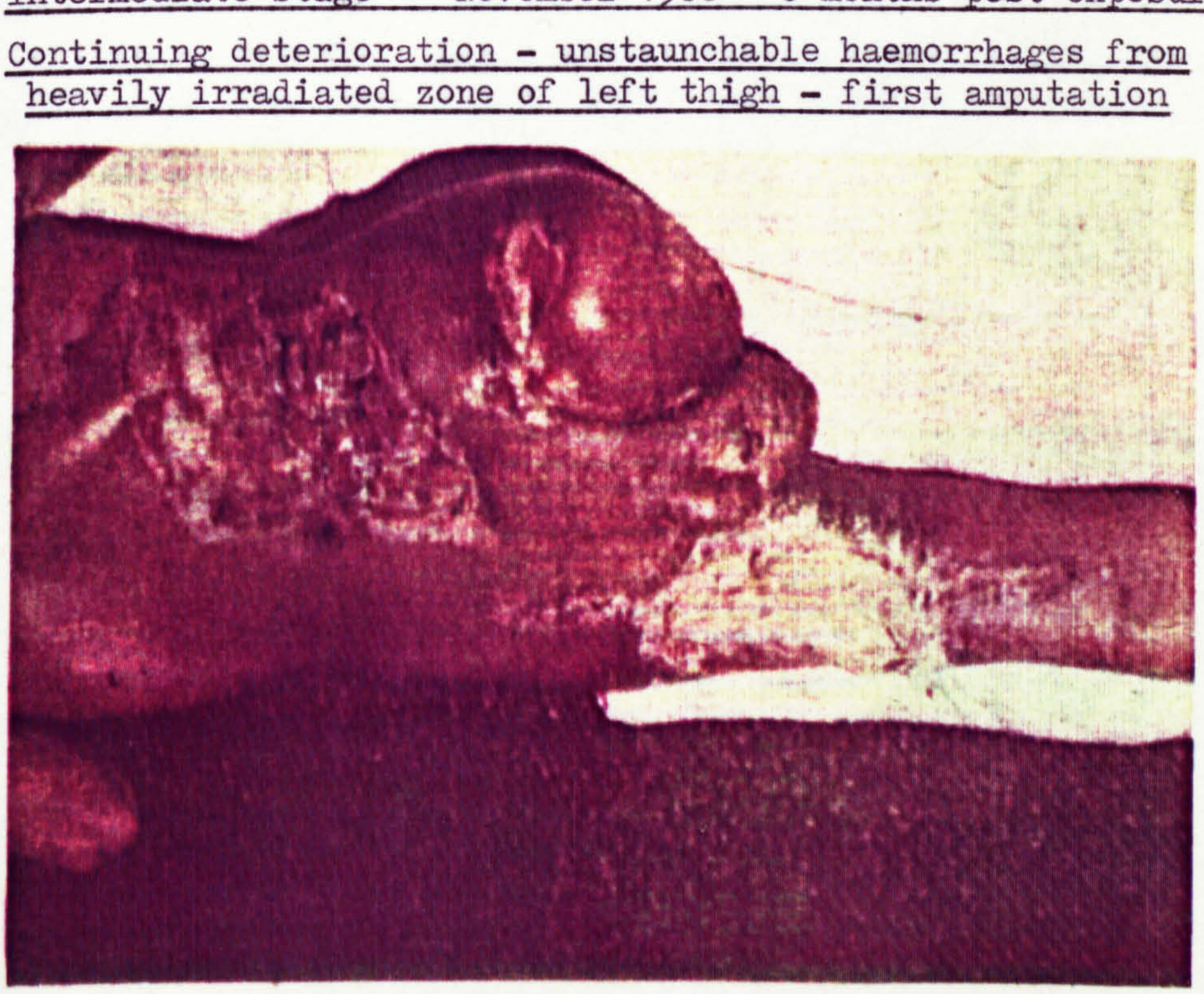
WELDER'S RADIATION BURNS - DEGENERATIVE COURSE

'Early stage' - July 1968 - 3 months post-exposure

Development of extensive necrotic scabs

'Intermediate stage' - November 1968 - 6 months post-exposure

Continuing deterioration - unstaunchable haemorrhages from heavily irradiated zone of left thigh - first amputation



'Late stage' - January 1969 - 9 months post-exposure - Further haemorrhaging Amputation of the right thigh followed

(Appendix II refers)

Fig 21

21 TABLES

Number	Title	Location in Text Page
I	Life Expectance Changes	55
II	Accidental Death - Average Risk of Fatality	88
III	Licensee Event Reports	106
IV	Stub Vector Attitudes	202

TABLE I
Life Expectance Changes

THE EXPECTANCE OF LIFE FROM BIRTH IN RELATION TO THE CHANGING POPULATIONS OF THE WORLD, WESTERN EUROPE AND RUSSIA OVER THE CENTURIES

DATE	EXPECTATION OF LIFE AT BIRTH	MILLIONS OF PEOPLE		SOURCE
		WORLD	W. EUROPE & RUSSIA	
(B.C. 10,000	18 years	1.0	——	Cosslett Palmer Putnam, Energy in the Future, MacMillan, London, 1954
1 A.D.	22 "	275	(61)*	" " "
1000	(22)* "	285	(63)*	" " "
1450	33 "	375	(83)*	" " "
1650	(33.5)* "	470	103	Everyman's Encyclopaedia, Vol. 10, Readers Union & J.M. Dent, London, 1968.
1750	34 "	694	144	
1800	(35)* "	919	193	
1840	41 "	1091	274 (1850)	" " "
1900	49.2 "	1571	423	" " "
1920	58.3 "	1811	487	" " "
1940	64.6 "	2249	573	" " "
1960	71.0 "	2995	641	" " "
1975	73.0 "	3967	728	Whitaker's Almanack, 113th Edition, 1981.
2000	(>76)* "	(6267)	(947)	

Apply to W. Europe and U.S.A. only

NOTES

(a) The bracketted figures are estimates. An asterisk (*) indicates an interpolation by the writer.

(b) The figures are 'accurate' in the case of those countries in which some form of census has been possible, otherwise they are broad estimates which vary by as much as 20% among those authorities held to be expert.

(c) There is a widely held view that the spurt in growth of the World population after 1650 was not due to increased fertility, but to a fall in mortality, particularly amongst children and young adults which coincided with the increasing standard of living attributable to the growth in the productivity of labour characteristic of the Industrial Revolution.

(d) C. Palmer Putnam does not seem to be wholely in agreement with the opinion quoted in Note (c) above. He observes that the population of China (a country where some sort of attempt to enumerate the total population has been made throughout its long civilised existence) together with that of all the West passed through a minimum in the 7th and 8th Centuries. There was little change until about 1600 when a population explosion began in both areas and which has followed broadly the same continuing pattern ever since. He attributes this, like others, to an increase in life expectancy, though the reasons for this are not fully understood. The effect of improving standards of living is less than might be expected. Some suggest that it might be due to an evolutionary change expressed as lengthening of the human life span.

TABLE II

Accidental Death - Average Risk of Fatality

PROBABILITY CLASS	CAUSE OF DEATH (Accident Type)	INDIVIDUAL'S CHANCE OF FATALITY (Annual risk to member of group exposed to the hazard - rounded-off figures)	SOURCE OF DATA
MUNDANE	Industrial Accidents (Construction sites, factories and mines)	1 in 2,500 (employees - UK)	(a,b)
"	Falls at home (Age group 45 - 65 years)	1 in 3,000 (UK)	(c)
"	Traffic Accidents	1 in 4,000 (UK and USA)	(c,d)
UNUSUAL	Fires	1 in 25,000 (USA)	(d)
"	Drowning	1 in 30,000 (USA)	(d)
"	Air Travel	1 in 100,000 (International)	(d)
"	Railway Passengers	1 in 400,000 (UK)	(e)
"	Struck by lightning	1 in 2,000,000 (UK and USA)	(c,d)
LOW PROBABILITY GROUP OF EVENTS		(Chance of death due to given cause not calculable. Data exiguous and unstable. Zero-Infinity hazards presenting vestigal risk of unlimited losses.)	
Actual	'Titanic'	1503 fatalities	(f)
"	'Andria Doria'/'Stockholm' collision at sea	59 "	(f)
"	Collapse of tower block flats - Ronan Point	4 "	(f)
"	Explosion at Flixborough petrochemical plant	28 "	(f)
"	Three Mile Island nuclear power plant	No casualties, but financial losses greater than $4 billion	(f)
Hypothetical		(These are potential accidents for which the assessed risk has been formally quantified)	
"	Canvey/Thurrock petrochemical installation (See note 'h' below)	1 in 10,000 - Notional estimate using data from analogous actual happenings	(g)
"	Nuclear Power - for a program of 100 reactors - Radiation accident - casualties among the public	1 in 5,000,000,000 (USA) Estimate derived by quantitative analysis of synthesised model	(d)

NOTES

(a) Report by H.M. Inspector of Factories for 1973.
(b) Wickenden and Mayhew, ATOM, June 1980, UKAEA house journal.
(c) F. R. Farmer (Ed.), Nuclear Reactor Safety, Academic Press, 1977.
(d) N. C. Rasmussen, U.S. Reactor Safety Study - Main Report, WASH-1400(NRC), 1975.
(e) Chambers's Encyclopaedia, Vol 11, 1950, p. 502 (tends to be an invariant statistic).
(f) See Appendix II.
(g) Locke, J. et al., CANVEY, HSE, London, 1978, Table 4, p. 25.
(h) Included as an exemplar of a hypothetical risk prediction, but anomalously placed in the Low Probability Group of Events. Note 10 refers.

TABLE III

Licensee Event Reports

(Two specimen sets of Licensee Event Reports excerpted from returns by U.S. nuclear power plant operators to the Nuclear Safety Information Center and issued after processing in February and April 1980)

FEB 26, 1980 — LER MONTHLY REPORT SORTED BY FACILITY
PROCESSED DURING FEBRUARY, 1980 FOR POWER REACTORS

FACILITY/SYSTEM/COMPONENT/ COMPONENT SUBCODE/CAUSE CODE/ CAUSE SUBCODE/MANUFACTURER	DOCKET NO./ LER NO./ CONTROL NO.	EVENT DATE/ REPORT DATE/ REPORT TYPE	EVENT DESCRIPTION/ CAUSE DESCRIPTION
ARKANSAS-1 FEEDWATER SYSTEMS + CONTROLS PUMPS OTHER DEFECTIVE PROCEDURES NOT APPLICABLE ITEM NOT APPLICABLE	05000313 79-022/03L-0 827712	111979 121879 30-DAY	DURING PLANT HEATUP TO HOT SHUTDOWN CONDITIONS, THE OPERATIONAL TEST (OP 1106.06) OF THE TURBINE DRIVEN EMERGENCY FEEDWATER PUMP (P7A) WAS NOT PERFORMED. HOWEVER, THE REDUNDANT MOTOR DRIVEN PUMP (P7B) WAS TESTED SATISFACTORILY WHILE IN COLD SHUTDOWN CONDITIONS ON 11-12-79 ON 11-20-79 THE P7A EMERGENCY FEEDWATER PUMP WAS SATISFACTORILY TESTED. THERE HAVE BEEN NO SIMILAR OCCURRENCES. REPORTABLE PER T.S. 6.12.3.2(B). THE P7A EMERGENCY FEEDWATER PUMP WAS NOT TESTED PER OP 1106 06 DUE TO A SCHEDULING MISTAKE WHICH WAS NOT COVERED BY THE STARTUP PROCEDURE 1102 0 2. THEREFORE, A STEP WAS ADDED TO THE STARTUP PROCEDURE TO PROHIBIT ANY FUTURE SIMILAR OCCURRENCES.
ARKANSAS-1 FEEDWATER SYSTEMS + CONTROLS TURBINES SUBCOMPONENT NOT APPLICABLE COMPONENT FAILURE MECHANICAL TERRY STEAM TURBINE COMPANY	05000313 79-024/03L-0 827885	120679 011080 30-DAY	DURING THE OPERATIONAL TEST (OP. 1106.06 SUPP. II) OF THE TURBINE DRIVEN EMERGENCY FEEDWATER PUMP (P7A), THE PUMP WAS DECLARED INOPERABLE ON LOW PUMP DELTA P. THE REDUNDANT PUMP (P7B) WAS STARTED AND PROVED OPERABLE. ON 12-6-79, THE P7A EMERGENCY FEEDWATER PUMP WAS REPAIRED AND SUCCESSFULLY TESTED. THERE HAVE BEEN NO SIMILAR OCCURRENCES. REPORTABLE PER T.S. 6.12.3.2.(B). THE SPEED GOVERNOR LOCK NUT WAS FOUND TO BE LOOSE ON THE TURBINE PUMP DRIVE. THIS CAUSED THE PUMP SPEED TO BE LESS THAN NORMAL THE PUMP SPEED WAS INCREASED TO ALLOW NORMAL OPERATION AND THE LOCK NUT WAS TIGHTENED
ARKANSAS-1 CHEM, VOL CONT + LIQ POISN SYS PUMPS CENTRIFUGAL PERSONNEL ERROR LICENSED & SENIOR OPERATORS ITEM NOT APPLICABLE	05000313 79-023/03L-0 827964	122179 011880 30-DAY	DURING A NORMAL MAKEUP OPERATION TO THE RCS, THE BORIC ACID PUMPS WERE INADVERTANTLY LEFT OPERATING. THIS RESULTED IN OVER BORATION OF THE REACTOR COOLANT AND AUTOMATIC WITHDRAWAL OF RODS ABOVE THE LIMITS PER T S 3 5.2.5.3. THE RCS WAS IMMEDIATELY DILUTED AND THE ROD INDEX WAS RETURNED TO THE NORMAL RANGE WITHIN THE ALLOTTED 4 HOURS. LER 50-313/78-025 WAS A SIMILAR OCCURRENCE OF THE ROD INDEX OUT OF LIMIT. REPORTABLE PER T.S .6.12.3 2.B. DURING A NORMAL MAKEUP OPERATION TO THE RCS, A REACTOR OPERATOR INADVERTANTLY FAILED TO SECURE THE BORIC ACID PUMPS. THE OPERATOR WAS COUNSELED AND COPIES OF THE FAILURE REPORT WERE DISTRIBUTED TO ALL LICENSED OPERATORS.
ARKANSAS-2 OTHR INST SYS REQD FOR SAFETY INSTRUMENTATION + CONTROLS TRANSMITTER COMPONENT FAILURE OTHER FISCHER & PORTER CO.	05000368 79-008/03X-1 825219	011479 011880 OTHER	DURING MODE 1 OPERATION, REFUELING WATER TANK LEVEL TRANSMITTER, 2LT-5639-3, SENSING LINE FROZE, MAKING THE TRANSMITTER INOPERABLE THE LOW RWT LEVEL TRIP (RAS) SIGNAL ON PPS CHANNEL "C" WAS BYPASSED PER THE REQUIREMENTS OF ACTION STATEMENT T.S. TABLE 3.3-3.6.B 09. THE REMAINING RWT LEVEL INDICATIONS WERE VERIFIED TO BE NORMAL. SIMILAR OCCURRENCES ARE LER'S 50-368/79-002 & 79-001. REPORTABLE PER T.S. 6 9.1.9.B. INVESTIGATION REVEALED THAT THE TEMPORARY HEAT LAMP PLACED IN THE TRANSMITTER BOX HAD BURNED OUT. THE LAMP WAS REPLACED AND REMAINED IN SERVICE UNTIL NOVEMBER, 1979, WHEN HEAT TRACING WAS PERMANENTLY INSTALLED.

APR 24, 1980 — LER MONTHLY REPORT SORTED BY FACILITY
PROCESSED DURING APRIL, 1980 FOR POWER REACTORS

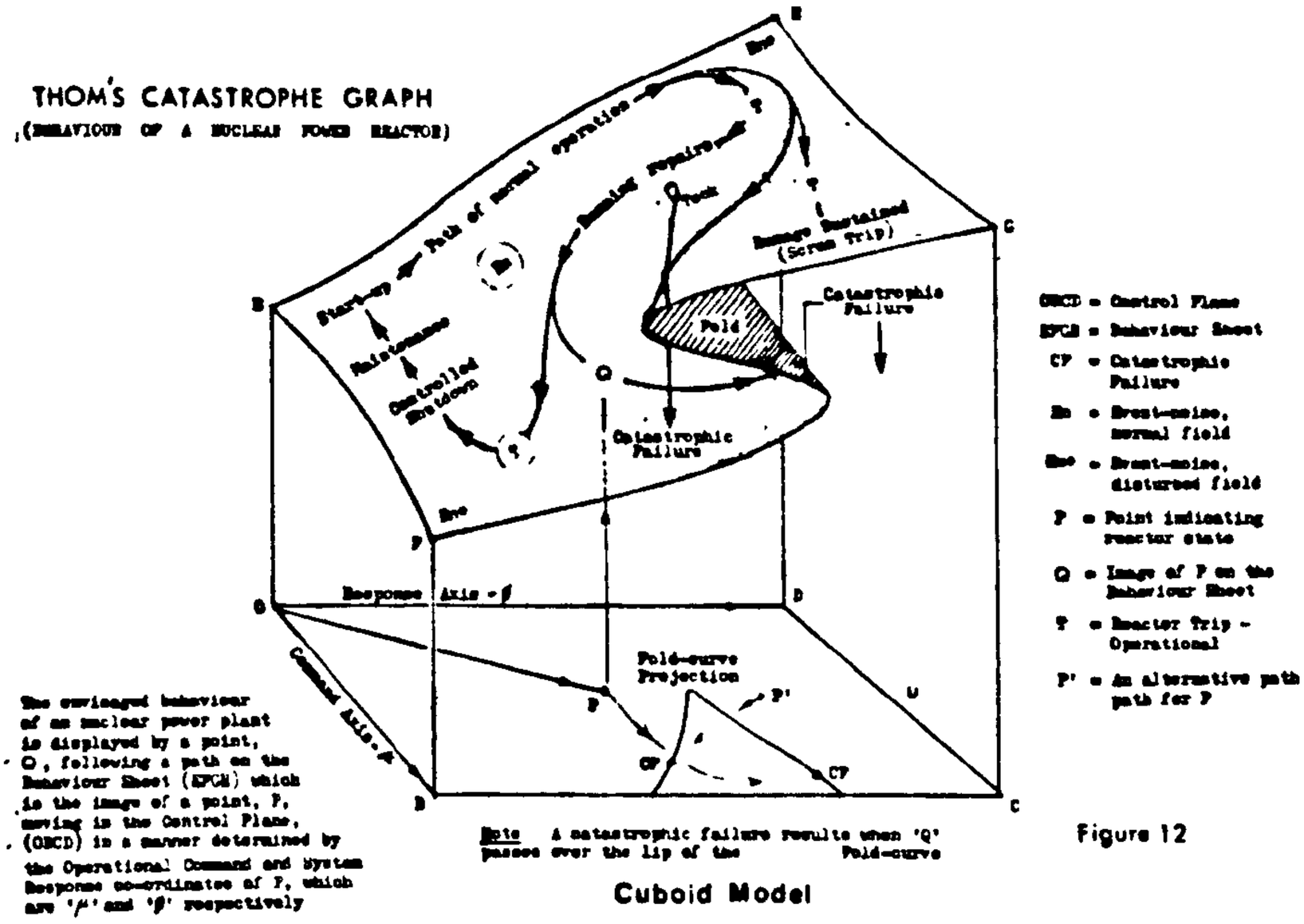
FACILITY/SYSTEM/COMPONENT/ COMPONENT SUBCODE/CAUSE CODE/ CAUSE SUBCODE/MANUFACTURER	DOCKET NO./ LER NO./ CONTROL NO.	EVENT DATE/ REPORT DATE/ REPORT TYPE	EVENT DESCRIPTION/ CAUSE DESCRIPTION
BEAVER VALLEY-1 PRCSS + EFF RADIOL MONITOR SYS COMPONENT CODE NOT APPLICABLE SUBCOMPONENT NOT APPLICABLE OTHER NOT APPLICABLE ITEM NOT APPLICABLE	05000334 80-015/04T-0 838555	030880 032180 2-WEEK	WHILE PERFORMING THE MONTHLY RADIATION MONITOR SURVEILLANCE TEST, IT WAS DISCOVERED THAT THE COMPONENT COOLING WATER RADIATION MONITOR HIGH-HIGH LEVEL ALARM DID NOT FUNCTION. THIS RADIATION MONITOR SERVES NO AUTOMATIC CONTROL FUNCTION AND IS BACKED UP BY THE RIVER WATER RADIATION MONITORS. THERE WAS NO SAFETY IMPLICATION INVOLVED WITH THIS INCIDENT. THE COMPONENT COOLING WATER RADIATION MONITOR HIGH-HIGH ALARM DID NOT COME IN WHEN THE TEST SIGNAL INPUT WAS HIGH ENOUGH TO CAUSE THE METER TO INDICATE OFF-SCALE, HIGH. SUBSEQUENT INVESTIGATION BY MAINTENANCE PERSONNEL REVEALED THAT THE ALARM POTENTIOMETER WAS OUT OF ADJUSTMENT.
BIG ROCK POINT DC ONSITE POWER SYS + CONTROLS BATTERIES + CHARGERS SUBCOMPONENT NOT APPLICABLE COMPONENT FAILURE OTHER EXIDE INDUSTRIAL DIV	05000155 80-002/03L-0 838237	012480 022180 30-DAY	DURING MONTHLY SPECIFIC GRAVITY CHECKS, CELL 14 OF THE BATTERY FOR CHANNEL C OF THE REACTOR DEPRESSURIZING SYSTEM, READ 1.191. THIS IS BELOW THE LIMIT OF 1,200 SPECIFIED IN TECH SPEC 11.4.5.3.A.2(B). ALL OTHER CELLS EXCEEDED SPECIFICATIONS AND THE CHANNEL IS DEEMED OPERABLE FOR THE SPECIFIC DEFICIENCY. THE BATTERY WAS PUT ON EQUALIZING CHARGE. INCIDENT SIMILAR TO RO-79-26 AND RO-78-34. NO HAZARD TO THE PUBLIC OCCURRED. THE CELL DID NOT RESPOND ADEQUATELY TO THE EQUALIZING CHARGE AND THE CHANNEL WAS REMOVED FROM SERVICE, AS ALLOWED BY TECHNICAL SPECIFICATION 11.3.1.5, TO REPLACE THE DEFECTIVE CELL ON 1/29/80. REPORTABILITY BASED ON TECH SPEC 6.9.2.B(2).
BIG ROCK POINT CNTNMNT ISOLATION SYS + CONT VALVES CHECK COMPONENT FAILURE NATURAL END OF LIFE UNION PUMP COMPANY	05000155 80-007/03L-0 838446	022480 031980 30-DAY	DURING ROUTINE OPERATION AT 1700 HOURS, EXCESSIVVE VIBRATION WAS NOTED ON CONTROL ROD DRIVE PUMP B2. THE PUMP WAS REMOVED FROM SERVICE AND B1 PUMP WAS PLACED IN SERVICE. INVESTIGATION REVEALED THAT THE SUCTION POPPET VALVES WERE DEFECTIVE. THE PUMP SUCTION VALVE WAS MANUALLY CLOSED ON 2/24/80 TO PROVIDE A REDUNDANT CONTAINMENT BOUNDARY PENDING COMPLETE REPAIR TO THE VALVES. NO HAZARD OCCURRED. REPORTABLE BASED ON TECH SPEC 6.9.2B(2). INVESTIGATION REVEALED WORN SUCTION POPPET VALVES ON THE PUMP AND DAMAGE TO PUMP PIPING HANGERS FROM THE VIBRATION. THE POPPET VALVES WERE REPLACED AND LAPPED AND THE HANGARS REPAIRED AND THE PUMP TESTED SATIFACTORILY ON 2/26/80. SIMILAR TO INCIDENT REPORTED AS RO-77-29.
BROWNS FERRY-1 DEMIN WATER MAKE-UP HANGERS,SUPPORTS,SHOCK SUPPRSS OTHER OTHER NOT APPLICABLE TENNESSEE VALLEY AUTHORITY	05000259 79-018/01T-1 826778	082379 031180 2-WEEK	WITH UNIT IN NORMAL OPERATION AT 95% POWER, INSPECTIONS WERE MADE IN ACCORDANCE WITH IE BULLETIN 79-14. DURING THIS INSPECTION, IT WAS FOUND THAT RESTRAINTS ON CERTAIN CSSC SYSTEMS WERE INOPERABLE IN THAT THEIR CONFIGURATION DID NOT CONFORM TO THE DESIGN SPECIFICATIONS. THERE WERE NO RESULTING SIGNIFICANT OCCURRENCES, NO PREVIOUS SIMILAR EVENTS AND NO DANGER TO HEALTH OR SAFETY OF THE PUBLIC. THIS EVENT WAS REPORTED UNDER T.S. 6.7.2.A(9). PIPE VIBRATION AND/OR IMPROPER INSTALLATION DURING CONSTRUCTION CAUSED THE INOPERABILITY ON RS TYPE RESTRAINTS, ON RHRSW. FIFTY OF THESE RESTRAINTS IN UNITS 1, 2, AND 3 WERE INSPECTED WITH REPAIR WORK REQUIRED ON NINETEEN OF THESE. THIS IS A FINAL REPORT.

Licensee Event Reports (LERs) are made by U.S. nuclear site licensees' to a data base at the Oak Ridge National Laboratory (ORNL) maintained by the Nuclear Regulatory Commission (NRC), the Advisory Committee on Reactor Safeguards (ACRS) and the Nuclear Safety Information Center (NSIC). After being collated and summarised, the LERs are issued monthly by the Licensee Operations and Evaluation Branch of the NRC. (Situation as at August 1980. See also Note 15.)

TABLE IV

Stub Vector Attitudes

Explanatory Note - In discussing the Event-noise (EN) features of the Behaviour Surface (EFGH) of the Cuboid Model, it is appropriate to assign meaning to its upward slope from E-F to G-H. The bumps, creases and folds that form the 'asperities', the 'wrinkles' and the 'fold-curve' which represent the En probabilities then appear as changes of slope with respect to the z-axis. The magnitude of these changes is indicative of the severity of the particular En experience, potential or realised, and is described by the tilt induced in the Stub Vector as 'Q' proceeds around the operational hysteresis loop and encounters the various Behaviour Surface irregularities.



Note A catastrophic failure results when 'Q' passes over the lip of the Fold-curve

Figure 12

Cuboid Model

SLOPE ANOMALY IN THE BEHAVIOUR SURFACE	STUB VECTOR ATTITUDES (surface cross-section and Vector tilt)	EVENT-NOISE EXPERIENCE (in terms of system stability)
System stable	↑	Normal operational state with minor Event-noise
Asperity	↖	Quasi-stable, major industrial accident, fault or incident, i.e. D-En or S-En
Wrinkle	↘	Unstable, severe fault or incident - En 'spike'
Fold-curve	↓	Catastrophic failure - severe radiation accident or disruptive fault with terminal shutdown, $Pr(\overline{L})$

22 REFERENCES

The name of the author, authors or source is followed by the year of publication (in brackets), title of the work, identity of the publisher or its origin otherwise and, where appropriate, the page, section or paragraph number or numbers. On occasion, certain other information is given, eg a note telling of the existence of another relevant document. In some instances, abbreviations replace the title of the company or institution under whose imprimatur the work appeared. The meanings are given in the legend below. The prefix 'J' or 'P' indicates a Journal or Proceedings of the learned society concerned. In the case of a periodical, both the title and volume number are underlined.

AHSB Authority Health and Safety Branch, UKAEA

AID Aeronautical Inspection Directorate

AQD Aeronautical Quality Assurance Directorate

BAC British Aircraft Corporation

BMJ British Medical Journal

BNES British Nuclear Energy Society

CEI Council of Engineering Institutions

CSC Civil Service Commission

CSS Council for Science and Society

CUP Cambridge University Press

DOE Department of the Environment

DSIR Department for Scientific and Industrial Research

FOE Friends of the Earth

HMSO His/Her Majesty's Stationery Office

HSE Health and Safety Executive

IAEA International Atomic Energy Agency

ICRP International Commission on Radiological Protection

IIASA International Institute for Applied Systems Analysis

INI See NII (title changed)

INucE Institution of Nuclear Engineers

LNG Liquid Natural Gas

MIT Massachusetts Institute of Technology

IMechE Institution of Mechanical Engineers

NASA National Aeronautics and Space Administration

NCB National Coal Board

NII Nuclear Installations Inspectorate, formerly Inspectorate of Nuclear Installations

NRC Nuclear Regulatory Commision (U.S.A.)

NRPB National Radiological Protection Board

OUP Oxford University Press

PWR Pressurised Water Reactor

RES Royal Economic Society

SIAD Society of Industrial Artists and Designers

SRD Safety and Reliability Directorate of UKAEA

SRP Society for Radiological Protection

SRS Systems Reliability Service, unit of the National Centre of Systems Reliability in the UKAEA

UKAEA United Kingdom Atomic Energy Authority

USAEC U.S. Atomic Energy Commission

WHO World Health Organisation

---

22 REFERENCES

Ablitt, J. F. (1960) Guide to Safety Report Requirements, Series of 5 Reports, AHSB/UKAEA, Culcheth, Lancs.

Aitken, A. (1977) 'Quantitative approach to reliability of control and instrumentation systems', Nuclear Reactor Safety (Ed. F. R. Farmer), Academic Press, New York, London, 105-107.

Altman, D. G. (1980) Misuse of statistics is unethical, BMJ, 280, 1182-1184.

American Physical Society (1975) Report to the Society by the Study Group on Light-water Reactor Safety, Reviews of Modern Physics - Supplement No. 1, 47, p. S.5.

Anderson, Ronald T. et al. (1982) 'Reliability Concepts and Definitions', Electronic Engineers Handbook, 2nd Ed., Fink and Donald Christiansen, New York, Chap. 28.3.

Archer, Bruce (1979) Design as a Discipline, Design Studies, 1, 17-20.

Arnold, V. I. (1984) 'Singular Mathematics', Review by B. Goodman of author's book on Catastrophe Theory, Nature, 309, 93-94.

Atherley, G. & Booth, R. (1975) Could there be another Flixborough? Sunday Times, 14 Sept., 61.

Austin-Morris Type Fault (1978) Safety check on 20,000 Minis, Daily Telegraph, 15 Dec., 2.

Bacon, Hilary & Valentine, J. (1981) Power Corrupts: The aruguments against nuclear power, Pluto Press, London.

Barankin, E. (1956) Towards an objectivist theory of probability, 3rd Berkeley Symp. on Maths, Stats and Probability, Vol. V, Univ. California Press, 21-52.

Barlow, H. B. (1983) Intelligence, guesswork, language, Nature, 304, 207-209.

Bell, G. D. (1977) 'The Calculated Risk' - A Safety Criterion, Nuclear Reactor Safety (Ed. F. R. Farmer), Academic Press, New York, London, 50.

Beninson, D. et al. (1969) Estudio de un caso de irradiacion humana accidental, Symp. Handling Radiation Accidents, WHO/IAEA, Vienna, 415 -.

Beninson, D. (1984) RA-2 Criticality Accident and Radiological Consequences, NRPB Seminar, 4 Sept.

Bennet, Glin (1983) Beyond Endurance, Secker & Warburg, London.

Bignell, V., Peters, G. & Pym, C. (1977) Catastrophe Failures, Open University Press, Milton Keynes.

Biles, M. B. (1969) Characteristics of radiation exposure accidents, Symp. Handling Radiation Accidents, IAEA, Vienna, 3-18.

Birkhofer, A. (1979) The German Risk Study: Summary, Gesellschaft für Reaktorsicherheit (GRS), Köln.

Bishop, R. E. D. (1963) On the teaching of design in the Universities, Proc. IMechE, (Ed. & Training Group), 177, 719-774.

Black, S. C., Niehaus, F. & Simpson, D. (1979) How safe is 'Too' safe? IIASA, Report WP-79-68, Laxenburg, Austria.

Blackett, P. M. S. (1962) Studies of War: Part II, Oliver & Boyd, Edinburgh & London.

Blake, William (1808) Preface to 'Milton'.

Blakeslee, T. R. (1980) The Right Brain: A new understanding of the unconscious mind and its creative powers, MacMillan Press, London. (See also Skoyles, J. R. - 1984, Springer, S. & Deutsch, G. - 1981.)

Borel, Emile (1950) Elements of the theory of probability (Trans. J. E. Freund), Prentice-Hall, New Jersey, 57.

Bortkiewicz, Ladislaus von (1898) Das Gesetz der kleinen Zahlen, Leipzig (See Keynes, J. M. - 1922, pp. 439-443).

Bourke, Vernon J. (1967) Augustine's view of reality, Villanova Press, Villanova, Pa, USA.

Bowen, J. H. (1976) Individual risk vs public risk criteria, Chem. Engineering Progress, 72, 63. (Excerpt Lees, F. P. - 1980).

Boyle, R. (1661) The Sceptical Chymist, F. Cadwell for F. Crooke, London.

Braunbek, Werner (1974) Planck, Max, Encyclopaedia Britannica: Macropaedia, Vol. 14, Chicago, 490(b).

Brobrovnikov, O. P. et al. (1969) Assessment of the probability of radiation accidents in nuclear power stations (in Russian), Symp. Handling Radiation Accidents, WHO/IAEA, Vienna, 471 - .

Bryan, W. M. (1974) Probability analyst calls Rasmussen accident study futile. Nucleonics Week, 14 April, 15.

Bryan, W. M. (1975) Simulated reliability experience in NASA 'Apollo Moon-shot' program, private communication, 5 November.

Calder, J. W. (1974) Report on the cause of and circumstances attending the overwind which occurred at Markham Colliery, Derbyshire, HMSO, Cmnd 5557.

Charlesworth, F. R. & Gronow, W. S. (1967) A summary of experience in the practical application of siting policy in the U.K., Symp. Containment and Siting of Nuclear Power Plants, IAEA, Vienna, 143 - .

Chicken, John C. (1982) Nuclear Power Hazard Control Policy, Pergamon Press, Oxford.

Chilver, Sir Henry (1977) Fitting Flixborough into a pattern, Nature, 265, 494-495.

Civil Service Commission (1959) Call for inspectors for Inspectorate of Nuclear Installations, Recruitment Circular S5061/59, Scientific Branch, London.

Comte, Auguste (1825) 'Philosophical Considerations on the Sciences and the Savants' (4th Essay), The crisis in industrial civilisation: Early Essays (Trans. Henry Dix). Hutton - Longman, London, 1877; also Heinemann, London, 1974.

Cotgrove, S. (1979) Catastrophe or Cornucopia? New Society, 47, 683-684, 859.

Cotgrove, S. (1982) Catastrophe or Cornucopia: The Environment, Politics and the Future, John Wiley, Chichester, New York.

Cottrell, Sir Alan (1976) The voice of the engineer in public policy, 21st Graham Clark Lecture, CEI, London.

Cottrell, Sir Alan (1980) 'PWR unlikely to be safe', says metallurgist, Nature, 283, 805.

Cottrell, Sir Alan (1982) The pressure on nuclear safety, New Scientist, 93, 773-776.

Cox, H. R. - The Lord Kings Norton (1973) Engineering and Design, Lecture SIAD, The Design Centre Bulletin, Mon. 21 May.

