International Institute for Applied Systems Analysis
IIASA www.iiasa.ac.at

Issues and Trends in Risk Research (Proceedings of two meetings at IIASA: "Technological Risk in Modern Society" [18-20 March 1988] and "Safe Technological Systems" [11-12 May 1988])

Segerstahl, B. and Kroemer, G.

IIASA Working Paper

WP-88-034

April 1988

Segerstahl, B. and Kroemer, G. (1988) Issues and Trends in Risk Research (Proceedings of two meetings at IIASA: "Technological Risk in Modern Society" [18-20 March 1988] and "Safe Technological Systems" [11-12 May 1988]). IIASA Working Paper. WP-88-034 Copyright © 1988 by the author(s). http://pure.iiasa.ac.at/3171/

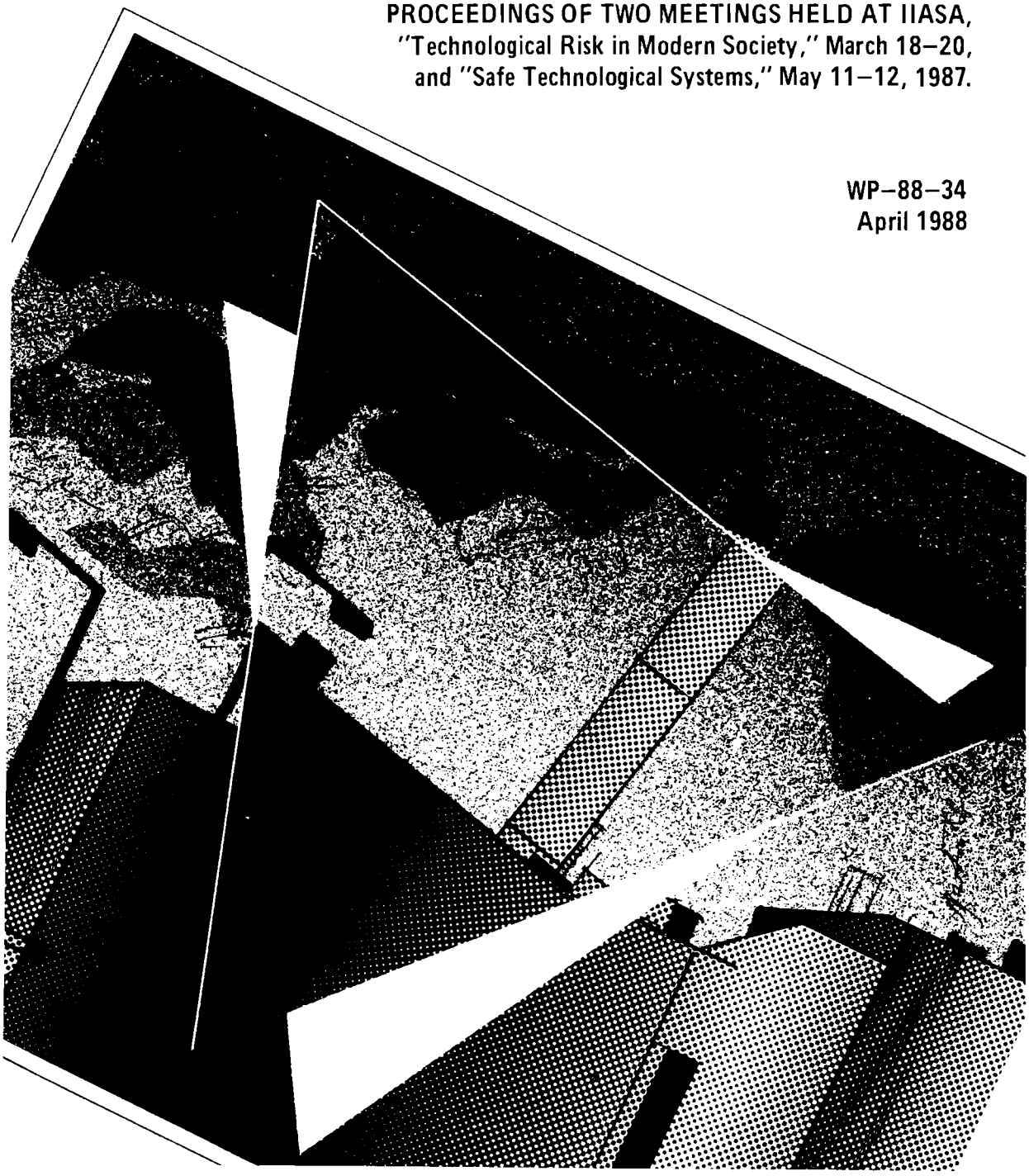
Working Papers on work of the International Institute for Applied Systems Analysis receive only limited review. Views or opinions expressed herein do not necessarily represent those of the Institute, its National Member Organizations, or other organizations supporting the work. All rights reserved. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage. All copies must bear this notice and the full citation on the first page. For other purposes, to republish, to post on servers or to redistribute to lists, permission must be sought by contacting repository@iiasa.ac.at

Issues and Trends in Risk Research

B. SEGERSTÅHL, G. KRÖMER: Editors

PROCEEDINGS OF TWO MEETINGS HELD AT IIASA, "Technological Risk in Modern Society," March 18–20, and "Safe Technological Systems," May 11–12, 1987.

WP–88–34
April 1988



ISSUES AND TRENDS IN RISK RESEARCH:
Proceedings of Two IIASA Meetings

B. Segerståhl
G. Krömer
Editors

April 1988
WP-88-34

PROCEEDINGS OF TWO MEETINGS HELD AT IIASA, "Technological Risk in Modern Society," March 18-20, and "Safe Technological Systems," May 11-12, 1988.

INTERNATIONAL INSTITUTE FOR APPLIED SYSTEMS ANALYSIS
A-2361 Laxenburg, Austria

FOREWORD

Research on risks resulting from our highly technological society has a long tradition at IIASA and has firmly established the institute as a center for a growing network of scientists concerned with technological risks. IIASA's research has been characterized by a small and dynamic group of scientists from many different disciplines and countries working together on a concrete technological risk problem. A major strength of the research has been its continuing focus on substantive problem areas with an evolving and often pioneering conceptual and scientific approach. Thus, IIASA has made important contributions to the general "risk" field in topics ranging from "decision making under uncertainty" and the "perception of risks" to the role of risk analysts in political and institutional processes.

At its June 1986 meeting, IIASA's Council decided to consolidate and strengthen the institute's research on technological risk. Extensive discussions within the institute and with outside organizations have taken place in an effort to ensure an optimal choice of issues to be addressed from the point of view of relevance and access to knowledge in the field. It was felt necessary to enter a fact-finding phase in order to evaluate the latest trends in risk research and to arrive at a meaningful set of issues on which to concentrate further research undertaken by the institute. Two meetings have been organized to this end:

1. Technological Risk in Modern Society: This meeting took place in Laxenburg from March 18-20, 1987, and was organized by IIASA in collaboration with the International Atomic Energy Agency (IAEA). Its goal was to design a research agenda for work related to safety issues and to the control and management of accidents in power systems or other potentially high-risk utilities. The meeting was divided into three sessions:

   1. Regional Risk Management: This topic covered aspects of regional development and planning related to potentially high-risk installations. The session emphasized economic aspects.

   2. Man-machine Interaction: A significant share of accidents or disturbances in complex operations are caused by what is commonly termed human failure. This session was devoted to this rather controversial subject.

   3. Management of Environmental Consequences: This session dealt with the use of regional- and global-scale transport models to study the environmental implications of accidental or continuous releases of hazardous substances. A further concern was the design of monitoring and warning systems.

2. Safe Technological Systems: This workshop was organized exclusively by IIASA and took place at the Institute from May 11-12, 1987. Instead of taking a given design and looking at ways and means to improve its safety, the meeting attempted to look at the impact of design principles and different types of trade-offs on the generic safety of technological systems.

   After numerous accidents in technological systems, it has become urgent to address the issue of how to improve the safety of technological systems. There have been discussions on inherently safe nuclear power plants, for example, but the general concept of inherently safe systems is subject to debate. Nevertheless, it is clear that in future system design, safety must assume a much more important role than in the past. Below is a summary of the three sessions of the meeting:

   Session I: Technical Concepts: Technical safety criteria, design principles, man-machine interaction, problem perception in different industrial sectors;

   Session II: General Safety Criteria: Complexity vs safety, human factors, PRA, safety and risk definitions, failure chains;

   Session III: Policies and Constraints: Societal, economic and institutional constraints, procedures, institutions, regulation, and licensing.

ABOUT THIS VOLUME:

As the two meetings are closely related to each other, it was decided, instead of creating two separate proceedings volumes as originally planned, to combine the outcomes of both meetings into one logical volume. This allowed us to rearrange the topics across the two meetings, thereby arriving at a more coherent documentation.

The papers included have been brought into proper context as far as possible, independently of in which session or workshop they were presented. In most cases, they are included as delivered by authors, without additional editing. The purpose of these proceedings is strictly documentary without emphasis on layout, style or thematic consistency.

Boris Segerståhl and Gerhard Krömer,
Editors, IIASA Task Force on Risk

ACKNOWLEDGEMENT

A great part of the success of the meetings and the visual quality of these proceedings are due to the organizational talents, patience and efforts of Laura Burton. We are grateful for her help in both organizing the meetings and putting all the material together in this volume.

TABLE OF CONTENTS

INTRODUCTION AND SUMMARIES

WELCOME ADDRESS

Prof. L. V. Konstantinov
Deputy Director General
International Atomic Energy Agency

CONTENT

1. INTRODUCTION

Good morning, Ladies and Gentlemen,

It is a pleasure for me to welcome you on behalf of the International Atomic Energy Agency at this Task Force Meeting. This meeting has been organized by IIASA in co-operation with the IAEA. The basic objective of our involvement, in addition to its scientific content, is to explore areas where co-operation between IIASA and IAEA might be useful in the future. Such a co-operation is not new and has proven useful in the past. In particular, I would like to remind you of the involvement of the IAEA in the IIASA Energy Programme some years ago. At that time, the co-operation concentrated on the assessment of the impacts of energy production, including comparison of risk of energy systems, public acceptance questions, and the CO_2 problem.