Coxon, T. (1971) The design of nuclear plant with internal coolant circuits as related to the Maximum Credible Accident approach, 4th Conf. Peaceful Uses of Atomic Energy, Geneva, 227-240.

Crick, M. J. & Linsley, J. F. (1983) An assessment of the radiological impact of the Windscale Reactor Fire of 1957, NRPB Report R135, HMSO.

Critchley, O. H. (1962) Some thoughts about criteria for fuel element temperature assessment in Calder type nuclear reactors, NII-R/19/62 (See Annex, Doc. No. 5, Temperature Control of the Magnox Heat Engine).

Critchley, O. H. (1965) A quantitative philosophy for nuclear power station safety assessment, INI Reactor Safety Note No. 5419, June, (Unpublished paper, restricted circulation to Industry).

Critchley, O. H. (1976) Risk prediction, safety analysis and quantitative probability methods - 'a caveat', JBNES, 15, 18-20.

Critchley, O. H. (1977) Nuclear Hazard Control: A new style of safety regulation, Report from a Simon Fellowship: 1974-1976 (unpublished).

Critchley, O. H. (1978) Aspects of the historical, philosophical and mathematical background to the statutory management of nuclear plant risks in the United Kingdom, Conf. Radiation Protection in Nuclear Power Plants and the Fuel Cycle, BNES, London, 11-18.

Critchley, O. H. (1980) Inspection and its role in the case for nuclear power, Meeting Directions in Nuclear Engineering Research, INucE, Paper 201.

Critchley, O. H. (1981) Technological progress, safety and the guardian role of inspection, Science and Public Policy, 8, 291-307.

Critchley, O. H. (1982) Energy, Engineering Inspection and the Safe Use of Nuclear Power, RISK: A Seminar Series, IIASA, Laxenburg, 515-562.

Culliton, Barbara & Waterfall, W. K. (1979) Person-rems and the future: Studies at Three Mile Island, BMJ, II/1979, 375-376.

Daily Telegraph (1973) Magnox reactor core corrosion problems, 26 Feb., 6. (Newspaper).

Daily Telegraph (1976) Rolls-Royce motorcar reliability claim, 5 March, 6-7. (Newspaper).

Dale, G. C. & Harrison, J. R. (1971) 'Fire Risk Criterion', 5. Safety in Operation, Safety of Nuclear Power Plants, Vol. III, 4th Conf. Peaceful Uses Atomic Energy, Geneva, 147.

Davies, L. Myrddin (1979) The Three-Mile Island Incident, Atomic Energy Technical Unit Brochure, UKAEA, Harwell, Oct.

Dickson, David (1974) Alternative Technology, Fontana/Collins, Glasgow.

Douglas, Mary & Wildavsky, A. (1982) Risk and Culture, U. Calif. Press.

Duckham, Helen and Baron (1973) Great Pit Disasters, David and Charles, Newton Abbot.

Edwards, J. (1982) Sizewell 'B' Power Station Public Inquiry, Nuclear Engineer, 23, 119-121.

Ehrenberg, W. (1977) Dice of the Gods, Marianne Ehrenberg and Birkbeck College, London.

Embrey, David E. (1976) Signal Detection Theory and Optimisation of Industrial Inspection Tasks, PhD Thesis, University of Aston in Birmingham.

Eves, Edward (1979) 75 years of motoring excellence, Eldorado Books, London.

Farmer, F. R. (1964) Reactor safety analysis as related to reactor siting, 3rd Conf. Peaceful Uses Atomic Energy, Vol. 13, Geneva, 405 -.

Farmer, F. R. (1967) Siting criteria - a new approach, Symp. Containment and Siting of Nuclear Power Reactors, IAEA, Vienna, 152-170.

Farmer, F. R. et al. (1970) Quantitative Safety Analysis, Nuclear Engineering and Design, 13, 183-244.

Farmer, F. R. (1975) Advances in the reliability assessment of reactor systems, ATOM (UKAEA House Journal), No. 230, 218-226.

Farmer, F. R. (1975 - 2) Accident Probability Criteria, JINucE, 16, 44-46 & 50.

Farmer, F. R. (1977) Today's risks: Thinking the unthinkable, Nature, 267, 92-93.

Farmer, F. R. (1978) What is acceptable risk? Conf. Acceptance Occupational Risk, International Fire, Security and Safety Exhib., Olympia, London, April, Paper 1.

Farmer, F. R. (1979) Nuclear Decisions, Nature, 278, 393.

Farmer, F. R. - Editor (1977) Nuclear Reactor Safety (Compendium), Academic Press, New York and London.

Farrington, Benjamin (1947) Greek Science, Vol. 1 (1944) p. 13 & Vol. 2 (1949) pp. 7-8, Penguin Books, Harmondsworth.

Feilden, G. B. R. (1963) Engineering Design, HMSO for DSIR.

Financial Times (1982) GPU sues Babcock and Wilcox for $ 4bn, 2 Nov., 6. (Newspaper).

Finetti, Bruno de (1972) Probability, Induction and Statistics, John Wiley, London and New York.

Finniston Committee (1980) Engineering Our Future, HMSO, Cmnd 7794.

Fischhoff, Baruch et al. (1981) Acceptable Risk, CUP.

Fishlock, David (1975) Questions over the future of nuclear power, Financial Times, 30 May, 10.

Fishlock, David (1979) Repair delays shut two nuclear reactors at Dungeness, Financial Times, 4 May, 1.

Flight (1915) Advertisement for AID staff, 23 July, VII, 537. (Magazine).

Flood, M. & Grove-White, R. (1976) Nuclear Prospects: a comment on the Individual, the State and Nuclear Power, Friends of the Earth et al., London, 1976.

Flowers, Sir Brian (1976) Sixth Report of the Royal Commission on Environmental Pollution: Nuclear Power and the Environment, HMSO, Cmnd 6618:
Specific references - (a) S.165-167, (b) S.289-290, (c) S.276, 283-286.

Fowler, D. H. (1975) Structural stability and morphogenesis: an outline of a general theory of models (Translation of René Thom's work), W. A. Benjamin, Reading, Mass.

Fremlin, J. H. (1979) Nuclear detective story, Nature, 282, 157.

Gardner, Howard (1984) Frames of Mind, Heinemann, London.

Gausden, R. (1979) Nuclear Establishments 1977-1978, Health and Safety Executive, HMSO.

Gausden, R. (1982) Nuclear licensing practices and procedures, Nuclear Engineer, 23, 141-145.

Gausden, R. (1982 - 2) Nuclear Safety: HM Inspectorate of Nuclear Installations Safety Assessment Principles for Power Reactors (3rd Ed.) HMSO, London.

George, Brian (1982) UK nuclear power: BYE BRITISH, Nature, 297, 96.

Gittus, J. & Matthews, R. (1984) Microcomputers 'will make Sizewell safe', New Scientist, 101, 6.

Glazebrook, R. T. (1913) Report of the Departmental Committee on accidents to monoplanes: 1912, HMSO, Cmnd 6506.

Gloag, Daphne (1980) Risks of low-level radiation - evidence of epidemiology, BMJ, 281, 1479-1482.

Gofman, J. W. & Tamplin, A. R. (1973) Poisoned Power, Chatto and Windus, London.

Goodman, G. T. & Rowe, W. D. (1979) Energy Risk Management, Academic Press, London.

Gowing Margaret (1974) Britain and Atomic Energy 1945 - 1952, Independence and Deterence, Policy Execution, Vol. II, MacMillan, London, 91-115.

Specific reference - (a) pp. 8-50.

Green, A. E. & Bourne, A. J. (1972) Reliability Technology, John Wiley, Chichester, New York.

Green, D. M. & Swets, J. A. (1974) Signal Detection Theory and Psychophysics, John Wiley, New York, London.

Griffiths, T. (1966) Private communication on philosophy of inspection for safety regulation of nuclear power as a major hazard industry.

Gronow, W. S. & Gausden, R. (1975) Licensing and regulatory control of thermal power reactors in the United Kingdom, Symp. Licensing and and Regulatory Control of Nuclear Installations (Legal Series 10), IAEA, Vienna, 205-221:

Specific references - (a) p. 213, (b) p. 205-221.

Groves, Leslie R. (1963) Now it can be told - the story of the Manhattan Project, Harrap Bros, New York.

Haefele, Wolf (1974) Hypotheticality and the new challenges: The pathfinder role of nuclear energy, Minerva, 12, 303-322.

Halliday, P. (1982) The Three Mile Island incident - Reactions from Overseas, Nuclear Engineer, 23, 44-49.

Hammer, J. G. D. (1980) Health and Safety: Manufacturing Industries - 1980, HMSO for HSE.

Hanauer, S. H. & Morris, P. A. (1971) Technical Safety Issues for Large Nuclear Power Plants, 4th Conf. Peaceful Uses of Atomic Energy, Vol. III, Geneva, 205.

Hayzelden, J. E. (1968) The value of human life, Public Administration, 46, 427-441.

House of Lords (1976) Parliamentary Debates; Lords, Vol. 367, Col. 1216, 29 Jan.

Hume, David (1748) Enquiry concerning human understanding, C. W. Hendel (Modern Edition), New York, 1955.

IAEA Report (1981) Annual Report for 1981: Nuclear Power, IAEA, Vienna (1982 publication), S. 74, 26.

ICRP Publication 9 (1965) 'Acceptable Risk', S. 34 - 39.

Johnson, L. Marvin (1970) Quality assurance program evaluation, Stockton-Doty Trade Press, Whittier, California.

Keynes, John Maynard (1922) Collected Writings, Vol. VIII: Treatise on Probability, MacMillan for RES, London, 1975:

Specific references - (a) p. 443, (b) p. 368, (c) pp. 427-433, (d) pp. 364-368 & 427-443.

Keynes, John Maynard (1936) The General Theory of Employment, Interest and Money, MacMillan Press (New Edition), London, 298.

Kirk, J. & Taylor, R. S. (1971) Design for the Safety of Gas-Cooled Reactor, 4th Conf. Peaceful Uses of Atomic Energy, Vol. III, Geneva, 160.

Kletz, Trevor A. (1976) 'Application of Hazard Analysis to Risks to the Public at Large', Chemical Engineering in a Changing World (Ed. W. T. Koetsier), Elsevier, Amsterdam, 397-412.

Kletz, Trevor A. (1977) What risks should we run? New Scientist, 74, 320-322.

Kletz, Trevor A. (1982) Safety Newsletters: No. 1 (1972) to No. 157 (1982), Petrochemicals and Plastics Division, Imperial Chemical Industries, Wilton, Middlesborough, Cleveland.

Komanoff, Charles (1980) 'Cost escallation at U.S. nuclear power stations', Energy Committee, House of Commons, Minutes of Evidence, Government Statement on the new Nuclear Power Programme, Wed. 12 March, House of Commons Paper, HC 397-v.

Kunreuther, Howard (1980) Societal Decision Making for Low Probability Events: Descriptive and Prescriptive Aspects, WP-80-164, IIASA, Laxenburg, Austria, 15-16.

N.B. Cleveland LNG explosion, see also F. P. Lees (1980), Case history 'b'.

Kunreuther, Howard (1982) RISK: A Seminar Series, IIASA, Laxenburg, Austria.

Laceby, M. A. (1976) The approach to safety in the aeronautical industry, private communication, May 21.

Laws, Frank A. (1917 & 1938) Electrical Communications, McGraw-Hill, New York, London (2 Editions).

Lee, T. R. et al. (1982) Report of Study Group on Risk Assessment, Royal Society, London, Nov., S. 5.11.

Lees, F. P. (1980) Loss Prevention in the Process Industries, 2 Vols, Butterworths, London.

Case Histories: Selected Events, Vol. 2, Appendix 3:

(a) A1, pp. 887 & 897 – Oppau At 7.29 and 7.32 am on 21 Sept. 1921, two terrific explosions occurred in the Oppau works of Badische Anilin und Sodafabrik. 1000 houses destroyed, 70% of the works and a crater some 250 ft in dia. and 50 ft deep created. The explosions involved some 4500 t. of 50:50 mixture of ammonium sulphate and ammonium nitrate. Detonations set off by blasting powder which was being used to break up storage piles of material which had become caked, a procedure which had been carried out without mishap some 16,000 times previously. The explosions killed 430 people including some 30 in the village.

(b) A2, pp. 897-898 - Cleveland, Ohio At approximately 2.40 pm on 20 October 1944 a cylindrical LNG storage tank at the Liquefaction and Regasification Plant of the East Ohio Gas Co. at Cleveland, Ohio, ruptured and discharged its entire contents over the plant and the nearby urban area. The LNG vapour ignited almost immediately causing great loss of life and extensive damage. More LNG flowed into the storm sewers where it mixed with air and exploded. The final death toll was 128 and the number injured was estimated at 200-400, the greatest loss occurring in the plant area.

Lester, G. & Rothman, H. (1977) Signals of the Future, R & D Management, 7, 89-100.

Levi, Isaac (1980) The enterprise of Knowledge: an essay on Knowledge, Credal Probability and Chance, MIT Press.

Lewis, H. W. et al. (1978) Risk assessment review group report to the U.S. Nuclear Regulatory Commission, NUREG/CR-0400, NRC, Washington, D.C.

Linnerooth, Joanne (1981) The Value of Human Life: A Review of Models, RR-80-25, IIASA, Laxenburg, Austria.

Locke, J., Dunster, J. H. & Pittom, Audrey (1978) CANVEY: an investigation of potential hazards from operations in the Canvey/Thurrock area, HMSO for HSE.

Lord, Walter (1976) A night to remember: the sinking of the Titanic, Allen Lane (Penguin Books), London.

Lovins, A. B. (1974) World Energy Strategies - Facts, Issues and Options, Ballinger for Friends of the Earth, London.

Lowrance, W. W. (1976) Of acceptable risk, William Kaufman, Los Altos, California.

McLain, Lynton (1977) Conviction may leave your firm wondering how it broke the law, The Engineer, 244, 32-33.

McNicol, D. (1972) A primer in signal detection theory, Allen and Unwin, London.

McWhirr, A. et al. (1982) Romano-British cemeteries at Cirencester, book reviewed by Peter Deeley, Observer, 28 November, 5, under heading 'Romans killed by lead'.

Maddox, John (1984) No end to nuclear decay? Nature, 307, 581.

Maistrov, L. E. (1974) Probability Theory: A Historical Sketch (Trans and Ed. by Samuel Kotz), Academic Press, New York, London:

Specific references - (a) p. 160, (b) p. 123, (c) p. 56 , (d) p. 18.

Malherbe, M. C. de & Ogorkiewicz, R. M. (1962) Design studies to aid the teaching of synthesis, Chartered Mech. Engineer, 9, 317-320.

Malherbe, M. C. de & Solomon, P. J. B. (1963) Mechanical engineering design tuition at Universities, Proc. IMechE, 178(Pt I), 779-808.

Mahon, Hon. Justice (1981) Mount Erebus Air New Zealand disaster, see Maurice Shadbolt (1984) and Gordon Vette (1982).

Marchetti, C. (1974) Hydrogen and nuclear energy, JBNES, 13, 353-362.

Meekcoms, K. J. (1980) The birth of aeronautical inspection and British aeronautical inspection between 1936 and 1945, AQD, Harefield, Middlesex, Feb. & Sept.

Mellor, David (1982) Sizewell's first skirmish, New Scientist, 94, 686-687, 689.

Milner, M. J. (1983) Quality assurance in the nuclear industry, Nuclear Engineer, 24, 170-176.

M.I.T. (1956) Report of the M.I.T. Committee on Engineering Design, Nov. 1956 (Cited by M. C. de Malherbe) Proc. IMechE, 177, 727.

Morgan, Karl Z. (1978) Cancer and low level ionising radiation, Bulletin of Atomic Scientists, 34, 30-41.

Mould, R. F. (1980) A history of X-rays and radium 1895-1937, IPC Building and Contract Journals, Sutton, Surrey.

Moulton, A. (1976) Engineering Design Education, Engineering, Design Council, April.

Nature - Editorial (1980) 'Let there be Light', Nature, 284, 588-589.

Nader, Ralph with J. Abbotts (1979) The Menace of Atomic Energy, W. W. Norton, New York.

Nelkin, Dorothy (1982) Blunders in the business of risk, Nature, 298, 775-776.

New York Times (1921) 1,000 to 1,500 perish as blast wrecks German dye plant, The New York Times, Sept., 22, 1.

N.B. Oppau disaster - see also F. P. Lees (1980) Case history 'a'.

Nuttall, A. K. (1946) 'Quality enhanced generally by AID presence in works', private communication from Chief Radar Engineer, Metropolitan-Vickers.

Oudet, L. (1960) Radar and collision (Trans. Rene´ Hague), Hollis and Carter, London.

Page, Talbot (1978) A generic view of toxic chemicals and similar risks, Ecology Law Quarterly, 7, 207-244.

Page, Talbot (1979) " 'Keeping Score': an actuarial approach to zero-infinity dilemma", Energy Risk Management (Ed. Goodman and Rowe), Academic Press, London, New York, 177-186.

Papon, Pierre (1979) Why France has had no public nuclear debate, Nature, 281, 94-95.

Parker, Roger Jocelyn (1975) The Flixborough disaster: Report of the Court of Inquiry, HMSO for Department of Employment:

Specific references - (a) S. 15, (b) S. 27, 28.

Parker, R. J., The Hon. Mr Justice (1978) The Windscale Inquiry: Report to the Secretary of State, HMSO for the Department of Environment, S. 11.24 & S. 17, Recommendation 12.

Pasquill, F. (1962) Atmospheric diffusion and dispersion of windborne material form industrial and other sources, Van Nostrand, London, also Horwood, Chichester, 1974.

Poisson, Siméon D. (1837) Reserches sur la probabilité des jugements en metière criminelle et matière civile, precédées des règles générales du calcul de probabilités, Bachelier, Paris.

Popper, K. & Miller, D. (1983) A proof of the impossibility of inductive probability, Nature, 302, 687-688 & 310, 433-434.

Porter, Robin (1982) The Silent Scourge, TIME, 120, 38-44.

Putnam, Cosslet P. (1954) Energy in the Future, MacMillan, London.

Rasmussen, N. C. et al. (1975) Reactor Safety Study: an assessment of accident risks in U.S. commercial nuclear power plants, WASH-1400, U.S. NRC, Washington, D.C.

Specific references - (a) Appendix XI, S.2.2, Comment 1, (b) Ibidem, S.2.1, Comment 5, (c) Main Report, Attachment 3, (d) Reviews of Modern Physics, 1975, 47, Supplement No. 1 and (a) above, (é) Main Report, Attachments 1 and 3, (f) Ibidem, S.6, 174.

Rasmussen, N. C. (1975 - 2) The Safety Study and its feedback, Bulletin of Atomic Scientists, 31, 25-28.

Ravetz, J. R. (1974) The safety of safeguards, Minerva, XII, 323-325.

Ravetz, J. R. (1976) Superstar Technologies, Barry Rose for the Council for Science and Society, London.

Ravetz, J. R. (1977) The political economy of risk, New Scientist, 75, 598-599.

Ravetz, J. R. (1977 - 2) The Acceptability of Risks, Barry Rose for the Council for Science and Society, London.

Reissland, J. & Harries, W. (1979) Scale for measuring risks, New Scientist, 83, 809-811.

Reymond, Arnold (1955) Histoire des Sciences Exactes et Naturelles dans L'antiquité Gréco-Romaine (2nd Ed.), Presses Universitaires des France, Paris. Also as 'Greek Science in Antiquity' (Trans. Ruth Ghoury de Bray), Methuen, London, 1927.

Rhodes, Gerald (1981) Inspectorates in British Government, Allen and Unwin, London:

Specific reference - (a) pp. 3-9.

Ritchie-Calder, Lord Peter (1969) 'Safest industry in the World', Parliamentary Debates, Lords, Vol. 305, Col. 792, 13 Nov.

Robens, Lord (1972) Safety and Health at Work: Report of the Committee 1970-1972, HMSO, Cmnd 5034:

Specific references - (a) S. 28, (b) S. 339 & 485, (c) S. 37.

Roberts, A. & Tregonning, K. (1980) The robustness of natural systems, Nature, 288, 265-266.

Rogovin, M. & Frampton, G. T. Jr (1980) Three Mile Island, Vol. I - A Report to the Commissioners and the Public, Special Inquiry Group, Div. Tech. Information and Document Control, U.S. NRC, Washington, D.C.

Roskill Commission (1971) Report of the Commission on the Third London Airport (10 Vols), HMSO for Min. Housing and Local Govt.

Roszak, T. (1972) Where the Wasteland ends, Faber and Faber, London.

(Also The Making of a counter culture, Faber and Faber, 1968.)

Rothery Inquiry (1880) Circumstances attending the fall of a portion of the Tay Bridge on 28 December 1879, HMSO, C. 2616.

Rothschild, Lord (1978) RISK: The Richard Dimbleby Lecture, The Listener, 100, 715-718.

Rowe, W. D. (1977) An Anatomy of Risk, Wiley-Interscience, New York, London.

Rowe, W. D. (1979) 'What is acceptable risk and how can it be determined?' Energy Risk Management (Ed. Goodman and Rowe), Academic Press, London, New York, 327-344.

Sale, Kirkpatrick (1980) Human Scale, Secker and Warburg, London.

Sandbach, F. (1980) Environment, Ideology and Policy, Blackwell, Oxford.

Sandia Lab. (1982) New PWR Accident Worst Consequences Report, Financial Times, 2 Nov., 5.

Schwartz, J. (1962) 'The pernicious influence of mathematics on science', International Congress on Logic, Methodology and Philosophy of Science (Ed. Nagel, Suppes and Tarski), Stanford University Press. *

Searle, V. H. (1950) 'Safety Factor', Strength of Materials, Chambers Encyclopaedia, Vol. 13, London, 224(b). 'New' Edition.

Self, Peter (1970) 'Nonsense on Stilts': Cost-benefit analysis and the Roskill Commission, The Political Quarterly, 41, 249-259.

Shadbolt, Maurice (1984) Disaster on Mount Erebus: The Riddle of Flight 901, Reader's Digest, 125, 163-200.

N.B. See also Gordon Vette (1982)

Shaw, J. & Palabrica, R. J. (1974) A critical review and comparison of nuclear power plant siting policies in the U.K. and U.S.A., Annals Nuclear Science and Engineering, 1, 241-254.

Shaw, J. & Sina, A. M. (1976) A quantitative comparison of the nuclear power plant sites in the U.K., Annals Nucl. Energy, 3, 501-513.

Simon, Christopher (1975) 'Flixborough': basic soundness of the Simon-Carves design of the plant, Private communication at Broomcroft Hall, Didsbury, Manchester, Nov./Dec.

S.J.R. (1896) Some effects of X-rays on the hands, Nature, 54, 621.

Skoyles, J. R. (1984) Alphabet and the Western Mind, Nature, 309, 409.

N.B. Letter concerning Left Brain: Right Brain competences, see also T. R. Blakeslee (1980) and Sally P. Springer and Georg Deutsch (1981).

Smith, Anthony (1980) The flight from science, BMJ, 280, 1.

Smyth, H. de Wolf (1947) Atomic Energy for Military Purposes, Princeton University Press.

Snow, C. P. (1959) The Two Cultures and the Scientific Revolution: The Rede Lecture 1959, CUP.

Speth, Gus (1980) Towards a troubled 21st Century, TIME, 116, 42.

Springer, Sally P. & Deutsch, Georg (1981) Left Brain - Right Brain, W. H. Freeman, New York, 1981.

N.B. See also J. R. Skoyles (1984) and T. R. Blakeslee (1980).

S.R.S. (1984) National Centre of Systems Reliability: Brochure by the Systems Reliability Service, UKAEA, Culcheth, WA3 4NE.

Street, H. & Frame, R. (1966) The Law and Atomic Energy, Butterworths, London.

Thedéen, T. (1979) 'The problem of quantification', Energy Risk Management (Ed. Goodman and Rowe), Academic Press, London, New York, 172-175.

Thomas, V. M. & Burgess, H. (1976) Safety Assessment of a Modern Winder Installation, Symp. on Transportation of Men and Materials in Shafts and Underground, Assoc. Mining Elec. and Mining Mech. Engineers, Manchester, Paper 4c, 1-9.

Thompson, Michael (1980) The Aesthetics of Risk: Culture or Context, Mountain, May/June, 73.

TIME (1982) Wreck of the Ocean Ranger, TIME, 119, 17.

Tribe, L. A. (1973) Channeling Technology through Law, Bracton Press, Chicago.

Tucker, Anthony (1980) Who keeps quiet when the reactors are cracking up? The Guardian, 31 Jan., 15.

Vance, H. S. (1957) Theoretical possibilities and consequences of major accidents in large nuclear power plants, USAEC Report WASH-740, Washington, D.C.

Veblen, Thorstein (1921) The engineers and the price system, B.W. Huebsch/Viking Press, New York. (Reprint by Augustus M. Kelly, New York, 1965.)

Vette, Gordon (1982) Impact Erebus, Hodder and Stoughton, Aukland, N.Z.

N.B. Very limited availability in Britain. See also Maurice Shadbolt, 1984.

Warren, J. P. (1982) The 50-year Boom-Bust Cycle, Warren/Cameron, Godalming, Surrey.

Wass, Douglas (1983) Government and the British Civil Service, Reith Lecture Series, BBC, 1982/1983.

Watson, S. R. (1981) On risks and acceptability, JSRP, 1, 21-25.

Weatherall, M. (1982) An end to the search for new drugs? Nature, 296, 387-390.

Weinberg, Alvin (1972) Science and Trans-science, Minerva, 10, 209-222 & 484-486.

N.B. See also Science, 177, 211 and Nature, 273, 93.

Weinberg, Alvin (1977) Is nuclear energy acceptable? Bulletin of Atomic Scientists, 33, 54-60.

Weinberg, Alvin (1978) Trans-science, Nature, 273, 93.

N.B. See also Minerva, 1972, 10, 209-222 & 484-486 and Science, 1972, 177, 211 referred to above.

Weinberg, Alvin (1979) Those who attack nuclear energy show a cynical denial of human ingenuity, Nature, 281, 335.

Werner, Sir Frederick (1982) The Perception of Risks, Risk Assessments: Report of a Study Group, The Royal Society, London.

White, D. J. (1975) Decision Methodology: A formalisation of the O R Process, John Wiley and Sons, London, New York.

Specific references - (a) pp. v, 1 & 2, (b) p. 131.

Williams, Sir Bruce (1981) Centre for Technical Change, British Technology, a new direction, Nature, 289, 110 & 114.

Wilson, R. (1975) The costs of safety, New Scientist, 68, 274-278.

Worthington, N. V. (1961) Fuel element temperature criteria for the operating reactor, CEGB Tech. Memo. 25.

N.B. See also D. Wilkie (1978) The disposition of can temperature thermocouples in a nuclear reactor, Nuclear Energy, 17, 47-56;

G. C. Dale & J. R. Harrison (1971) referred to above, and

O. H. Critchley (1984) Temperature Control of the Magnox Heat Engine, Document No. 5 of Annex.

Wylie, F. J. (1978) The use of radar at sea, Hollis and Carter, London.

Zahler, R. S. & Sussmann, H. J. (1977) Claims and accomplishments of applied Catastrophe Theory, Nature, 269, 759-763.

Zeeman, E. C. (1977) Catastrophe Theory: Selected Papers 1972-1977, Addison-Wesley, Reading, Mass.

Specific reference - (a) pp. 3-8.

N.B. See also New Scientist, 76, 806.

* In a further reference to the theme of J. Schwartz (1962) above see T. Mulvey, The pernicious influence of mathematics, Physics in Technology, 1976, 7, 186.

23 ANNEX

SUPPORTING PAPERS FROM PUBLISHED WORKS

Document Number	Title	Pages
1	Risk prediction, safety analysis and quantitative probability methods - a caveat. J. Br. Nucl. Energy Soc., 1976, 15, 18-20.	355-358
2	Aspects of the historical, philosophical and mathematical background to the statutory management of nuclear plant risks in the U.K.: Symp. on Radiation Protection in nuclear power plants and the fuel cycle, Br. Nucl. Energy Soc., London, 1978, Vol. 1, 11-18.	359-367
3	Inspection and its role in the case for Nuclear Power. Meeting on Directions in Nuclear Engineering Research at Cambridge, Sept. 1980, Inst. Nuclear Engineers, London, 1980, Paper No. 201.	368-378
4	Technological progress, safety, and the guardian role of inspection. Science and Public Policy, 1981, 8, 291-307.	379-396
5	Thermal Control of the Magnox Heat Engine. An abridged revision of an Inspectorate of Nuclear Installations Report, INI/R/19/62, prepared for and published by the Ministry of Power, Millbank, London, October 1962 - Edited version dated July, 1984.	397-432

DOCUMENT NUMBER 1

RISK PREDICTION, SAFETY ANALYSIS AND QUANTITATIVE PROBABILITY METHODS - A CAVEAT

Synopsis - A critique of attempts to displace the qualitative philosophy of technical design safety assessment that has been evolved in the nuclear power industry and is characterised by the design basis concept of a maximum credible accident (MCA) with a quantitative systems methodology. This initiative is criticised from an objectivist standpoint on grounds of the metaphysical nature of the very low failure rate probabilities educed, the inherent instability of the data base and the failure to take the design-to-construction interface and the incidence of human error properly into account. Eight criteria for data validation are proposed and a plea is made for a pragmatic strategy of design assessment and safety management that combines the proven worth of the MCA with the quantitative methods and other mathematical tools in a rational balance.

On an ethical note, the orientation of the quantitative systems approach towards appraisal of technological risks in terms of lethalities rather than by a pursuit of safety through excellence in engineering is denigrated. Moreover, the proposition that the inevitable, but essentially trivial, low level environmental pollution emanating from a nuclear power plant can be merged with the consequences of a very unlikely, but nonetheless possible, major radiation accident is seen as an undesirable tendency in radiological protection. It is deceptive and could lead to policies deriving from expediency rather than from a due concern for public safety. Moreover, by positively linking detriment on the one hand with investment in protective measures on the other an economic criterion is established that could lead to a progressive reduction in safety standards below the high levels now expected in matters of protection of the public.

J. Br. Nucl. Energy Soc., 1976, 15, Jan., No. 1, 18-20

Correspondence

Risk prediction, safety analysis and quantitative probability methods—a *caveat*.

O. H. Critchley*

Nuclear engineering is notable not only for its internal concern with safety, but also for the effectiveness of the practices which it has evolved and for the impact which these have had and are still having elsewhere in safety technology. It is reasonable then to suggest that certain current attempts to introduce a mathematical methodology which would substantially modify or even replace long-standing and proved procedures should be carefully examined before the initiative receives general acceptance I refer to the increasing use of quantitative techniques as the determinant of value judgements in nuclear safety assessment, hazard evaluation and risk prediction.

It would be trite to do more than note the influence which numbers have had upon man and the importance of their role in policy-making. While their precision and certainty are essential to the conduct of human affairs, their magic has beguiled and often misled the great—not the least, Pythagoras (though today we are perhaps more rational than he). The quotation of figures can swing the course of an argument, not always wisely, and even Mark Twain in his day was sceptical of the intrusion of numbers into politics, distinguishing 'lies, damned lies and statistics'.[1]

It would be stupid to deny the important role which numerical methodologies have played in nuclear plant safety assurance in the areas of reliability and design optimization. Nevertheless, it is not unreasonable to sound a note of caution when these attempts to quantify value judgements intrude into realms of nuclear safety where factual data is notoriously weak and personalities and politics are notably strong On the other hand, criticism which springs merely from a nostalgic attachment to the old ways is worthless.

There has long been in use[2,3] a group of broadly similar analytical methods of design guidance known severally as 'the design basis accident', 'the maximum credible accident', 'the maximum hypothetical accident' and so forth. They have formed a basis for nuclear plant safety analysis and are related to a concept of design, construction and maintenance of components, systems and plant and of continuing operation and surveillance to such standards of excellence that failure may be deemed 'incredible'.

The methods drew limited support from operational research in appropriate areas. This provided artifices such as the 'fire risk criterion' in the Magnox stations which prescribed an upper safe limit for the operating temperature of the fuel[4,5] and logic for assessing the provision of sufficient control rods to assure certainty of pile shutdown. Reliability methods were also widely used in the design, safety assessment and proofing of electric and electronic control and safeguarding systems.

This simple synthesis served the industry well during the first cycles of nuclear power station building in the UK. However, in its simple form it appears to be less than adequate in application to more advanced nuclear plant where a dangerous fault sequence can lie hidden in the complexities of the design or it is necessary to apportion investment among the parts of a diversified safeguarding provision.

An intriguing aspect of the new numerical methodology being proposed is its seeming presentation of reactor risks as quantified lethality, attributing a prospective number of deaths and malignancies to a given nuclear power programme. Such notions of harm are among the findings of the US Rasmussen study[6] and of certain other similar initiatives elsewhere. The problem of nuclear safety, as indeed that for safety assurance in the face of any other major technological hazard, has two poles, namely, dangers and safeguards, the task being to design out the first and to ensure compliance with the second. Accidents grow on apathy: safety on vigilance. Indeed, slackness in matters of radioactivity in general and in nuclear power in particular could undoubtedly give rise to an unacceptable toll of harm. In spite of this the Rasmussen brief pays scant attention to vigilance. Maybe its philosophy is affected by the acknowledged coupling of its approach to that used for safety and quality control assessment of space missions and military hardware. For any technological initiative there is an acceptable risk related to the objectives which it aims at achieving and to that part of the environment and population on whom harm may be inflicted. In exploration and even in the passive use of military might, safety lies in successfully skirting the brink of disaster. In civil affairs it lies in pushing safeguards and surveillance to reasonable limits of economic tolerance.

There is also a strange bias in the Rasmussen criteria for accident selection, as perhaps the most dangerous of all, reactor pressure vessel failure, is dismissed as too small 'to contribute to the overall risk'.[7] But it could happen: unquantifiable without doubt, immensely disastrous—yes, impossible—no.

Reliability methods make an essential contribution to technical design management in electronic control, computers, military hardware, aircraft and in many other applications However, these are all notable as manifold replication industries where the axioms, on which the statistical and probability techniques stand, are met. Criteria for meaningful application of the methods are that

(*a*) performance requirements for the plant and its subsystems must be clearly and finally specified:
(*b*) manufacture and construction of the components, subassemblies and the plant must be verified by inspection to be according to specification;
(*c*) the materials used in all aspects and phases of manufacture and construction must comply with relevant specifications and come from quality-assured supply;
(*d*) failure rate data must be drawn from verifiable sources established by user experience and/or realistic and reproducible tests;
(*e*) such data when it is drawn from inferences deriving from observation of the performance of analogous systems does not meet criterion (*d*) and therefore must have an appropriate uncertainty factor attached to it;

* Simon Fellow, University of Manchester on secondment from the Nuclear Installations Inspectorate of the Health and Safety Executive. (The views expressed are the personal opinions of the writer.)

(*f*) the sources of all data must be accessible for verification and the confidence limits or uncertainty factors must be stated;
(*g*) an independent analyst using the data must compute a similar figure or figures; and
(*h*) there must be enough user experience so that all credible faults and failures have occurred or the sequences leading to them have been identified.

Although the internal decision logic of such statistical and probability methods may be impeccable, there is doubt about their meaningful extrapolation into the realms of safety analysis, risk prediction and design guidance in respect of plant which is largely experimental or prototype. Even when constructed in nominally similar groups, such plant exhibits variations introduced to meet local site situations which render each unit largely unique. The methods will be unreliable if the axioms on which the decision logic is structured are not true. Further, owing to the paucity of the failure rate data in respect of novel or 'one-off' features, the confidence limits may be so wide that predictions are of little substance.

No high-risk, major-hazard, safety-assured plant like a nuclear reactor should be built unless it is so well designed, constructed and operated that disastrous failure cannot be foreseen in the anticipated circumstances of its existence: that is, such an event must be 'incredible'. Thus, the permitted net chance of occurrence of a catastrophic radiation accident arising from any envisaged cause must tend to be vanishingly small. A risk so forecast cannot be true. The true hazard is given by the summation of the occurrence probabilities of all accident-producing causes which includes an almost infinite spectrum of unexpected, unusual or highly improbable though possible happenings or coincidences. At the present time, at least, the task of catching such a large number of rare, random and diverse things is Sisyphean. There is, thus, a severe limitation on the input data which vitiates any quantitative predictions, and such serious accidents as might occur will be most likely to be 'rogue' events which would not be identified in the quantifier's philosophy. For example, quantitative predictions of explosion risks for the Flixborough factory based on its design and 'reliability data' would have had little bearing on what in fact happened[9] as the causes of the disaster are attributable to a management weakness.[9,10] The recent nuclear power station failure at Browns Ferry is a similar example of a serious incident precipitated by a freak cause.[11]

It is therefore not surprising that the threatened excursion of quantified decision theory into nuclear plant design and safety analysis has been viewed with misgivings by many experienced engineers, some of whom have published their doubts.[2,12,13] In fact not even 'Rasmussen' is fully confident of its validity.[14]

Support for the foregoing strictures has also been expressed by William Bryan, an experienced safety engineer who spent some ten years in the US space programme as a safety analyst and reliability expert. He has stated that the much-publicized Rasmussen study is 'an exercise in futility' whose methods have long since been discarded in the aerospace industry as useless for developing the kind of probability numbers the Rasmussen group seek.[15] This is rather extreme as it excludes certain positive outcomes of the study. It presents a way of making a thorough, consistent and wide-ranging safety appreciation of highly complex, major-hazard plant. Indeed, many protagonists of it justify their acceptance for just this reason, even though sceptical of the validity of the figures. No doubt this aspect has its value. The question left is whether this 'spin-off' is really in the ultimate such an efficient and effective way of disclosing design weaknesses and subtle failure modes or whether better methods could be developed which do not have the primary objective of making numerical predictions.

Also questionable are concomitant methods of population dose evaluation which group together releases of radioactivity to the environment from unrelated sources. On the one hand are those which are authorized during the operation of the plant or will arise from unplanned but unavoidable minor radiation handling accidents. This relatively small effusion of radioactivity will properly be a major design factor and can be reasonably attributed to a nuclear reactor during its life. It is possible for it to be controlled downwards if need be. On the other hand are those massive releases which might occur as the result of a major plant disaster. To bridge the innate discontinuity in a logic which sums the products of events which may be reasonably expected to happen with those which must not, there is an implicit postulation of inevitability of occurrence of the untoward and forbidden. While no plant, however well built and managed, can be expected to run absolutely risk-free, this philosophy of accepting disasters so as to make prophecies about the harm which may be attributed to a nuclear power programme is questionable. Nuclear plant designers and safety engineers must be guided by an aim which secures that major plant disasters do not occur. Their designs and precautions must make them 'incredible'. Of course, experience in safety has shown that there is very little which is impossible. For this reason, the worst consequences of a plant accident must be known, not as a basis for safety philosophy, but as a guide for siting, emergency planning and damage control needs. If such an untoward catastrophic event occurs, it should be in spite of human endeavours and not because of failure which could be attributed to a permitted weakness in design.

There are other reasons, more political in nature, which suggest that it is unwise to place reliance on quantitative probability methods of risk assessment and design guidance for nuclear plant at this stage. Efforts directed towards such quantification of value judgements in safety and the mathematical activities necessary to derive them could divert attention from hazard-generating factors outside the assumptions on which the judgements are based. It follows that they could lead to ill-founded confidence in the safety of nuclear plant or, indeed, of other major-hazard installations either in respect of judgements about their ultimate safety or in making comparisons of one system against another. There could thus be an undesirable impact on top level decision making which rests with politicians and administrators but not with engineers.

Another disturbing feature is that figures which give a vanishingly small though really spurious prediction about the chance of occurrence of a major plant or system accident could have the effect of directing design and quality of construction downwards to some quantitatively assessed level of adequacy instead of upwards towards the best reasonably achievable in the state of the art.[16] This tendency could effectively hamper an inspector who would otherwise press for the highest available standards of design and construction which it might be reasonably practicable to attain and for progressive improvements in them. While back-fitting of safeguards is not always feasible and may be undesirable, it is generally agreed that safety must always be forward-looking and move towards a continuing reduction in accident possibilities.

The critical examination set out above does not aim at denigrating reliability analysis or other related studies but

CORRESPONDENCE

merely at cautioning against the unjustified extension of their quantitative aspects to an area to which at this stage they may be inapplicable. Nor is it suggested that there is something wrong with the safety assessment of nuclear reactors or other plant in the UK. Where, as in the case of reactors, major-hazard plant has been subject to a thorough safety appreciation, the operational scene is one of substantially trouble-free working.

However, the problem of safety assessment is made more difficult by the complexities of new designs. It is imperative that these are subjected to searching, thorough, consistent and reproducible safety analysis. Simple techniques such as those based on a maximum credible accident do not appear to be adequate in the case of more complex modern types, e.g., UK pressure tube and fast reactors. It is doubtful if anything of lasting value can be provided by artifices of probability stretched beyond valid limits, even as a spin-off stratagem using the tactics but discarding the numbers.

If such quantitative techniques are to be eschewed, then what can be used instead? No doubt decision theory can provide logical methods which can be developed within the traditional framework. Bourgeois has hinted at a solution[17] and a reference to possible suitable procedures is even given in the Rasmussen study.[18] It seems that the required tool may come from a development of Boolean logic which is applied so successfully to problems of switching in computer peripherals and other devices.

The history of plant disasters is the story of the unexpected often combined with slack operation, and of components, subassemblies and materials which carry unexpected defects and weaknesses. Therefore, in spite of the utility or otherwise of the various methods of safety analysis, it is impossible to overstress the importance to safety of sound basic engineering design, of high standards of construction (with confirmation of effective quality assurance) and of vigilance in securing a high standard of operation by staff of adequate calibre.

REFERENCES

1. TWAIN M. (PAINE A. B. (ed.)) Autobiography. Colliers and Sons, New York, 1925, 1, 246.
2. COXON T. The design of nuclear plant with integral coolant circuits as related to the Maximum Credible Accident approach. *Proc. 4th Int. Conf. Peaceful Uses Atom. Energy, Geneva*, 1971, III, 202–216.
3. GRONOW W. S. and GAUSDEN R. Licensing and regulatory control of thermal power reactors in the United Kingdom. *Proc. symp. Principles and standards of reactor safety*. International Atomic Energy Agency, Vienna, 1973, 527 and 528.
4. CRITCHLEY O. H. *Some thoughts about criteria for fuel element temperature assessment in Calder type nuclear reactors*. Nuclear Installations Inspectorate, Health and Safety Executive (formerly of the Ministry of Power), 1962, report 19.
5. DALE G. C. and HARRISON J. R. Safety of nuclear power plants—5. Safety in operation. *Proc. 4th Int. Conf. Peaceful Uses Atom. Energy, Geneva*, 1971, III, 147.
6. RASMUSSEN N. C. *et al.* Reactor safety study (draft)—an assessment of accident risks in US commercial nuclear power plants: summary report. US Atomic Energy Commission, 1974, WASH-1400.
7. RASMUSSEN N. C. *et al.* Reactor safety study (draft)—an assessment of accident risks in US commercial nuclear power plants: summary report. US Atomic Energy Commission, 1974, WASH-1400, § 2.9, 15.
8. PARKER COURT OF ENQUIRY. *The Flixborough disaster*. Her Majesty's Stationery Office, 1975, § 1, 76–90.
9. PARKER COURT OF ENQUIRY. *The Flixborough disaster*. Her Majesty's Stationery Office, 1975, §§ 27, 58 and 210.
10. ATHERLEY G. and BOOTH R. Could there be another Flixborough? *The Sunday Times*, 1975, 14 Sept., 61.
11. NORMAN C. Candle power at Browns Ferry. *Nature*, 1975, 257, Oct., 525–526.
12. HANAUER S. H. and MORRIS P. A. Technical safety issues for large nuclear power plant—risk analysis. *Proc. 4th Int. Conf. Peaceful Uses Atom. Energy, Geneva*, 1971, III, 201–216.
13. KIRK J. and TAYLOR R. S. The design for safety of gas-cooled reactors. *Proc. 4th Int. Conf. Peaceful Uses Atom. Energy, Geneva*, 1971, III, 151–162.
14. RASMUSSEN N. C. *et al.* Reactor safety study (draft)—an assessment of accident risks in US commercial nuclear power plants: summary report. US Atomic Energy Commission, 1974, WASH-1400, § 2.23, 29.
15. BRYAN W. *Nuclear Week*, 1974, 4 Apr.
16. CRITCHLEY O. H. Discussion contribution. *The handling of radiation accidents*. International Atomic Energy Agency, Vienna, 1969, 480–481.
17. BOURGEOIS J. *et al.* Evolution des idées françaises sur la sûreté des réacteurs. *Proc. 4th Int. Conf. Peaceful Uses Atom. Energy, Geneva*, 1971, III, 163–172.
18. RASMUSSEN N. C. *et al.* Reactor safety study (draft)—an assessment of accident risks in US commercial nuclear power plants: Appendix II (Vol. 1)—Fault tree methodology. US Atomic Energy Commission, 1974, WASH-1400, 7.

ERRATA

(i) Correct page number in reference '2. COXON, T. The design of nuclear plant with integral coolant circuits .....' to read 227 instead of 202-216.

(ii) Replace reference '13. KIRK J. and TAYLOR R. S. The design for the safety of gas cooled reactors .....' by

13. BIRKHOFER, A. et al. '2. Technical and scientific fundamentals: The Design Basis Accident', Reactor Safety in the Federal Republic of Germany, Proc. 4th Internat. Conf. on Peaceful Uses of Atomic Energy - Volume III, Geneva, 1971, 114-115.

DOCUMENT NUMBER 2

ASPECTS OF THE HISTORICAL, PHILOSOPHICAL AND MATHEMATICAL BACKGROUND TO THE STATUTORY MANAGEMENT OF NUCLEAR PLANT RISKS IN THE UNITED KINGDOM

Synopsis - The subject matter treated is epitomised in the listing of the topic headings with their relevant sub-paragraphs as set out below:

Historical Background (1 - 10)

The Fleck Inquiry and the Nuclear Installations Act
Adequacy of safety and the level of investment in safeguards:
The tradition of safety by foresight, not hindsight·

The vast potential of the atomic energy hazard (11 - 12)

Emergence of a new administrative style in the management of nuclear safety (13 - 16)

The leading role of the engineer in the nuclear industry

The evolution of a technology of a new kind (17 - 19)

The problem of the balance between risk and investment in safeguards (20 - 22)

Interest in methods using probability in safety analysis

The logic of safety analysis - 'Deterministic' and Quantitative Approaches (23 - 27)

Aspects of Quantitative Safety Analysis

The problem of induction (28 - 29)

The approaches which preceded to dawn of probability (30 - 32)

Probability and resolution of the enigma of induction (33 - 40)

Use of the probability of rare events in engineering safety analysis
Some reservations about quantitative probability methods
Quantitative analysis as a tool in qualitative assessment

Concluding overview (41 - 43)

Acknowledgements, References and Notes (44 - et seq.)

3. Aspects of the historical, philosophical and mathematical background to the statutory management of nuclear plant risks in the United Kingdom

O. H. CRITCHLEY, MSc, FIEE, FInstP, Superintending Inspector (Nuclear), Health and Safety Excecutive

There is an ancient but extant school of philosophy which asserts that the only reality is change and another, more recent and also current, which holds that the causes of the future must already exist and can be observed and analysed scientifically (ref.1). The two are combined in a theme which examines the impact of modern technology upon Western society especially in respect of atomic energy and its regulation, consequent developments in safety and the emerging new role of the engineer. Qualitative and quantitative methods of risk assessment are discussed from the viewpoint of espistemology and a synthesis combining elements of both in a systematic approach to hazard management is suggested. Finally, it is noted that problems arising from the interaction of technology, society and politics may not be soluble by mathematical logic alone.

HISTORICAL BACKGROUND

1. "Nothing is permanent but change" said Heraclitus in about 500 BC. Though this is a principle in metaphysics of which determinists have always been sceptical, it has nevertheless gained some currency recently (ref.2). However, few would deny that the main agent of social change is the advance of technology and its impact on the modes of industrial production and the demand for goods and services so stimulated. And the rate of change is accelerating and the style changing. While man has obviously benefited, the process has less pleasant and disturbing features which call for the intervention of the State. On the one hand as the discoveries of science have made available more powerful forces and agents for use in industry, so the potentiality for serious accidents and calamities increases. For example, liquid natural gas as a fuel is more useful and easier to transport than coal, but its disaster potential is many times greater. It is likewise for atomic energy. On the other hand the expectation in the community for a longer life of better quality has risen correspondingly among all classes and access to modern means of communication has made them more vocal in demanding it. Thus, the achievement of safety in its broadest sense becomes ever more important.
The management of safety in the nuclear industry expresses all aspects of the history and progress of a modern high-technology in microcosm, indeed being a recognised forerunner for other industries (ref.3).

2. The demands of the body politic for control of something in the presumed interests of society are normally expressed by political intervention, leading to legislation and its implementation by the executive. Such action in respect of nuclear safety as an acknowledged entity followed the Windscale Plutonium No. 1 Pile incident (ref.4) in October 1957. Although this accident was minuscule in its detriment to property and human health, its serious potentiality was universally recognised. Further, the story of events and human factors leading up to it are typical of the pattern of causation of a major industrial plant catastrophe, such as that repeated at Flixborough (ref.5) some 17 years later and indeed of many other disastrous happenings elsewhere, eg petroleum gas transport.

The Fleck Inquiry and the Nuclear Installations Act

3. Though they were published two decades ago, close attention to the findings of Fleck's characteristically independent enquiry into the organisation of safety in the UK atomic energy industry after the Windscale affair (ref.6) is still most relevant to the theme of safety management of high-technology today. Fleck recognised that the burgeoning nuclear industry in Britain had been highly safety conscious from its inception and had already made substantial and novel contributions to safety technology, a fact to which Gowing (ref.7) and others have drawn attention. This in itself was clearly not enough.

4. Like the rest of the nuclear industry, the Windscale plant had been of necessity staffed at all levels with competent engineers and managers of high calibre who had been successfully achieving their production targets. The seeds of Windscale and future accidents thus lay, not so much with the hazards of the complex and rapidly advancing technology, but with the blindness of self-satisfaction. Further, the safety status of such a plant and its operations could be perturbed by technical innovations and modifications to operating procedures which, while appearing safe when assessed at their locus of application, could hold unrecognised dangers. Again, divergent

tendencies arising from the usual personal and inter-departmental conceits had to be resisted and a confident and easy interchange of technical information and intentions fostered instead. Study of the incident had shown that these aims were unlikely to be secured in a local plant based organisation. To meet these desiderata and to check the inevitable drift towards complacency as time went by monitoring was necessary. This was not available from any of the existing regulatory bodies such as HM Factory Inspectorate and something of wider scope than the detached enforcement of regulations was required.

5. Looking for a new approach, Fleck saw an analogy in the air transport industry which had a continuing safety problem. He recommended that safety surveillance should be entrusted to an independent specialist division in the Authority and that safety in the emerging commercial applications of atomic energy should be overlooked by a new statutory body similar to the Air Registration Board (ref.8). This latter group would work in concert with a similar but more elaborate structure in the Atomic Energy Authority itself. Also, it could draw upon the technical expertese of the Authority while remaining free to interpret the information and advice supplied according to the needs of any particular operation in the commercial sector.

6. An inescapable accompaniment of any such system is that the safety officer or inspector who does the monitoring inevitably participates in and shares responsibility with the party falling under his surveillance because control involves him in complex technical judgments. In addition, the plan or process under review may not be assessed so much for its scientific justification as for the manner in which this has been reached and the supporting arguments often invoke managerial factors. Not least, safety must be achieved without undue restraint on technical progress and the decisions are seldom clear cut but are reached by discussions, leading to a balanced assessment of risk against safeguards to be adopted.

7. Fleck's recommendations were largely written into the Nuclear Installations (Licensing and Insurance) Act 1959 and they resulted in the establishment early in 1960 of the Nuclear Installations Inspectorate which has been described by Joslin (ref.9).

Adequacy of safety and the level of investment in safeguards

8. Not only did the novel and peculiar scientific and engineering features associated with the hazards of the industrial use of atomic energy give rise to many problems which required new and unusual solutions, but the very great emphasis put upon safety itself led to difficulties in organising the safety assessment of the plant and processes and in matters of personnel management. The central recurring question is "how safe is safe?" and what level of investment in a particular item is needed to achieve adequate safety? The need to balance investment against the level of safety to be achieved was clear, but safety defied measurement so the initial approach was almost entirely qualitative. Moreover, there was little or no quantitative data. The difficulties were overcome by an intuitive development of the traditional safety factor concept common to engineering design. The problem which is not unique to the nuclear industry has yet to be satisfactorily resolved and merits further consideration.

The tradition of safety by foresight, not hindsight

9. The attitude of "safety by foresight rather than by hindsight" was assimilated to the nuclear industry in Britain from the beginning. As this led into largely untrodden ground the new inspectorate had to develop a novel style of consultative regulation and inspection with participative overtones. Of necessity it drew upon the theory and practice of safety management which had evolved in the United Kingdom Atomic Energy Authority and its precursors during the wartime period of collaboration with the United States. A blend of these elements had to be adapted to the unprecedented task of regulating the exploitation of a technology which had moved outside the envelope of close government and Authority control.

10. The approach adopted involved the safety assessment and acceptance, within a licensing regime, of the design, siting, quality control and inspection during construction and commissioning and of the rules and supporting instructions for the operation and maintenance of reactors, nuclear fuel manufacturing and processing plants and other installations. Consequently, a style of regulation was evolved to cope with a new form of corporate management in which safety decisions on matters of design and operation had to be reached by debate among designers, operators and safety assessors so as to secure that the most economical and effective mode of safety technology was used. As noted earlier, characteristic of this type of statutory safety surveillance is a measure of shared responsibility among the parties to the safety debate because the inspector participates in and contributes to the decision making process. This is in antithesis to control by statutory regulations where the obligation is on the operator to comply and there is no formal place for discretion in technical interpretations. In such statutory control the situation is one of either compliance or breach, though the inspector may contribute by advising on ways of securing compliance.

THE VAST POTENTIAL OF THE ATOMIC ENERGY HAZARD

11. Man's ability to release atomic energy made radio isotopes of all kinds and levels of activity available in large quantities compared with the previous era. The peculiar and insidious hazards of radioactivity were multiplied by many orders on those associated with the use of radium and x-rays which had already

taken a serious toll among those working with them. There was now a lethal potential and longer term detriment to large numbers of people and extensive damage to property was possible. A massive release of radioactivity to the environment surrounding a nuclear power station could follow a major catastrophic accident to the plant. In a study published by the U.S. Atomic Energy Commission (ref.10) it was estimated that an extremely severe accident to a nuclear power reactor giving rise to a major release of radioactivity could "kill thousands (over 5,000) injure thousands more and cause billions of dollars in property damage" and those so affected would know little of it until they became ill or were otherwise advised of the harm that might have been done to them. This extreme estimate has been confirmed, though substantially tempered by the use of quantitative analysis in a hazard assessment which directs attention to the small level of risk rather than to the grave consequences of a major accident (ref.11). Again, the hazard from ionising radiations emitted from "nuclear matter" (ref.12) is especially treacherous in its nature as many victims of over-exposure have found to their cost. Except in a few of the most serious cases there has been no sensory warning of impending harm and only in a very few of these any immediate evidence of injury, though the cumulative effects are obvious. The fission products held in a reactor core were identified by de Wolf Smyth and Wigner in about 1944 as "a particularly vicious form of poison gas with considerable military significance" (ref.13).

12. As Smyth has recorded, in the government agency which directed the work leading up to the major release of atomic energy in the USA early in December 1942, there was a Health Division whose major objective was to ensure no one suffered serious harm from the peculiar hazards of the enterprise. Under General Groves direction, a feature of the safety approach was to make the safety factors so large that the chance of failure was very small compared with other hazards and, where knowledge was lacking, every feasible precaution was observed (ref.14).

EMERGENCE OF A NEW ADMINISTRATIVE STYLE IN THE MANAGEMENT OF NUCLEAR SAFETY

13. Traditionally, policy direction and the higher management of government and quasi-government bodies engaged in regulatory activities, such as inspection and safety surveillance, have been almost exclusively the province of the generalist administrator who exercises "financial and other control ... over the work of ... engineers and other specialists" (ref.15). This pattern was implicit in the philosophy of the Northcote-Trevelyan Report of 1854 which laid the foundations of modern government organisation in Britain (ref.16). It was based on the concept of a superior kind of intellectual activity which can perceive a problem in outline and not obscured by a confusing mass of technical details. Thus, a broader and more general solution can be achieved. It derives from antiquity when the management of affairs of commerce and the state emerged in a society where intellectual functions were sharply delineated from manual skills, even those which required the highest orders of creative mental activity. For example, Seneca, one of the most perceptive of the Roman philosophers and lawyers described mechanical invention as "drudgery worthy only of the lowest of slaves". Fulton and the passage of years have only diluted this classical attitude which is still influential today and is, indeed, inherent in the way in which management is normally effected in industry and government (ref.17,18). Thus, the professional is deputed to the carrying out of subordinate functions according to policy determined by a superior structure and in the formulation of which he has little say.

The leading role of the engineer in the nuclear industry

14. The rapid advance of technology has so complicated industrial management and civil administration that changes in their traditional organisational structure became necessary and control in many circumstances passed into the hands of engineers. Nowhere has this been more the case than in the nuclear industry. From the start of its application in war and later in peace it would have been veritably impossible to have developed the technology of atomic energy successfully without professional engineering control in all aspects of its management, and during the last war it was true even to the highest level of government. This exceptional feature of the industry is instanced by the successes of General Groves (ref. 14), in the case of the Manhattan atomic bomb project in the USA, and of Sir Christopher, now Lord Hinton, in Britain.

15. In a similar manner, safety which is central to the successful exploitation of atomic energy has evolved in the general framework of the command of policy by professional engineers and scientists. An outstanding example is the emergence of the International Commission on Radiological Protection (ICRP) which is a learned professional body of a new type, dominating international policy in matters of radiological protection and receiving almost unquestioned world acceptance. The statutory regulation of the industry has followed a pattern which in the UK has been described on many occasions by members of Inspectorate (NII), eg., in 1973 by Cronow and Gausden (ref.19).

16. While the approach of the NII into new ground in safety regulation not surprisingly evoked some criticism (ref.20,21), it has contributed materially to the very high standard of safety in the nuclear industry. It is a fact that no one has been killed nor has anyone been seriously injured by radiation on any licensed nuclear site. Further, there is evidence of a spin-off into the realm of conventional industrial safety where the accident record in "nuclear" plant is better than that in the generality of industrial premises.

THE EVOLUTION OF A TECHNOLOGY OF A NEW KIND

17. These novel, peculiar and complex safety problems of design and operation associated with the use of atomic energy in power production in particular, called for safety concepts of a new type as well as for the further development of existing techniques. In addition to those of plant operation within safe limits, there were other new problem areas, being chiefly those associated with such things as criteria for the choice of sites for reactor plant, reactor containment technology, remote handling techniques, criticality considerations in the use and storage of fissile materials, rigorous anti- contamination measures for the handling of material such as plutonium, the management of active wastes and, last but not least, commercial considerations of liability and insurance.

18. The foregoing strategems were not only assimilated to the nuclear industry in Britain from its start, but important national contributions were made in plant management tactics. Among them were the Technical Plant Safety Committee as a means of self-inspection and a structured step approach to technical safety assessment of design, from the early formalised proposals to that of the full scale operation of the plant. The latter is met by a scheme which proceeds in several stages and has a formal beginning for a given installation in an initial safety report (ref.19) describing the design and safety features of the proposed plant and justifying its operational safety by analyses, fault studies and supporting calculations. It is required that the report be assessed by an independent group of engineers who can weigh the safety arguments and specify any steps which have to be taken to reinforce weak points, recommend improvements and specify further fault studies. Such an assessment for a nuclear power station, say "Magnox", would take 20 - 30 man-years of highly skilled, well qualified and experienced engineering effort.

19. The involvement of the NII in its supervisory role which has been described by Gronow and Gausden (ref. 19) is largely concerned with executive safety assessment and the necessary supporting executive inspections. These are higher tier operations which confirm by special studies, sampling inspections and tests on site and technical investigations that the utility's and constructor's safety assessments are sufficient in depth, are sound, well founded and are properly implemented on the construction site.

THE PROBLEM OF THE BALANCE BETWEEN RISK AND INVESTMENT IN SAFEGUARDS

20. The inspector's main task is to confirm the operator's assurance that his installation, built and operated in accordance with the relevant plans and designs is safe, and not to demand that it be safer than safe. This inevitably involves the inspector in the question of where to put a proper limit on his inspectorial requirements for the expenditure of effort and money on safety, but satisfactory means of resolving the dilema are elusive.

Interest in methods using probability in safety analysis

21. As the qualitative approach shows no obvious way of setting a limit on the required investment in safeguards without a conceptual reduction in safety, by 1965 the NII were actively considering the utility of quantitative probability methods in their technical design safety assessment (22). They were not found very rewarding (ref.19) and, other than for the use of quantitative probability techniques in selected areas where adequate and stable data were available, eg., in the assessment of instrumentation and control systems and for determination of the "Fire Risk Criterion" which sets the upper limit of the output gas temperature in a "Magnox" reactor (ref.23), they were not pursued much further at this stage. Nevertheless, in the UKAEA through the activities of its Health and Safety Branch, interest was maintained and in 1967 Farmer published his quantitative approach to reactor site selection (ref.24). Activity was extended from the reliability analysis of components and sub-systems to the quantitative assessment of the installation as a whole and this has been described in detail (ref.25). The methodology is akin to that used in the Rasmussen "Reactor Safety Study" (ref.26) and it is now fostered by the Systems Reliability Directorate of the Authority for a wide range of industrial safety investigations and studies, notably the recent Canvey Island (petro-chemical installations) safety report.

22. Interest in Quantitative Safety Analysis (QSA) has increased greatly in recent years and has had many advocates which includes some Russian engineers who published their method in 1969 (ref.27). The movement is part of the growing use of systems analysis in public policy making (ref.28), but this has not been received uncritically. While the NII employ the method in certain selected areas of design assessment (ref.29) it is interesting to note that it also had apparently only limited use in the US National Aeronautics and Space Administration which used mixed quantitative and iterative techniques of "design-make-test-fail-fix" to establish the reliability of its moon-shot vehicles.

THE LOGIC OF SAFETY ANALYSIS -"DETERMINISTIC" AND QUANTITATIVE APPROACHES

23. The qualitative or so called "deterministic" approach to design safety analysis begins with the implicit assumption that no major technology is risk free. Thus, if there is a sequence of events and faults which may conceivably lead to an accident, then in spite of all precautions that accident has a continuing finite potentiality to happen which can never be dismissed. It is a view of causation which has received some eminent support of an ontological

Mind such as that of the American pragmatist, Peirce, in his theory of chance (ref.30). The assessment process follows by identifying the significant risk modes by qualitative safety analysis. The technology or activity, eg. use of a nuclear installation, is then weighed in terms of the maximum adverse consequences of various postulated serious accidents. In an early application, the analyst identified a very serious accident in a credible mode which was assumed to bound a spectrum of less serious incidents and this was called the Maximum Credible Accident (MCA). A credible mode means that a mechanism by which the accident can be precipitated is conceivable and may be accepted as reasonably possible.

24. The ways in which the MCA could occur were examined by fault studies, by qualitative safety analysis programmes and by operational research techniques. The assessed liklihood of the accident occurring was then minimised by modifying the design appropriately so as to provide barriers of various kinds against any identified fault initiating a chain of events which could, in the ultimate, precipitate that accident. These barriers, which included containment structures, design limitations, engineered safeguards, operational restraints, regimes of inspection and other such strategems aimed, not only at preventing the accident but also at securing that the consequences of a given MCA were socially and economically tolerable, eg. of minimum detriment without the plant boundary or restricted zone. This latter was established as part of the siting policy which was determined by assessment of the fission product release from the plant to the environment in the event of the MCA and relating this to an Emergency Reference Level (ERL) of postulated radiation dose to the population likely to be exposed.

25. Beyond the MCA there was envisaged a second tier concept of a possible, highly improbable Maximum Hypothetical Accident (MHA) which could conceivably break through barriers established at the MCA thresholds. It was posited that the chance occurrence of such a disastrous accident mode could be made vanishingly small if not impossible, by appropriate barrier strategies. For example, in the case of a gas cooled nuclear reactor in a pre-stressed concrete pressure vessel catastrophic failure by bursting is virtually impossible and this limits the extent of any conceivable calamity to the core. Nevertheless, the consequences of the MHA were taken into account in siting policy in subsequent control of residential development and in planning emergency schemes.

26. The maximum accident approach has fallen into desuetude of recent years and has been largely replaced by a variety of quantitative and quasi-quantitative methods.

Aspects of Quantitative Safety Analysis

27. Quantitative safety analysis which is a systems approach makes the assumption that all chains of future events can be associated with a probability of occurrence which is expressible in numerical terms. Therefore, given suitable data, it is possible to deduce a definite risk for a required failure rate in numerical terms within calculable confidence limits. For example, in applying it to assess the risk which may be associated with a nuclear power programme, individual failure rates for the components, sub-assemblies and subsystems which make up the plant are collected in data banks. These elements are then used in calculations of the reliability analysis type using "fault trees" and "event trees" to cast the chances of various possible fault sequences giving rise to certain assessed releases of radioactivity to the reactor environment. The results may then be averaged over the expected operational life of the plant or of a group of reactors to give a probable rate of exposure per year per person at risk. Thus the risks attributable to the technology may be expressed in quantitative terms of probable lethalities per year among the exposed population or in shortening of the average life span. The result may be compared with similar risks for existing hazards taken from statistical tables. Thus, the risk attributable to a nuclear power programme can be compared with the lethality attributable to that associated with public transport, dam failures, lightning and so on. The acceptability of the technology or activity can then be weighed in terms of the social need for its introduction against the imposed risk. If the balance is favourable then the risk is judged to be "acceptable". For example, the Rasmussen Safety Study (ref.26) assesses the accident risks from a large atomic power programme at orders less than that to which people in the USA are exposed in normal living. Though it specifically avoids making any recommendations, a decision maker would conclude on scientific grounds that nuclear power is an acceptable risk.

THE PROBLEM OF INDUCTION

28. All safety analysis techniques whether qualitative or quantitative are attempts to make rational forecasts of future events and as such involve the so-called "problem of induction". Induction is the name given by philosophers to the process of making inferences from past and present experience about what will happen in the future. While it is one of the fundamental problems of the metaphysics of engineering, it is in fact nothing more than the application of commonsense. However, that attribute, like many other common things such as gravity and inertia, is far from simple and has presented an intractible challenge over the ages to some of the world's greatest intellects and is still a matter of intense debate with political overtones.

29. While induction may be the most frequent form of reasoning, it presents great difficulties to epistemology, that is the theory of knowledge. Although in a given case one event may follow another in a seemingly orderly chain, there is no reason why we should

infer that this will happen in the general. From the standpoint of methodology it is not good enough to say such an event is likely to happen or to believe that it will, for such inferences can not be established by strict logical reasoning. Wittgenstein dismisses the proposition with the statement that belief in any casual nexus between events of the present and future happenings is superstition (ref.31). Yet in spite of this theoretical dilemma orderly civilised life would be impossible unless reliance can be placed upon inductive reasoning, for it is the basis of all planning. Bertrand Russell in his "Principia Mathematica" described it as the ability to make plausible guesses. More particularly, the argument concerns the relationship between causality and the stochastic nature of the universe and has developed as understanding of the latter has advanced and it may therefore be useful to pay some attention to this aspect.

THE APPROACHES WHICH PRECEDED THE DAWN OF PROBABILITY

30. Cicero, the sceptical Roman augur and politician, in his dialogue on prophecy envisaged causation as a sequence of causes leading up to a future event in which each acted through a link on the next. To foretell the future it was necessary to have knowledge of these causal factors and the nature of the links between them. There is no hint of probability in this argument. Unfortunately, information about the state of the links is available only to the Gods and not to man. So much the worse for augury. Shortly after this revelation he was proscribed and killed.

31. St Thomas Aquinus and the Schoolmen (ref. 32) put future happenings into three classes. There were inevitable events which happened because they were "natural" and "necessary", such as the falling to the ground of an unrestrained object. Those events which were predictable with less certainty were classed as "natural" but not "necessary" because they could be influenced by a perturbing force such as that exercised by the hand when a thing was thrown. The third type of event was seen as neither "natural" nor "necessary" and could not be predicted by the laws of science. Such things just happened and were termed "contingencies".

32. David Hume, the British empiricist, also tried to rationalise the theory of causality, but foundered on the problem on induction, sharing with his predecessors an almost total ignorance of probability.

PROBABILITY AND RESOLUTION OF THE ENIGMA OF INDUCTION

33. The understanding of induction which is still far from complete, has improved with man's grasp of the relatively new discipline of probability. Generalising from the science of statistical mechanics which about a century ago was resolving many of the knotty problems of physics, James Clerk Marwell was moved to observe that Logic could deal only with certainty, doubt and impossibility, whereas reason went beyond these things. The link was provided by "the calculus of probabilities" which was "the true logic" for man and science (ref.33).

34. Now that probability has allowed an escape from the impasse of the problem of induction, the debate has moved on to the understanding of probability itself and that may be more difficult and contentious than the former challenge. A current view of a determinist flavour which would reject qualitative and thus subjective probability is that a definite numerical frequency like a failure rate exists for all events. Then, if this number can be ascertained or be shown to lie between determinable confidence limits, it is possible to assign a mathematical probability of occurrence in numerical terms to such an event. An example is the chance of one's death from a given cause eg, cancer from smoking cigarettes. It is central to actuarial operations in the insurance industry, applying to such things as expectation of life tables, etc. and is a basic premise in systems analysis.

Use of the probability of rare events in engineering safety analysis

35. Probability now plays a major role in technical design safety and reliability assessment which is a form of inferential reasoning used in engineering design and management of plant operation. In particular probability is used in the aspect of plant accident risk prediction which attempts to forecast the very unlikely occurrence of disastrous accidents in hazardous installations which, like nuclear power stations, are normally reliable, well-built and well-run. The application employs methods which have been developed for expectation of rare events such as the inundation of coastal lands by exceptional high tides. A mathematical technique for making calculations of this kind was published by Poisson in 1837 as his "Law of Large Numbers" which was renamed by Bortkiewicz of "horse kick" fame the law of small numbers (ref. 34).