As you are aware, the IAEA is a governmental organization whereas IIASA is a non-governmental institution which is performing research in an international setting. The past has shown that these two different types of organizations can well complement each other in specific tasks. Since the IAEA has participated in the programme planning of this meeting, it is thus clear that some priorities of the present programme of the Agency are reflected in the programme of this Task Force Meeting on Technological Risk in Modern Society.

Before going into more detail on the topics of the sessions, I would like to mention some related activities of the Agency which receive emphasis after the Chernobyl accident.

1.1. International Conventions:

Within a short time after the accident, the Agency has prepared two conventions:

* The Convention on Early Notification of a Nuclear Accident, and

* The Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency.

Both conventions have entered into force, and the number of countries which ratified them is steadily increasing.

1.2. Operational Safety:

In order to prevent future accidents, more emphasis is given to assisting Member States in safe operation and to facilitate feedback of experience. These activities include:

* Operational Safety Review TEams (OSARTs)

* Incident Reporting System (IRS)

* Teams for the Analysis of Safety-Significant Events (ASSETs)

1.3. Basic Safety Principles for Reactors:

The International Nuclear Safety Advisory Group (INSAG), a standing Advisory Group of the IAEA, is preparing a document on the "basic safety principles for existing and future reactor types, with special attention given to those principles which emerge from post-accident analyses."

1.4. Nuclear Safety Standards Codes and Guides:

NUSS documents developed by the Agency from 1974 to 1985 will be reviewed and updated in the light of lessons drawn from Chernobyl.

1.5. Man-Machine Interface:

I will touch this problem later and now would like to inform you that the Agency, on the invitation of Japan, is preparing, in

co-operation with NEA and CEC a major conference in Tokyo, 15-19 Feb., 1988, on Man-Machine Interface in the Nuclear Industry (Control and Instrumentation, Robotics, and Artificial Intelligence).

1.6. Radiation Protection:

Here, the work concentrates on data collection, model validation, and intervention levels. I will come back to this later.

1.7. Probabilistic Safety Analysis (PSA):

In addition to its regular programme, which includes assistance to Member States in an inter-regional technical co-operation programme, the Agency is now also preparing guidelines on how to perform PSA. The objective is to reach a certain degree of standardization, quality assurance and comparability of results.

Probabilistic Safety Analysis is a tool also used in Risk Management. So let me now turn in more detail to the session topics of this task force meeting,

* Regional Risk Management
* Man-Machine Interaction, and
* Management of Environmental Consequences.

2. DEVELOPMENT OF REGIONAL RISK MANAGEMENT

What today is called Risk Management is the product of a long development, which started with the debate about risks of energy systems in the early 1970's.

The first step was comparison of risks in energy systems; the second step was cost-effectiveness of risk reduction measures; and the last step now is regional risk management.

2.1. Comparison of Risks

Comparative studies on risk and impacts from nuclear, coal, oil, solar and hydroelectric power served the purpose to put energy related hazards into proper perspective.

Early studies concentrated first on specific aspects of the risks involved in energy production. More recently, specific problems such as severe accidents, sulphur dioxide releases, acid rain, and CO_2 were singled out.

However, the value of risk comparisons for various energy sources rests not with the overall results, but with the iden-

tification of major risk contributors in each of the fuel cycles investigated.

In this context, it is important to recognize that a quantitative comparison of the risks is only one factors in determining a national "mix of energy" in a country. Other aspects include: energy demand, international trade, industrial development, balance of payment, security of supply, capital costs, etc.

2.2. Cost-effectiveness of Risk Reduction Measures

Cost-effectiveness techniques are a rational tool for optimizing policy decisions on the allocation of funds to safety.

In 1983, the IAEA started a Co-ordinated Research Programme: "Comparison of Cost-Effectiveness of Risk-Reduction Among Different Energy Systems." The main purpose of this programme is to activate and co-ordinate within its Member States a certain number of national case studies, utilizing the cost-effectiveness approach.

Fifteen Member States are cooperating with the Agency in these research efforts. The second research co-ordination meeting report is available, and it is planned to publish the final report in 1988.

2.3. Regional Risk Management

The recent history of catastrophic industrial accidents (such as Seveso, Bhopal, Chernobyl, and recently Basel) had dramatically underlined the need to identify, assess and manage risks from complex industrial activities in order to minimize occupational and public risks and environmental effects.

In the last few years, the attention in various countries and in several international organizations has been drawn to the necessity to identify and implement unified "safety policies" regarding the risks from technological activities.

For instance, after the Seveso accident, the Council of the European Community has adopted several "directives" related to major hazard installations, air pollution from industrial plants, and other risks.

Several industrialized countries like USA, France, Netherlands, Sweden, FRG, etc. have in the last years implemented risk assessment case studies in large industrialized areas.

Risk management implies the definition of quantitative safety criteria and standards, and development of guidelines and procedures.

Risk management at the plant level cannot resolve the multiple objectives of a decision-making process related to environmental impacts, health, and socio-economic effects. The assessment and the management should be broadened to include regions where different industrial facilities are located and should also include emergency planning.

Therefore, the regional approach seems to be the most appropriate for the complex problem of technological risk management. In this regard, the IAEA, the United Nations Environment Programme (UNEP), and the World Health Organization (WHO) are initiating a joint project "on the assessment and management of health and environmental risks from energy and other complex industrial systems." This new research effort will be conducted through the implementation of case studies in developed and developing countries. It has the objective to establish a unified systematic procedure for making decisions about risk in highly industrialized areas within a country.

3. MAN-MACHINE INTERFACE

A more fundamental understanding of the interaction between man and the machine is necessary in industrial work situations to serve as a basis for more error tolerant task and equipment design.

Mistakes and errors are common to both machines and humans. Failure data of equipment are quite well recorded; however, this is not the case for human error. The reasons are partly that they are not recorded at all, and partly that, due to fear of being reprimanded, humans are reluctant to put their own mistakes down in writing. An attempt to overcome this problem has been made e.g. in a Joint INPO/EdF effort on a "Human Performance Evaluation System" where mistakes can be reported anonymously. This has led in the nuclear power area to an increased information base. A similar procedure has been in use for many years with good results in commercial aviation.

Human error data form the basis for improving the man-machine interaction. This can be achieved by:

a) adjusting equipment to be more error tolerant;

b) improving human behaviour through training;

c) providing the operator with additional aids to improve his understanding of the status and behaviour of the plant.

The answers to a) and b) are clear: more automation and better training. However, the operators cannot be trained for all unlikely but possible and sometime unexpected accident scenarios. Therefore, it is necessary to select accident sequences for training, including simulator training, which are sensitive

to human error and which at the same time improve understanding of plant behaviour in general. The Agency has recently produced two reports on this subject.[1] As an interesting side aspect, I should mention that such training also has its risk. Given an abnormal situation in a plant, the operator is more likely to assume that this is part of an accident sequence for which he has been trained and might thus follow the wrong course of actions.

Regarding c), there is a rapid development of operator computer aids. The trend here is to extend the capacities of these computer aids to assist also in normal operation. They provide the operator with relevant information about all safety significant systems, their status and often also expected developments and recommended actions, to enable timely action if required.

Finally, I would like to mention one particular recent development. I have emphasized before that Probabilistic Safety Analysis is an important tool to analyze plant safety. The rapid development of computer technology makes it possible to store the results of a complete level-1 PSA (i.e., up to core-melt) on a Personal Computer. In this way information about the new risk profile of the plant under certain operating conditions can be retrieved in a short time (typically in about 10 seconds). Such information includes new core-melt probability, ranking or probabilities of accident scenarios, and importance ranking of safety systems.

4. MANAGEMENT OF ENVIRONMENTAL CONSEQUENCES

In the area of management of environmental consequences, the IAEA is active in two separate but complementing areas: probabilistic consequence analysis and real-time assessment of hazards to the environment during or immediately following a nuclear emergency situation.

The probabilistic consequence is becoming an important part of many stages in the life of a Nuclear Power Plant. It is being utilized in the preliminary or siting stages, in the definition of engineered safety features and in the rapidly growing in importance subject of emergency planning. The Agency is convening a Technical Committee this summer to study existing computer codes for the consequence analysis and to define future needs and research for improving the models, based on experience gained from incidents in recent years. I am certain that Probabilistic Consequence Analysis is going to become an important tool for industry

---

[1] IAEA-TECDOC-XXX, Identification of Failure Sequences Sensitive to Human Error, Report on a Technical Committee Meeting, 5-9 May 1986, VIC, and IAEA-TECDOC-XXX, Experience with Simulator Training for Emergency Conditions, Report on a Technical Committee Meeting, 15-19 September 1986, VIC.

and regulatory bodies helping to promote better safety for the public and workers alike.

Following the Chernobyl accident and following the Convention on Early Notification of a Nuclear Accident, INSAG recommended that the Agency "should, in collaboration with WMO, review and intercalibrate models of atmospheric transport ... and establish a database for validation studies..."

The Agency, in cooperation with the WMO, has embarked upon this programme and is now at the stage of establishing the database. The planned validation study will probably be more emergency-response oriented than the usual model validation studies and its results will serve to define the source of errors and their magnitudes, to suggest means and methods for improvement of the models, and, finally, to arrive at better real-time models. The results of this study, which should be concluded during 1988, will be made public so that every Member State can benefit from it.

In addition to this study, the Agency is convening this fall an "Advisory Group on the Use of Real-Time Models in Predicting the Radiological Consequences of a Nuclear Accident and Determining the Necessary Protective Measures." This is carrying the utilization of the models one step further and should, with additional implementation of real-time model updating (with radiological on- and off-site information), provide a complete set of emergency oriented models for real-time application, should a nuclear emergency occur.

Well, Ladies and Gentlemen, let me conclude by saying that the IAEA is placing considerable emphasis on the topics of this meeting. I was only able in this welcome address to highlight some of the issues. If more information on Agency programmes is needed, I am sure that the staff members of the Agency who participate in this meeting will be happy to provide it to you. I wish you interesting discussions, and I would be glad if, as an outcome, concrete recommendations for co-operation between the IAEA and IIASA would emerge.