36. More recently interest in this kind of prophecy has increased greatly and diverse methods of prediction and especially systems analysis have flourished under the stimulus and encouragement of politicians and administrators. The apparent reduction of dilemmas to a choice between numerical values is attractive because it enables proximate decision makers to compensate for lack of knowledge of the disciplines involved, and this is especially so in technology.

Some reservations about quantitative probability methods

37. A common criticism of quantitative methods of risk prediction is that their results are only truly meaningful when derived in what

may be called "closed situations". In these, all the relevant factors operating in the casual sequences are known and can be rationally quantified. Allowances can be made for recognisable lacunae and impingeing variants and stray effects which might perturb the sequences. The numerical chance of occurrence of a rare event may then be realistically calculated between comprehensible confidence limits as Rasmussen attempts to show in the Reactor Safety Study (ref.11).

38. While this may be the state of affairs for the "closed situation" of a scientific experiment on the laboratory bench or for a planned series of observations (indeed, it is the investigator's aim to achieve such a state), it is a dubious assumption for a complex and hazardous industrial plant or process. In such cases, casual temporal and physical factors and other things beyond the analyst's control or ken may disturb the expected pattern of causation. Then, the postulate of adequate knowledge about cause and effect is false and any confidence limits which might be cast to meet the deficiencies could be so wide as to be empty.

39. A further criticism is due to Keynes (ref.35) who wrote of the danger of assuming without justification that a statistical frequency is stable. He associated this fallacy with Poisson's suggestion of "what is certainly false, that every class of event shows a statistically regularity of occurrence if only one takes a sufficient number of instances of it. .....some statistical frequencies are, within narrower or wider limits, stable. But stable frequencies are not very common, and cannot be assumed lightly".

Quantitative analysis as a tool in a qualitative assessment

40. If the statistical frequencies on which a systems analysis of a technological process is based are not stable or contain major elements of instability, the predictions drawn from it will be unreliable and may be false and misleading. Nevertheless, the structured approach and disciplined data search and management needed for such an analysis can throw light on previously unrecognised dangers in the plant and process and on weaknesses in the provisions made to secure safety. As such, systems analysis is a valuable tool. In fact, what is needed is a synthesis of qualitative and quantitative methods in a systematic approach which draws on all appropriate aids to decision making according to the nature of the task, be it design safety assessment or other operation. This latter is in fact the style of safety analysis in technical safety assessment adopted by the NII (ref.29) and is equally suitable for the safety analysis of other hazardous installations.

CONCLUDING OVERVIEW

41. Finally, in respect of all the foregoing considerations, it is worth taking into account an important anthropological factor which may bear upon use of probability techniques in the realm of politically related decision making and one which may have attracted less than due attention. As the planners who commissioned the Roskill cost-benefit exercise which justified Cublington as the abortive choice of location for the Third London Airport found out, the subjective reaction of the population affected by a decision is more significant than any rational arguments based on actuarial computations.

42. The man in the street (there is no average man, he is a mere statistic) is a distinct individual who will behave in a personally characteristic style. He is more likely to be influenced by his concept of the nature and consequence of a hazard, should it effect him, than on mathematical variations in some calculation of its predicted frequency. He is perverse; he may be prepared to accept the very considerable risk of riding a motorcycle, yet refuse to travel by air. This irrational personalised response to risk and chance is readily observable. If it were not so the football pool section of the gambling industry would collapse tomorrow and very few Premium Bonds would be sold, for the personal chance of winning a fortune in such a way is almost zero. Moreover, the problems which have to be solved are not infrequently confounded by inadequacies of data and by political and social considerations. Weinberg has defined them as "trans-scientific" and holds that to treat them by the methods of conventional scientific analysis is inappropriate (ref.36).

43. The concept of probability and its use in inductive reasoning are new to human thought and, naturally, are not yet fully grasped. While some of its applications have been naive, probability is rapidly becoming assimilated into our culture as a powerful intellectual tool. In parallel with the emergence of probability methods, certain new styles of qualitative reasoning are making an appearance. They aim at solving the enigmatic problem of forecasting the behaviour of complex systems by perceiving them as wholes rather than as chains of linked elements and causes whose group behaviour may be predicted by exhaustive calculations. Among them is Thom's hypothesis (ref.2) that such systems may be seen as particular structures of temporary stability but containing complexities of multifarious interacting parts in constant flux. Each one moves predictably towards a "catastrophe" resulting in its metamorphosis or end as the case may be. Thus, while the pursuit of detailed calculations concerned with the specific behaviour of the elements and their effects on one another may be of little general relevance, the pattern of behaviour of the whole can nevertheless be profitably analysed and the specific future trend or trends identified.

ACKNOWLEDGEMENTS

44. The above passages are largely drawn from

work done by the author during his tenure of an honorary Simon Fellowship in the Department of Liberal Studies in Science at Manchester University from 1974 to 1976. Hence, he wishes to express his gratitude to the Health and Safety Executive, the Department of Energy and to the Simon Committee of Manchester University for the unique and valuable opportunity which was afforded to him. In particular, he is grateful for the encouragement, advice and support he received from Mr E.C. Williams, Professor Brian Harvey and Mr R. Gausden. Likewise he wishes to note the valuable help and guidance given by Professors F.R. Jevons and M. Gibbons and other erstwhile academics at Manchester University and also more recently that from Dr J. Shaw of Queen Mary College, London. In addition, the essential part played by typing and secretarial services must be recognised. Finally, though Mr Gausden, now Chief Inspector of Nuclear Installations, has kindly granted permission for the paper to be published, the views expressed are solely the author's and in no way are they those of the Health and Safety Executive or of colleagues in the Nuclear Installations Inspectorate or elsewhere.

REFERENCES AND NOTES

1. TAYLOR, K. Henri Saint Simon 1760 - 1825 Croom Helm, London, 1975. 30.
2. THOM, R. Structural stability and morphogenesis. Benjamin, Reading, Mass., 1975.
3. RITCHIE-CALDER. Radiological Protection Bill Debate. Lords, 305, 1969, Oct.28. Col.792.
4. PENNY, W. Windscale Pile No.1 Accident. HMSO, Cmnd 302, Nov. 1957.
5. PARKER, R.J. The Flixborough Disaster. (Dept. Emp.) HMSO, 1975.
6. FLECK, A. The Organisation and Control of Health and Safety in the UKAEA. HMSO, Cmnd 342, 1958.
7. GOWING, Margaret. Independence and Deterence - Britain and atomic energy, 1945-1952. Vol.II, MacMillan, London, 1974. 91.
8. FLECK, A. (ibidem as 6). paras 34-35.
9. JOSLIN, S.W. & GRIFFITHS, T. Design and operation of nuclear power stations:(a) Nuclear Installations Act 1959. Cong. Roy. Soc. Health, Scarborough, 1962. Sec. L, Radiation (42/62). 104.
10. VANCE, H.S. Theoretical possibilities and consequences of major accidents in large nuclear power plants, USAEC, WASH-740, 1957.
11. Rasmussen, N.C. The Safety Study and its feedback. Bull. At. Scientists, 1975, 31. 25-28.
12. "Nuclear matter" is a legal entity and is defined in S.26 of the Nuclear Installations Act, 1965. It means any fissile material in the form of uranium or plutonium as metal, alloy or chemical compound or any other fissile material which may be prescribed, if the foregoing are not "excepted matter", and includes any radioactive material produced in the fission process or made radioactive by any radiation arising from that process.
13. SMYTH, H. deW. Atomic energy for military purposes. Princeton Univ. Press, 1947. 64.
14. GROVES, L.R. Now it can be told. Harper, New York, 1962. 86-87.
15. FULTON. The Civil Service, Vol.2: Report of Management Consultancy Group. HMSO, Cmnd 3638, 1968-1969.
16. CHAPMAN, R.A. The higher civil service in Britain. Constable, London, 1970. 23-36.
17. ASHBY, E. Technology and the academics. MacMillan, London, 1966.
18. SALOMON, J-J. (Trans. by Lindsay). Science and Politics. MacMillan, London, 1973. 5-6.
19. CRONOW, W.S. & GAUSDEN, R. Licensing and regulatory control of thermal power reactors in the UK. Proc. Symp. on Principles and Standards of Reactor Safety, IAEA, Vienna, 1973. 521-527, 528.
20. FLOWERS, B. 6th Report of the Royal Commission on Environmental Pollution: Nuclear Power and the Environment. HMSO, Cmnd 6618, 1976. S. 280-S. 296 & S. 531.
21. PEDDIE, R.A. The management of large, high-technology projects. Lecture to Inst. Elec. Engineers, London, 19 February 1976.
22. CRITCHLEY, O.H. Some thoughts about criteria for fuel element temperature assessment in Calder type nuclear reactors. INI/R/18/62. Min. of Power, Insp. Nuclear Installations, London, 1962.
23. DALE, G.C. & HARRISON, J.R. Safety of Nuclear Power Plants - 5. Safety in Operation. Proc. 4th Int. Conf. on Peaceful Uses of Atomic Energy, Geneva, 1971. Vol.III. 147.
24. FARMER, F.R. Siting criteria - a new approach. Proc. Symp. on Containment and Siting of Nuclear Power Reactors, IAEA, Vienna, 1967. (SM 89/34).
25. FARMER, F.R. et al. Quantitative safety analysis. Nuc. Eng. & Design, 1967, 13. 183-244.
26. RASMUSSEN, N.C. et al. Reactor Safety Study. WASH-1400. US Nuc. Reg. Commission, 1975. (NUREG-75/014).
27. BOEROVNIKOV, O.P. et al. Assessment of the probability of radiation accidents at nuclear power stations. Proc. Symp. on Handling of Radiation Accidents, IAEA & WHO, Vienna, 1969. 471-481.
28. HOOS, Ida R. Systems analysis in public policy. California Univ. Press, Berkeley and London, 1972.
29. GAUSDEN, R. Safety assessment criteria. Health and Safety Executive, HM Nuclear Installations Inspectorate. Report NII/R/5/77, 1978.
30. PEIRCE, C.S.S. Collected papers, Vol.II: Elements of Logic. Harvard Univ. Press, Cambridge, Mass., 1932.
31. WITTGENSTEIN, L. Tractatus Logico-Philosophicus. Routledge & Kegan Paul, London, 1962. 5.1361 79.
32. BYRNE, E.F. Probability and Opinion. Martinus Nijhoff, The Hague, 1968. 203-204.
33. JEFFREYS, H. Theory of Probability. Oxford Univ. Press, 1948. 1.
34. MALSTROV, I.E. (Trans. S. Klotz). Probability Theory: a historical sketch. Academic Press, New York and London, 1974. 160.
35. KEYNES, J.M. Treatise on Probability. MacMillan, London, 1973. 368.
36. WEINBERG, A.M. Trans-science. Nature, 1978, 273, May. 93.

* After thought. Perhaps "certainty" might be a better word, but would limit the idea to be conveyed.

DOCUMENT NUMBER 3

INSPECTION AND ITS ROLE IN THE CASE FOR NUCLEAR POWER

Synopsis - The contents of this paper which was a contribution to a wide ranging discussion on the scope for further research in nuclear power by the industry, the universities and polytechnics, the utilities and those statutory bodies concerned with nuclear engineering is epitomised in the paragraph titles listed below.

Paragraph	Title
1	Relevance of the Energy Crisis
2	Nuclear Power and its Hazards
3	The Foundations of Nuclear Safety
4	The Strange Phenomenon of Public Hostility
5	The Problem of Securing Public Acceptance of Nuclear Power
6	Towards a Solution
7	The Nature of Inspection
8	The Evolution of Modern Inspection
9	Inspectorates and Inspectors
10	Some Relevant Research Topics
11	Summary
12 - 13	An acknowledgement and References

Directions in Nuclear Engineering Research
Cambridge 19 September 1980
Institution of Nuclear Engineers

Paper No. 401...

Inspection and its Role in the Case for Nuclear Power

by

Octavius E. Critchley

Consultant and Partner of Reardon-Critchley International
London and Edinburgh

1. Relevance of the Energy Crisis

The looming supply difficulties which face a World already overdependant on oil are focusing attention on the need to secure stable and continuing sources of energy and so to be free from this thraldom. Of the many options other than a greatly intensified exploitation of coal, only atomic energy is readily available and can be a growing rather than a dwindling source. Alternatives like wave and wind power are not feasible before an oil shortage could heighten international tensions to a level where any peril from nuclear power generation shrinks into insignificance when compared with the horror of modern war (Boyle 1979). The health and safety reckoning owing to the prolific production and burning of fossil fuels cannot be ignored, but they have been hallowed by long acceptance, although in the long term the human and environmental detriments attributable to them may well outweigh those of atomic energy. In contrast, the dangers of nuclear power, real and imagined, have effectively frustrated its once happily envisaged function as man's main and inexhaustible future power source. It is appropriate therefore to examine how the vital nuclear option might be freed in time from these present curbs which are holding back its further development and wider use as an alternative to oil.

2. Nuclear Power and its Hazards

Without doubt the utilisation of atomic energy is a very dangerous process. The hazards to man and his environment which are associated with it have the disturbing property of being unknown except by backward extrapolation from the destruction caused by atom bombs, by the unforseen consequences of weapons testing and by speculation about a few well publicised radiation accidents. The measures for accident prevention are thus based in the main on theoretical studies and postulated event sequences leading to severe faults which, though very unlikely, could have very harmful and destructive effects. Scenarios of the worst accident to a power reactor such as the well known U.S. Nuclear Regulatory Commission study of 1957 depict a grim and heavy toll of human deaths and injuries and heavy property damage. Notwithstanding these prognostications, in over 20 years of commercial nuclear power plant operations, in Western countries at least, no member of the public has been killed or even harmed, in spite of dubious special pleading to the contrary (Gofman and Tamplin 1973) and very few of the operating staff have been hurt. It has in fact been the 'safest industry in the World' and such notable incidents as have occurred, e.g. 'Browns Ferry' and 'Three Mile Island' have been safely contained, though in these cases the plants have sustained serious damage.

3. The Foundations of Nuclear Safety

To what then can this paradox of safety-in-danger be attributed? It is certainly not inherent in the technology as the experiences of 'Windscale Plutonium Pile' incident, the 'Enrico Fermi' meltdown, and the 'SL1' reactor prompt criticality explosion among a number of other incidents have shown. They are all examples of the occurrence of the unexpected whose causes have been revealed after the event.

The answer is that it can be attributed to the novel and innovative approach to health and safety which has characterised the atomic energy industry from its start. The dangers associated with the large scale release of nuclear energy were immediately recognised by Groves who ensured that all possible care was taken to safeguard his employees

/Contd..

2o1-2 ree

in the Manhattan Project and associated works (Groves 1962). This philosophy of safety by foresight rather than hindsight has continued and been further developed. An important application is the precept of requiring prior safety assessment of design of plant before construction or modification. An underlying principle which is unitary posits that, not only is safety of the plant as a whole dependent on that of its component systems, but that good design must ensure as far as possible that the performance of the parts linked together secures a greater level of safety for the whole entity with overlapping protective zone reinforcing one another. This is also expressed in the guardline concept of protective instrumentation in depth.

The principle of unitary safety in engineering applies to management systems as well as to hardware, particularly as the former are prone to break into disparate sub-groups to perform technically distinct functions and drift into introversion. Co-operative working is not inherent in human society and identifiable groups in organisations tend towards hierarchial entities rather than to merge as sharing teams. Such behaviour in the management of large, complex and risk prone plants can be inimical to safety and among the special measures taken in nuclear installations to promote functional integration are the practices of maintaining a plant technical safety committee and that of requiring submission of a 'safety report' ensure that the safety of the design of the plant, any modification, change in operation or experiment has been assessed and considered before it is put into effect (Gronow and Gausden 1975 and Haire and Shaw 1979).

While it is the duty of management to evoke unity of function in the organisation it controls, it can be itself beset by the same individualistic trends. This foible was disclosed in the working of the UKAEA prior to the occurrence of the Windscale incident inquiry (Fleck 1957) and more recently in the U.S.A. following the Three Mile Island accident (Rogovin and Frampton 1980). Restructuring of both bodies to overcome the weakness was recommended. In the case of the United Kingdon Atomic Energy Authority (UKAEA), the Fleck Committee strictures were met by establishment of a Safeguards Division with responsibility for overall monitoring of safety, but with an advisory rather than an executive role. It had two branches, one devoted to radiation protection and the other of the nature of an inspectorate called the Authority Health and Safety Branch (AHSB) concerned with siting, the overlooking of safety in plant and process design and operation and criticality. The Committee made analogous proposals for the then burgeoning civil sector of the nuclear industry (Fleck 1958) with a recommendation for the formation of an independent licensing and inspecting body which led to the establishment of the Nuclear Installations Inspectorate (NII) under the Nuclear Installations (Licensing and Insurance) Act 1959 (Joslin and Griffiths 1962).

Much of the duty of both AHSB and NII Was concerned with the oversight of the safety aspects of work in design offices and of activities in factories and on power station and other nuclear sites during construction, commissioning and operation managed by the Authority cf Generating Boards and other licensees as the case might be. Without executive authority over this lower tier, AHSB had recourse to the management board of the Authority in the case of serious differences of opinion which could not be resolved in direct debate with the managers involved. Similarly, Nuclear Installations Inspectors were without the powers of prosecution normally given to government inspectors, for example to members of H.M. Factory Inspectorate, but could invoke more general sanctions through the licensing regime. A novel kind of participative regulation maintained by a continuing dialogue between licensees and inspectors had come into being and, thus, the sustained level of adherence to the required safety procedures which have been described in detail by Haire and Shaw (1979) is evoked rather than imposed. Although this style of supervision might appear to be weak, it has in fact a profound but subtle influence on those who fall under its aegis. These offices by requiring members of the lower tier to report, to explain and to render an account has a most stimulating, powerful and integrative effect (Vickers 1967). It can be one of the most important benefits of an inspectional regime, not least by correcting innate introspective trends in management structures and by encouraging conversation among their elements which otherwise drift in isolation.

AHSB had its own research facilities as well as being able to call more widely on Authority resources. These were made available as appropriate to NII who could also require licensees to make specific investigation relating to safety features of their installations, though research of a more general nature was commissioned from universities and commercial services.

/Contd...

4. The Strange Phenomenon of Public Hostility

In view of the great attention which is being paid to the achievement of safety in nuclear plants and the consequent investment of money and human effort which has been rewarded by an outstandingly good accident record by the industry, the public hostility to atomic power is not easy to understand. As it seems not to be related to any balanced view of risks and benefits, it may be attributed to factors other than the true safety of the plants. Among these may be distinguished:

(i) Lack of understanding of the actual nature of the nuclear hazard;

(ii) Perception of the hazard as totally unacceptable in spite of its presentation as an exceedingly small risk;

(iii) Emotional associations with atomic weapons;

(iv) Fears about the safe management and disposal of active nuclear wastes;

(v) Apprehension that the standards of safety will decline as the scale of nuclear operations increases;

(vi) Fears that plutonium and other fissile materials might fall into the hands of terrorists;

(vii) Concerns about the proliferation of nuclear weapons;

(viii) Fear that civil liberties may be eroded by spreading security precautions (Flood and Grove-White 1976);

(ix) Objection to the growth of bureaucratic power in the nuclear corporations (Cotgrove 1978); and

(x) Hostility to Technological progress in which nuclear energy has led the field.

Attempts to assuage critics by quantitative safety analysis, presenting the risks as negligibly small in comparison with those of every day life, have failed because the objections do not primarily relate to the efficacy of engineered safeguards. Moreover, the relevance of such techniques is in question because they are pertinent to design and not to its realisation in the physical entity of the operating plant on site. Risk assurance in that domain depends on successful inspection and not on the inconstancies of prediction for it cannot account for the vagaries of human error which inspection may apprehend.

5. The Problem of Securing Public Acceptance of Nuclear Power

Acceptance of the nuclear option as one of the nation's long term sources of electric power cannot be won without a struggle on two fronts, one political and the other engineering. Consideration of the ten factors listed above reveals that the opposition is primarily of a political kind and does not in truth relate to the achievement of greater reliability in the hardware of nuclear installations which have already been shown to be exceedingly safe when compared with other industrial dangers. Truly, the phenomenon of the toleration of the mortality and maim caused by motor transport which is one of the greatest modern hazards to life and limb is proof that acceptance by the public of this risk turns, not on logically weighing it against benefit, but upon the need to endure the dangers so that the activity of motoring with its high utility may be enjoyed.

In the political field, the dedicated opponent of a technology can always find a new conjectured technical weakness to attack when an earlier one has been contained (Nelkin 1975). When plant reliability and safety have been demonstrated beyond reasonable doubt to be adequate, though not absolute, and the chance of a major catastrophic

/Contd...

accident is known to be negligible, the proper response to critics is not to suffer a permanent state of seige, but to carry the controversy on to opposition ground by showing that technical stagnation can bring unacceptably harsh social detriments, that it is not possible to remain stationary and that the choice is to advance or regress • with the latter leading to deterioration in the standard of life and derogation of national status to levels which may well be incompatible with social justice, political tranquility and the existence of democracy.

6. Towards a Solution

Public acceptance of nuclear power would seem to turn on two points. The first is political and requires the conversion of the sensible, silent majority of the public to the view that the utilisation of atomic energy is essential to their wellbeing and things may soon be unpleasant without it. The existence of Holland gives evidence that the case can be won. Eight-tenths of that land are below the maximum Spring tide surge, yet its industrious population dwell there in prosperity and content, confident that their engineers have built and can maintain a system of dykes and sluices which can keep out the flood from the sea. These defences are not absolute and have on occasions been overwhelmed by a combination of exceptionally high tides and storms with heavy loss of life and damage to property. Yet, they are demonstrably sound and accepted as adequate in the knowledge that all reasonable steps which could be taken have been taken in spite of the fact that on those rare occasions when they have failed, the scale of the disaster has exceeded that most pessimistically envisaged for the worst reactor accident (Everyman's Encyclopaedia 1968).

A change of this kind involving a major shift in public opinion cannot be brought about without effort, but it is possible and necessary. The design of a successful campaign is a major research in itself which should be pursued. To be successful it must inspire confidence among the informed public who must feel that they are being assured and not beguiled. The image of the persuaders is of paramount importance and must be one of veracity and relevant professional authority. As Cottrell claimed during his Graham Clark Lecture of 1976, the voices of competent nuclear engineers are likely to be more convincing than those of professional publicists, politicians or eminent scientists expounding out of their field.

While it is not appropriate here to explore the tactics which might win the political case for nuclear power in the national consensus, the second contention which is technological and calls for engineering research will be examined in more detail. The body politic must be satisfied beyond reasonable doubt that, though unquestionable safety cannot be obtained, adequate safety has been realised in the design of nuclear power stations and that the safety aims so expressed can be attained in their construction, commissioning, maintenance and continuing operation. That is to say that they are safe in concept and, if the designer's intentions are fully met, then in no way will there be a serious accident with dire effects off site. But, engineering experience gives a lie to this hope as human error cannot be designed out because it can always circumvent that design. Therefore, in the building and running of such installations determination to adhere faithfully to the prescribed specifications, however sincere, is not enough, but the fact that it has been done must be verified in all respects, and that independantly. It is then possible to give the concerned public a confident promise that the power station and its reactor can meet the safety claims and do not present an unacceptable hazard.

This kind of scrutiny and quality assurance is the duty of engineering inspection, but it goes beyond the mere checking of plans, materials, parts, fabrications and performance of tasks, being concerned as well with the way in which these things come about, the relationships between workers and supervision, the reliance which can be put upon their work and the more subtle consequences of their interactions on the interpretation of the design, a thing which is seldom wholly complete. If engineering inspection can meet this challenge effectively and convincingly, then the battle for nuclear power is in sight of being won.

7. The Nature of Inspection

The literature contains few descriptions of engineering inspection, the generic term

/Contd...

being defined in the dictionaries as 'looking closely into or examining officially, especially for faults or errors': true enough but inadequate. Again, while the administration of health and safety inspection and the medical and physical things which it must find or prevent are dealt with exhaustively, out of 500 sections in the Robens Committee Report of 1972 only some ten discuss the function of inspection itself. It is worthwhile therefore to review the topic briefly before consideration of research in the discipline.

Though faults in design occasionally cause accidents, they are mostly due to human failings in interpretation or implementation of it.

Never deliberate unless malicious, the human factor is usually a story of cutting corners, boredom, fatigue, ignorance, lack of training, ambiguous instructions, poor communications, weak supervision, failure to obey rules or comply with regulations, concealment of mistakes, personal unsuitability for the given task or carelessness, all such transgressions usually being compounded by a measure of arrogance. Discounting the common toll of site and factory accidents as irrelevant to the case, faults in the generality of industrial processes and things made by them may endanger the public image, but seldom have serious consequences for health and safety. Product checking is often cursory and defects are left for the user to find. This state of affairs is not satisfactory in the case of complex and costly installations and processes in which faults can cause heavy financial damage, harm to workers and the public and perhaps fatalities. Human error must then be revealed and corrected before it can precipitate events of this kind and the necessary checking, testing and verification of design and exposure of errors are the defined role of inspection. While good management must be untiring in its attempts to correct human frailties, in the long run unless subject to oversight, the management line itself can exhibit these failings and the scene may be set for a major mistake. Internal or self-inspection is an important part of health and safety management, but it can be afflicted with the same defects and must also cope with internal organisational barriers which can defeat the most assiduous quality control examiner, safety officer or representative.

The task then is to establish an internal regime of inspection of assured consistency and efficacy which can interact profitably with an external surveillance. Engineering inspection whether it concerns plant safety or quality assurance exhibits common characteristics and in its executive applications where an outside inspectorial body overlooks the performance an in-house or lower tier group or the inspectional element of a firm, corporation or establishment has its focus in management structure and morale rather than process or product, though these latter must be given the attention they merit.

Effective quality assurance or safety surveillance when involved with high technology, e.g. nuclear installations, cannot be attained in a go/no-go gauge style nor by a regimen of strict compliance with the details of an engineering specific ation or the rigid enforcement of regulations. This kind of inspectional work can only proceed satisfactorily, and secure safety, in an atmosphere of participation which allows justifiable discretions instead of insistence that technical requirements be fully met or that safety rules and instructions be obeyed in their entirety. While strict observance of these things may be appropriate in the case of the traditional engineering production and factory safety, the drafting of specifications and safety rules for plant employing advanced technology and particularly where there is an element of novelty is complex and imprecise and interpretation is invariably needed. Such is the case in the system of safety assessment and inspection established by the NII whereby a broad technical safety requirement for a nuclear plant or process is written as a condition of licence to which the operator must respond by submitting his proposals for approval by the inspector. The latter then becomes party to the arrangement which he will have duly assessed as appropriate to the circumstances (Cronow and Gausden 1975).

While justifiable discretionary flexibility in the interpretation of specifications, rules and regulations may be appropriate to the safety inspection of nuclear power reactors, it cannot be extended to the general industrial health and safety management of the factory side of the power station. Again, proper relaxation must be distinguished

/Contd...

from lax observance of quality and safety norms and clear lines of accountability for the exercise of discretion must be identified.

8. The Evolution of Modern Inspection

It became clear shortly before the First World War that the product consistency, reliability and safety of flying machines being made for the British Army could not be assured on the basis of foreman inspection, and an Inspection Department for aeronautical material was formed in 1914 (Army Orders 1914). The inspectional procedure was based on a traditional go/no-go philosophy with Government examiners and viewers stationed at every critical point of production in the aircraft factories who were instructed to reject all out-of-specification material. By 1918 many thousands of "Ministry" inspectors of various grades were in post. A system designed to monitor small scale quality manufacture of a few machines was not a success in large scale production of aeroplanes of increasing technical complexity and it is said that a worrying assortment of scrap was coming in increasing quantity off the production lines as well as Sopwith Pups, Camels and SE5s.

After the War Lt.Col. Outram was appointed to head Directorate of Aeronautical Inspection (AID) and was charged with re-organising the inspection of aeronautical matériel. Drastic staff reductions followed and by the early Twenties his AID numbered but a few hundred of elite staff. Outram introduced concepts of delegation and 'executive inspection' which were well suited to maintenance of the quality of the supply of successive generations of ever more complex and sophisticated aeroplanes to the RAF between the Wars (Outram 1930). By delegation of inspection he was not only able to reduce his staff by many-fold, but transferred responsibility for product quality to the manufacturer where it properly belongs. Contracts were awarded only to firms which secured a certificate of approval from the Ministry on AID advice and to be approved meant meeting a tight specification which included such things as assessment of the organisation for its technical competence to meet the terms of the contract, good working conditions, attention to the welfare of employees and a clean and well ordered factory. It was necessary to have a chief inspector who reported to the managing director or his deputy and was responsible for the observance of the specification, the quality of the product and compliance with the AID and purchasing department's conditions. The chief inspector was accorded formal AID approval which became a much esteemed accolade. Great emphasis was placed on maintaining the identity of materials and this was secured by a release note and bonded store procedure. By virtue of the concept of 'executive' or supervisory inspection, the AID inspectors took no part in direct inspection but were responsible, not so much for the quality of the product though evidence of its acceptibility would be required, but to confirm that the contractor's inspection system was working satisfactorily, that the firm's chief inspector certified that the specification was fully met and for signing documents which authorised payment for partial or full completion of contract. This last power provided an important means of exercising pressure on the firm to comply with the AID's requirements. Sampling inspections and tests were carried out by AID Examiners of various grades and there was back-up from a well equipped Test House. The AID inspection system covered all matériel used by the RAF and included radio, radar, clothing and furniture and weapons among other things as well as aircraft. There is little doubt that the AID properly shares the credit with other parts of the British aircraft industry for production of the superb generation of aircraft which made its mark in World War II.

The system continued with little change until 1975 when it had become outmoded by the increasing complexity and range of modern military hardware and the need to adapt to a general NATO quality assurance arrangement for all types of military supply (Defence Standards 1973 and 1976). There are an interesting number of parallels between the inspectional regimes of the pre-1975 AID and that of the NII, although there has been no direct interchange of information.

Again, the reputation of the Air Registration Board which was the civil side sister of the AID attracted attention in the re-organisation of the nuclear safety arrangements which followed the Windscale Plutonium Pile fire and it was recommended that the body to be set up to regulate safety in the commercial sector of the atomic energy industry

/Contd...

should be modelled on it (Fleck 1958). It was not adopted on grounds that such a body would have too great a say in matters of policy which should not be delegated to an organisation not answerable to Parliament.

9. Inspectorates and Inspectors

The Factory Inspectorate, the Alkali and Clean Air, Mines and Quarries and the Nuclear Installations Inspectorates are government organs concerned with statutory safety regulation. They perform the higher tier function of 'executive inspection' which is to confirm that the legal responsibilities of occupiers, operators, the National Coal Board, quarry managements and licensees for safety have in fact been met, though the approach to safety regulation varies greatly amongst them. Any direct inspection or testing such as that made from time-to-time by HMFI is of an investigational, sampling or confirmatory kind. Therefore, their work is basically the inspection of management and of the performance of in-house safety functions and duties.

'Executive inspection' of the foregoing regulatory type makes great demands on the skill and professionalism of the inspectors who in the case of the three technological inspectorates, 'Alkali', 'Mines' and 'Nuclear', must also be highly qualified specialists in an appropriate branch of engineering or applied science. An industrial background with managerial experience is an advantage and often essential. To be effective an inspector must command respect which depends upon his technical competence, being a product of the right mix of qualifications, experience and an imponderable personal quality which may be identified as a potential to secure the objectives of the safety legislation with which he is concerned amicably and only rarely and in special circumstances seeking recourse to legal sanctions (Robens 1972).

The three senior industrial inspectorates, 'Factories', 'Alkali' and 'Mines', have achieved notable successes in their work over many years and have won public respect and esteem throughout the world as well as in Britain. The Prime Minister (Thatcher 1979) has drawn attention to the essential part the NII must play in securing the safety of nuclear power. The concerned members of the public have learned by experience that they can put trust in statutory inspectional and regulatory bodies when they have proved themselves to be competent, independent and disinterested. Thus, the NII is establishing itself as an essential complement to the design, construction and operational sectors of the nuclear power industry, making a safer whole in which public confidence may be properly placed.

10. Some Relevant Research Topics

Inspection has been identified as a function of great antiquity, ranging from the collection of tributes in ancient times, through many police operations to the chairing of a major committee of inquiry (Ayres 1935). Surprisingly then, there has been little or no academic interest in the topic and it has had less than due recognition as an engineering discipline, though this is one of its major areas of application today. The opportunities for research are thus extensive and of great breadth. Excluding the technical matters which are the subject of safety inspection such as personnel protection, management of toxic substances, radiation protection and safety engineering among others, the topic is mainly interdisciplinary and is of the nature of 'liberal studies in engineering' to paraphrase a well established title. Nevertheless, it is very much an engineering study because it requires, at least in the high-technology and advanced scientific industry fields, the approach and sensibility of the experienced professional engineer. This may well account for the lack of interest in the ranks of social scientists as they are not properly equipped to take it up.

Although the openings are legion, the list below is limited to a few major research topics. Among these are:

(i) The invention of a means of assessing the efficacy of specific inspectional techniques in comparative terms, preferably expressed as a figure of merit;

/Contd..

(ii) A broad study of means of interpreting inspectors' reports and of reports by licensees and operators supplied to inspectors, such as the Licensees Event Reports (LERs) which are collected for the U.S. Nuclear Regulatory Commission, so that meaningful data of safety relevance can be gained from them (Carbon 1979);

(iii) A comparative study of the diverse modes of safety and quality assurance inspection which have been developed with a view to assessing the contributions they can make to industrial safety;

(iv) In view of the importance of inspection as a complementary factor in a unitary philosophy of engineering safety, weak or ineffective inspection can be a major cause in accident genesis and particularly in relation to events like the Three Mile Island incident. There is a need to develop:

(a) Personality profiles of effective inspectors for the assessment and selection of applicants for key inspectional posts, and

(b) Means of assessing techniques of inspection most likely to detect 'loss of resistance to failure' in complex and technical sophisticated systems with high hazard potential, e.g. nuclear power plants; and

(v) Strategies for sampling inspections and tests and for the best apportionment of inspectional effort between site or shop contact and technical safety assessment of design.

11. Summary

An attempt has been made to support the claim that the continuing development and expansion of nuclear power are necessary to meet a probable energy famine in the foreseeable future. Failing that, there will be a growing and intractable energy shortage which can destroy the country's standard of life, debase national status, threaten public tranquillity, seriously increase international tensions and, perhaps, undermine democracy. Therefore, the need to convince the public to accept and promote the nuclear option is pressing.

The debate over the very small risks associated with nuclear power lies outside the domain of scientific method, as experimental results must be extrapolated into the realm of hypotheticality, and no firm conclusions can be drawn from them (Häfele 1974). The case to be put which is interdisciplinary has two sides of which one is political and has not been dealt with in any detail except to note that a Micawber-like quiescence is likely to prove disastrous. Instead, the arguments in favour of nuclear power should be shifted on to opposition ground by pointing out the serious detriments which can come from a failure to meet future energy needs. The other is that nuclear engineers have made thermal reactors exceedingly safe. They will not fail on account of intrinsic design defects, but a serious accident could be caused by human error which can affect every aspect of design, construction and operation. However, such shortcomings can be anticipated and prevented by inspection which is a discipline which has arisen to overcome human failings. It can complement design and operational excellence and so make the chance of a major plant accident truly negligible. This argument can be put convincingly to the informed public with good hope of acceptance.

Inspection is a neglected discipline and there is much scope for study and original work. In many areas a positive research contribution may be made which would enhance the effectiveness of inspection and add still further to safety and success in the nuclear debate. Several important topics have been identified as worth investigation.

/Contd...

12. An acknowledgement

Finally, the opinions expressed are entirely those of the author for which he takes full responsibility. They are in no way attributable to any former colleague or associate nor is it suggested that they are supported by any previous employer or principal. But, this disclaimer must not denigrate the stimulating and seminal influence of the many discussions and debates with these people and the generous encouragement they so often gave. In particular, mention must be made of Messrs T. Griffiths, E.C. Williams and R. Gausden, erstwhile and present Chief Inspectors; of Messrs F.R. Charlesworth and P.B. Woods, Senior Deputy Chief and Deputy Chief Inspectors respectively, of H.M. Nuclear Installations Inspectorate; and of Mr S.G. Luxon, a Deputy Chief Inspector in the Hazardous Substances Division, all being members of the Health and Safety Executive. Last, but by no means least, the guidance and helpful advice given by Dr J. Shaw of the Department of Nuclear Engineering in Queen Mary College of the University of London is gratefully acknowledged.

13. References

Army Orders 1914 Military Aeronautics, A.O.5/1914 (January), 1/Gen. 1363.

Ayres, Edith 1930-1935 Inspection, Enclopaedia of Social Sciences Vol. 8, New York and London, MacMillan, 71-74.

Carbon, Max W. 1979 Review of Licensee Event Reports (1976-1978): NUREG-0572, Washington, D.C., U.S. Nuclear Regulatory Commission.

Cotgrove, S.F. 1978 Nuclear Power safer than Windmills? (Letter), London, The Times, Monday 27 November, 13.

Cottrell, A. 1976 The voice of the engineer in public policy - 21st Graham Clark Lecture, London, Council of Engineering Institutions.

Defence Standards 1973 and 1976 Basic Inspection Requirements for Industry, Ministry of Defence, 05-21, 05-22 and 05-29.

Everyman's Encylopaedia 1968 Floods and Inundations, London, Dent, 331.

Fleck, A. 1957 Report of Committee to examine the organisation of the United Kingdom Atomic Energy Authority, Cmnd 338, HMSO.

Fleck, A. 1958 Report of Committee of Inquiry into the organisation of the control of Health and Safety in the United Kingdom Atomic Energy Authority, Cmnd 342, HMSO, S.25-S37.

Flood, M. and Grove-White, R. 1976 Nuclear Prospects, London, Friends of the Earth.

Gofman, J.W. and Tamplin, A.R. 1973 Poisoned Power, London, Chatto and Windus.

Gronow, W.S. and Gausden, R. 1975 Licensing and regulatory control of Thermal Power Reactors in the United Kingdom, Proc. Symp. on Licensing and Control of Nuclear Installations, Vienna, IAEA.

Groves, Leslie R. 1962 Now it can be told: the story of the Manhattan Project, New York, Harper.

Häfele, Wolf 1974 Hypotheticality and the new challenges, Minerva, 12, 303-322.

Haire, T.P. and Shaw, J. 1979 Nuclear power plant licensing procedures in the United Kingdom, Progress in Nuclear Energy, 4, S. 8, S. 9 and S. 11.5, 161-182.

Haire, T.P. and Shaw, J. 1979 Nuclear power plant licensing procedures in the United Kingdom, Progress in Nuclear Energy, S. 5 - S. 12 and S. 14.

Hoyle, Fred 1979 Energy or Extinction? London, Heinemann.

/Contd...

Joslin, S.W. and Griffiths, T. 1962 The Nuclear Installations Act 1959 and its application, Proc. Congress of the Royal Society of Health on the Design and Operation of Nuclear Power Stations: Section L - Radiation, Scarborough, 104-109.

Nelken, Dorothy 1975 The political impact of technical expertise, Social Studies in Science, 5, 35-54.

Outram, H.W.S. 1930 British Aeronautical Inspection, The Air Annual of the British Empire, London, Gale and Polden, 226-250.

Robens, Lord 1972 Safety and Health at Work: Report of the Committee - 1970-1972, Cmnd 5034, HMSO, S.206 - S.216.

Robens, Lord 1972 ibidem S.226 and 227.

Rogovin, M. and Frampton, T. (Jr) 1980 Three Mile Island: Vol. I-A - Report on the Commissioner and the Nuclear Regulatory Commission, Washington, D.C., N.R.C. Division of Technical Information and Document Control.

Thatcher, Margaret and Howell, D. 1979 PM stresses importance of Nuclear Power expansion, Financial Times, 27 June, 1 and 12.

Vickers, Charles G. 1967 Towards a Sociology of Management, London, Chapman and Hall 86.

Octavius H. Critchley
30th July, 1980

DOCUMENT NUMBER 4

TECHNOLOGICAL PROGRESS, SAFETY AND THE GUARDIAN ROLE OF INSPECTION

Synopsis - Public attitudes to technological hazards are examined in the light of the series of disastrous accidents that have afflicted plants, systems and vehicles thought to have been unquestionably safe before the event. Since the Industrial Revolution and more particularly in this century, succeeding generations have become increasingly distressed by the hazards that are concomitant with technological progress, concerns much exaccerbated with the advent of nuclear power. This disquiet has now reached a stage at which the need for technological innovation itself is being questioned. Nonetheless, it is certain that technical progress cannot be halted without severe and incalculable societal and political consequences. Efficaceous technological hazard management has, therefore, become a social necessity.

The history of major accidents bears witness to human error as the principal cause of these incidents. Inspection is the function that has evolved in society to check human mistakes and oversights. It may be classified in four hierachical levels of increasing complexity and involvement of the judgement and discretion of the inspector from the mundane tasks of 'Viewing' to the august chairmanship of an official inquiry. In the field of engineering inspection, a notable development was the creation of the Aeronautical Inspection Directorate (AID) immediately before the First World War to ensure reliability in the manufacture of warplanes. The AID has been the indirect antecedent of the sophisticated modus operandi of modern engineering inspection, and particularly that which has come into being in the nuclear industry. In the regulatory field, these practices have been exemplified by the approach developed by the Nuclear Installations Inspectorate (NII).

Whereas the doubts about the safety of nuclear power plants which still pervade public opinion have not been allayed by the various efforts in public relations made by the utilities and government bodies which currently dominate the industry, it is suggested that people would be more likely to tolerate the risk if they were convinced that they were efficaceously protected by well-organised and accountable inspection. On the other hand, such inspection when backed by statutory authority must avoid the trap of ratchetting safeguarding investment in areas where safety may be already adequate, the criterion of adequacy being one of the most difficult of the challenges that faces regulatory science.

Technological progress, safety, and the guardian role of inspection

O H Critchley, MSc, ARCS, FIEE, FInstP, FINucE, CEng,
Reardon-Critchley International,
9 Sutton Lane,
Hounslow, Middlesex,
TW3 3BB, UK

'Not even God himself could sink this ship' commented a well-wisher just before the mighty White-Star liner, *Titanic*, left Southampton on her maiden voyage to New York. She foundered in the icy waters of the North Atlantic a few days later during the early hours of 15 April 1912, some five hundred miles East-south-East of Halifax, Nova Scotia, with the loss of more than 1500 lives following a freak encounter with a huge iceberg South of its expected haunt. It happened in spite of every reasonable precaution, scientific and human, being taken to avoid such an occurrence. The sea was calm, though deathly cold, and the visibility good. She lay holed beyond the capacity of her powerful pumps in a busy shipping lane with passing vessels less than an hour's steaming from her site, yet their wireless rooms were deaf and their bridges blind to her cries of SOS and distress rockets, though she took nearly 3 hours to sink.

Towards the end there was panic on the decks which added to the death roll and, though many famous and eminent men sacrificed their lives, 156 women and children still perished.

Within 3 years a further 1800 lives had been lost in shipping accidents, excluding another thousand odd with the controversial sinking in 1915 of the *Lusitania* a few miles off the West of Ireland by a German torpedo. This awesome mortality coupled with a mounting score of factory and mine fatalities brought a new awareness of safety to the body politic as the hazards were no longer confined to the proletariat but affected all sections of the community. Working people whose unions were growing stronger were thus able to press effectively for greater safety in pit, on shop floor and construction site.

In fact, safety had become part of the great humanitarian change which had its birth in Europe and America a little more than a century ago. A growing trend, rather than a sudden change, it began in Britain with free elementary education through Forster's Board School Act 1870, to be followed over the next few decades by laws ensuring the purity of food and drink, control of foul factory effluents, for old age pensions, national health insurance and unemployment benefits, moves towards the full emancipation of women and legislation to improve working conditions in factories and mines. Of course, there was stimulated interest in the safety of life at sea and many inter-

---

uring World War II, a radio operator and radar chnician, with nearly 600 hours of airborne e, and escaped unharmed from several shes. Graduated in Physics at Imperial College, ndon, 1949. Electronics and instrumentation search thereafter. Founder member of the clear Installations Inspectorate of the Health d Safety Executive; he retired as a Superintend- Inspector in 1979. He was concerned with inspection, technical services, technical safety, ssment of design for Advanced Gas-cooled ctors, and radiation protection. In 1974–76, mon Fellow, Department of Liberal Studies in ence, Manchester University.

 0302-3427/81/040291-17$02.00

national conferences held and conventions signed, notably in respect of wireless telegraphy and provision of lifeboats. Before this awakening of public conscience, but for some notable exceptions, industrial risks were taken to be more or less inherent in one's way of life. The 'madness of hatters', scrotal malignancy in chimney sweeps and the respiratory diseases of miners and glass cutters were taken to be unavoidable.

Cost of change

History teaches that the introduction of a new technology almost invariably brings with it unforeseen consequences which not only disturb the established social order but are often very damaging to man and his environment. Eventually, these adverse effects are understood and the dangers are, thereafter, avoided, mitigated or accepted. In the entrepreneurial enthusiasm to secure the benefits of innovation, the lesson from the past is often unlearnt, but in arresting cases such as the examples just cited there is a permanent imprint upon society and its mores. This is especially so when there are many victims, children are involved or the circumstances grisly, and popular reactions seem to obey a sort of power law relating to the number of casualties,[1] the extreme reaction to the tragedy of Aberfan[2] being a case in point.

Few can deny that technology has brought great benefits to mankind, liberating him from slave civilizations, substituting leisure for druggery, relieving him of pain and disease and disseminating culture, albeit often of depressingly shallow content, widely amongst the masses. Without it, Western civilization with its liberal, humanitarian ethos could not have attained the heights that have so far been reached. Yet, there is a counterpart of hazard associated with each advance in a kind of proportion to the potency of the agency exploited. For example, the invention of nitrated explosives has been one of the most commercially rewarding of technical innovations, making possible great achievements in civil engineering, giving more ready access to the Earth's mineral riches and enabling canals and highways to be cut through hard rocks impermeable to pick and shovel. But, the cost in human terms has been high with heavy loss of life and limb and extensive property damage caused by unforeseen plant explosions such as that at Faversham, Kent, in 1847, a few months after the discovery of gun cotton (nitrated cellulose) and nearly 80 years later at Oppau on the Rhine near Ludwigshafen in Germany when over 1,000 people were killed, many more injured and the town wrecked.[3] Not least, the new explosives made war more murderous; civilians could now be attacked with bombs and shells and battle casualties counted in millions instead of thousands.

Growing doubts

In addition to the pressure for more specific protection for life at sea, in factories and in mines, there has been growing concern about more general threats to citizens, community and environment as people have become aware of the apparently inexorable, and often unwanted, thrust of technical and medical innovations which have brought unpleasant consequences and unexpected side-effects to mar their vaunted benefits. The drug Thalidomide comes into this latter group; high octane leaded petrol may soon prove culpable; and, in addition to the worries about atomic energy, there are growing doubts on the consequence of exposing populations seeking longevity to some of the products of modern food technology, the highly refined cereals used in the manufacture of bread and pastries.[4]

While efforts to protect the environment, to conserve economic resources for use by future generations are commendable, and, indeed, essential, it is unrealistic to think that the political majority of the people in any developed country are going to accept regression to a more primitive and less

abundant life style. The reaction to the coming famine of natural resources and, of course, fossil fuels would be a demand for a continuing advance of technology to beat the shortages and science would be expected to discover new ways to maintain the desired supply of customary creature comforts. This reaction will be particularly true for energy which, though it may be more economically used, may nevertheless be needed in increasing and not diminishing amounts.[5] For example, an economy in which hydrogen manufactured by atomic power replaced oil as the main local energy source can be envisaged as commercially viable early in the next century.[6] Assuming satisfactory solution of the questions of reactor safety and nuclear waste disposal, such a hydrogen based economy would be ecologically safe and environmentally very clean as the combustion product would be water instead of the pyro-products of the hydrocarbon fuels, oil and coal, ie the oxides of carbon, sulphur and nitrogen, now massively contaminating the atmosphere, locally and globally.[7] Notwithstanding the environmental gains, hazards of a new kind would be introduced as hydrogen, the most flammable of gases, replaced stable hydrocarbons as the basic fuel and energy source.

technological progress and innovation cannot be stopped without severe social consequences which are likely to be beyond the power of known political institutions to manage, the way ahead lies in an approach which makes the benefits maximal and the threats and detriments minimal, so ensuring that the introduction and exploitation of the technics remain under the control of democratic agencies and institutions and does not slip into the hands of elite, technocratic bureaucracies. Unfortunately, the very complexity and the capital-intensive nature of high-technology invites such a transformation and political science must be ready to meet the challenge.

Among schemes for monitoring technical innovation is one advanced by Ravetz[8] 'for those cases in which technical competence is likely to be monopolised by a few specialists concentrated in institutions committed to the same interest', eg national electricity generating utilities and atomic energy agencies. Nevertheless, the proposed 'Technical Innovation Commission' (the task of which would be 'to foster the discovery, assessment and diffusion of reliable information about advanced technical projects so as to provide conditions for effective monitoring with appropriate public participation . . .') is not enough for it would operate in the political rather than the practical industrial realm of plant, operators and accidents, at least in respect of high-technology, major-hazard installations. Moreover, it is the pit, shop-floor and site from which the troubles come. The toxic cloud of the virulent poison, 'dioxin', which spread over Seveso was emitted from the factory and not the board room of Givaudan, yet the administrative responsibility lay with the latter.

Risk acceptance

While some of the reactions to technology border on the fatuous or lack any obvious rationality other than being displacement responses to different threats and fears,[9] there is nevertheless justifable unease. Brett-Crowther has drawn attention to a disturbing political aspect of technological progress which he defines as technocracy: "the tendency of unelected officials, secure in established posts, and having the advantage of government authority as well as an apparent impartiality, to offer advice and take decisions as if science and technology were boundlessly good and reliable, fully understandable elements of a material universe which was also entirely rational."[10] Indeed, some of these technocrats are tempted to define this kind of lordly imposition of their concept of 'progress', coupled with a beneficiently motivated but imperious interference in the discretionary areas of human conduct, as a sort of 'divine right' of administrative government. There

is an associated belief in elegant risk mathematics by which hazards may be reduced by presenting them in a mist of vanishingly small numbers, a tendency which might be likened to Sorokin's 'quantophrenia'.[11]

Public toleration of the danger from a technology, from an inadequately managed environmental threat or from unhealthy or risky social activities or involvement does not depend on probability of its realization, unless the chance is disturbingly high. The ordinary person will accept a risk known to be very small, heedless of any consequences, though they may be severe, but does not normally act so as to subject himself to a clearly perceived and likely chance of death, injury, or particularly unpleasant sequel. The topic is highly controversial and the subject of much research. Farmer puts the threshold of popular concern for risks endured during normal living as 10^{-4} [12] and there is some evidence on a broad statistical basis to support his figure; but few people are average and the range is very wide, not only among individuals but as a function of the perceived nature of the threat and personal feelings about it: a person who wouldgo to great lengths to avoid walking under a ladder might well refuse to wear a seat-belt in the front passenger seat of a sports car.

Dutch courage

When people at large see that a technology is worthwhile because it serves their needs and pleasures, eg in the cases of air and motor transport, the risks are taken with little complaint or hesitation. An interesting example of the phenomenon is given by the case of the Netherlands. But for the elaborate system of dykes which effectively keep the waters back, 80 percent of its land would be washed over by the sea at the equinoxial spring tides. Occasionally, though very rarely, these defences are overwhelmed and the inundations flooding in from the North Sea have drowned tens of thousands. Yet, people continue to live happily in that country though folk tales abound to remind them of their peril. Dutch engineers are highly competent and respected for their sound and reliable work in building and maintaining the sea walls; but the caprice of tides and extremes of weather have on past occasions proved beyond the ranges of these defences, and so it will be for ever because considerations of cost determine their height and there can always be a surge of water driven by tides and storms which will exceed that economic limit.

The reasons for acceptance of these rare cataclysms are profound and beyond the logic of cost-benefit analysis. Such social phenomena are not well understood, as the contrariety of the spate of theories on the acceptability of risks shows. In this case, however, acceptance probably turns on the basic human social instincts to follow traditional paths of established worth and to put trust in the judgment of respected leaders and in the wisdom of experts of high repute. It is known that all that is reasonably practicable has been done under the circumstances and that advances in the sciences of meteorology and hydrography, by making possible more effective prediction of the approach of danger coupled with efficacious modern communications and transport, can reduce the hazard to one of inconvenience rather than drowning. Thus to leave a comfortable and prosperous existence in Holland to avoid a very remote risk of death in an unlikely, uncontained flood would have been seen by the Dutch public as behaviour lacking in commonsense. On the other hand, evidence of increased risk attributable to incompetent engineering or other kinds of human error would not readily be tolerated, to say the least.

Safety technology

Accident experience drawn from the domain of large and complex technical installations and systems – aeronautical, coal mining, marine, nuclear and petrochemical, has been the story of the unexpected leading to

sensational events, often disastrous in human, environmental, financial and operational terms. These happenings, combined with the toll of life and limb in more mundane industries which are caused by apathy, carelessness, ignorance and negligence on the part of both managements and workers have shown that strong watchdog functions are needed; not only to enjoin compliance with health, safety and environmental protection standards, but to ensure that management does not become lax about safety and keeps abreast of dangers associated with technical change.

Few disastrous accidents in advanced technical systems have been caused by failures of equipment or structures although they have played a contributory part in the event sequence, but by human fallibility mainly as operational mistakes and blunders. Examples of disasters in which human error has been the salient causative factor are the Tay Bridge collapse in 1879,[13] the *Gen. Slocum* horror of a living funeral pyre for nearly 1,000 people in New York's East River in 1904,[14] the foundering of the *Titanic* referred to above, the R-101 airship explosion which killed 46 including 11 notable people in 1930,[15] the Aberfan tip slide of 1956,[2] the Thalidomide tragedies of the early 1960s, the Flixborough petrochemical plant explosion in 1974 and the nuclear plant accidents at Windscale in 1957 and that at Three Mile Island in 1979; all of which have transcended their scores in fatalities or financial loss by their impact on public opinion to produce exceptional political reactions which have resulted in vigorous government intervention and strengthened safety regulation of the technology and its practice. Profound changes in the administration of safety technology and equipment have been encouraged through government funding and research. A stage has been reached at which 'safety engineering' and 'regulatory science' can be defined as distinct disciplines, meriting the foundation of University departments in their name.[16]

In the realm of high technology, safety can not be assured merely by the enforcement of regulations or by routine observance of codes of practice, no matter how conscientiously. These are responses to things which have happened and are inadequate in the face of that which is new and unexpected. Hence, an added forward-looking technique of 'safety analysis' has come into being which consists broadly in assessing the design of the plant so that possible fault and accident event sequences may be discerned with a view to devising engineered safeguards or prescribing plant operating procedures and rules which can forestall them or abort their progress to catastrophe,[17] but even such foresight can be rendered futile by human mistakes[18].

And so over the past half century there have been novel and very positive developments in safety technology and regulatory practice which have been inspired by military necessity as well as concern for workers and public safety. They have led directly to the notably high levels of safety achieved in the nuclear industry in particular which, although potentially very hazardous, has during the 40 years of its existence, in the Western world at least, caused only three deaths, very little proven harm to the health of its employees and none to the public which has been established beyond question. There has been little or no lasting environmental damage and there has been an apparent spin-off from the safety conscious atmosphere in 'nuclear' plants of a general industrial injury rate running at less than one-third of that for industry as a whole.[19]

Human error

Disastrous happenings in man-made systems, aircraft, buildings, factories, coal mines and ships are very rarely, if ever, the result of single, unique act or thing, but come about because a series of consequent events leads to the catastrophic conclusion. This postulate has a sophisticated analogy in Thom's

Catastrophe Theory which is a relatively new development of mathematical logic to describe the evolution of forms in nature. It has been much elaborated and can be applied to a wide range of biological, physical, psychological and social phenomena including economics[20]. The development is in keeping with a change in the attribution of blame in reviews of serious plant and systems accidents. Previously, news reporters, the general public and even government investigators have looked for a sole precipitating act, fact, fault or erring person, thus seeking some specific agent or scapegoat on which to place the responsibility for the untoward happening.

Despite the fact that the application of Thom's hypotheses to the problems of safety are far from obvious and that the present scientific approach, which is mainly dedicated to quantification, appears to need considerable refinement before it can yield convincing and definitive results in accident and process loss prevention[21], there has emerged a better understanding of fault causation through the work of a number of inquiries and related studies[22]. Of particular relevance are those which have followed some of the more sensational nuclear plant incidents, notably the Windscale Plutonium Pile fire[23] and that at Three Mile Island in Pennyslvania, USA[24]. The latter which is classic has been exhaustively studied by Presidential, Congressional and regulatory commission (US NRC) teams, not excluding multifarious investigations by concerned research bodies[25]. The new tactics amount to a systems approach, although perhaps not overtly so oriented. Catastrophic events in complex or large plants and technological systems are seen as the interaction of an ensemble of things, equipment, components, structures, procedures, external influences and men, all actually but not obviously related, which become linked together in the manner described earlier, to make the fault sequence or sequences that end in the ultimate calamitous happening. A result has been to discourage what has been the notably mechanical approach of many previous formal inquiries, turning more towards recognition of the part which human behaviour plays, if not directly, then to set the scene for a better understanding of the engineering malfunctions which caused the disastrous event.

Flexible theory

This is in keeping with a general trend to replace philosophical mechanism[25] with more flexible systems conceptualisations, explaining an untoward event as a system's response to unexpected changes in its circumstances, internal and external. Thus, the ultimate catastrophe is seen as the interaction of physical and human factors which cohere in the given situation, thus driving the system irreversibly towards breakdown or destruction, as in Thom's theory. The approach has disclosed the not surprising fact that men plays the main part in accident causation through carelessness, ignorance, negligence, stupidity and frequent capricious aberrations in his performance of actions which are often of a routine kind.

Though attention has been directed to the importance of this factor which has been defined as 'human error', in the case of nuclear accidents, it is equally responsible for disastrous failures in other advanced or complex technological systems, like petrochemical installations.

The baneful influence of human error has long been realized, but perhaps not overtly identified in plant and systems accidents.[26] Human error is a continuum and not something unique and manifest unexpectedly in control room, on a ship's bridge, in signal box or diver's cab. Everything in the man-made world may tautologically be defined as an artefact or the result of action by an artefact. Even in those few cases where the accident may appear to be attributable wholly to failure of components, equipment, structures or mechanical or electrical systems, there is almost invariably an elemen

of human blunder or mischance, often at the level of design. The exceptions are those rare events in which there has been a true lack of knowledge and the factors to which the failure was due were scientifically unknown before the thing happened. Such was the radar-assisted collision between the luxury Italian cruise ship, *Andrea Doria*, and the Norwegian liner, *Stockholm* off New York in 1956 which sank the former with much loss of life and injury.[27] Both ships were fitted with the most up-to-date of available devices and systems to ensure the safety of life at sea and were crewed by alert, efficient and well trained officers, but without the falsely trusted help of radar, traditional methods of navigation would have prevented the collision. The truth has been revealed; interpretations of the 'Rule of the Road' take the failings of radar into account[28] and seamen now have no excuse for being unaware of the hazards of unwitting reliance on novel scientific aids.

Approaches to control

If one accepts that human failings are at the root of most industrial accidents and the cause of serious process losses and those faults which when affecting large installations or means of transport could result in harm to people, damage to property and injury to the environment, then one must conclude that the best means of preventing such untoward things is to find ways of detecting or correcting human error before it can lead to the unwanted event. Moreover, inquiries into accidents could profitably place more stress on the part played by people in accident situations and in particular on management blunders, defaults and inadequacies[29] which have received less than due attention in the past. Board room and design office are as prone to make mistakes as operators and workers.

There is much current interest in the discovery of means to detect and anticipate human error. In accord with the present popularity of numerical probability concepts in science, serious attempts are being made to classify, measure and quantify human error.[30] Though such work may throw light on its manifestations and vagaries and perhaps create a better terminology, the tractability of such an amorphous and capricious phenomenon to mathematics and quantification is open to doubt. It would seem that greater progress might be made by combining traditional engineering practices with the powerful facilities of data collection and analysis provided by information science.[31]

The traditional approach has derived from the reaction of the body politic to the cost of faults and to the dangers and disasters caused by human mistakes. To reduce the threat and its expensive consequences, it has evolved the art of 'inspection', a generic term for a group of diverse activities all concerned with the detection of errors, faults and mistakes of various kinds by examination, and particularly close examination, of the circumstances and systems in which they may arise. Its practice ranges from routine piece part examination of the products of repetition engineering to inquiries of a constitutional nature when the functions of august public bodies may be reviewed. It will be worthwhile to look closely at the role of inspection in the pursuit of health and safety in industry and particularly in advanced-technology plants and systems as represented by nuclear power stations.

Informed inspection

Protection of the community, citizens and workers and the environment against undesirable aspects of human activities and the ill-consequence of human error has long attracted intervention by the state, and may be broadly called inspection. It is inherently a police function with its origins in antiquity when its main task was to ensure proper performance of the duties assigned to public officials, eg the collection of taxes, tolls, customs, tributes and the surveillance of

trading by merchants.[32] In modern societies governments regulate many less tangible things, such as commodities and banking. The state can not achieve these ends by the promulgation of rules alone as they become dead letters, even when backed by severe penalties for infraction, unless some form of surveillance is imposed. This is the object of police power which in its broadest sense is the exercise of the authority of the state in the interests of all citizens. Policing is carried out by special bodies of people who, as the police proper, enforce restraints against such anti-social activities as are defined as criminal, and civilian officials who are generally known as inspectors, concerned with such commercial things as the regulation of weights and measures and industrial safety.

The bodies concerned with industrial safety have grown up piecemeal and show great diversity. The two senior inspectorates in Britain are those responsible for safety in factories and in mines and quarries, the former identifying its birth with the appointment of 4 inspectors in 1833 to enforce the 'Act to regulate the labour of children and young persons in mills and factories' and the latter with the appointment of the first 4 mining inspectors in 1850. Later additions to the roll were the Alkali Inspectorate which dates from 1863, the Explosives Inspectorate which came into being in 1875, the Nuclear Installations Inspectorate about which more will be said later and the Radiochemical Inspectorate, both of which were established in 1960. There has been an attempt to impose a measure of unification under the Health and Safety at Work Act 1974, implementing recommendations made in the Report of the Robens Committee of 1970–72. A further stage of integration was recommended with the eventual aim of an amalgamated service oriented more towards the formulation of safety policies and the provision of expert advice and assistance in safety matters to industry than to the enjoinment of safety norms by field inspections.[33]

Whether these varied activities are susceptible to a centralised administrative control, 'speaking with one authoritive voice on matters of health and safety', is still far from clear. Moreover, competent opinion in properly informed quarters is by no means convinced that the enhancement of advisory, code drafting and other 'policy' functions with a diminished role for inspection as recommended by Robens[33] will be any more effective in the achievement of greater industrial safety than its promotion by inspectors making visits to premises and installations which result in persuasive personal contacts backed by a hint of enforcement. It is appropriate, therefore, to examine the long established art of inspection which Ayres[32] identified as a practice ranging from quality control in manufacturing through civil police work and the surveillance of matters of health and safety, which has already been viewed in some detail, to its highest level in a public inquiry when the presiding officer, often a member of the judiciary, is known as the 'Inspector'.

Illusory control

The esteem which was once accorded to the engineering discipline of inspection has waned of recent years as the purchasers of mass-produced motorcars learn to their cost. The above reference to 'inspection' by Professor Edith Ayres,[32] dated 1935, is unique. It has been replaced in later editions of the same source by a highly mathematical effusion on 'Quality Assurance' and all direct reference to inspection deleted. The Robens Committee Report of 1970–72 devotes only 10 of its 500 sections to the art of inspection and even these concern its administration rather than its practice. Lastly, there is a judgement by an eminent safety scientist, and not untypical in some establishment circles, that:

> There is a widely held and, in my view, rather quaint opinion to the effect that inspection is the primary source of safety. Again, from my point of

view, it is a somewhat gratifying opinion, but it is not, I fear, entirely true. Certainly, the new look which an inspector can give to a situation which has become over familiar to the operating management enables safety issues to be raised and improvements suggested. But I suspect that these improvements are essentially marginal. The thing that really provides safety is a proper management attitude and a proper management understanding of the science, technology and engineering of the operating plant.[34]

The statement is notable for its apparent lack of understanding of the part to be played by inspection in the given circumstances of safety surveillance of an advanced-technology installation. Most certainly, inspection is not a 'source of safety', nor could or should it be. Competent management is its true source. The role of inspection which remains paramount is then to assess the quality of that source which, as the author says, is 'a proper management attitude and an understanding of the science, technology and engineering operation of the plant'. The inspector must have the appropriate engineering attainments to make the required assessment and be vested with the necessary authority so that he can, if required, take effective steps to ensure that management discharges its responsibilities efficaciously.

Engineering safety

The nature of engineering inspection as applied to nuclear power reactors which may be taken as a paradigm has been described in detail by Gronow and Gausden[35] and by Haire and Shaw.[36]

Engineering inspection which is concerned with the product quality of engineered artefacts and plant and systems, particularly safety in this instance, can be identified at 4 discrete levels; and, though of less concern to this study, other types of inspection may also be classified in a like manner:

(i) *Viewing* – routine scruinty of manufactured work-pieces with little or no exercise of discretion, eg printed circuit boards for computers, product quality of confectionary and quality control test of photographic films. It is the most commonly identified kind of inspection and has been the subject of a number of studies in social science;[37]

(ii) *Examining* – a higher order function, being examination of products, structures, equipment, machines and systems to confirm compliance with specifications or rules and permits a necessary exercise of discretion and is often an interpretive function, eg customer acceptance inspection and routine factory inspection of minor premises;

(iii) *Executive Inspection* – it requires high and appropriate professional attainments for its effective conduct and may be divided in two sub-classes, ie:

(a) *Managerial Inspection* – investigation of the manner in which persons, teams and groups discharge their contractual obligations or perform their official duties, eg staff inspections in large organisations like the Civil Service, with a view to assessing management or professional competence, inspection of schools;

(b) *Assessment-Inspection* – chiefly an engineering activity concerned with the extent to which a design intent is achieved in plans, designs and specifications for a technological plant, system or piece of equipment and with confirmation of the satisfactory attainment of these goals in the manufacture, construction, commissioning

and in use or operation of these things which usually involves design office, shop floor and site contacts (an example is the technical safety assessment of design in nuclear engineering as applied to power reactors – [38]);

Note – Executive Inspection often combines the two sub-classes when, in addition to technical assessment of the design of an installation or system, its organization and staffing are also subject to scrutiny and report and such is often the case in the statutory inspection of nuclear installations, eg power reactors; both activities are essentially participatory and involve the formulation of technical policy, the inspector being continuously required to make critical professional judgements;

(iv) *Inquiry* – the highest order of inspection and is concerned with the examination and assessment of the roles, appropriateness of function, efficacy, integrity and propriety of state, commercial and social institutions, corporate bodies, government functions and programs.[39]

Unresolved problems

Management fully aware of its role and of 'the science, technology and engineering of the operating plant' may be expected to run a safe factory or installation. An efficient management will have this capability and a proper concern for safety, but human error is everywhere, afflicting even the most able of men and organizations. The task of executive inspection is, then, to enquire, to seek explanations and to perceive changes or modifications in plant, processes and performance of the human part of the entity which may provide evidence of the 'loss of resistance to failure' that so often appears as a portent before an accident. The duty of the inspector is not to tell the operator or management how to do the job, but to assess the performance of the system and to judge the capability of its elements to work in co-operation with one-another. Intervention by an inspector provokes an introspective reaction in management, encouraging those of its components drifting towards egotism and introversion, which is a centrepetal bias inimical to safety, to become more outward looking and communicative. If the foregoing criteria are met, then a management is more likely to be able to discharge its safety responsibility efficaciously and have the resilience and flexibility to abort the progress of a fault or mistake which could lead to a disaster.

It cannot be denied that executive inspection so involved in safety surveillance is labour intensive, costly and may at times impose severe financial burdens on the managements of factories and other installations subject to it. This is especially pertinent when an inspectional safety assessment discloses a serious fault or weakness in the design of a plant, imposing a late change, an affair widely publicised in the case of the Hartlepool nuclear power station which the CECB claimed cost £25 000 000.[40]

No design which contains significant novelty can be expected to be perfect in its early realizations in hardware, as this is a state of grace attainable only by trial and error and through experience in use.[41] The inspector must wisely resist a tendency to ask for apparently desirable features or modifications in an entity which is already adequately safe, lest the job be priced out by ratchetting costs. Furthermore, an important aspect of the technical safety assessment of an engineering design is to discover flaws and weaknesses and arrange for their correction before they

have been irreversibly incorporated during the progress of construction and commisioning of the plant of system. Although retrospective modifications are exceedingly expensive, safety must be defended and in the case of a serious threat, the fault giving rise to it must be rectified; in extreme cases even to the extent of stopping construction or of shutting down the installation. Clearly, the balance which must be struck between problematical dangers and the cost of removing them presents the inspector with a most difficult task and is one of the main challenges facing regulatory science.

Summary

In spite of the fact that the responsibility for regulatory safety inspection in Britain is spread amongst a number of specialist inspectorates, it is, perhaps, the most fully developed, efficient and satisfactorily operating regime of its kind, this being especially true for commercial nuclear installations. The latter aspect is a complex mix of engineering, legal and managerial practices which has been largely modelled on the notable developments in safety technology which have characterised atomic energy since the Manhattan Project in World War II, its skill being transferred from that milieu to the UK Atomic Energy Authority[42] and so to the Nuclear Installations Inspectorate (NII).

There has thus come into being a versatile scheme for the licensing and inspection of reactors and other atomic energy installations prescribed under the Nuclear Installations Act 1965, which has received a delegation of statutory administrative responsibility to a engineering body unusual in Western democratic government practice. It is a history which began with developments to meet the needs of the military aeronautics industry early in 1914 and, though full, rich and interesting, has received less than due attention with only a few scanty references in specialised technical literature.

An attempt to make good some of that deficiency is contained in the Appendix.