Thank you very much for your attention!

SUMMARY: REGIONAL RISK MANAGEMENT

Dr. Friedrich Niehaus
International Atomic Energy Agency

I would like to comment upon the concepts of the session which I had the pleasure to chair. I must say that for me this was one of the easiest sessions to chair in the past 3 or 4 years. The reason was that we took the remarks of Prof. Segerståhl very seriously: IIASA is a non-governmental institution, and therefore, the discussions were scientific and I did not find anybody in the session who was promoting or defending some kind of governmental policy decision. This is the reason why I think the cooperation between the Agency and IIASA would be valuable as it was in the past. In this summary, I would like to remind you of the presentations which we had with some highlights as I perceived them. I would like to briefly summarize the discussions and then to give an overview of what I think could be future areas of cooperation coming based on the discussions in the session.

If we go through the presentations, we had first the presentation of Mr. Slater about risk management of potentially hazardous industrial installations. Mr. Slater reviewed for us the steps of the analysis which has to be done. He gave a large number of practical examples and stressed the fact that we need simple reliable but also robust results which can be used for decision-making. He emphasized that criteria are needed to judge the results and in principle he convinced at least me that the basic tools are available. However, there is clearly room for improvement. In the discussion, we concentrated on the problem of uncertainties and to what extent we are able to model human error correctly.

The next presentation was on the European Approach to Risk Management by Mr. Amendola. He informed us about the Post-Seveso directives of the European Community and a number of benchmark exercises which are being undertaken for nuclear power, but also in the area of the chemical industry to investigate uncertainties and answer the question how reliable are the results. In the discussion, we touched on the problem of secrecy of studies and also on how to insure quality of the studies if they are being kept secret.

We then had the presentation on Decision Criteria for Siting of Complex Industrial Facilities by Mr. Keeney. He informed us about the different methodologies which can be utilized. He gave us a set of objectives which can be utilized in making such decisions and reminded us to separate between the means and the ends. He made one remark which I still have to think about. He said: "acceptable risk is the risk of the best alternative." I think this is something which maybe we should not forget. The discussion centered around the discrepancies between the normative and

the descriptive approach and also on the problem of what happens if you have many decision-makers.

The presentation on Emergency Planning and Preparedness by Mr. Hayns raised the problem how to define the accidents for which to do emergency planning. He suggested that what is necessary is training, monitoring, dose predictions, communication, human factor, and for some of these he proposed to use computer tools. The discussion centered on the problems of communication and how to deal with the large mass of data which have to be utilized.

We then had a presentation on Risk Management in the Netherlands by Mr. van Kuijen. He informed us about the policy in the Netherlands, the criteria which are being used and which are being discussed everywhere in the world at the present time. He gave us a number of practical applications of risk criteria, e.g. the use of contours of iso-risk (10^{-6}) around a chemical plant for making decisions on construction permits for new private homes. The discussion, of course, then centered on the problem of how to deal with these results in the light of the uncertainties inherent in risk assessment studies, and on the practical use.

We then had a presentation on Advanced Safety Criteria for Nuclear Power Plants - Proposal to Limit Catastrophic Releases by Mr. Kröger. The new item which he brought up in his presentation is that he proposed worst-case criteria which are not subject to the probability of occurrence. Even under those conditions, no public sheltering or evacuation would be necessary. The discussion then centered on the topic on how this relates to, for instance, the emergency reference levels which exist in the U.K. or to the recommendations of the ICRP and the IAEA.

Finally, I would like to refer to the presentation of Mr. Costa-Ribeiro concerning Industrialization, Infrastructure, Risk Management: The Case of the Cubatao Area in Brazil. In this presentation, he gave us some examples of real problems, how the problems have been treated in Brazil so far, in something like a crash program. He also demonstrated that it is very easy in the beginning to set priorities. However, at a later stage, after solving the worst problems, it becomes important to do a thorough analysis and to consider costs and benefits. The discussion, in addition to the purely scientific content, also concentrated on the problem on how to use a regional approach, how to aggregate the various types of risks and the interaction from various facilities.

Well, this in brief I think was what I at least would like to remember from the presentations which we had. We then had a discussion about the area of regional risk management. We tried to structure the discussion with regard to the tools, the criteria, the use, organizational aspects, and future work. We discussed how to do crisis management and how to communicate risk information in the light of the uncertainties. It was stressed

that in evaluating the tools, it is necessary to have real applications, to have demonstrations how they are being utilized and to see what use they are and maybe what is useless. The problem was raised to what extent we really know how good the tools are. It was suggested that it is necessary to have an assessment of the quality of the tools, especially as they relate to different purposes for which they are being utilized. The problem was raised again how to bring together different data and different results for different facilities if one takes a regional approach. Also the problem was stressed on how really to do risk identification, because this of course is a crucial part and it also relates to the problem of completeness of the studies. A word of warning was given on the use of computerized systems and the dangers if everything is computerized. One may be using a good tool, but one does not completely understand what is behind this tool.

On the topic of criteria, we discussed how the results of an analysis can be compared with the criteria which are being proposed with appropriate methods for calculations including problems of quality assurance or standardization and which attributes should be utilized in these different criteria, because of course this is one of the crucial parts for establishing any rank order of alternatives. Again we mentioned the problem about different organizations which are involved. It is necessary to have an integrated approach towards risk management. In connection with these criteria, we also discussed the problem of acceptable risk, public attitudes, and the recommendation was that we should admit that this is a social and political process and that we should try to start with something which looks reasonable and go ahead and see how the social and political process goes. On the topic of uses, we discussed the problem that it is necessary to have some kind of standardized approach, a procedures guide. A word of warning was given to be very careful in using numbers and that it has to be clear what is the meaning of the numbers and where they are coming from.

On the topic of organization, we discussed the problem that there are no useful models at the present time of cooperative decision-making, especially under time constraints and within a hierarchical system. An additional aspect is how to integrate risk management into organizational structures right from the beginning.

This is in very short words the summary I have to offer for the discussion period. Based upon my notes, I will try to summarize areas which emerged for future work. First, the problem of uncertainties, including the problem of the quality of the tools. The main items here: risk identification, as I have mentioned before, and model uncertainties. There was agreement on how to treat the data. This is something we have more or less under control. But the model uncertainties are very important and of course the problem of human factors was discussed. But this will be treated in another summary. Another area of work which

seems fruitful from our discussions is to deal with criteria. It is necessary is to start the process including selecting different attributes. This is something which in the nuclear field at IAEA we have started. One report is available and another one is under preparation. A meeting on safety principles will be held shortly. It is very important from a conceptual viewpoint and from a scientific viewpoint how to treat the uncertainties and how to show compliance in light of these uncertainties.

Another topic which seems to be very fruitful for future work is real applications to case studies; this is what we have proposed in the document which was distributed to you about the joint project with the UNEP and WHO. It would be very useful if IIASA could help in this effort to develop a procedures guide, a standardized approach which one can give to other countries including the problem of aggregation of different effects. This problem occurs in particular when you go from the plant level to the regional level.

Another area which could be useful for future work is cooperative decision making under time constraints in a hierarchical structure and considering multiple organizations. I think there was general agreement on that.

In the area of emergency planning, we discussed that emphasis has to be given to crisis management and means of communication. I think I don't have to stress again the use of computer tools.

The last topic is organizational aspects of risk managements: how to integrate risk management into the organizational structure to insure consideration right from the beginning.

This is in very short words the summary as I have perceived it and I would like to thank everybody who contributed in my session. Thank you.

SUMMARY: MAN-MACHINE INTERACTION

Prof. Björn Wahlström
Technical Research Centre of Finland

Mr. Chairman, Ladies and Gentlemen, I am not going to give a summary of the presentations and the discussions we had in the man-machine interaction session. Instead I am going to pick up some of the ideas and recommendations for a further discussion.

A large part of the discussion during the session was devoted to an argument on to what extent the human actors could be included in the modelling approach of a probabilistic risk assessment (PRA). I am well aware of the arguments in that discussions because I have in my own laboratory representatives of both the PRA and the human factor community. There we have, however, been able to reach a friendly co-existence of both approaches. I think it is necessary to get some agreement with respect to the large lines on what is possible to do and what is not. In this connection we had the suggestion by Dr. Niehaus to conduct a workshop to settle the disagreement between the two approaches. I think such a workshop is important to have, although I consider it to be a short-term issue. If such a workshop is arranged, it is clear that it should involve all parties working with different aspects of the problem.

There was also a suggestion that IIASA should look into the use of expert systems. I will, however, deliberately not give that as a suggestion because I think IIASA will take up that subject regardless of what we are recommending.

Going back a bit to the discussions we had before the workshop, I think we all can agree that IIASA should not go into nuclear power as a specific subject. I think it is more important to look at the risks of modern technology in more general terms in order to be able to make fair comparisons between different approaches. Nuclear power provides on the other hand one important example, and IIASA should here build connections to other organizations, like IAEA, which are working in that field.

In the man-machine group, we were yesterday evening discussing what we should propose as a subject to be taken up by IIASA. Much of our discussion went around different decision-makers and their decision-making situation as parts of our technical systems. This subject involves many of the things we have been discussing: the policy-maker, the regulators, the designers, the operators, the safety analysts, etc. We should be able to understand the characteristics of the decision-making situation and the consequences of decision errors. This means that we have to consider the complexity of the systems and the tools the decision-makers are using. In short, we have to build models of how decisions are made in our technical systems.

Considering decision-making, it is clear that IIASA should narrow down on the systems approach of the technology and the "low probability-high risk" sequences of events. In modelling such sequences, we have to consider self-organizing systems as in the emergency planning situations Prof. Dynes was talking about. Another theme which should be involved in such a modelling effort is how to plan for the unexpected. I think the only solution here is to make our decision-making systems more robust, and here is a connection to the risk control approach Prof. Rasmussen was talking about.

My own vision is that it should be possible to get some general descriptions or models of the decision-making activities in the society when a new technology is introduced, assessed, adopted, and used. The models should certainly involve the different actors, their tools, and how they handle information in their decision-making situations. Such models should be possible to use for the detection of possible problems and thus for the improvement of the decisions made.