A conclusion to be drawn is that all approaches to safety are asymptotic, and absolute reliability (which may be equated with safety) is unattainable. This is certainly true of attempts to secure ever greater safety by design and by organizational improvements in management, as the evidence confirms. Such improvements will be likely to be marginal. Human error will always break through to confound such efforts. Thus, the greatest gains are likely to derive from well directed inspection, because inspection bears directly on human fallibility. That is the purpose for which it has been developed.

Acknowledgements

The opinions expressed, some of which may be considered controversial, are entirely those of the author for which he takes full responsibility. They are in no way attributable to any former colleague or associate nor is it suggested that they are supported in any way by any previous employer or principal. Nevertheless, this disclaimer must not exclude the influence of many discussions and debates with these people and the generous encouragement, not without some criticism, which they so often gave. In particular, mention must be made of Messrs T Griffiths, E C Williams (deceased) and R Gausden, all erstwhile Chief Inspectors of Nuclear Installations, of Mr S G Luxon, a former Deputy Chief Inspector of Hazardous Substance in the Health and Safety Executive and of Professor Brian Harvey who was at one time HM Chief Inspector of Factories and latterly and until retirement one of the three senior Members of that Executive. Last but by no means least, the assistance given by Dr John Shaw of the Department of Nuclear Engineering in Queen Mary College of London University, is gratefully acknowledged.

Appendix: Antecedants of the NII [43 44]

Notwithstanding the reservations of some senior military officers, it had become clear to the Army Council by 1913 that aeroplanes were going to play a very important military role and that their engineering, being very complex and the most advanced technology of its time, merited special consideration. It was further recognized that 'foreman inspection' which was then the usual practice in the manufacture of sophisticated artefacts would not be adequate to detect and correct errors in workmanship, particular under conditions of large scale production, which could lead to accidents and the loss of expensive machines and pilots who would be costly to replace. The military consequences could be disastrous. To meet the need for high quality and reliable manufacture of military aircraft, an 'Inspection Department for Aeronautical Material' was formed early in 1914 (Army Orders, Military Aeronautics, AO 5/1914 – January). The new inspectional body was set up at Farnborough, Hants, and recruited a small body of highly qualified engineers from both the Army and civilian life, the latter being sought by discreet advertisements in the technical press, eg:

> Candidates for Examiner appointments should be gentlemen having good theoretical and practical training in engineering . . . . Preference will be given to gentlemen unfitted for military service. These appointments give patriotic men, having the necessary qualification an unequalled opportunity to serve their country. Salary from £3-14s. to £4-4s per week . . . . (A substantial amount at the time.) . . . Viewers are needed at 38s to 48s weekly.

The inspectional procedure was based on a traditional go/no-go philosophy with Government examiners and viewers stationed at every critical point of production in the aircraft factories who were instructed to reject all out-of-specification material. After the outbreak of World War I, there was an explosive growth of the aeronautical industry and at the Armistice in 1918 the Aeronautical Inspection Directorate or AID as it came to be known, employed 18 000 odd inspectors, viewers and examiners, either on its own strength or as agents. The change in size brought with it a change in function and at all key points in the processes of aircraft production throughout Britain a representative of the AID was stationed to detect faulty workmanship.

The result was not that which was expected, that was a marked improvement in both production flow and quality. Although the machines which went into service were well made and out of the last 28 000 aeroplanes accepted by the AID, there were only 9 cases of accidents in service which were traceable to defective workmanship, the proportion of rejects found in the production lines was steadily increasing, reaching as much as 90 percent in some factories. Growth of the industry had altered the scene from one in which an engineering inspector could be identified as a personality in the manufacturing process, able to participate in the work by assuring product quality, to one in which an agent of an impersonal government presence imposed the requirements of the specification in an inflexible manner. The result was to take away the responsibility for good workmanship from the site of production and instead of a feeling of involvement in the effort and product quality, there arose an attitude of 'let it go through because it is the job of inspection to find it.'.

By 1917 there was a dire need for aircraft and the rising tide of scrap in the aeronautical factories was a cause for serious government concern. It was felt that a measure of militarisation might improve morale and enjoin better workmanship. With this in mind, senior ranks in the Aeronautical Inspection Department (AID) were granted General List commissions in the Royal Flying Corps with apparently no very great effect on the shop floor.

Clearly, the system had broken down and, so, at the end of the War when the vast

flow of airplanes was no longer required and the huge staff of whom over 10 000 were directly employed by the AID had to be stood down, an opportunity to remodel the whole inspectional function was taken. Within 12 months of the Armistice, the strength of the Directorate had been reduced to some 500, mainly people of previously senior rank. The slimming process continued as part of the re-structuring and even during the early 1930s the complement did not exceed 300, although aircraft production was still substantial and technical innovation continued apace. The responsibility for good workmanship and quality was now placed wholly on the manufacturer who carried out his own inspection, though under AID approval and supervision. The name principally associated with the AID during this period and until his untimely death at the end of the War was that of Lt Col H W S Outram.

The scene was changed to one in which each firm tendering to make any aeronautical materiel ranging from minor components to complete machines, had to agree to terms of contract which defined not only requirements for inspection, but that the working conditions were of a high standard, eg that the lavatories were clean and pleasant. A most important condition was that the contractor should appoint a Chief Inspector with direct access to the most senior levels of management, the person appointed being further subject to approval by the AID, carrying with it authorisation to certify that the products leaving the factory met the specifications. This approval, having formal government recognition of competence, became a much esteemed accolade.

Great emphasis was placed on maintaining the identity of materials and this was secured by a release note and bonded store procedure. By virtue of the concept of 'executive' or supervisory inspection, the AID inspectors took no part in direct inspection but were responsible, not so much for the quality of the product though evidence of its acceptability would be required, but to confirm that the contractor's inspection system was working satisfactorily, that the firm's chief inspector certified that the specification was fully met and for signing documents which authorised payment for partial or full completion of contract. This last power provided an important means of exercising pressure on the firm to comply with the AID's requirement. Sampling inspections and tests were carried out by AID Examiners of various grades and there was back-up from a well equipped Test House. The AID inspection system covered all matériel used by the RAF and included radio, radar, clothing and furniture and weapons among other things as well as aircraft.

While AID approval when granted to an inspector was a valuable vocational qualification, failure of inspection was a serious misdemeanour. If a bad failure occurred in service, its source could be identified and the firm's Chief Inspector could be held to be reprehensible with loss of AID approval and probably employment. Thus was the AID presence transformed from that of a horde of officials scrutinising, checking, cross-checking and stamping the bits and pieces of production, to a few officers of long experience and recognized ability who could achieve esteem and respect amongst contractors and their staffs. This can be confirmed by reference to the literature of aeronautics during the period.

Outram's important contributions to engineering inspection by his concepts of 'delegation' and 'executive inspection' should be given their due recognition. In application they proved to be well suited to maintenance of the quality of the supply of successive generations of ever more complex and sophisticated aeroplanes to the RAF between the Wars. By delegation of inspection he was not only able to reduce his own staff by many-fold, but transferred responsibility for product

quality to the manufacturer where it properly belongs. There is little doubt that the AID properly shares the credit with other parts of the British aircraft industry for production of the superb generation of aircraft which made its mark in World War II.

The system continued with little change until 1975 when it had become outmoded by the increasing complexity and range of modern military hardware and the need to adapt to a general NATO quality assurance arrangement for all types of military supply (Defence Standards 1973 and 1976). There are an interesting number of parallels between the inspectional regimes of the pre-1975 AID and that of the Nuclear Installations Inspectorate, although there has been no direct interchange of information.

The Air Registration Board which was the civil side sister of the AID was largely modelled on the lines of the latter and it also earned much esteem in its regulation of the commercial aspects of the aeronautical industry and of air transport. This attracted the notice of Sir Alexander Fleck (later Lord Fleck) who was chairman of the commission of inquiry set up by Mr Harold Macmillan after the Windscale Plutonium Fire, which was charged with making recommendations for re-organization of safety in the nuclear industry and for regulation of its commercial aspects. Fleck saw analogies between the task of the regulatory body needed for the burgeoning nuclear power industry and the work of the Air Registration Board and recommended tht the proposed inspectorate be modelled on it. While this general line was followed, it was thought appropriate to set up an Inspectorate of Nuclear Installations in the Ministry of Power so that matters of policy would not be delegated to an organization not answerable to Parliament.

The Nuclear Installations Inspectorate to which its name was changed began its life in April 1960 with commencement of the Nuclear Installations (Licensing and Insurance) Act 1959. Its philosophy and procedures have derived with appropriate modifications from those extant in the UKAEA at the time and thus are a compound of the traditions and practices of both the aeronautical industry and those which had grown up in the Authority.

References

1. Richard Wilson, 'The cost of safety', *New Scientist*, 1975, 68, pp 274–275.
2. On October 21, 1966, spoil Tip No. 7 which held the main part of the slag from the Aberfan colliery workings slipped without warning, descending part of the village where it engulfed a school and some houses. 116 children and 28 adults were killed and 28 children injured. A tribunal of inquiry which reported in 1969 found that several local employees of the National Coal Board were responsible because of their negligence. The disaster caused a profound and sustained shock in the nation who supported a generous aid fund.
3. The works of Badische AnilinFabrik at Oppau on the Rhine near Mannheim exploded with great violence on September 21, 1921, destroying the factory and a large part of the town, killing more than 1000 people and injuring hundreds. The disaster was caused by an unexplained explosion of a store of 200 tons of ammunium sulphate. The plant had run without incident for many years and all precautions had been taken to make such an event impossible.
4. Medical research is finding that many items of Western diet thought to be harmlessly nutritious, eg wheat, bovine protein, particularly in cow's milk, fat and salt, are responsible for cardiovascular and alimentary tract diseases. Reported at the conference on 'Disease and the Evironment', Oxford, March 21–23, 1981. Proceedings to be

published by the Society for Environmental Therapy, Manchester and London.
5. Coslett P Putmann, *Energy in the future,* (London, Macmillan, 1954).
6. C. Marchetti, 'Hydrogen and nuclear energy', *Journal of the British Nuclear Energy Society*, 1974, **13**, pp 353–362.
7. The risks caused by the burning of fossil fuels are higher than generally recognized. The oxides of sulphur are released into the atmosphere in vast quantities and there are suspicions that the measured increase in carbon dioxide is having a world-wide climatic effect. There is a considerable amount of radioactivity discharged in coal-fired power station flue gases as recently reported by the National Radiological Protection Board.
8. Jerome R Ravetz, *Superstar Technologies,* (London, Council for Science and Society and Barry Rose, 1976).
9. O H Critchley, 'Inspection and its role in the case for nuclear power', *Proc. Conf. on 'Directions in nuclear engineering research,* Inst. Nuclear Engineers, Cambridge, 19 September 1980, pp 201–10.
10. M R Brett-Crowther, 'Uncertain decision making on environmental problems', *Science and Public Policy*, October 1980, 7, No. 5, p. 380.
11. R G Stansfield, '. . . to expect no more exactness than the situation permits', at the Conference for Rethinking Applied Anthropology, Society for Applied Anthropology, Edinburgh, 12–15 April 1981, paper for session on Truth Telling.
12. F R Farmer, Accident probability criteria, *Journal of the Institution of Nuclear Engineers,* 1975, **16**, 44–46.
13. John Prebble, *The High Girders*: the story of the Tay Bridge disaster, (London, Secker and Warburg, 1956).
14. The *General Slocum* was an excursion steamer loaded with holiday makers on a church excursion which sailed from a New York City pier on the East River at 9 a.m. on June 16, 1904. She caught fire shortly after leaving. The captain made an error of judgement; and instead of beaching her at once on the river flats a few hundred yards away, he sailed with her blazing from stem-to-stern to an island several miles away. Very few on board escaped uninjured.
15. The R-101, one of the largest hydrogen filled airships, left Cardington on a trial flight to India with 53 persons on board including the Air Minister, Lord Thomson. She caught fire and crashed near Beauvais in France at 2.30 a.m. on October 4, 1930. There were 3 survivors. The cause of the explosion has not been clearly established, but it is of interest that it was the first time smoking was allowed on board.
16. A unit dedicated to teaching and research in industrial safety and hygiene was established in the University of Aston in Birmingham in 1968 under Professor Gordon Atherley, being the first such academic venture in Britain.
17. F R Farmer et al., 'Quantitative Safety Analysis', *Nuclear Engineering and Design,* 1970, **13**, pp 183–244. Another approach with more qualitative philosophy is: J Bourgeois et al. 'Evolution des idées françaises sur la sûreté des reácteurs' in *Proceedings of 4th Conference on Peaceful uses of Atomic Energy,* Volume III, Geneva, 1971, pp 163–172, (United Nations, New York, USA).
18. Mount Erebus Air Disaster, 'New Zealand DC-10 with 257 on board crashes into volcano on Antarctic sight-seeing flight.' *The Times,* 29 November, 1979, p. 1 and "Antarctic jet crash cover-up charged: 'an orchestrated litany of lies', *The Guardian,* 28 April 1981, p 6. Gross human error by the Air New Zealand management caused this terrible air accident, involving a reliable and well maintained aeroplane, piloted by an experienced

crew who knew the route well and were assisted by every available navigational aid: a mystery at the time. A Royal Commission of inquiry under Mr Justice Mahon later found that the flight path program in the DC-10's computer had been modified by 27 miles over new ground without the crew being told. Taken over an unfamiliar route during the most hazardous part of the flight by automatic control and blinded by Polar light, the pilot had no time to take the avoiding action needed to avert the crash.

19. M B Biles, 'Characteristics of radition exposure accidents', *Symposium on Handling of radiation accidents, May 1969, Proceedings*, IAEA/WHO, Vienna, 1969, pp 3–18. The paper compares the general industrial accident rates over 15 years for US atomic energy factories with those for American industry as a whole and shows that the former is lower by a factor of 3, a finding confirmed recently and in Europe generally.
20. E C Zeeman, *Catastrophe Theory, selected papers*: 1972–1977, (Reading, Mass., Addison-Wesley, 1977).
21. O H Critchely, 'Risk prediction, safety analysis and quantitative probability methods – a caveat', *Journal British Nuclear Energy Society*, 1976, 15, pp 18–20.
22. F R Farmer et al., *'Nuclear Reactor Safety'*, (New York, London, Academic Press, 1977).
23. Sir William Penny, *'The Windscale Pile No. 1 Accident of 10 October 1957'*, (London, HMSO, Cmnd Paper 302, November 1957).
24. M Rogovin and G T Frampton (Jr), *'Three Mile Island*: Vol. I – A report to the Commissioners and the public by the Special Inquiry Group', (Washington, DC, US Nuclear Regulatory Commission, January 1980).
25. The accident to the PWR nuclear power plant at Three Mile Island near Harrisburg, Pennsylvania, USA has produced a vast literature, official and independent. Two papers which summarise respectively the plant and the human (management) aspects are: 'Three Mile Island' (editor's review), *Nuclear Energy*, 1979, 18, pp. 165–167 and R F Pocock 'Three Mile Island: a potpourri of articles', *The Nuclear Engineer*, 1980, 21, pp. 71–83.
26. The acceptance of mortality and the calculation for human error have been the characteristics of Christian ethics.
27. L Oudet (translated by René Hague), *Radar and Collision*: a handbook for mariners, (London, Hollis and Carter, 1960). The book contains several studies of 'radar-assisted' collisions at sea and deals at length with the *Andrea Doria/Stockholm* incident of 25 July 1956; also see *The New York Times* of 27 July for a graphic account.
28. F J Wylie (editor) *The use of radar at sea*, (London, Hollis and Carter, 1978). Official guidance to seamen in a number of countries advises navigators when sailing in conditions of poor visibility to rely on traditional practices, not on radar.
29. W J Lanoutte, 'TMI and human factors', *Bulletin of the Atomic Scientists*, January 1980, p. 20.
30. D E Embrey, 'Approaches to the improvement of human reliability in industrial systems', Conference of the British Occupational Hygiene Society, Nottingham, 7–10 April, 1981.
31. Max W Carbon, *Review of Licensee Event Reports (1976–1978)*: NUREG-0572, (Washington, DC, US Nuclear Regulatory Commission, September, 1979).
32. Edith Ayres, 'Inspection in *The Encyclopaedia of the Social Sciences*, Volume 8, (New York, Macmillan, 1935).
33. Lord Robens, 'A note on the history of occupational safety and health legislation in Britain' (Appendix 5), and 'Summary: Chapter 7 – The inspector-

ates' (Sections 476 and 477) in *Safety and Health at Work*: Report of the Committee 1970–1972, (London, HMSO, Cmnd 5034, 1972).
34. J H Dunster, 'Some reactions to the accident at Three Mile Island', *Nuclear Energy*, 1980, **19**, pp. 139–146.
35. W S Gronow and R Gausden, 'Licensing and regulatory control of thermal power reactors in the United Kingdom' in the *Proceedings of Conference on Principles and Standards of Reactor Safety*, 1973, IAEA, Vienna, pp. 521–538.
36. T P Haire and J Shaw, 'Nuclear power plant licensing procedures in the United Kingdom', *Progress in Nuclear Energy*, 1979, 4, pp 161–182.
37. David E Embrey 'Signal detection theory in the analysis and optimisation of industrial inspection tasks', a thesis submitted for PhD in the University of Aston in Birmingham, September 1976, (Boston Spa, Weatherby, British Library, loan reference 8819:7F).
38. J F Ablitt, 'Reactor safety reports: preparation, contents and independent assessment technique', as Lecture No. 40 issued to Reactor Safety Course, October 1964 (Education Centre, UK Atomic Energy Authority, Harwell, Didcot, Berks).
39. Typical official government inquiries are the Warren Commission set up by President Johnson in November 1963 to report on the assassination of President Kenedy and, in Britain, the 'Royal Commission on Environmental Pollution: Sixth Report – *Nuclear Power and the Environment* chaired by Sir Brian Flowers and issued in September 1976 (London, HMSO, Cmnd 6618, 1976). The latter is relevant because its Sections 280 to 296 and 531 comment adversely on the NII, casting doubt on its methods and relevance of its specialisms, eg 531(19) 'The criteria and methods of working of the NII should be reviewed. . . ' This criticism was coolly received though the review was put in hand.
40. R A Peddie, 'The management of large high-technology projects', a lecture given to the Institution of Electrical Engineers at Savoy Place, London, on February 19, 1976.
41. Private communication in 1974 from William Bryan of the National Institute of Applied Research, Sacramento, California, USA, one-time senior reliability engineer, NASA: 'We did not put a man in the moon by quantitive reliability analysis but by a design-make-test-fail-fix iteration.'
42. Margaret Gowing, 'Health and Safety', Chapter 15 in *Independence and Deterrence – Britain and Atomic Energy, 1945–1952:* Policy Execution, Volume II. (London, Macmillan, 1974, pp 91–115).
43. O H Critchley, *The NII: a new style of safety regulation*, Simon Fellowship Report, Department of Liberal Studies in Science, Manchester University, 1974–1976 (unpublished).
44. K Meekcoms, *The Birth of Aeronautical Inspection*, and *British Aeronautical Inspection — Between 1936 and 1945*, AQD, Ministry of Defence, Harefield, Middlesex, 1980.

DOCUMENT NUMBER 5

THERMAL CONTROL OF THE MAGNOX NUCLEAR HEAT ENGINE

Synopsis - The paper in its original form was written in October 1962 as a report on a 'Free-thought' research into one of a number technical problems that arose in the course of regulatory inspection during the early phase of the first British nuclear power program. The paper is offered now in its revised form as an example of how a complex and sophisticated technological system may be inspected in circumstances where the inspector's expertise could not reach the level of that possessed by the particular 'very highly qualified experts' who designed it (R. J. Parker 1978). The question facing the inspector is, then, not to be a judge of the scientific merit of their findings, but to appraise their proper deployment in the case under scrutiny. To meet this requirement, a functional presentation of the elements and actions of the particular system in its holistic contribution to the plant as an entity is needed. This what the approach described attempts to do.

The treatment is by no means out-of-date because the nine Magnox power stations operated by the utilities have a prospective useful life that extends into the first decade of the next century or longer. It describes how a relatively few fuel element can temperature thermocouples may be best disposed amongst upwards of the 25,000 or more fuel elements in the nuclear core, the ratio between the two populations being of the order of several hundred to one.

Effective temperature control of the system is necessary to assure safe thermal conditions, taking into account the narrow temperature margin between the reality of the hottest, but unknown, fuel element and the melting point of the Magnox (a magnesium alloy) cladding and consequent inflammation of the exposed uranium metal rod. The operational problem is to strike a proper balance between the thermal efficiency of the reactor in the useful heat it delivers to the turbines and the chance of fuel element fires in the core in the event of a LOCA. The prescription for optimisation of the can temperature parameters is called the 'Fire Risk Criterion'.

The paper is also offered as an example of the ideographic modelling of an engineering problem that would otherwise be difficult to communicate verbally. The complex statistical relationships between the can temperature parameters and the reactor operating limits and margins are depicted in Figure 5 of the document. The utility of the presentation in ideographic form may not be appreciated by those outside the engineering vocation because most people not schooled in the discipline do not easily follow the engineer's line of reasoning. It is one that is mainly inductive, involving Gestalts, visuo-spatial concepts, synthesis and judgements. Those not trained in engineering, or in certain kindred professions, tend to be limited to the more general intellectual faculty in which their thoughts are engrossed in analysis and deduction with an affinity for quantitative relationships. Their cogitations use constructs that are linguistic and logical rather than intuitive. The competent and creative engineer can think fluently in either mode. The existence of two different kinds of intellectual activity side-by-side in the same brain has been established by recent neuropsychological research (Springer and Deutsch 1981, T. R. Blakeslee 1980) It is also mentioned in Section 8.1.1.

THERMAL CONTROL OF THE MAGNOX NUCLEAR HEAT ENGINE

by

Octavius H. Critchley

(A study of fuel element temperature distributions, can temperature measuring provisions and thermal operating limits in the gas-cooled, graphite moderated nuclear power reactor using Magnox clad, uranium metal fuel elements.)

Reardon-Critchley International
(Scientific, Safety and Health
Consultancies and Services)

9 Sutton Lane
Hounslow
Middlesex TW3 3BB
England

December 1984

TABLE OF CONTENTS

Preface to the revised edition

1 Introduction

2 Characteristics of the Maximum Credible Accident

3 Strategy for thermal management of the Magnox nuclear core

4 The can temperature pattern

4.1 Standard deviations

5 Criteria for fuel element can temperature measurement

5.1 Verification of the statistical model

5.2 Reactor control

5.2.1 Trip thermocouples and reactor protection

6 Operational temperature limits and confidence margins

7 Temperature measuring points needed for a typical Magnox Reactor

8 Operating temperatures and margins

9 Can versus channel gas outlet temperature measurements

10 Overview

11 Acknowledgements

12 References

13 Appendix: Meaning of Symbols

LIST OF FIGURES

1 Typical reactor gas circuit after 'Burst Duct' accident and loss of pressure: Quasi-static conditions

2 Shape of ducting at civil magnox stations

3 Predicted Fuel Element Can Temperatures at Hottest Level

4 Can Temperature Distribution

5 Fuel element can temperature distribution at hottest level in core of a Calder type reactor showing safety margins

6 Temperature measuring points needed for thermal model verification and to determine the standard deviation of the difference between measurement and prediction

7 Reactor Thermal Control Loop

8 Temperature measuring points needed for reactor control

9 Surveillance - Control and trip thermocouples showing the hottest systematic and actual can temperatures

Preface to the revised version

This paper is an abridgement of a report entitled,

'Some thoughts about criteria for fuel element temperature assessment in Calder type nuclear reactors',

which was written by the author when a member of the Technical Section of the Inspectorate of Nuclear Installations (INI). It was published early in October 1962 and circulated widely in the U.K. nuclear power industry during the ensuing 18 months. It was read to a public meeting of the Nuclear Power Group of the Institution of Mechanical Engineers in London on 2 January 1964 in collaboration with Dr. N.V. Nowlan, an erstwhile colleague.

The need for a generic study of the function and distribution of fuel element temperature surveillance thermocouples in the Magnox reactor core may be less than obvious in a retrospect of more than two decades. The Inspectorate, itself a novel essay in engineering inspection, was breaking new ground. Regulation of nuclear power reactors required the wise and expeditious solution of many complicated and unfamiliar technical problems. Models were required so that these problems could be presented to the inspectors, a mix of plant construction and commissioning engineers and R and D scientists from a variety of specialisms, as integral parts of the Inspectorate's regulatory task, yet broken down into individual technical assignments. The models by their ideography enabled unfamiliar concepts bearing on ranges, limits and the interactions between disparate, complex systems, both technical and human, to be conveyed clearly and unambiguously with economy in words. Among the more pressing of them at the time was that of temperature and flux management of the Magnox reactor core. It was one of paramount interest as the Maximum Credible Accident was catastrophic rupture of a main coolant duct which was thought likely to be followed by a spreading fire in the core and release of fission products to the environment.

The model offered by the study, as depicted herein, presented the decision parameters affecting the various fuel element can temperature operating limits and margins in terms of the given thermocouple provision in the core in a manner that could be readily grasped and appraised, not only in cloistered discussions in the Inspectorate itself, but in one that could be used to make a point across the table in negotiations with the electric power utility's engineers. It facilitated the discussions

by enabling the points at issue to be put in direct and comprehensive terms which would have been difficult to achieve by conventional engineering drawings and talk alone.

The purpose served by re-issuing the paper is, then, twofold. Firstly, it is a contribution to the philosophy of engineering in which the artifice of modelling, as it has long been used in atomic and particle physics, is employed to describe the inaccessible thermal reality of the fuel element population in the reactor core. Secondly, it is an attempt to give long overdue recognition to the Magnox technology as a viable energy option.

The experience that has been acquired in nuclear technology since the earlier paper was written has provided sure and abundant knowledge of the systematic parameters and random factors that affect fuel element can temperature measurement. Moreover, the scatter in the values has been reduced by better and more effective methods of quality control in fuel element manufacture. Many less thermocouples than suggested by the statistics of the model are now known to be adequate for core temperature management. Therefore, as surveillance of the neutron flux pattern in the Magnox core can be achieved with fewer can temperature thermocouples than thought to be necessary from considerations of thermal statistics, some of the material in the earlier text that dealt with core stability has been deleted.

When the report was first issued, the channel contact method of can temperature instrumentation by thermocouples appeared to be one of promise, but this aim was not realised in practice because of contamination of the channel-in-situ contacts by deposition of graphite from the coolant. A further cause was fatigue fracture of the in-pile connections by movement of the core blocks. On the other hand, the method of obtaining such thermal data by 'hard-wired' can temperature thermocouples installed during commissioning and initial fuel loading proved to be more reliable, although the technique had the disadvantage that the connections would be severed in the process of fuel changing, though some could be reinstated with the new fuel. In the long run, the build-up of information in data banks maintained by the principal licensees and the United Kingdom Atomic Energy Authority together with the greater confidence in the quality of the nuclear fuel have provided a reliable store of data on which predictions about core behaviour can be based.

The relatively trouble free nucleonics of the Magnox heat engine over so many years justifies confidence in the basic reliability and safety of its behaviour as a commercial heat source for electricity generation, although the story of its conventional features have been less happy. One may conclude, therefore, that Magnox in a pre-stressed concrete pressure vessel is one of the safest nuclear fission reactors available in today's state of the art. This view may be extrapolated to the Advanced Gas Cooled Reactor which shares with Magnox the low power density, large thermal mass of the core and its certain containment by the pre-stressed concrete pressure vessel, despite the teething problems that have afflicted the first of the commercial AGR units.

Although the Magnox reactor may appear to be obsolescent, it seems likely that it will be making an important contribution to Britain's energy balance into the first decade of the next century. The eight CEGB Magnox stations have been assessed as having a prospective further life of between 30 to 35 years (David Fishlock 1984). Moreover, the gas-cooled technology has positive advantages over PWR (C.P. Haig 1979, 1980), and in certain situations it can provide a base-load system of choice with its relatively simple engineering, proven reliability, inherent safety and ability to use natural uranium. However, in the case of AGR some enrichment is necessary because the stainless steel cladding impairs the neutron economy.

1 Introduction

Knowledge of the thermal state of the core of a nuclear power reactor is necessary for its safe and efficient operation and the Magnox type has a very large number of fuel elements for which the cladding temperature is a parameter of prime importance. Unfortunately, in a reactor of this type it is feasible to provide only very limited can temperature measuring facilities and, if the data is to be properly used, it must be treated statistically. To this end the deviations of the fuel element can temperatures from their calculated design values are taken as separable into systematic components assumed to be exactly known, and random components ascertainable in magnitude but of unknown incidence. From this a most probable fuel element can temperature distribution, or thermal model, may be constructed.

The temperature measuring instruments are then arranged to monitor the essential safety and control aspects of the fuel element population, namely, overall core stability, the difference between measurement and prediction and hottest can temperatures likely to be reached in certain channel groupings. Within these sampling strata, a randomised distribution of measuring points is desirable and formulae for determining the minimum numbers of temperature measuring instruments needed for each function are deduced.

Operating temperatures and margins in relation to such transient temperature excursions as may be expected to occur under fault conditions are discussed. As an example, the case of a hypothetical, though typical, gas cooled Magnox reactor is considered.

A most important conclusion is that, while the Magnox reactor may be satisfactorily controlled in normal operation and protected against large scale catastrophic accidents, it is impossible by any arrangement of the very limited temperature instrumentation feasible to protect the reactor against the effect of a capricious fault involving only a few channels, as the probability of detecting such a temperature excursion must be small. Safety in such cases, therefore, depends upon very high standards of design and quality control during fuel element manufacture, prudent and effective thermal management of the reactor core during operation, prompt detection of an abnormal condition by means of the burst-fuel-can detection facilities and, in the event of damage to fuel, containment of any fission products that escape to the coolant.

TYPICAL REACTOR GAS CIRCUIT AFTER "BURST DUCT" ACCIDENT AND LOSS OF PRESSURE: QUASI - STATIC CONDITIONS.

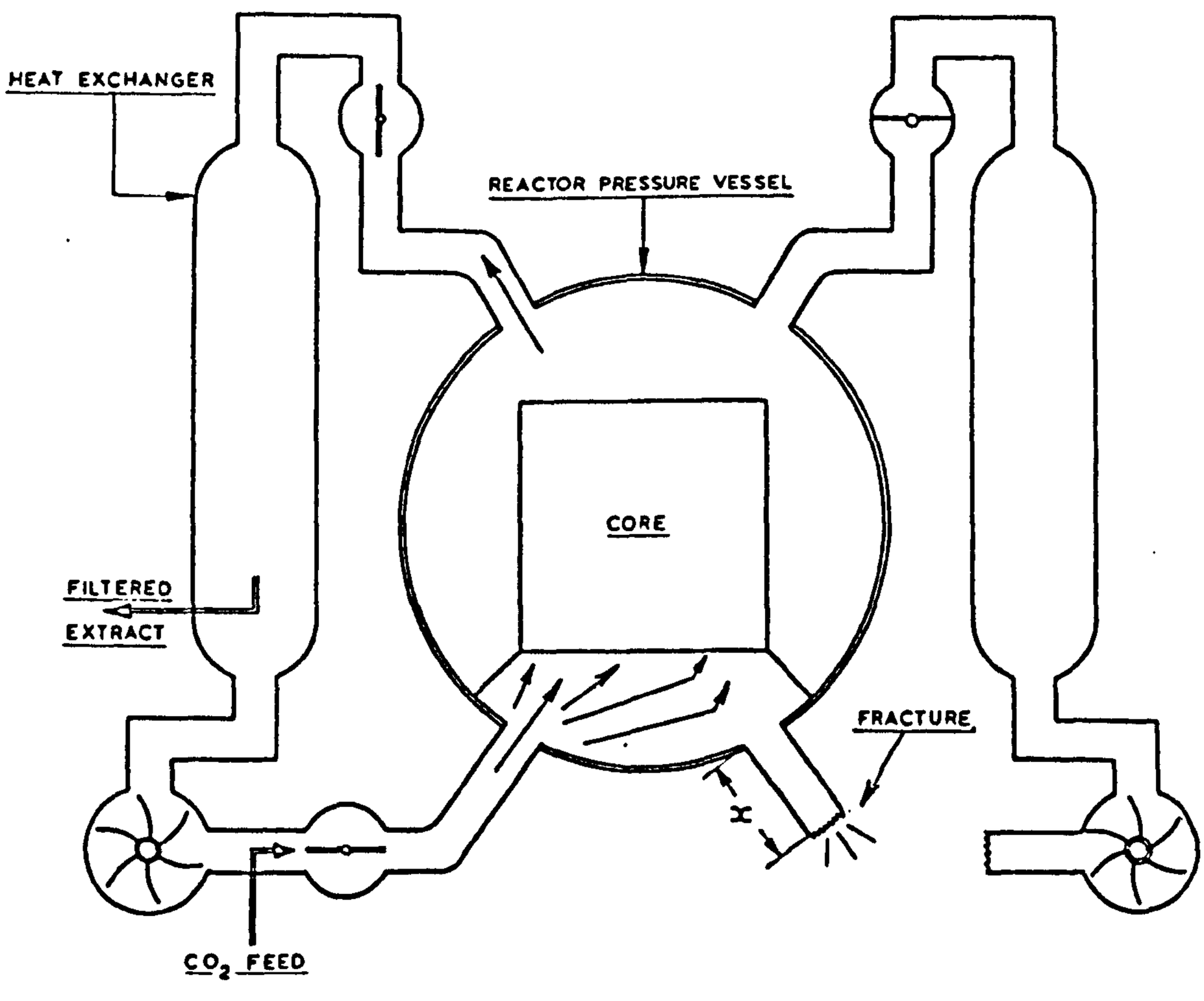


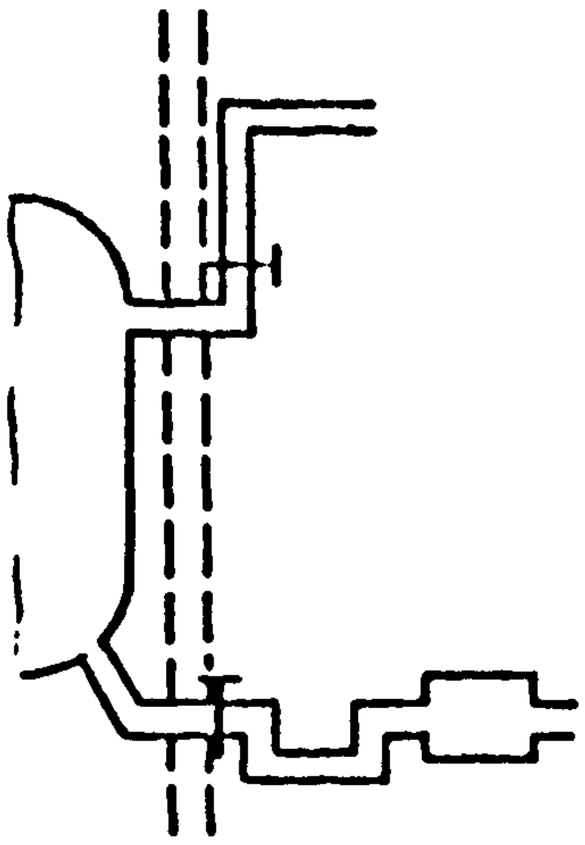
Fig 1

2 Characteristics of the Maximum Credible Accident

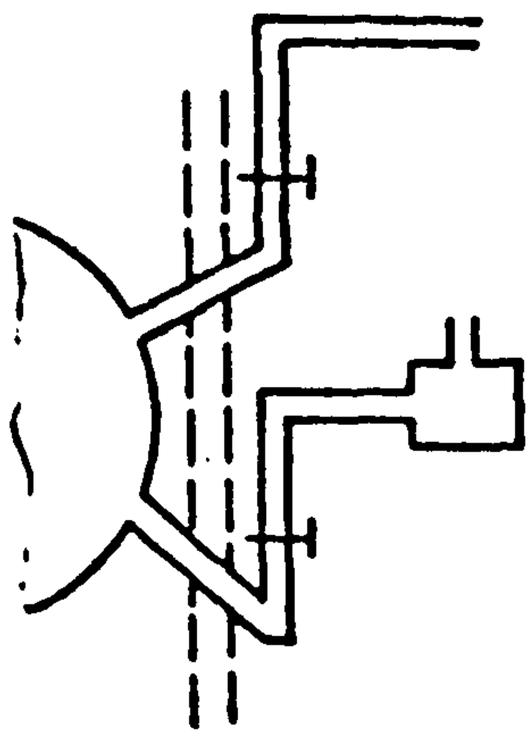
The design of a typical Magnox, gas-cooled, graphite moderated nuclear power reactor is shown diagrammatically in cross-section in Figure 1 and the several coolant duct arrangements in Figure 2. The reactor is depicted in the state of the maximum credible accident (MCA) with one of the bottom main coolant ducts completely severed. The ducts are between 5 ft to 6 ft in diameter and total rupture of one of them would result in catastrophic depressurisation of the whole coolant circuit. The event would inflict major damage on the core structure and inflammation of fuel elements in the hottest channels or of those at the time suffering cladding weaknesses or already faulty could follow. The CO_2 coolant discharged from the pressure vessel in the course of this 'Burst Duct' LOCA would be replaced by air which, reacting exothermically with the hot irradiated graphite, could combine with further fuel can ignitions to produce a major core fire and a massive release of fission products, mainly iodines, to the environment.

The mechanics and possible radiological consequences of the accident have been described in some detail by F.R. Charlesworth et al. (1970). The envisaged outcome could be very serious for people in the vicinity of the plant and it has been estimated that in an extreme case there might be a large number of casualties and fatalities. The indicated fuel can temperature used for thermal control of the core is determined by a statistical method referred to as the 'Fire Risk Criterion' (Dale and Harrison 1971) which aims at limiting the severity of damage to the fuel following the LOCA. Siting and control of development policies (Shaw and Palabrica 1974) have the objective of minimising the radiological detriment by restricting population growth and residential and other developments in the environs of the plant.

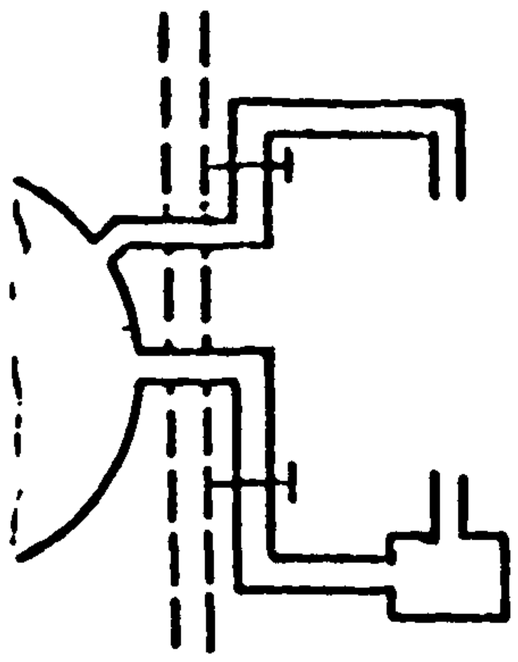
Post-LOCA damage control has been extensively studied and has reached a stage of considerable sophistication. Among the measures provided is a facility to stop the fission process by boron dust injection should other means of control be lost (David Fishlock 1975, 1976), though this would bring to an end the useful life of the installation affected.



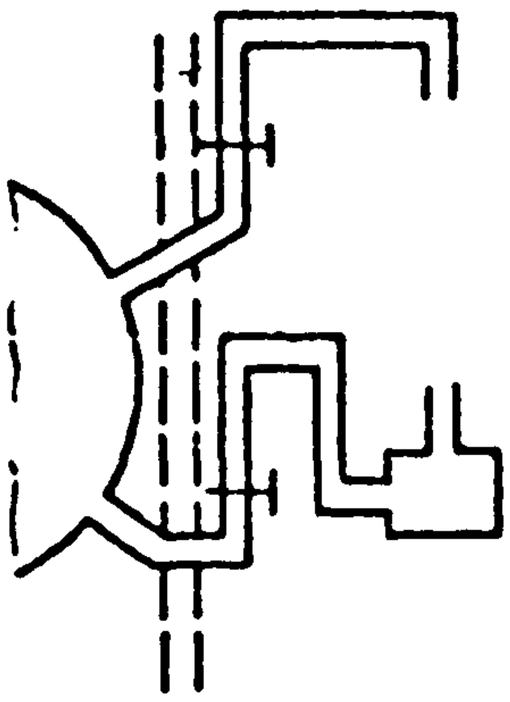
BERKELEY



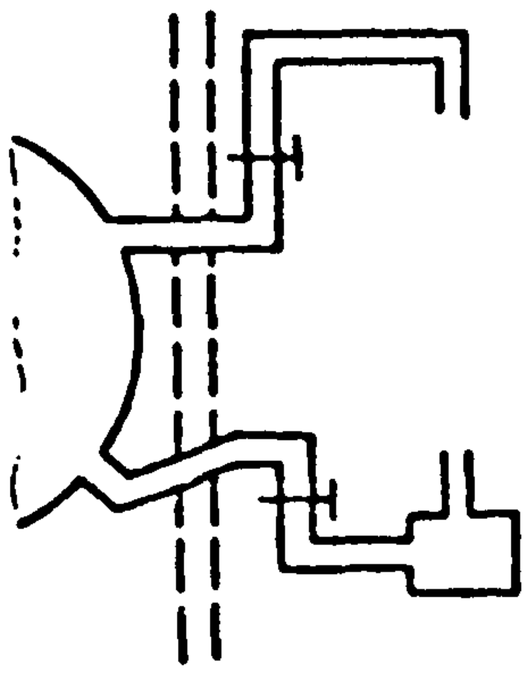
BRADWELL



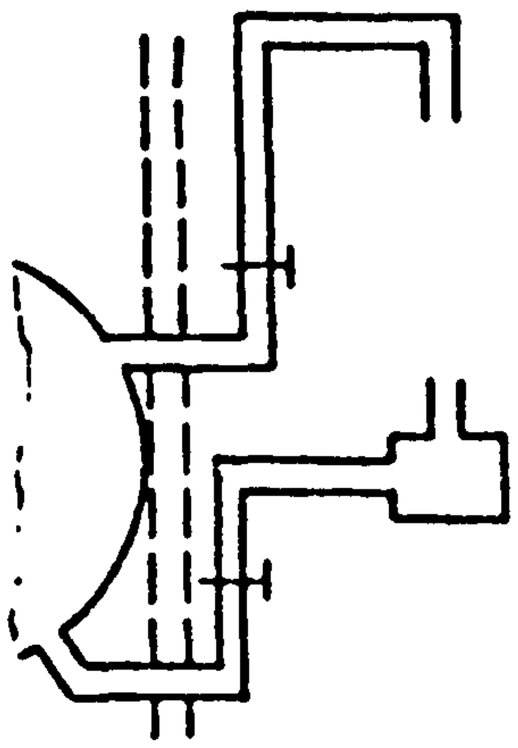
HUNTERSTON



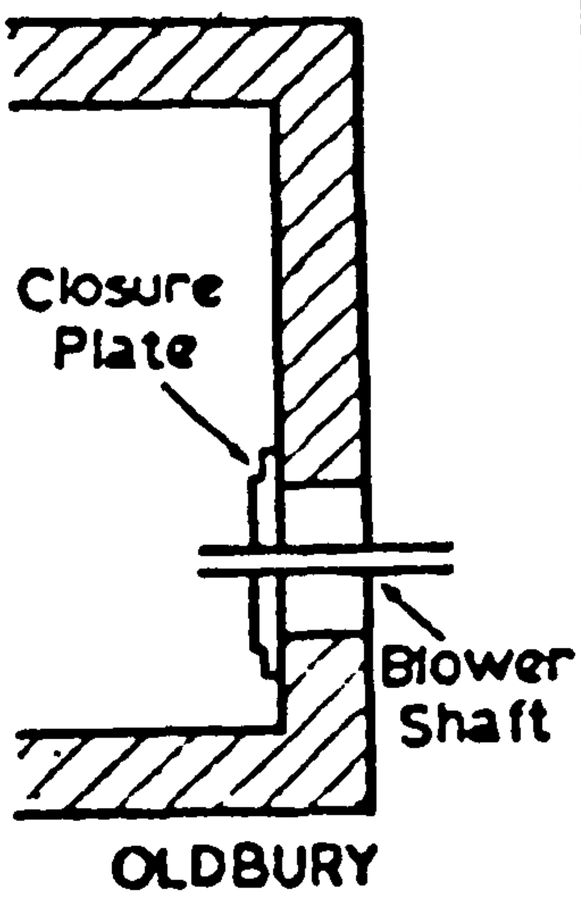
TRAWSFYNYDD



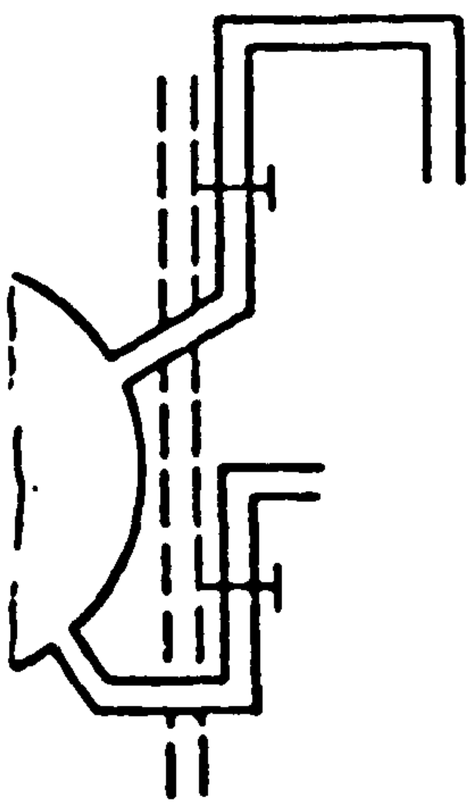
HINKLEY POINT



DUNGENESS



OLDBURY



SIZEWELL

TECHNICAL DETAILS

Coolant gas - CO_2

Pressure - 150-600 psi

Vessels, Steel

Membrane thickness

4in. - 6in.

Internal diameter

60ft - 70ft

Duct diameter

5ft - 6ft

Oldbury - Pre-stressed concrete vessel with a steel liner, also for Wylfa (not shown)

Fig 2 Shape of ducting at civil magnox stations

3 Strategy for thermal management of the Magnox nuclear core

A nuclear reactor is a heat engine and sure knowledge of the thermal state of its core is essential for its safe and efficient operation. The temperature of the fuel elements, which is a most important parameter, must be a compromise between two conflicting needs. On the one hand, the core must be run as hot as possible for maximum thermal efficiency. On the other hand, there are hazards if the reactor is run at too high a temperature, as a fuel element melt-out or fire may occur. Hence, the maximum fuel element temperature must be kept below an upper bound, set so that any credible accidental upward temperature excursion will not be enough to make any fuel element dangerously hot. In the case of Magnox plant, this is determined by the need to ensure an adequate margin between the temperature of the can of the hottest fuel element in the core and an upper value of about 630°C. at which the natural uranium fuel, clad with magnox (a magnesium alloy), will melt and inflame in the CO_2 coolant.

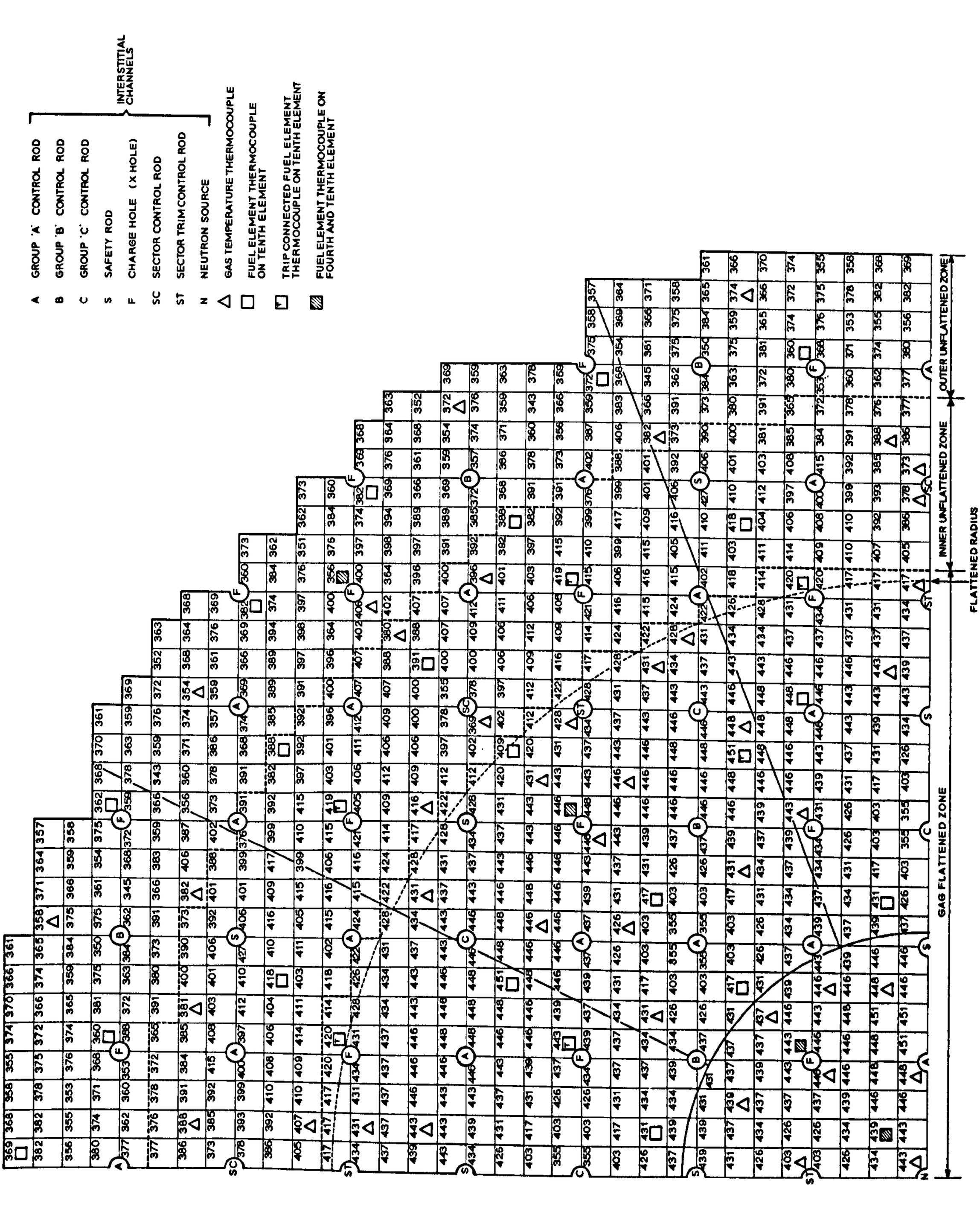
At first sight, it would seem desirable to measure the temperature of all fuel elements, and a reactor could be run with safety by scanning the lot so as to present the hottest can to the control system. The controls could then be adjusted to maintain the greatest core heat output for the maximum permitted can temperature. Unfortunately, in the case of the civil power stations there may be upwards of 25,000 fuel elements in 3,000 or more channels, and the instrumentation needed would be so complex and costly that this is not practicable. However, it is unnecessary for the purposes of safe and efficient control as statistical methods of temperature analysis may be used. A thermal model, representing the core, may be inferred from design data, information from 'rig' experiments and from studies of the behaviour of reactors of similar types. The model may then be used to define temperature limits for safe operation.

Safetywise, the most significant core temperatures are those of the hottest fuel elements, and for the Calder type reactor, these are the temperatures of the Magnox cans in the hottest plane across the core, as portrayed in Figure 3 for a quadrant of the core of a typical reactor of this kind. From knowledge of the neutron flux distribution, the rating pattern, channel coolant mass flow and Stanton number, the nominal temperature of the can of every fuel element may be estimated, but the actual values will differ from those calculated because of random deviations in the flux, rating, flow and heat transfer parameters from

Predicted Fuel Element Can Temperatures at Hottest Level

IN ONE-QUARTER OF THE CORE OF A COMMERCIAL NUCLEAR POWER REACTOR OF THE CALDER TYPE AS CALCULATED FOR SYSTEMATIC EFFECTS ONLY

Fig 3



their design values. Hence, in a steady state condition of maximum power generation, the can of each fuel element may be taken to be at a temperature in part precisely calculable, but to which must be added a second part of random incidence, so that the actual temperature of an unmonitored can may be predicted in terms of the odds against it exceeding some set limiting maximum. If these odds are sufficiently large then there will be no normal fuel element with a can hotter than this upper limit, because of the cut-off arising from the finite value of practical engineering tolerances. That is to say, the effects causing temperature variations arise from errors in construction and manufacture of the reactor and its components, and those errors that pass inspection do not have a continuous range of magnitude from zero to infinity, but have a real maximum value at which there is a certainty of rejection and exclusion from the process.

The strategy for safe reactor operation is, first, to calculate the so-called 'systematic temperatures' that are obtained by adding the specifically known variations to the design temperatures and, second, to assess the magnitude of the contributions attributable to the random effects. From these values it is possible to set safe operating temperature limits for the fuel and to prescribe instrumentation so that, not only may the calculations and assessments be confirmed, but the reactor run with confidence inside them. Moreover, in accepting that such a reactor may be safely operated on the basis of the assessed temperatures associated with the model, an assumption is made that only reasonably small errors of random incidence in manufacture and construction remain after fuel loading and commissioning, much of the relevant data being obtained during the latter phase.

4 The can temperature pattern

In commissioning a Magnox reactor an attempt is made to equalise the maximum can temperatures by adjusting the channel mass flows. Nevertheless, the actual maximum can temperatures are spread over a range of 100°C or more principally because of flux flattening, the higher rating of the central as compared with the peripheral regions of the core, perturbations in the flux pattern and differences in heat transfer parameters. The criterion for the operational temperature limits is the temperature of the cladding or cans of those fuel elements considered to be running hottest. There are several methods for defining and calculating the temperature expected to be reached by the hottest can in each channel (D. Wilkie 1978) during steady-state full power operation, but all have a common pattern.

From design considerations, a temperature, T_D, may be computed for each fuel element can, but systematic effects in construction, plant arrangement and fuel element manufacture (e.g. known irregularities in coolant mass flow, voids in the core, proximity of neutron absorbers, variations in Stanton number, etc.) give rise in each case to a calculable error, δA. Thus, at full power under steady-state conditions each can may be expected to run at a so-called 'systematic' temperature,

$$T_S = T_D + \delta A.$$

Figure 4 gives the systematic distribution of hottest can temperatures for the quadrant of the typical Calder type core shown in Figure 3.

On account of a local combination of systematic effects or because of some temporary condition such as the proximity of an empty channel, effect of absorber pattern, etc., one or more cans will be expected to be hotter than the rest and will have the peak systematic temperature, T_{SP}. Now, although T_{SP} is calculable and its site thus known, it is not necessarily the highest can temperature in the core because of the influence of further effects of a random nature. The actual temperature of a can must, therefore, include this random effect.

$$T_A = T_S \pm \delta B,$$

where δB is the random error in the prediction. Likewise, the temperature of the 'peak systematic' fuel element can may be expressed as $T_{SP} \pm \delta B$.

In Figure 5 a histogram of the frequency of the calculated systematic can temperatures is displayed. The figure provides a model that gives an ideographic portrayal of the can temperature pattern in the

Can Temperature Distribution

AT THE HOTTEST LEVEL FOR ONE-QUARTER OF THE CORE OF A COMMERCIAL NUCLEAR POWER REACTOR OF THE CALDER TYPE AS OBTAINED FROM CALCULATIONS BASED ON SYSTEMATIC EFFECTS ONLY

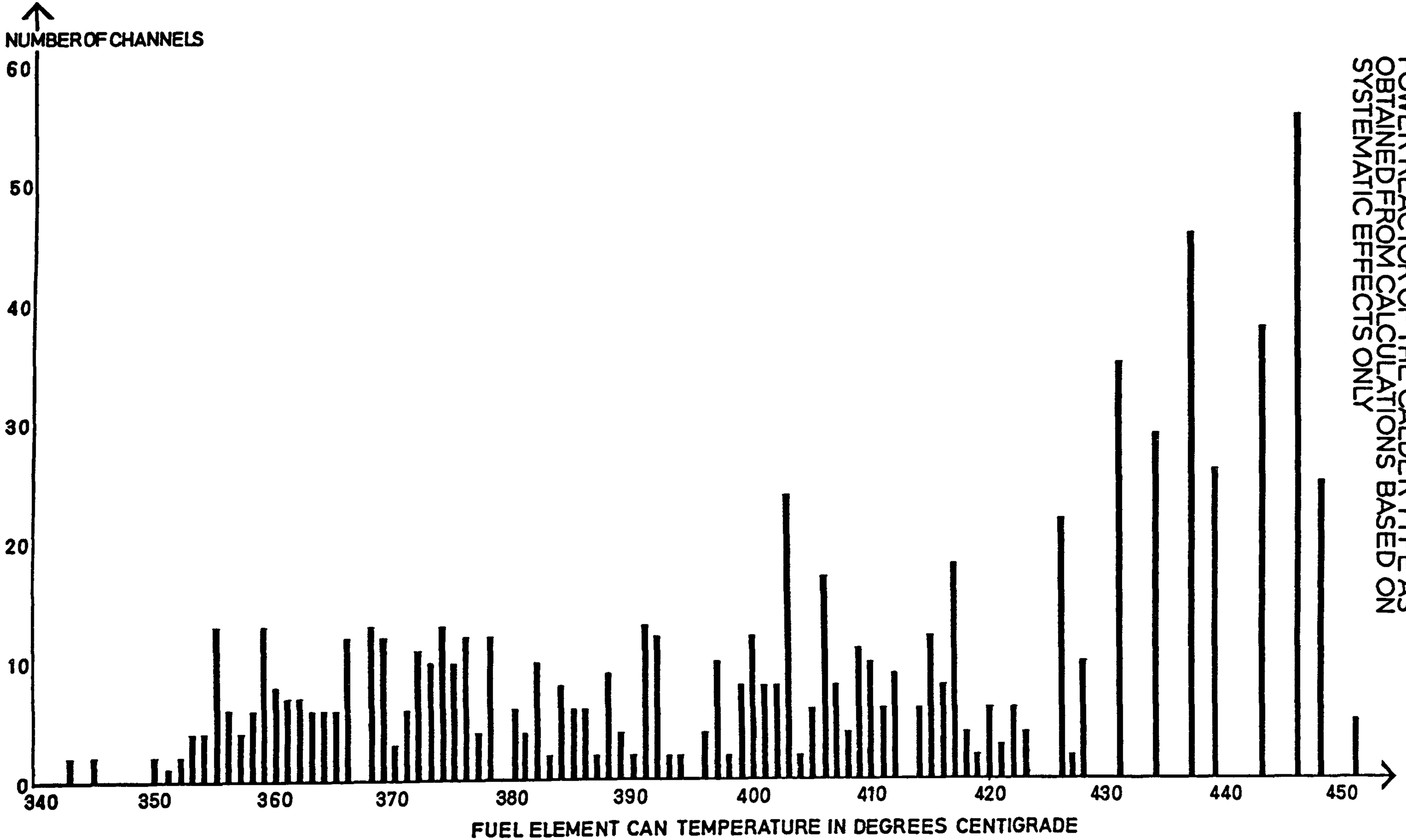


Fig 4

core, showing the margins and control parameters, and will be used to explain the control strategy. The smooth leptokurtic curve represents the probable frequency distribution of can temperatures whereby some of the temperature limits may be expressed in statistical terms. The derivation is considered to be reasonable because the actual can temperatures, most of which are unknown because they cannot be measured, will not vary in discrete steps as indicated by the histogram, but may be associated with a more continuous function owing to the incidence of the 'randoms'. Thus, the upper skirt of the smooth curve shows the expected frequency of can temperatures above the peak calculated systematic value T_{SP}.

The random error is relatively small because δB arises from the residual uncertainties in the estimation of the systematic effects and from likely errors in calculations and measurements which may, with equal chance, be either positive or negative. In spite of the fact that it cannot be specifically predicted in any particular case, a measure of this random error is the standard deviation, σ_B , and

$$\sigma_B = \frac{\Sigma\ \delta B^2}{n - 1}\ .$$

This standard deviation, σ_B, may be estimated from either rig experiments or from operational temperature measurements after commissioning a reactor.

As some cans are likely to be hotter than the peak systematic temperature, T_{SP}, for safe operation of the reactor it is necessary to set some upper limiting temperature, $T_{A\ max}$. This must be sufficiently above T_{SP} so that the chance of the random scatter giving rise to a can hotter than this limit is acceptably small. Applying statistical theory,

$$T_{A\,max} = T_{SP} + \lambda\ \sigma_B,$$

where λ is number of standard deviations needed to make the chance of there being a can hotter than $T_{A\ max}$ so small as to be accepted as impossible in the case of practical reactor operation. The probability and associated value of λ may be calculated by non-central 't' statistics (Colin Stevens 1957), although a satisfactory approximation may be obtained by use of the normal law. Further, there must be a sufficient margin (Φ) between $T_{A\ max}$ and the nominal can melt-out temperature ($630^{o}C$) so that in the conditions of the worst credible fault a can that happens to be or near $T_{A\ max}$ will not be raised to the melt-out value. These relationships are shown on the temperature axis in Figure 5.

FUEL ELEMENT CAN TEMPERATURE DISTRIBUTION AT HOTTEST LEVEL IN CORE OF A CALDER TYPE REACTOR SHOWING SAFETY MARGINS

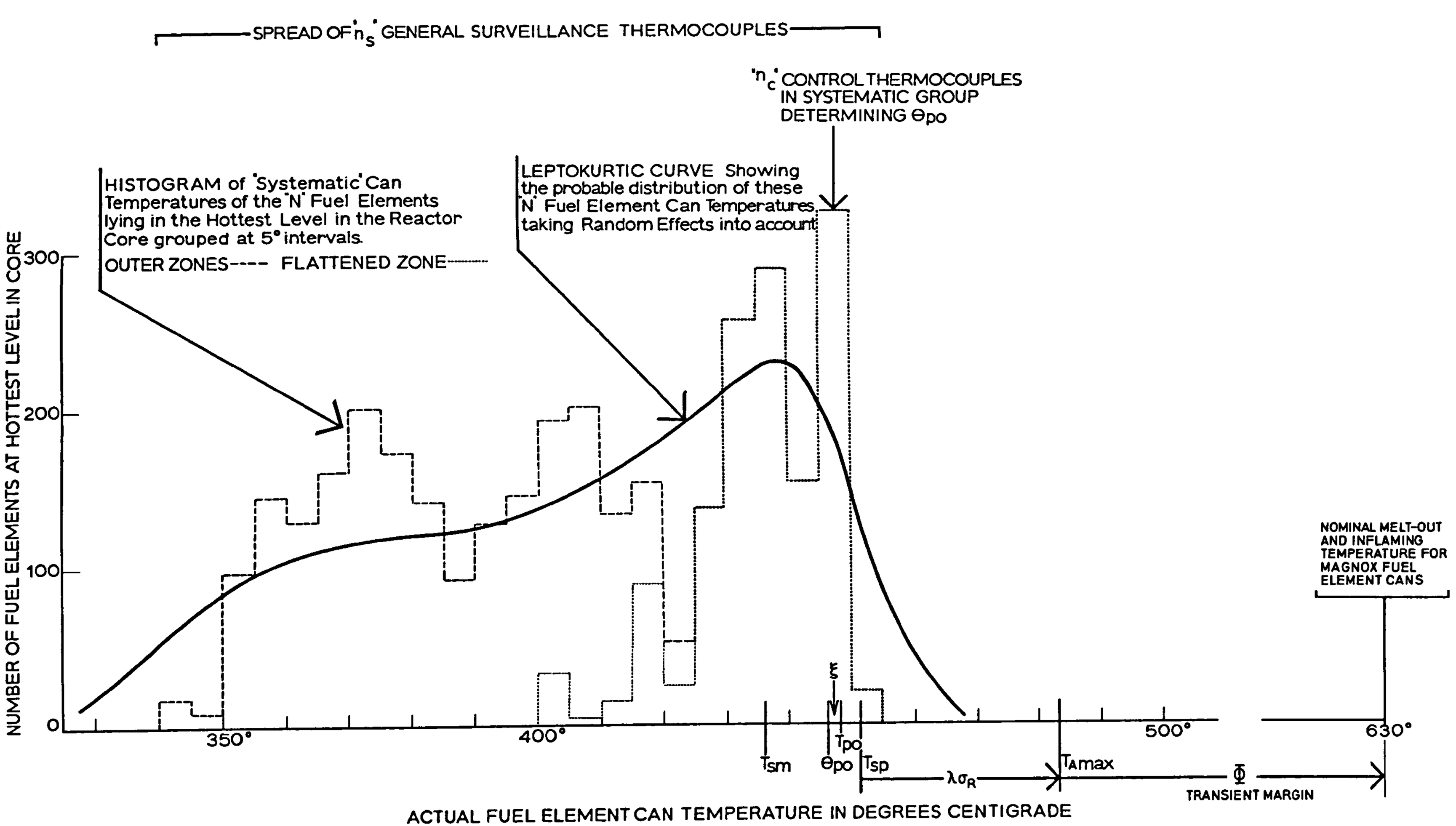


FIG 5 413

For a reactor to be run at its maximum power output consistent with safety, information about the thermal state of the core and the instantaneous temperatures of the hottest cans must be continuously available. As the number of can temperature measuring points is limited to a fraction of the total number of fuel elements, the required information must be inferred from a sample. Obviously, such an estimate will be less definite than that derived from rapid scanning of every fuel element, and it may be objected that statistical concepts are being substituted for measurable quantities. Nevertheless, the can of a fuel element is not an isothermal surface, and point metal temperatures when used to represent the whole are themselves statistical extrapolations. Further, no instrumentation, however comprehensive, is likely to be fault free, and there is no certainty that the hottest temperature is in fact being displayed.

Using sampling theory to treat the data, estimates of mean and peak temperatures, the scatter, and the probability that some values are above a set upper limit may be reliably estimated and, to run the reactor, the mean can temperature of a designated group of fuel elements may be measured to the desired precision (ξ).

4.1 Standard deviations

The standard deviation, σ_B, expreses the dispersion of the actual can temperatures about their predicted systematic values, and it is the parameter to be used in fixing the maximum permissible operating temperatures. Before the reactor has been run, measured temperatures will not be available and a predicted value of σ_B must be used to set temperature limits. For this purpose a value σ_R is used which is the standard deviation assessed from estimates of random effects and expected errors in measurement and calculation, and as σ_R will be nearly equal to σ_B and should be slightly larger, it is a safe substitute to use during commissioning.

At an early stage when the potentialities of a reactor design are being assessed, the concept of a distribution of systematic temperatures is useful to avoid the labour of calculating several thousand fuel element temperatures.

The standard deviation of systematic effects is then expressed as

$$\left[\frac{1}{n-1} \sum \delta A^2\right].$$

It may, however, be confusing if this distinction is not kept clearly in mind.

For the typical reactor of Figures 3, 4 and 5 the standard deviations for random and systematic effects are respectively $\pm$ 8°C and $\pm$ 30°C. A good working estimate for the standard deviation of the difference between measurement and prediction (σ_B) would be $\pm$ 7.5°C.

5 Criteria for fuel element can temperature measurement

In applying the postulate of the statistical model to the reality of thermal conditions in the core, the link between theory and reality is the limited network of temperature measuring points. The number needed to get adequately representative samples on which control decisions can be based will be determined by the allowable margin of uncertainty and the confidence limits imposed. It is impossible, however, to make any sound quantitative decisions about the number and disposition of these points, without knowing the purpose for which the information is being obtained. In addition to purely operational requirements, other criteria which may determine the number of temperature measuring points necessary are:-

(i) Verification of the model and determination of the standard deviation (σ_B) of the difference between prediction and practice, and measurements for experimental studies aimed at improvement of the model by validation of assumptions and investigation of any unexpected effects.

(ii) Information for instant-by-instant control of the reactor in terms of nominal 'hottest cans' and designation of trip thermocouples.

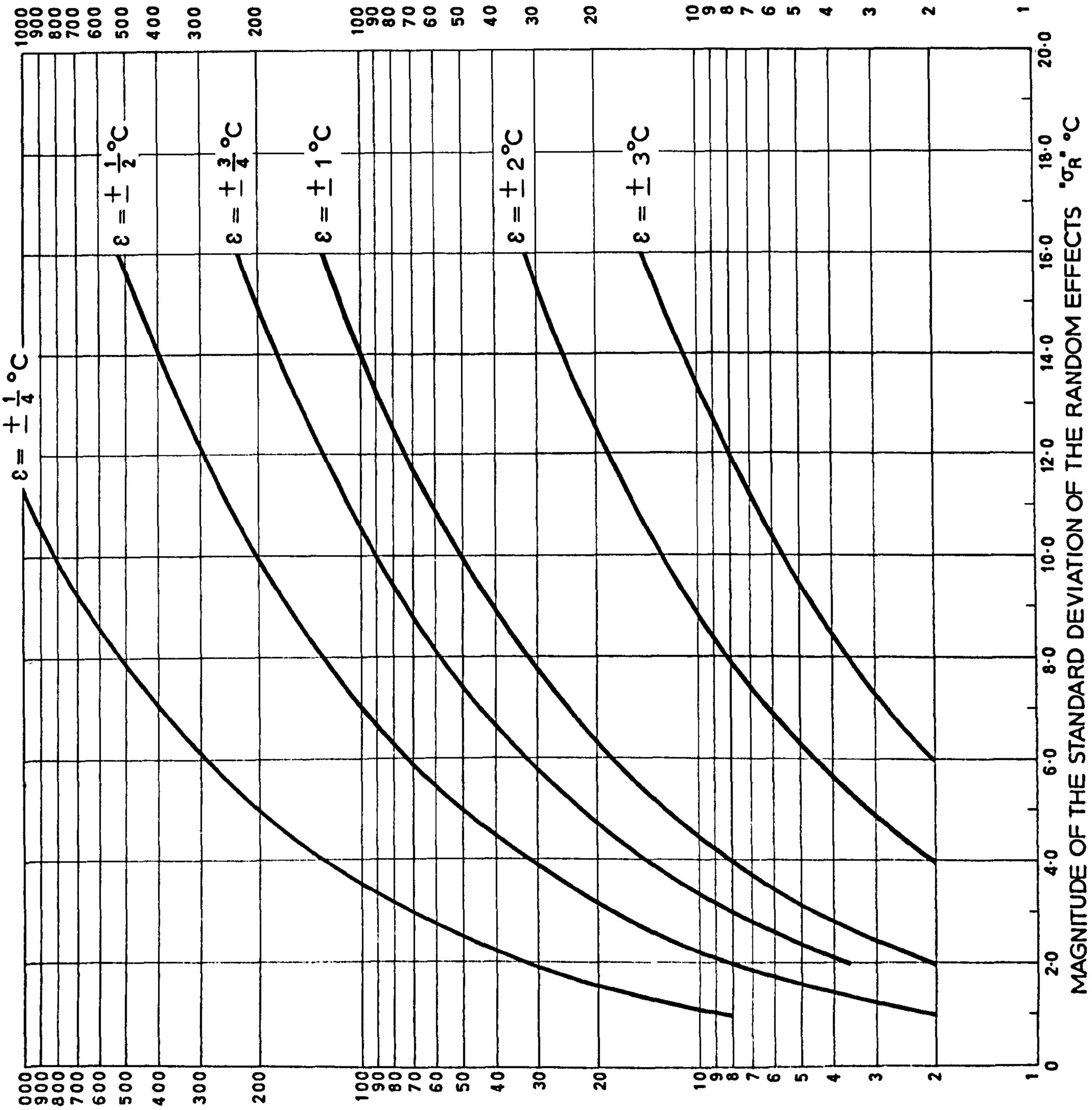
(iii) Redundancy to compensate for instrument wastage.