We should naturally put the subject also in an international framework and consider how different cultures and societies are influencing the decision-making systems. Just taking a small example of differences between countries, I here in Austria in my hotel saw a life-saving device which I have seen elsewhere only in Norway. It was a string in the bathroom by which you could call the hotel personnel. There was a slight difference in the man-machine interface, especially in connection with a procedure for how false alarms could be cancelled. The questions which came to my mind was whether or not the device is based on regulation, what kind of risk calculation has been used, and why only Austria and Norway have gone for this solution.

If IIASA would like to take up something along these lines, I think there will be things to do for many years. I also think there are research communities in many places of the world which would be interested to support and join such work. We tried yesterday to find a label for such a program, but we were not able to get a catchy phrase. However, including key words such as technological risks, decision-making systems, human interaction, and system models, I think the subject can be specified accurately enough. If this is a subject to be brought up, I think IIASA will not have any problems in finding persons willing to work out the details of a research program.

Before finishing, I would like to bring up one point which we have been discussing in our group. It has to do with a systems-induced interaction which may induce safety threats in a complex environment. We are today in most places searching for increased performance, which has to be considered very natural, to save resources be being more efficient. In some cases, however, it may happen that the new practices in some unexpected way are decreasing the safety margins inherent in the old practices.

In the case, the system development is made by small exploratory moves, then it is easier to handle all the preconditions for safety. There are, however, also cases where the development is going in quantum jumps, and then it is far more difficult to make all the system changes necessary to maintain an acceptable safety. There are always risks in adopting new methods because long-term effects cannot be seen beforehand. By systematic efforts, however, it should be possible to avoid too dangerous trial-and-error by and large.

I really think IIASA has an important role in promoting international cooperation in the systems and risk areas. Coming from a small country, I often like to stress the importance of international cooperation, and I also think that the large countries will get a similar benefit. We clearly get additional operating experience with the possibility of early warning based on events elsewhere. The "natural" experiments like the accidents at TMI, Bhopal, and Chernobyl require also a very careful analysis in order to fully utilize all the lessons to be learnt. Such work requires an international dialogue to utilize all expertise available for the verification of the models we are using for predicting the resulting safety level of the technologies.

In maintaining and developing a deep and narrow expertise, it is sometimes difficult to find discussion partners in a small country, and then such have to be sought abroad. I think also it is important to note that our world is interconnected and that decisions in other parts of the world are influencing ours. The Chernobyl accident provides one example as we in Finland were well on the way with a decision to build a fifth nuclear power plant unit. After the accident, the decision was postponed, and it is now very unlikely that such a decision will be made in the near future with all the implications it may have.

1. REGIONAL RISK MANAGEMENT

1.1. RISK MANAGEMENT OF POTENTIALLY HAZARDOUS INDUSTRIAL INSTALLATIONS

Dr. David Slater
Technica, Inc.
Columbus, OH, USA

Synopsis

What is Risk Management?

Many of the current problems being faced today by industry have to do with the impact of modern science and technology on society.

Science, essentially knowledge, harms no one, but technology or the implementation of science in practice by definition is an action to which there is an inevitable societal reaction. It has been proposed by humanists that technology can have no legitimacy unless it inflicts no harm.

Managers of technology use should therefore ensure that they comprehend and respect the laws of science applicable to their technology and exercise care in assessing the probable consequences which, should they be harmful, require that they abstain from employing the technology until they have found ways of making it "safe." To be legally permissible or socially desirable, management of technology must conform to the legal maxim of "mutuality of liberty" -- the principle that one man's freedom of action ends where it would injure another.

It is clear then that an assessment of the risk, i.e. whether the technology has the potential for harm ought not to be decided unilaterally by the proponents. But it is these proponents who must manage its practical exploitation, taking into account the economics and the politics as well as the technology. Indeed it has been suggested that currently top management with a background in banking and law is lacking the vital technological dimension to understand the full implications of the technological liability.

The present challenge is to communicate a numerical assessment of system performance to decision-makers in a format that they can readily appreciate. Managing risk is fundamental to company survival. Historically, management information systems have been tailored to produce data on parameters essential to managing financial "risk," cash flows, profitability, etc. More recently, the management of research and development has addressed the areas of technical risk. But only in the wake of disasters like Bhopal has management finally realized that "risk" management is not just these factors, it is not even just ensuring that there is enough insurance coverage for their liabilities (the classic insurance definition of risk management), but it must

include the understanding and control of the potential for harm from the exploitation of technology.

What is Needed?

Management of technological risk in common with management of most enterprises requires an overall strategy, detailed plans, and ways of monitoring current status and projected performance.

Decisions are then required on the continuing appropriateness of the plans and the measures to be taken to implement the strategy and correct any deviations in real performance versus chosen targets. Put this way, the requirements for fiscal, technical, and liability (risk) management are identical in form.

Risk management requires decisions. Decisions need hard data. These data should reflect:

* current situation, status
* predicted behavior, trends
* importance ranking of needs
* cost effectiveness of solutions
* an indication of assumptions, limitations and uncertainties (= confidence)

The need is for an organizational structure that will allow production of plans and targets, monitoring and assessment of the present situation, of proposed modifications or new ventures, and an effective control system for implementing the decisions.

The Risk Management Program

The first requirement in any program is an ability to communicate the information to the participants. If top management is essentially legally or fiscally trained, the information needs to be put in terms that can be understood by them. (It is also more likely to be understood by the general public.) The second requirement is for a clearly understood process for making technological decisions. This should contain three elements:

* first quantify - to know
* secondly model - to predict
* thirdly rank or prioritize - to decide.

Quantification

Currently quantitative risk analysis is becoming firmly established worldwide as it does provide numerical results which represent more or less, depending on the quality of the analyst and the techniques employed, the actual risk picture of the system and its potential impact on society.

Modelling

As part of the RA process, the response of the system to process impacts, containment failure, human error, etc. needs to be modelled. When these elements are combined together and aggregated for whole plants, complexes or industries as present day computer packages allow, then there is made available to management an ability to examine the potential effects of decisions or options on a "what if?" basis.

Decision

Given numerical results from quantitative risk calculations and systems modelling (reliability, unavailability, loss rates, etc.) that can be directly integrated with numerical data on costs, effects, etc., decision-making ought to be relatively straight forward. (The fact that it is seldom so simple reflects the need to incorporate the other vital elements that reflect society's response.)

For practical managers whose goals are essentially private, pragmatic and short-term, decisions are simple. The goals are to put the technology to use in the most economical and effective way as possible, with what little thought given to the long-term consequences being regarded as the responsibility of others.

Risk Management Criteria

There has to be a way of incorporating a public, humanistic, and long-range element into the process. In any organization, goals and targets are an essential part of a management program. Similarly in many potentially hazardous industries, safety goals and targets are finding more and more acceptance. But it is widely felt in these industries that it would simplify matters if there were "norms" or criteria of acceptability which could be used as society-approved safety levels. A demonstration that these criteria have been achieved would then be a necessary and sufficient defense in the event of the inevitable accident.

It is now realized that with many of the present day technologies the goal of "mutuality of liberty" is not obtainable. As the cost of requiring that the design and operation of these technologies be modified to meet this maxim is too large to contemplate, society needs to face pragmatically an existing situation and "accepted" level of risk that has grown out of the last hundred years of operation. This is enshrined in the current engineering codes and standards, most of which are recognized worldwide. It is still possible to meet the humanistic goals, but not today. A phased program of pragmatic criteria of acceptability progressively modified to decrease the risks or increase the safety by stages would help achieve a managed change, perhaps geared to overall quality of life and longevity expectation, and to natural disease and accident risks.

Examples

There are a number of examples of how potentially hazardous industry is coping with the problems of managing risk, and these will be outlined. Risk management decisions on process choice, siting, layout, routing of transportation hazards, etc. will be illustrated using risk contours, F/N curves and occupational indices. Finally, the role of more formal decision-making techniques such as importance ranking and hierarchical decision aids will be discussed.

Conclusions

Risk management of potentially hazardous industry is undergoing a serious rethink in the wake of recent incidents. It is recognized that internal goals and targets are needed in quantitative terms and that the skill must be available to provide numerical data on the risk of current and planned operations. It is felt that a concerted and socially supported set of guidelines on acceptable risk either national or internationally would be a major contribution to simplifying and identifying the responsibilities of management. These have to be set, however, against a background of what is practicable and realistically achievable.

In the absence of such criteria, management must balance liabilities and penalties from hazardous operations themselves using the best risk quantification and decision aids available. This will inevitably lead to a wide range of corporate attitudes with some adopting a more aggressive stance than others, being willing to take risks that perhaps society should not allow.

1.2. THE EUROPEAN APPROACH TO RISK MANAGEMENT

Dr. A. Amendola
Systems Engineering and Reliability Division
Joint Research Centre, Commission of the European Communities, Ispra, Italy

ABSTRACT

EEC directives concerning the major accident hazards of certain industrial activities and the assessment of the environmental impact of technological systems are described and commented upon. Thereafter, a short overview of the research activities sponsored by the Commission of the European Communities is presented, with particular emphasis on those concerning the assessment of state-of-the-art models and procedures for risk analysis both of nuclear and chemical facilities.

1. INTRODUCTION

Risk management is a very comprehensive subject covering a significant number of very different topics which range from hazard identification to the measures adopted for reducing risks to accepted levels and for facing emergencies.

It includes, therefore, criteria for risk assessment, evaluation of costs and benefits of alternative measures, public perception and acceptability, as well as decision making.

In reality, risks are managed at very different levels by different decision makers (such as industrial companies, plant operators, local and governmental control authorities, international bodies); a complete treatment of the subject would require an in-depth analysis of the decisional structure, which should give account of the different situations in the EEC countries. Furthermore, a comprehensive treatment would require to deal with the diverse hazard sources such as nuclear plants, chemical processes and storage facilities, transportation of hazardous materials, waste disposal, biotechnologies, products, etc. Furthermore, risks of accidents should be distinguished from risks connected with continuous emissions and impacts on health and environment should be discussed both at short-time and long-time scale.

Sinergetic effects between different sources should also be discussed.

As a consequence, if clear restrictions are not assumed with respect both to the scope and to the extent of the subject proposed to the author for the present workshop, the paper would result either in a punctual and fragmentary listing of somewhat disparate attitudes according to the single hazard sources or in a generic and abstract philosophical statement since the different technological sectors are not yet approached with uniform criteria. On the contrary, by restricting the scope, some activities which can be considered as exemplary can be discussed to a sufficient extent. In particular, the paper is focused on:

- the way the so-called Seveso Directive is being implemented for the control of the hazards presented by certain industrial installations;
- the description of a more recent directive on the assessment of the environmental impact of new projects; and
- the description of research projects aimed at establishing a common awareness on the advantages and limitations of available methods, models and procedures for probabilistic safety assessment both of nuclear and chemical facilities, as well as on the associated uncertainties.

2. THE POST-SEVESO DIRECTIVE

The overall Community policy for preventing accidents in the chemical industry is set up by the EEC Directive 82/501/EEC of 24 June 1982 on the major accident hazards of certain industrial activities. The system established by the Directive has been in force since January 1984 and results in a quite successful on-going implementation process under the responsibility of the DG XI (Environment) /1,2/.

The Directive covers all the aspects to be included in a risk management policy for process and storage installations in which dangerous (i.e. toxic, flammable or explosive) substances are involved in quantities presenting risks of major accidents (waste disposal, mines, nuclear, military and transport hazards are excluded).

The member countries were obliged to conform their legislations to the Directive by January 1984, so that this could be effective by January 1985 for all new plants, with a tolerance period for existing installations expiring in 1989. The requirements of the Directive can be summarized as follows:

- each member country must appoint a competent authority;
- all manufacturers are required to prove to the competent authority that they have identified the major hazards and adopted safety measures when dealing with dangerous industrial activities. These are identified through a list of 178 dangerous chemicals which are or may be involved in the activity;
- when these substances are involved in quantities exceeding specified thresholds, the manufacturer must submit a safety case and supply all information needed for the establishment of emergency plans;
- the authorities have to evaluate the safety report and to ascertain that the most appropriate measures to prevent major accidents have been taken; the authorities must provide inspections to ascertain that the safety measures are observed during operation;
- the manufacturer must provide in-site emergency plans and must inform the public on the risks presented by the activities as well as on the immediate measures to be taken in case of emergency;
- on the basis of the information provided by the manufacturer, off-site emergency plans must be prepared by the authorities;
- major accidents must be notified to the competent authorities, who must supply accident reports to the Commission;
- the Commission must keep the records of major accodents at the disposal of member states for preventing purposes;
- all provisions should be subjected to revision according to experience.

The relevance that the Directive gives to inform the public and to report accidents should be noticed; despite the sensitivity of this matter, important achievements are being obtained. In particular, the Major Accident Reporting System has become operational. It differs from other industrial incident data bases /3,4,5/ since the information recorded is based on a very detailed collection form /6/ which has been adopted by the standing Committee of National Competent Authorities,

who are responsible for the reporting to the Commission.

The retrieval and analysis of experienced events will certainly constitute a basic element of the Commission's policy of prevention.

The above mentioned Committee constitutes an established forum for the exchange of information in order to ensure the establishment of common standards in the implementation and the control of the Community legislation.

The Commission, in collaboration with the national authorities, also organizes regular workshops for the national inspectors as well as conferences aiming at establishing states-of-the-art on selected topics (such as the conference on Emergency Planning to be held in Varese in November 1987).

All these activities are strongly contributing to a harmonized implementation of the Directive.

As a result of the on-going process, an amendment in the Directive has been proposed and adopted in 1987 concerning the threshold for notification of particularly dangerous substances such as chlorine and phosgene. A new amendment is being studied to better cover the problem of isolated storage which dramatically emerged after the Sandoz accident in Basel.

It is also worth remarking how after the major disasters in Mexico and India, worldwide initiatives are assuming the EEC Directive as a milestone.

The safety case issue is of particular interest for the present workshop. The Directive establishes which are the items that must be included into the notification procedure, but it does not specify applicable methods of analysis and criteria for acceptability. These are left to the national legislations, even if a mutual exchange of information on safety cases is promoted, as described above.

Now, in some countries - such as The Netherlands - quantitative risk acceptability criteria are being introduced /7/; in other countries such as the United Kingdom, the Health & Safety Executive suggests in its guidance on the contents of "Safety Cases" that: "While it may be possible for manufacturers to write a Safety Case in qualitative terms, HSE may find it easier to accept conclusions which are supported by quantitative arguments. A quantitative assessment is also a convenient

way of limiting the scope of the Safety Case by demonstrating either that an adverse event has a very remote possibility of occurring or that a particular consequence is relatively minor."

In other countries, purely qualitative analyses are used. The major debate in the industry about the use of probabilistic risk assessment concerns on the one hand the maturity of discipline and, on the other, possible misuse and resource waste in indiscriminate PSA adoption. The CEFIC position paper asks for a flexible approach and considers the use of quantified risk analysis only justified in selected cases /8/.

3. THE DIRECTIVE ON ENVIRONMENTAL IMPACT ASSESSMENT

The Directive (85/337/EEC) on the assessment of the effects of certain public and private projects on the environment has been emitted in June 1985 and should be enforced by the member states by July 1988. According to this Directive, "the environmental impact assessment will identify, describe and assess in an appropriate manner ... the direct and indirect effects of a project on the following factors:

- human beings, fauna and flora;
- soil, water, air, climate and the landscape;
- the interaction between the factors mentioned above;
- material assets and the cultural heritage."

Information to the public deserves a particular attention: "any request for development consent and any information gathered according to the Directive are made available to the public; the public concerned is given the opportunity to express an opinion before the project is initiated."

The Directive may have a heavy impact on the environmental policy of the EEC countries since it practically covers all kinds of man-made systems with the exception of projects serving national defense purposes and those already sufficiently covered by a specific set of national legislation.

The information that must be supplied for the concerned projects includes among others:

"- an estimate of expected residues and emissions (water, air and soil pollution, noise, vibration, light, heat, radiation, etc.) resulting from the operation of the proposed project;
- where appropriate, an outline of the main alternatives studied by the developer and an indication of the main reasons for his choice, taking into account the environmental effects;
- a description covering the direct effects and any indirect, secondary, cumulative, short, medium and long-term, permanent and temporary, positive and negative effects of the proposed project on the environment resulting from:
  . the existence of the project,
  . the use of natural resources,
  . the emission of pollutants, the creation of nuisance and the elimination of waste,
  and the description by the developer of the forecasting methods used to assess the effects on the environment;
- a description of the measures envisaged to prevent, reduce and, where possible, off-set any significant adverse effects on the enenvironment."

The projects which are subject to the most stringent obligations when exceeding established sizes are:

- crude oil refineries and gasification/liquefaction of coal on bituminous shale;
- thermal power stations, other combustion installations and nuclear power reactors;
- permanent storage or final disposal of radioactive waste;
- integrated work for the melting of cast-iron and steel;
- extraction and processing of asbestos;
- integrated chemical installations;
- motorways, railways, airports, trading ports; and
- waste disposal installations for the incineration, chemical treatment or land-fill of toxic and dangerous wastes.

Other projects might be subject to the judgement of the member states; these include activities concerning agriculture, extractive and

energy industry, processing of metals, manufacture of glass, chemical, food, textile, paper and rubber industry, infrastructure projects and others (among which holiday villages and hotel complexes).

This summary should be sufficient to focus on the R&D activities which might be promoted by the need to comply with the obligations laid down by the Directive.

4. R&D ACTIVITIES

The Joint Research Centre of the Commission of the European Communities is involved in many R&D activities related to relevant aspects of the management of risks connected both with nuclear installations and with hazardous industrial ones, i.e. risk identification, data acquisition and decision making. However, since the JRC is not directly involved in the particular decisional processes, its research programme is mainly aimed at providing decision makers (industries, control authorities, etc.) with decision support systems (DSS) and validated data, models and procedures for risk identification and assessment.

As far as Decision Support Systems are concerned, the IRIMS and SRA projects should be mentioned.

IRIMS (Ispra Risk Management Support System) has been developed in collaboration with IIASA after a comprehensive study of regulatory processes /9/. Its goal is to look at the complete cycle of hazardous substances, including the risks of manufacture, transportation, use and ultimate disposal of waste. The system /10/ has three main parts: a number of data bases containing information relevant to environmental impact, risk analysis and optimization; and a decision support tool which the decision maker uses to shape his decisions. At present, IRIMS is a demonstration prototype version designed to show the feasibility of integrating data bases and simulation models through an intelligent interface; a first operational tool is expected after completion of a case study of the risks associated with the production, transportation and use of chlorine in The Netherlands, which is being performed in collaboration with the VROM Ministry and IIASA /11/.

Whereas IRIMS is a support tool for sectorial or regional risk management, the SRA (System Response Analyzer) is being developed as a generator of multiple incident scenarios in which various combinations of failures are accounted for: machine failures, human failures and procedure failures; it is, therefore, aimed at improving DSS's for operators of hazardous plants. The concept has been developed with reference to nuclear systems by starting from a dynamic probabilistic safety analysis methodology /12/ and by including simulative models of human operators /13,14,15,16,17/.

As far as data acquisition is concerned, the reader is referred to the already mentioned MARS /6/ for chemical incidents and to the European Reliability Data System /18/ which collects and harmonizes component reliability, incident and plant availability data from nuclear power plants in Europe.

As far as assessment of methods and procedures for PSA are concerned, comparative studies performed independently by different teams on a same reference object (Benchmark exercises) have proved to give deep insight into models, procedures and uncertainties linked with reliability assessment /19/ and to significantly contribute to the establishment of a common awareness on all relevant problems (advantages, limitations, cost-effectiveness of the different methods, states-of-the-art in the model and in the data field, etc.).

Indeed, a major issue in any PSA is constituted by the problem of the associated uncertainties and of the reproducibility and comparability of the results, especially when analyses, performed at different times and/or by different experts, must be used for decisional purposes (optimization, back-fitting of old plants, choices among alternatives, acceptability, etc.). Consequently, there has been an important effort to try to develop guidelines and common PSA procedures. Rather than starting from establishing normative guidance, JRC has set up an RBE programme with the first goal being eventually to obtain commonly agreed state-of-the-art procedures. The approach followed is to define a common study case and have this analyzed by different teams. The teams happen to represent industry, authorities and research centres in a rather well-balanced way and, thus, the RBEs help to establish a

better dialogue and common language between the various parties involved in PSA.