It seems that the can temperature thermocouple still provides the only direct means of measuring fuel element can temperature despite the fact that it gives a point value on the surface of the cladding. Channel gas outlet temperature measurement, though an important parameter, gives a value for the string of elements with no indication that a particular element may be running too hot, but so much is now known about fuel element quality and performance that the latter is of diminished value.

With the exception of the groups disposed for the investigation of special features and for reactor tripping, the measuring points should be distributed on an equal weight basis, being randomised so that no one aspect takes on more importance than another. A further consideration is that the instruments and circuits for control and safety surveillance must be independent of one another, a principal which it is generally agreed is not only sound, but essential if interactions and common mode effects are to be avoided.

TEMPERATURE MEASURING POINTS NEEDED FOR THERMAL MODEL VERIFICATION AND TO DETERMINE THE STANDARD DEVIATION OF THE DIFFERENCE BETWEEN MEASUREMENT AND PREDICTION (σ_B)

FIG 6



5.1 Verification of the statistical model

Safe operation of a reactor depends upon correct forecasting of the thermal behaviour of the core from an assumed knowledge of the specific systematic effects and of the magnitudes of the random effects. Thus, the parameter to be determined by sampling is the standard deviation (σ_B), of the difference between the predicted systematic temperatures and measured values, and the acceptable standard error in this determination is the criterion by which the number of measuring points needed can be assessed. Then from sampling theory (C.E. Weatherburn 1961) one can obtain the standard error ε_B of the standard deviation σ_B from

$$\varepsilon_B^2 = \frac{\sigma_B^2}{2\, n_s} \qquad \text{.....(1)}$$

To determine n_s in the design stage it is appropriate to use σ_R in place of σ_B and define an acceptable value of ε_B. The magnitude of n_s for several values of ε_B has been plotted in Figure 6 for a range of values of σ_R.

These measuring points would be attached to fuel elements at the hottest level, but this is not essential because, if the temperature of one can in the channel is known, then that of the others is calculable from flux and coolant mass flow data. In this case, however, a larger allowance must be made for measurement errors, and it is, therefore, more efficient to measure the temperature of the hottest can, though some provision should be made to confirm assumptions about the axial temperature distribution.

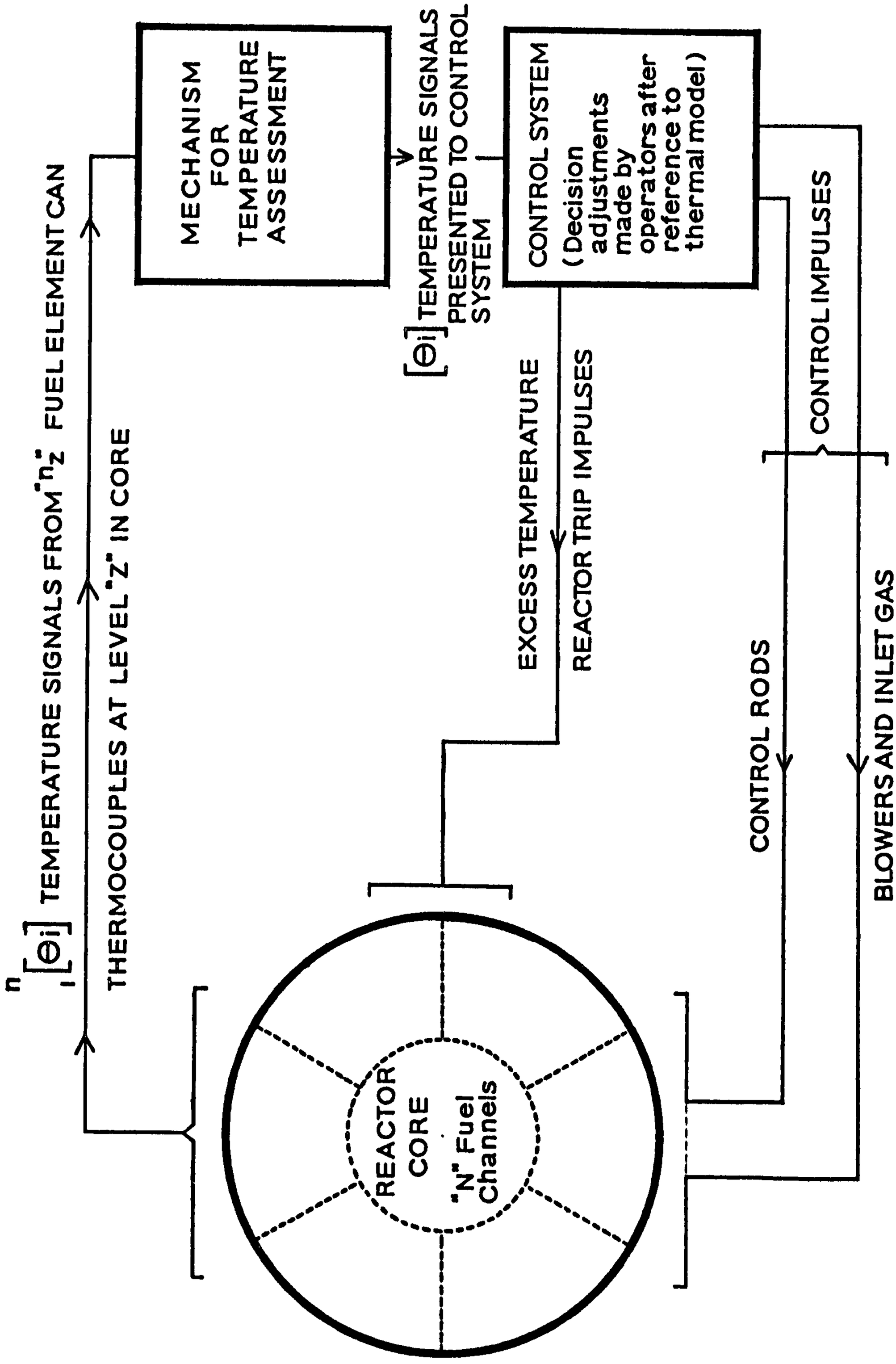
5.2 Reactor Control

In full power steady state operation, the reactor must be run so that the can temperatures are effectively at their calculated systematic temperatures, the maximum thermal output being determined principally by the scatter of the actual temperatures about the predicted maximum values. The function of the control instrumentation is to realise the desired safe thermal output by holding the fuel element cans close to the designated temperatures.

The reactor core and thermal control apparatus form a servo loop as shown in Figure 7. As rapid response to temperature changes and freedom

Reactor Thermal Control Loop

Fig 7



from overshoot are essential for stable, efficient and safe operation, can temperature thermocouples rather than channel gas outlet temperature instruments are desirable.

It is not feasible to have instrumentation to indicate the temperature of the hottest point on every can and thermal control of the reactor must be based on a confident assessment of the instantaneous distribution of can temperatures, particularly those of the hottest cans, made by referring to the systematic model, which has been confirmed at a known error (σ_B) by verification measurements. An allowance must be made because the can temperatures are estimated from a sample rather than from knowledge of the temperatures of the whole population of fuel elements in the core. The optimum number of measuring points may be determined by considerations of convenience and reliability in operation and of the balance between capital investment in instrumentation and revenue loss through derating. This is a problem in the economies of sampling inspection (Owen L. Davies 1956) too complicated for treatment here. However, the number (n_c) of can temperature thermocouples needed to control the reactor, or a sector of its core, at a level of confidence (X) within a given derating allowance for a precision of sampling (ξ) by measurements obtained from a systematic group containing N_c fuel elements is given by:-

$$n_c = \frac{N_c}{1 + \beta^2 (N_c - 1)} \qquad \text{.....(4)}$$

where $\beta = \frac{\xi}{x\,\sigma_B}$, or $\frac{\xi}{x\,\sigma_R}$ very nearly since $\sigma_B \doteq \sigma_R$

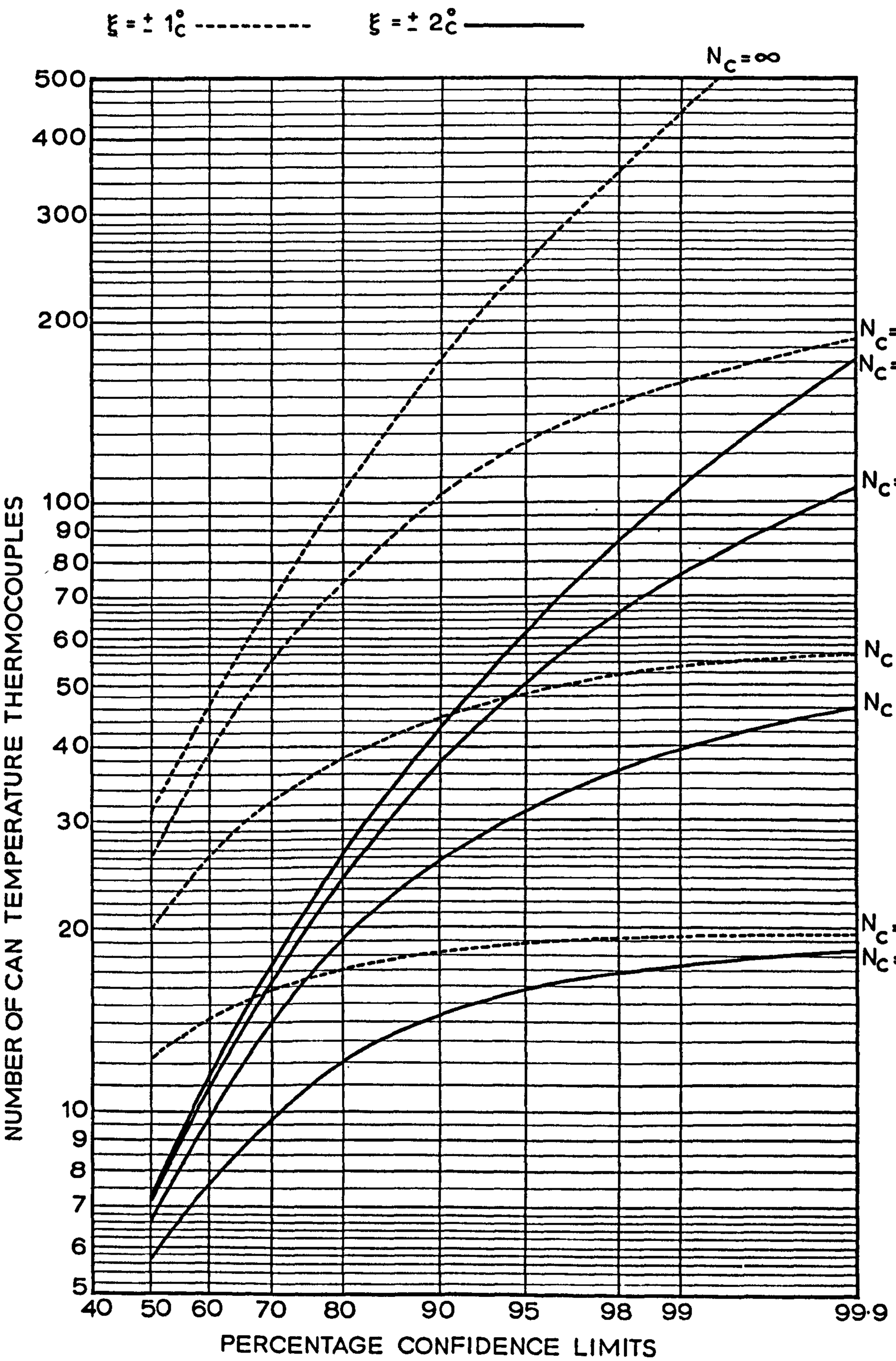
and x = a multiplier appropriate to the confidence limits X, defining the percentage of cases in which the precision of sampling ξ is not exceeded.

The curves in Figure 8 show the relation between the number of control thermocouples needed and the confidence limits for a given precision and various sizes of control group, and a derivation of equation (4) is given by Yule and Kendall (1947).

If the core is divided for operation into sectors under independent temperature control, then in determining the numbers of control thermocouples required each must be treated as a separate unit. Clearly, more instrumentation will be needed than if the core alone were the operational unit. The distribution of thermocouples in a quadrant of a typical Magnox reactor is shown in Figure 9.

TEMPERATURE MEASURING POINTS NEEDED FOR REACTOR CONTROL ($\sigma_R = \pm 8°C$)

FIG 8

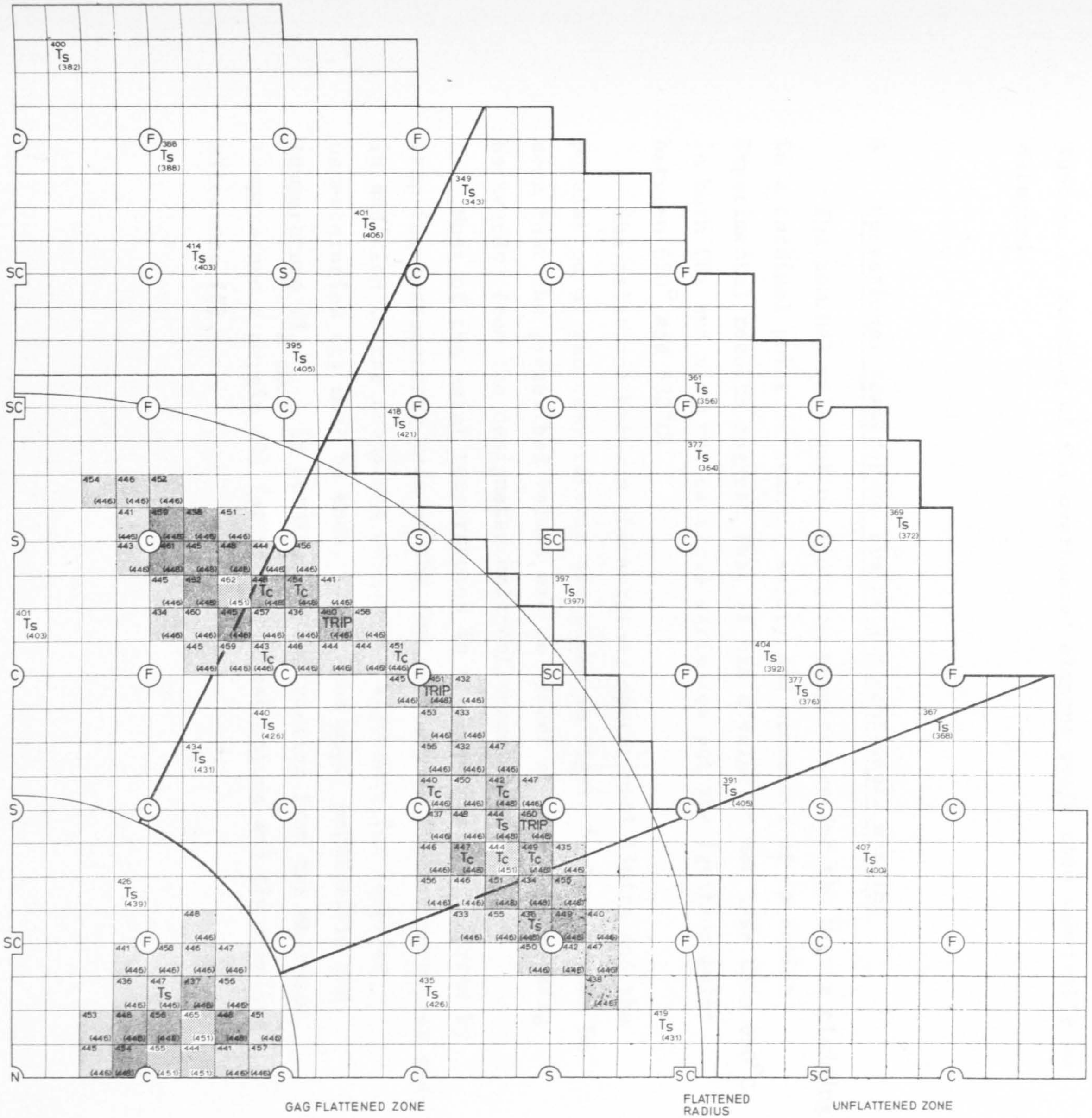


5.2.1 Trip thermocouples and reactor protection

The instrumentation for safety shut-down of the reactor in event of mal-operation or occurrence of anticipated faults should be separated from that for normal operational control. Hence, independent 'trip' or quick acting excess temperature limit stop instrumentation is needed, and this may be provided by 'trip allocated' can temperature thermocouples and associated equipment, the number required being determined by the safety circuit philosophy. For 'two-out-of-three' protection, three such thermocouples would be needed per sector, sited in the peak systematic fuel element cans, independent of the control and surveillance instrumentation, shutting down the reactor when a sector temperature exceeded the maximum by a suitable margin. These trip thermocouples will respond reliably only in the event of a sector or whole core temperature excursion. This is a consequence of reactor control by a relatively small number of temperature measuring points, the general assumption being made that the reactor will behave in a predictable way and that any digressions from normality will affect the core as a whole, a sector or a large region.

In the case of small isolated faults which cause overheating of a few or even only one of the fuel elements, it is not possible by any arrangement of the relatively few metal temperature measuring points to cover the whole core and give any acceptable probability of detection. Such incidents, however, are likely to be very infrequent, arising from occasional fortuitous combinations of anomalies, such as odd system faults, exceptional errors in operation, fuel elements damaged during loading into the reactor or other defects or chance obstructions to the channel gas flow. The fault could lead to a local temperature excursion, unlikely to be observed by the instrumentation and to a channel melt-out or fire.

It is illusory to think that a reactor can be protected against such exceptional events by rigorous inspection of the fuel, by great care during loading, by strict operational discipline and by imposing conservative operational safety margins. These precautions may reduce the likelihood of an unusual, anticipated fault, but over a number of years of reactor operation such an event must be accepted as possible. In fact, they are more likely than the postulated catastrophies against which such elaborate safeguards have been taken. Hence, it would seem



361 Ts (356) — SURVEILLANCE MEASURING POINT

454 Tc (448) — CONTROL CAN TEMPERATURE THERMOCOUPLE

460 TRIP (448) — TRIP ALLOCATED CAN TEMPERATURE THERMOCOUPLE

(C) — CONTROL ROD

SC — SECTOR REGULATING CONTROL ROD

(S) — SAFETY ROD

(F) — CHARGE CHUTE LOCATION HOLE

(N) — NEUTRON SOURCE

454 — ACTUAL TEMPERATURE OF HOTTEST CAN IN CHANNEL

(448) — SYSTEMATIC TEMPERATURE OF HOTTEST CAN IN CHANNEL

FIG 9
SURVEILLANCE · CONTROL AND TRIP THERMOCOUPLES SHOWING THE HOTTEST SYSTEMATIC AND ACTUAL CAN TEMPERATURES

that for the greatest safety it is necessary to devise some means by which abnormally high can temperatures in the core may be immediately detected.

It might be thought that indication of the gas outlet temperature for every channel would suffice, and it is a feasible scheme of instrumentation. While there would then be added protection, this would not be complete, because there would be little or no response to hot spots or overheating in reduced or stagnant coolant flow. The lag in indication of the temperature also introduces an undesirable delay in response to the fault.

It seems that the most promising means for detection of such faults is through the burst cartridge detector or similar instrumentation. Rupture or burning of the overheated element would then inevitably be detected.

6 Operational temperature limits and confidence margins

The nominal melt-out or ignition temperature for the Magnox cladding is a cardinal point in reactor safety and economics of operation. Experimental results suggest that it has a value of not less than 650°C in both CO_2 and air, but cautious estimates put the ignition point between 620° and 630°C.

The relations between the margins, operational limits and the population of can temperatures are shown in Figure 5 where it can be seen that the prescribed values are in effect obtained by 'working backwards' from the designated melt-out temperature.

Most of the metal temperatures in the core must be inferred by sampling measurements made by the few can temperature thermocouples and, in addition to the transient margin, an allowance for sampling uncertainties (ξ) must be made. Thus, the upper permissible can temperature ($T_{A\ max}$) is obtained by subtracting from the melt-out temperature a margin (Φ) for transient excursions and the sampling allowance (ξ).

7 Temperature measuring points needed for a typical Magnox Reactor

The typical Magnox reactor as depicted in Figures 1, 3, 4 and 5 has some 3,200 fuel channels, a T_{SM} of 436°C , maximum and minimum systematic temperatures of 451°C and 343°C respectively and a random standard deviation (σ_B) of ± 8°C. Operating at full power under steady state conditions, an adequate number of temperature measuring points are needed for model verification, reactor control and safety circuit trips. Assuming that these are can temperature thermocouples, sited in the hottest layer of fuel elements across the core, the requirements are:

Function	Minimum Numbers needed
(a) For model verification and assessment of the standard deviation (σ_B) of the difference between prediction and measurement, using equation (1) and allowing a standard error (ε_B) in the estimation of (σ_B) of ± 1°C.	32
(b) For reactor control through nine independent sectors at a precision of ± 2°C and 99% confidence limits, the operating temperature is maintained with reference to the 448°C systematic group of fuel element cans. The central sector contains 20 cans of which 17 are monitored and the 8 peripheral sectors contain 10 cans each of which 9 in each are monitored.	89
(c) For trip or excess temperature shut-down of the reactor on a 2 out of 3 safety philosophy in 9 independent sectors, using 20 channels at 451°C and 7 at 448°C.	27

A minimum number of 148 can temperature thermocouples would therefore seem necessary for safe and efficient operation of the reactor. Nevertheless, some extra measuring points may be desirable to carry out experimental studies and some provision must be made to allow for wastage through instrument failures. These additional points would be extra to those defined above. The arrangement of can temperature thermocouples for the core of a typical Magnox reactor is shown in Figure 9.

8 Operating temperatures and margins

Safe operating temperatures and margins for the typical reactor at full power in steady state and with the temperature instrumentation described in Section 7 above are set out below. The basic reference temperature is the nominal point for Magnox melt-out or ignition in CO_2, and the relations are shown diagrammatically in Figure 5.

The actual mean operating temperature (T_{po}) of the control group of cans must not exceed	448°C
Allowance for precision of measurement (ξ) of the control group mean	2°C
Hence indicated mean operating temperature (θ_{po}) the control group of cans must not exceed	446°C
Maximum expected mean temperature for peak systematic group of cans (T_{SP})	451°C
Standard deviation for random effects, σ_R, used in early operational phases in lieu of σ_B	± 8°C
Margin between T_{SP} and $T_{A\ max}$ where $T_{A\ max}$ is the upper maximum limit for dispersion of fuel element can temperatures from their systematic values, set at a value so that it is incredible that any normal fuel element in a normal channel will be hotter than $T_{A\ max}$	32°C
(The margin is $\lambda\ \sigma_R$ where λ is the appropriate to multiplier. Take $\lambda = 4$.)	
Upper limit of temperature, $T_{A\ max}$ very unlikely to be reached by any can	483°C
Nominal ignition in CO_2 and can melt-out temperature	630°C
Transient margin (Φ)	147°C
Probability that the temperature of the can of any fuel element in the reactor exceeds $T_{A\ max}$ as calculated by normal law statistics	0.0017

It should be noted that the maximum permitted can operating temperature is directly dependent on the nominal melt-out temperature and the transient margin, (Φ). It is good practice to take a realistic value for the melt-out temperature and to set the transient margin appropriately, basing it on credible faults occurring to normal fuel elements in normal channels, that is operational faults capable of

being detected by the instrumentation. To try to ensure protection against rare and isolated small scale faults with any acceptable level of confidence, must involve uneconomic derating of thereactor or perhaps shutting it down.

9 Can versus channel gas outlet temperature measurements

A number of channel gas outlet temperature thermocouples are also appropriately sited in the core, a typical arrangement being shown in Figure 3. If the individual channel mass coolant flows, the Stanton numbers and axial neutron flux profiles are known, then the respective can temperatures may be inferred from the channel gas outlet temperatures. The likely errors in can temperature assessment by this method are put at between ± 3°C to 4°C, depending on the stability of the values assumed for the other parameters. In comparison, the estimated error in can temperature as measured by a directly attached thermocouple is put at ± 2°C. On the other hand the figure derived from gas temperature is an aggregate for the whole fuel element stringer, while the metal temperature is a spot value for a point on one can. It must be noted that the data given above is dated and values now available will have been refined and could be quoted with greater confidence. Finally, the metal temperature is a prompt indication whereas the gas temperature suffers a delay in response. This is a disadvantage if the latter is used for trip or control purposes.

10 Overview

Since the first version of this document was published, the Atomic Energy Authority and the electrical power utilities in Britain have had more than 500 reactor-years experience with Magnox units. While most of the operational difficulties have lain with the steam raising auxiliaries, the salient reactor problems have been ones of internal corrosion, core restraint weaknesses and faults in the external main coolant duct assemblies. These disabilities have been satisfactorily overcome (David Fishlock 1984). The statistical approach to thermal management of the reactors, associated with the 'Fire Risk Criterion' (Dale and Harrison 1971), outlined above and modelled ideographically in Figure 5, was generally adopted and has been justified by results in practice. The technique has been refined over the years and its application made more efficaceous, energy-wise and safety-wise, by research and introduction of sophisticated data processing facilities.

The aim of the study presented here was not to elaborate the 'Fire Risk' methodology already well developed in the industry, but to offer an inspectional guide for assessment of the provision and disposition of fuel element can temperature thermocouples in Magnox reactor cores. The suggested figure of 148 randomly place thermocouples in the hottest plane was determined by a 'Transient Margin' (Φ) of 147°C and a 'Temperature Margin' ($\lambda\ \sigma_R$) of 32°C to allow for the presence of 'out-of-spec' fuel elements and rogue random effects. This gave an interval of some 180°C between the assumed highest temperature can in the core and the nominal melt-out and inflammation point for Magnox alloy cladding. Such a thermocouple provision is patently pessimistic. It was also assumed that the interval presented by the summated margins would not be exceeded in less than 100 LOCAs. However, the greater reliability of instrumentation systems, better knowledge of the dispersion and distribution of systematic and random errors and enhanced confidence in the quality control of fuel element manufacture have led to reductions in the theoretical temperature excursion that might follow a LOCA. Despite that, the resulting contribution to thermal efficiency by optimisation has been lost in practice by temperature limitations imposed to minimise the rates of graphite errosion and steel corrosion.

While the 'unquestionable safety' (Kirk and Taylor 1971) of the containment provided by the pre-stressed concrete pressure vessel (PCPV)

and internalisation of the boilers characteristic of 'Oldbury' and 'Wylfa' have made the risk of a catastrophic LOCA negligible in their case, the remaining 14 of the Magnox reactors operated by the utilities have steel main pressure vessels. The latter group have a prospective operational life of at least 450 reactor-years. Despite the higher risk factor attributable to a steel membrane, the reliability of these massive steel containment vessels is high, being put at not less than 2×10^{-5} per service-year for catastrophic failure (Phillips and Warwick 1970). Taking a reliability of the order of 10^{-5} reactor-years for the main coolant ducts in combination with a 'Fire Risk' probability of 10^{-2} per LOCA, the overall theoretical probability of a serious radiation accident for this particular causal sequence is of the order of 10^{-7} per reactor-year. It is a metaphysical figute and such event will not occur as an outcome of the envisaged sequence. Furthermore, the chance of a catastrophic duct failure has been substantially reduced by recent advances in structural engineering (David Fishlock 1984), giving the Magnox system a very favourable safety prognosis in comparison with other reactor types, and an even better case can be made for Magnox in PCPVs.

11 Acknowledgements

The opinions expressed are entirely those of the author for which he takes full responsibility. They should not be attributed to any former employer or principal and it is not in any way suggested that they have been those of the Nuclear Installations Inspectorate, either when the paper was originally published or at any time later. It is appropriate for him to express again his gratitude for the encouragement he received from Major General S.W. Joslin, the then Chief Inspector of Nuclear Installations, to pursue what was, at the time, 'free thought' research and, later, for his agreement to release of the report for publication. The author also wishes to acknowledge the helpful guidance he received from Mr. F.R. Charlesworth, Head of the Inspectorate's Technical Section, during preparation of the original version. In reference to the present work, he thinks it proper to note that his official contacts with the NII terminated in August 1980 when he left the service of the Health and Safety Executive. In no way, therefore, did the author receive any sponsorship from either of these two bodies, nor is such a thing implied.

12 References

Charlesworth, F.R. et al. (1970) Leakage from a ruptured containment after accidental depressurisation of a Gas Cooled Reactor. 5th Annual Health Physics Soc. Midyear Symp., Vol. 3. Idaho Falls, 151-170.

Dale, G. C. and Harrison, J. R. (1971) 'Safety of Nuclear Power Plants', S.5 - Safety in Operation. 4th Conf. on Peaceful Uses of Atomic Energy, Geneva, 147 et seq.

Davies, Owen L. (1956) Design and Control of Industrial Experiments. Oliver and Boyd, London, 111-112.

Fishlock, David (1975) Questions over the future of nuclear power plants. Financial Times, 30 May, 10.

Fishlock, David (1976) New emergency system for U.K. nuclear power stations. Financial Times, 2 Nov., 15.

Fishlock, David (1984) Clean bill of health for ageing reactors. Financial Times, 3 Aug., 15.

Haigh, C. P. (1979) The correct reactor answer lies with gas cooling. The Guardian, 29 Aug., 16.

Haigh, C. P. (1980) Two good reasons to reject PWR. Nature, 284, 210.

Phillips, C. A. G. and Warwick, R.G. (1970) 'Steel Pressure Vessels', Quantitative Safety Analysis. Nuclear Engineering and Design, 13, 227-229.

Shaw, J. and Palabrica, R. J. (1974) A critical review and comparison of the nuclear power plant siting policies in the U.K. and U.S.A. Annals of Nuclear Science and Engineering, 1, 241-254.

Stevens, C. (1957) Confidence limits of range of a search radar. Applied Statistics, 6, 214-222.

Weatherburn, C.E. (1961) Mathematical Statistics, CUP, 136-137.

Wilkie, D. (1978) The disposition of can thermocouples in a nuclear reactor. Nuclear Energy, 17, 47-56.

13 Appendix: Meaning of Symbols

Can Temperatures, Calculated, Actual and Indicated

T_{SM} = the expected average value of fuel element can temperatures at the hottest level in the core with the reactor operating under design conditions.

T_D = the basic design temperature for the fuel element can, being a function of the flux distribution, rating pattern, coolant mass flow and Stanton number, but ignoring systematic and random perturbations of these parameters.

T_S = the systematic fuel element can temperature calculated with respect to known perturbations but ignoring random effects.

T_{SP} = the peak systematic fuel element can temperature, being the peak value of T_S. (This differs from some definitions in that it is a calculable temperature for a specific can or group of cans and does not have an associated probability.)

Probabilities, Confidence Limits and Multipliers.

Λ = the probability that there is an actual fuel element can as hot as the extreme upper limit of the range of fuel element can temperature scatter (with the reactor in normal full power operation in a steady state).

$P(=m)$ the probability that a group of ψ fuel elements, however taken, in a common horizontal layer across the core contains exactly 'm' can temperature thermocouples.

$P(<m)$ = the probability that a group of ψ fuel elements, however taken, in a common horizontal layer across the core contains less than 'm' can temperature thermocouples..

X = confidence limits for reactor temperature control, defining the percentage of cases in which it is expected that the allowance for precision of sampling (ξ) will not be exceeded.

λ = the multiplier to give a temperature margin ($\lambda\sigma_B$) between T_{SP} and $T_{\Lambda max}$ so that the chance Λ of there being a fuel element can as hot as $T_{\Lambda max}$ is acceptably small.

x = the multiplier appropriate to the control confidence limits (X), defining the percentage of cases in which the allowance (ξ) for precision of sampling will not be exceeded.

$T_{\Lambda max}$ = the extreme upper limit of the range of fuel element can temperature scatter owing to random effects and very unlikely to be reached by any fuel element can in the reactor core in normal full power operation. (The probability Λ of such an event is defined in terms of a temperature margin $\lambda\sigma_B$ above T_{SP}, and will be very small.)

T_A = the actual temperature of a fuel element can, being the highest temperature experienced on the can surface.

T_{po} = the actual mean can operating temperature of the group of fuel elements chosen for control.

θ_{po} = the indicated or measured mean can operating temperature for the group of fuel elements chosen for control.

Temperature Deviations

δ_A = the known or systematic component of the deviation of the fuel element can temperature from its design value, T_D.

δ_B = the unknown component of the deviation of the actual fuel element can temperature from its calculated systematic value, T_S.

Standard Deviations

σ_B = the standard deviation of the difference between the measured or indicated fuel element can temperatures and the corresponding calculated or systematic values.

σ_R = the deduced standard deviation for the random effects which perturb the fuel element can temperatures and distribute them about their calculated or systematic values. ($\sigma_R \approx \sigma_B$).

Error Allowance and Margins

ε_B = the standard error permitted in determining σ_B.

ξ = the allowance for precision of sampling in determining the measured or indicated mean temperature of the group of fuel elements chosen for reactor control.

Φ = the margin allowed for a temperature excursion between $T_{A\,max}$ and the nominal temperature for melt-out or ignition of the Magnox fuel element cans.

Channels and Measuring Points

N = the total number of fuel element channels in the reactor core.

N_c = the total number of fuel elements in a group selected for reactor temperature control.

n_c = the number of fuel element can temperatures which must be measured from the group of N_c fuel elements in order to obtain for reactor temperature control an indicated sample mean fuel element can operating temperature (θ_{po}) at the required precision (ξ) within the confidence limits (Λ).

n_s = the number of can temperature measuring points distributed at random in the layer of hottest cans across the core which are needed to determine σ_B and to verify the thermal model.

n_Ψ = the number of randomly distributed fuel element can temperature thermocouples needed for core stability surveillance.

Ψ = the minimum number of continuous channels in a group, however disposed, which is expected to include a designated number 'm' of can temperature thermocouples at a common horizontal layer in the core.

m = the number of fuel element can temperature thermocouple signals indicating temperature excess needed by the safety circuits for an alarm or trip.