The program started in 1982 with an exercise on systems reliability analysis. The auxiliary feedwater system of the EDF plant Paluel was chosen as a reference and 11 teams (10 from the EC and one from Sweden) carried out a qualitative analysis (FMEA) and a quantitative analysis (fault tree construction, quantification and analysis), structured to identify sources and magnitude of the uncertainties. The spread in the results was found to be larger than expected. This was for an important part due to modelling; hence, it was concluded that systematic qualitative analysis, a more precise definition of the decision framework for which the analysis has to be performed (licensing versus best estimate) and the use of (computerized) modelling procedures could help to improve robustness and credibility. A second conclusion was that the common cause failure and human failure issues needed deeper consideration and so they were chosen as topics for the next RBEs /20/.

The Common Cause Failure RBE (CCF-RBE) started in mid-1984. This time a German plant (Grōhnde) of KWU design was chosen. The reference systems were those providing auxiliary feedwater in case of a loss of preferred power (a 2x100% start-up and shut-down system and a 4x100% emergency feed system). This time 10 teams (including one from Sweden and one from the USA) participated. The CCF-RBE helped to achieve first a common understanding of various types of dependent failures, then an agreement on the domain of application of the various explicit and implicit (parametric) models and to assess the merits and limitations of the latter /21/.

Currently, a benchmark exercise is under way on human reliability assessment. Two different study cases are being analyzed: potential operator errors in carrying out routine functional tasks based on written procedures, and human reliability aspects involved in operators responding to an emergency /22/.

The overall experience with the benchmark exercises has proven that the approach followed was very powerful for agreeing on state-of-the-art procedures and methods; therefore, it is being now extended to non-nuclear hazard analysis /11/. Reference system will be an ammonia storage facility linked with a sea terminal and a process plant.

Participation from industry, authorities, expert and research organizations will provide a frame similar to that of the nuclear PSA projects. However, the extent of the analysis will be a complete risk assessment (from qualitative hazard identification up to the evaluation of risk contours). The final results are expected by the end of 1989.

5. CONCLUDING REMARKS

Independently of the assessment criteria that will be finally adopted by the member states, the EEC Directives are certainly improving the general awareness of the public, authorities and industry on the need for implementing concrete measures to prevent accidents and to protect the environment; concrete measures are already operative.

They also open a great potential for R&D: selected examples of Commission-sponsored activities relevant to the aims of this workshop have been presented which can contribute to the establishment of a common way of thinking among all parties involved in the real decisional process.

REFERENCES

1. G. Del Bino, Community Environmental Policy: Priority for Prevention, ISS/WHO/IPCS World Conference on Chemical Accidents, Rome, July 1987.
2. P. Testori-Coggi, The Community policy on major accieent hazards: important achievements in an on-going process, ISS/WHO/PICS World Conference on Chemical Accidents, Rome, July 1987.
3. P. Bockholts et al., A Survey on Industrial Accieent Data Bases, EUR 11072 EN, CEC-JRC, 1987.
4. G.C. Bello (Editor), Proc. of EuReDatA/3ASI seminar on Incident Data Bases and their Use in Risk Analysis, Milano, TEMA, October 1985, S.P. No. I.05.E3.86.13, CEC-JRC, Ispra, 1986.
5. J.J. Clifton and A. Wilkinson, MHIDAS: Major Hazard Incident Data Service, ISS/WHO/IPCS World Conference on Chemical Accidents, Rome, July 1987.
6. A. Amendola, The Major Accident Reporting System in "Reliability Data Bases", A. Amendola and A.Z. Keller (eds.), D. Reidel Publishing Company, Dordrecht, NL, 1987.
7. K. Van Kuijen, Risk Management in the Netherlands, Task Force Meeting on "Technological Risk in Modern Society", IIASA/IAEA, Laxemburg, March 18-20, 1987.

8. J. Clerinx and L. Jourdan, Quantitative Assessment of Risks from Installations in the Chemical Industry, ISS/WHO/IPCS World Conference on Chemical Accidents, Rome, July 1987.

9. H. Otway and M. Peltu, Regulating Industrial Risks; Science, Hazards and Public Protection, Butterworths, London, 1985.

10. IRIMS: the Ispra Risk Management Support System, a computer based prototype, edited by System Engineering and Reliability Division, Technology Assessment Sector, EUR 10862 EN, 1986.

11. A. Amendola and P. Huastrup, Risk Identification and Management: an integrated approach, ISS/WHO/IPCS World Conference on Chemical Accidents, Rome, July 1987.

12. A. Amendola and G. Reina, DYLAM-1, a software package for event sequence and consequence spectrum methodology, EUR 9224 EN, 1984.

13. A. Amendola, G. Reina and F. Ciceri, Dynamic Simulation of Man-Machine Interaction in Incident Control, Proc. of the 2nd IFAC Conf. on Analysis, Design and Evaluation of Man-Machine Systems, Varese, 1986, Pergamon Press.

14. G. Mancini, Modelling Humans and Machines, in Intelligent Decision Support in Process Environments, E. Hollnagel, G. Mancini and D.D. Woods (eds.), NATO ASI Series, Springer-Verlag, Berlin.

15. P.C. Cacciabue and U. Bersini, Modelling Human Behaviour in the Context of a Simulation of Man-Machine Systems, in Human Decision Making and Control, J. Patrick and K. Ducan (eds.), North-Holland, Elsevier, Amsterdam, 1987.

16. A. Amendola, U. Bersini, P.C. Cacciabue and G. Mancini, Modelling Operators in Accident Conditions: Advances and Perspectives of a Cognitive Model, Post NATO-ASI Conf. on Intelligent Decision Support in Process Environments, Ispra, November 11-14, 1986, to be published in International Journal of Man-Machine Studies.

17. U. Bersini, P.C. Cacciabue and G. Mancini, Cognitive Modelling: a Basic Complement of Human Reliability Analysis, 9th SMiRT Post-Conference Seminar on Accident Sequence Modelling: Human Actions, System Response, Intelligent Decision Support.

18. J. Amesz et al., The European Reliability Data System: Main Developments and Use, ANS/ENS Int. Top. Meeting on Probabilistic Safety Methods and Applications, San Francisco (CA), February 1985.

19. A. Amendola, Uncertainties in Systems Reliability Modelling: Insight Gained through European Benchmark Exercises, Nucl. Eng. Des., 13 (1986) 215-225.

20. A. Amendola, Systems Reliability Benchmark Exercise, Final Report, CEC-JRC, Ispra, EUR 10696, 1985.

21. A. Poucet, A. Amendola and P.C. Cacciabue, Common Cause Failure Reliability Benchmark Exercise, Final Report, CEC-JRC, Ispra, EUR 11054 EN, 1987.

22. A. Poucet, Survey of Methods Used to Assess Human Reliability in the Human Factors Reliability Benchmark Exercise, 9th SMiRT Post-Conference on Accident Sequence Modelling, Human Actions, System Response, Intelligent Decision Support, München (FRG), August 24-25, 1987.

1.3. EMERGENCY PLANNING AND PREPAREDNESS

M. Hayns, G. Meggitt, W. Nixon
UKAEA, Safety and Reliability Directorate
Culcheth, Cheshire, United Kingdom

1. INTRODUCTION

The expressed goal of this workship is to design a research agenda for work related to safety issues and to the control and management of accidents. Therefore, this paper approaches the topic of emergency planning and preparedness by posing the question "what research needs can be identified to assist in both the planning of emergency response, and in its implementation". Thus, emergency planning and preparedness requires organisation of a wide range of services for rapid and co-ordinated response to a variety of emergency situations. There are problems at two levels:

i) anticipating the types of emergency and the challenges they pose for pre-planning purposes and

ii) ensuring that an adequate system exists for evaluating the actual emergency when it occurs to decide upon appropriate counter measures.

In its broadest interpretation, emergency planning and preparedness requires input from a very diverse range of expertise, these include, for example, firefighting and medical treatment of casualties, decontamination of people and places, operation of remote surveillance equipment and dose assessment. Much work is underway in these existing and identifiable areas of expertise - it is a real difficulty to bring it together with a co-ordinated programme on emergency planning but this is not addressed further here. In order to identify where research might be directed, it is useful to break the topic down into five headings. Each of these will be addressed in the presentation, but here are only very briefly mentioned. Further, many of the topics are directly related to nuclear emergencies. Rather than try to generalise, the nuclear application is used to provide the structure, but many of the topics covered will also be pertinent to other related hazards.

2. TRAINING

Whilst the training of nuclear plant operators has long been recognised as an important item, training for emergency response has usually be restricted to "practices" and "handbook" reading. We believe that there is a good case for the development of "simulator software" which would mimic telemetry and other input data. Noting that this type of simulator could absorb lots of resources, it is nevertheless considered that investment in the development

of cost effective systems is worthwhile; particularly if it is recognised that co-ordination of development has the potential to bring substantial returns.

3. MONITORING

The monitoring of releases and their consequences have been the subject of a great deal of work; instrumentation systems which telemeter results back to base stations for rapid assessment have been vigorously developed. Whilst a great deal of data may be generated by networks of such instruments, the collation and interpretation of that data has yet to receive equivalent attention.

4. DOSE PREDICTION AND INTERPRETATION

The interpretation of this data would be greatly assisted by improved computer based dose prediction systems. These employ models of the release of radioactivity, and its subsequent dispersion, either in the atmosphere, or aquasphere, and provide more or less complicated interactive facilities to cope with incoming telemetry data. A wide range of models have, or could be developed whose complexity shall be determined by their desired end use.

5. COMMUNICATIONS

One crucially important area which is common to many emergency and other management systems is that of communications. This involves not only the actual communication medium, but also the acquisition and presentation of the data. Other associated problems include optimising the location of emergency planners, the use of, say, satellite radiolocation finders for continual monitoring of emergency teams and the nature of the information links needed between all relevant personnel. There is no doubt that the electronic revolution offers the basic technology - what is needed now is the definition of detailed requirements to take best advantage of it, taking cost-benefit matters into consideration.

6. HUMAN FACTORS

Just like the plant itself, any emergency response depends to a greater or lesser extent upon the actions of human beings. Planning, may be subject to human error, but it is to be hoped that review and availability of time would make its intrusion acceptable. However, the highly stressed situation during an actual emergency could lead to errors and misinterpretation. Methods have been developed which can identify weak spots in operations, so far as human actions are concerned and it would be valuable to apply these to the emergency response case.

7. CONCLUSIONS

In this paper we have tried to steer clear of proposals which fall into "main stream" technical topics, even though they are highly pertinent to emergency planning and procedures. Our concern there would be to re-evaluate and focus such work for the benefit of emergency situations. Rather, we have concentrated on areas where attention to data processing, information management and communications could yield substantial benefits for relatively little cost, and which have not received a great deal of attention as yet. We believe that the wealth of information potentially available now could be made much more accessible and useful and could argue for cost effective research efforts in these areas.

1.4. RISK MANAGEMENT IN THE NETHERLANDS: A QUANTITATIVE APPROACH

C. J. van Kuijen
Ministry of Housing, Physical Planning and Environment
Directorate-General for Environmental Protection
The Netherlands

1. INTRODUCTION

For over 150 years The Netherlands has had legislation aimed at the prevention of nuisance and danger caused by industrial activities. After its most recent revision this legislation (The Nuisance Act) is an effective tool to regulate these activities. It contains a permitting system allowing the competent authorities - viz. the municipalities or the provinces - to decide whether a certain activity is acceptable at a certain place and which conditions should be attached to the permit in the interest of protecting the population and the environment. The application for and the draft of the permit are open to public inspection. The public can object to the draft both in writing and in public meetings. Moreover, a comparable legislation for physical planning offers possibilities to create and maintain sufficient distance between industries and the population.
However, these systems of legislation do not offer any explicit criterion for the judgement by the authorities or the public of the risks of the industrial activities. So, they are only tools for the implementation of a decision concerning risky activities, not a tool for the decision-making process itself.
The same holds for other risks that can endanger the population or the environment, as the presence of carcinogenic substances in the environment or the transport of dangerous substances.
This led the Dutch government to the formulation of a policy for risk management within the framework of an environmental policy. This policy has been approved by Parliament in 1985 (ref. 1).

2. ENVIRONMENTAL POLICY

The aim of an environmental policy is to define and to realize the environmental conditions to ensure a good environment. These conditions will often pertain to the Netherlands as a whole. Achieving and maintaining this general environmental quality is the most

important objective of environmental policy at the national level. In addition, specific conditions will be necessary in parts of the country in order to protect special living communities or species or forms of use to offer opportunities for development. Environmental policy must be directed at achieving and maintaining such a particular environmental quality as well.

In the light of these objectives, the required changes in the behaviour of diverse groups of producers and consumers can be established. These are the target groups of environmental policy. Depending on the target group in question, it will have to be determined what "mix" of regulatory, stimulatory and communicatory instruments is most effective in achieving the necessary change in behaviour. The choice regarding the package of measures will have to be made jointly by the environmental policy sector and other policy sectors of the government.
So, this "strategic" environmental policy is formulated and implemented along two tracks: an effect-oriented and a source-directed policy.

The effect-oriented policy must make clear which objectives are being pursued with respect to the quality of the environment and the tasks for target groups implied by these objectives. This will have to be based as much as possible on insights into the environmental conditions necessary to be able to manage risks for the environment on the one hand, and into possibilities for environmental renovation and their costs on the other.
The intended environmental quality will be formulated with the help of, often, quantitative descriptions of the required environmental conditions, such as, for example, the highest allowable concentrations of substances in water, soil and air, or the highest allowable exposure of organisms or goods to noise or radiation. Ultimately, the environmental quality will have to be such that the risks to the interests to be protected are negligible. This quality level is designated as the target value.
For most environmental conditions (concentrations of substances etc.) the target value can only be reached in the long term. In such a situation the target value has to be reached in several smaller steps, taken in an interim period. This will be done with the help of environmental quality objectives which can be realized in the short or

medium term and which reasonably guarantee that the risks will remain limited to on acceptable level. Such quality objectives are the result of a trade-off between what is desirable from an environmental view-point and what is technically, economically and otherwise (for example, from a land-use perspective) possible. The space which within this trade-off can take place (= the "grey area") is bounded on one side by the level at which the risk for people, animals, plants, goods and forms of use is maximally allowable and on the other side by the level at which the risk is negligibly small. This approach is presented in figure 1.

As a first step along this path both levels have been determined for people. Establishing the distinguished levels for other kinds of risks - for example, to plants, animals and goods - is an even more complicated task, especially because of the complex relationships (for example, in populations and living communities) and reactions (for example, photochemistry) that play a role. Nevertheless, it is expected that, with the help of research into eco-systems and ecological processes, more parts of the intended risk management system can gradually be filled in.

In additon to this effect-oriented policy, a source-oriented policy is necessary that makes clear the way and the tempo in which the behaviour of target groups will be "corrected", with attention paid to the environmental quality objectives and tasks formulated in the framework of the effect-oriented policy. Such a policy will have to establish priorities with respect to the measures to be instituted, in case a target group runs the risk of being confronted with a total of requirements that exceed its technical or economic possibilities. Knowledge about the circumstances under which the target group operates and about its motives and perspectives is indispensable in determining an adequate package of regulatory and stimulatory measures for target groups. Research and direct and indirect communication with the target groups will be of great importance. This two-track policy is presented schematically in figure 2.

3. DEALING WITH RISKS

Within this framework an external safety policy has been worked out. This policy is directed toward preventing unusual incidents with undesirable consequences for the surrounding area involving activities with dangerous substances and toward limiting those consequences as much as possible. Managing the so-called "smal probability-large consequence" risks requires special attention.

3.1. Risk and risk management

The concept risk connects that what we do with the undesired consequences thereof. Risk is defined as the chance of undesired events occurring in relation to the possible extent of the events' consequences for the population.

There are a number of sequential steps in the process of dealing with risks:

1. Identifying the dangers to people or the environment*
2. Estimating the extent of these dangers. Both the chance and extent of exposure as well as an agent's detrimental properties play a role in this.
3. Determining the acceptability of the risk of the activity and the desired risk reducing measures: risk assessment.
4. Control: maintaining a situation of acceptable risk.

Risk for people can be expressed in different ways.
Individual risk: the chance that a person spending 24 hours a day during a year on a certain spot will die as a consequence of incidents with the activity under consideration.
Group risk (or societal risk): The chance that accidents will occur which cause the death at the same time of more than a certain number of people. This concept is used especially in determining the risks from accidents of which the societal consequences can be sizable.

*"Risk to people" refers in this paper only to people living outside the industrial plant. For decision-making concerning the safety and health at work other procedures are in force, based on the Work Environment Act.

Application of the group risk concept makes it possible to take the size of the group of people who can be simultaneously victims of an undesired event better into account in the decision regarding risk acceptability. Recent accidents such as those in Bhopal and Mexico City illustrate the importance of this approach.

3.2. Risk identification

In the case of external safety the identification of the hazard is mostly rather obvious (for instance, fire or explosion or the release of toxic gases). For other risks, which have a less direct cause-effect relation, for instance the effects of long-term exposure to toxic substances, the identification requires much more study.

3.3. Risk estimation

In order to be able to evaluate risks against quantitatively formulated environmental conditions, quantification of these risks is required.

At this moment quantification of the risk of "disaster type" incidents is completely feasable. In this field the progress of science aided by the progress in data processing capability, has been remarkable. So, in 1982 my Ministry decided to initiate a project to develop a computerized risk quantification scheme using the most recent information available in the fields of the dispersion of heavy gases, unconfined vapour cloud explosions and fire ball radiation, and the response of man to exposure to large concentrations of toxic chemicals during a relatively short period. This computer model is now operational (ref. 2). It enables calculations to be made from basic data such as plant layout, population density data and meteorological data. These data are processed via effect and consequence calculations toward the final result: the individual risk curve and the group risk curve (or FN-curve).

The accuracy of this model has recently been systematically analysed (ref. 3). The inhaerent uncertainty in the modelling has been found to be a factor 3 and the uncertainty in the estimated frequencies about 10. Although this uncertainty is still large, the results of the model are considered to be reliable enough and close enough to observed effects and frequencies to be usable for decision making.

3.4. Risk Assessment

For this step in the decision-making process the two levels mentioned above (fig. 1) had to be determined with the two aims of external safety policy in mind, viz. the protection of the individual aqainst undue risks and the prevention of disasters in which many are killed at the same time.

The starting point for determining the maximum acceptable level for individual risk is the frequency per year of death from natural causes. This number is the lowest for children between 10 and 15 years old, viz. 10^{-4}. Recently my government has decided that a new location-specific industrial activity will not be allowed if it imposes an additional risk of more than 1 percent of this base value (see also ref. 4).

The maximum acceptable level for individual risk is thus 10^{-6}.

It seems reasonable to set the range in wich risk limitation can be required ("grey area") at two orders of magnitude. So, the negligible level for individual risk is 10^{-8}.

For the maximum acceptable group risk level a chance of 10^{-5} per year of an incident with maximum 10 deaths has been chosen.

A chance of 10^{-7} per year with 10 deaths is taken as negligibility level for group risk.

Further, a heavier weight must be assigned to the larger consequences of accidents. It has been decided in this connection that a consequence n times greater must correspond to a chance n^2 smaller, as it appears from literature that the seriousness of the societal consequences of an incident is judged to increase with the square of the number people killed.

These risk criteria are depicted in figure 3.

A differentiating policy is desirable for both individual and group risks falling within the grey area, to wit: risks from new industrial activities falling in this area are only acceptable after

- adequate risk reduction measures have been instituted or safer alternatives have been chosen, aimed at reaching the target value of 10^{-8} for individual risk;
- the permitting authority has weighed the risks and disadvantages of the activity involved against its benefits and is convinced that the relationship between risks and benefits is acceptable;

. the interests and perceptions of the population liable to the risk of the activity have been considered by the permitting authority in an balanced and responsible way.

Risk reducation can be achieved along two tracks. First of all in situ, by measures such as the layout of the plant, the application of additional safety devices and the use of a less hazardous activity. Secondly, by zoning. Often a combination of both types of reduction is wanted. Limiting the size of the zones by means of measures on the installation and maintaining sufficient distance to sensitive areas promote both prudent space use and the good "fitting in" of installations where activities with dangerous substances take place. One of the major advantages of risk quantification is, that it can provide information about the cost effectiveness of different sets of risk reducing measures, and that it provides a tool for zoning.

3.5. Risk control

When it has been decided what an acceptable level of risk is, decisions have to be made and implemented to safeguard this situation. Which specific measures have to be taken will depend on the type and scale of the activity involved.
Generally speaking the following actions will or may be required.

1. For stationary sources the license under the Nuisance Act will have to specify what safety provisions have to be taken and what procedures should be followed to test these safety devices.
2. The municipal authorities will have to achieve the implementation of the required zoning-measures and to maintain them.
   Where necessary distances between the installation and the population cannot be achieved, removal of vulnerable dwellings or the hazardous installations will have to be considered.
3. In case of risks associated with the transport of hazardous materials again action will be promoted either by improving the safety of the means of transport or by means of routing and zoning, or both.

4. APPLICATIONS

4.1. Implementation of the Post Seveso-Directive

Recently the concept of an administrative order has been published by

my government to implement this EEC-Directive on the major-accident hazards of certain industrial activities.
This new legislation will require the industries concerned to provide the competent authorities with a notification comprising a quantitative risk analysis. For the decision-making concerning new activities the approach mentioned above will be followed.
For existing activities, about which notification has to be presented at the latest on 8 July 1989, the further policy concerning measures to be taken, will be formulated after that date on the basis of the insight into the installations safety that will than be obtained from the notifications.
As far as the safety and health at work is concerned, the Directive is already imbodied in the Work Environment Act.

4.2. Natural gas pipelines

Over the years there has been a considerable argument about the distance that should be kept between natural gas lines and housing developments. In The Netherlands land use has to be as optimal as possible, so every meter counts. Yet the safety of the populations has to be quarded. It was to settle this dispute that is was decided to make a risk analysis of those lines, and size safety distances on the basis of the risk criteria put forward. It was concluded that the group risk criterion could not be applied for the very reason that the frequency of incidents grows with increasing length of the line, while on the other hand the people affected are different-ones along a line (and not the same-ones as in the case of a plant). It was therefore decided that the safety distances should be based on individual risk alone. The results of this analysis are in part depicted in figure 4. The solid lines represent the best estimate of the risk. The shaded areas represent the estimated 95% confidence interval.
As can be seen, at some instances the risk may be twice as high as the best estimate, but also may be zero. Yet parties involved felt sufficiently confident to accept the best estimate as the value to use in determining the size of the safety zônes. As a result, a directive concerning zoning along main transmission lines for natural gas has been published by my Minister in 1984 (ref. 6).

4.3. Liquefied petroleum gas (LPG)

The approach I have presented here was also adopted in the LPG policy.

In 1978 the large oil companies in the Netherlands expressed their expectation that the market for LPG as motorfuel and feedstock would see a spectular growth. Within a few years import and transport were expected to grow from 1 million tons a year to 10 million tons a year. And these transports would pass trough densely populated areas and cities. The safety of these activities was a subject of general concern for the public and the authorities.
The Dutch government commissioned a study to examine the safety of all parts of the chain of activities from the importation in the sea harbors to the distributions at gas-stations selling LPG (ref.7).
The results of these studies formed the basis for the policy statement of the government to Parliament in 1984 (ref.7).
In this "LPG-nota" the risk contours are translated into safety distances to be applied to unloading facilities, depots and storage tanks, and measures are presented to increase the safety of barges and roadtankers.
Because of the difference in risk that was calculated between stations situated within city limits and those at the side of highways at sufficient distance from houses, it was decided that the opening of new stations selling LPG will only be allowed outside city limits, at a minimum distance of 80 meters from the nearest houses. Existing stations which are located within 15 m distance from dwellings will be closed.
For the other existing stations located at larger distances (up to 120 m from dwellings) a program of risk preventing measures will be executed. The costs of this (about 125 million guilders) will be beared by the LPG selling companies.
Another example is the comparison of the transportation in barges and other means of transportation. From this comparison it was concluded that transport by barges can be allowed, provided that some constructive changes will be realised. Legislation concerning these changes is in preparation.

4.4. DSM (Dutch State Mines)

This is a large industrial facility in the south east of The Netherlands. Within the framework of a study concerning integral zoning around DSM, a risk analysis has been made. The resulting risk contours facilitated the decision about the expansion of existing dwelling facilities and the erection of new ones (fig. 5).

4.5. Transport of dangerous substances

Recently in the Rijnmond area the risks of the transport of chlorine and ammonia have been tackled.
From the results, the iso-risk contours and F-N curves for the various routes and modes can be examined.

5. PLANS FOR THE FUTURE

The development of these computer assisted methods has also been a starting point for more advanced developments. My Ministry is presently engaged in a collaborative exercise with the Joint Research Centre of the EEC and IIASA, to develop a decision support system. This system will allow to combine data on the risks of different modes of import, production, storage, transport and use, with data on economics etc. to help the decision maker to seek an optimal solution for complicated problems.
Other lines of developments are groundwater transportation models, long term atmospheric models and the effects of incidents with nuclear installations.

It may be remarked that the methods described above are aimed at dealing with risk problems only, not with problems connected with the perception of risk or with different views on the further development of our society. The nuclear power problem is an example of such a still more complicated issue.
In these sort of problems it is tempting to devote all efforts to solve the risk issue only, to find out later that solving the risk issue did not solve the problem.

6. CONCLUSION

In this adress I have presented the framework of our approach toward the problem of risk management. I have to admit that this approach is not unchallenged. In particular from the side of industry much scepticism regarding the usefullness of quantitative risk assessment in decisionmaking is made known.
Firstly, it is being argued that the data needed for quantitative risk-analyses in many cases are too scattered to justify a casuistic

approach. We agree that the data-base needs further improvement. This will be one of our main objectives for the near future. On the other hand there remains the fact that decisions have to be made about the acceptability of risk, often in relation to very complex situations. In our opinion such decisions will have a more solid basis in case a quantitative risk-analysis is disposable, how inperfect our data may be, than in case when such decisions are taken on the basis of qualitative assessment only. Of course the decisionmaker should be aware of the uncertainties involved and accomodate these uncertainties in his final-decision. To quote my former Minister Pieter Winsemius: "There is no substitute for thinking".

Secondly, quite a number of people in industry fear that the use of quantitative risk data may jeopardize the willingness of the public to accept additional hazards, even if the risk involved is very marginal. On this point we don't agree. Of course, we also do recognize the fact that the public attitude is determined by risk-aversion, especially where non-voluntary risks are involved. However it is just for this reason that we prefer a normative approach. In the view of my government it is only by means of politically established standards that endless disputes about the acceptability of a specific type of hazard can be avoided. We are sure that ultimately industry will recognize that this is to his interest too.

REFERENCES

1. Indicatief Meerjaren Programma Milieuhygiëne 1986 - 1991, Tweede Kamer, 1985 - 1986, nr. 19204, 1 en 2 (Also available in an English and French version).

2. Reports on the Safeti Package, Technica, London, 1982 - 1985.

3. De onzekerheid van effectberekeningen in risico-studies, AVIV, Enschede 1986.

4. Kuhlman, A (1981): Einführung in die Sicherheits Wissenschaft. Verlag TUV Rheinland, Friedr. Vieweg & Sohn.

5. Risico-analyse van ondergrondse buisleidingen, TNO, 1983.

6. Circulaire van de Minister van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer inzake zonering langs hogedruk aardgastransportleidingen, nov. 1984.

7. LPG Integraal, TNO, 1983 (Also available in an English version).

8. Integrale Nota LPG, Tweede Kamer, 1983 - 1984, nr. 18233, 1 en 2.

Dealing with risks in environmental policy

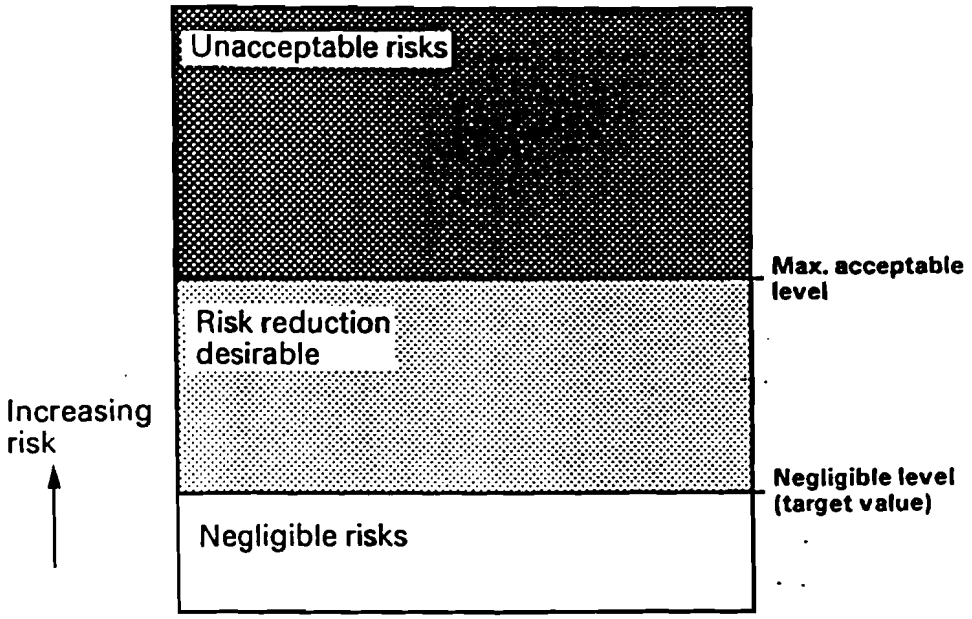


FIGURE 1

Two track policy

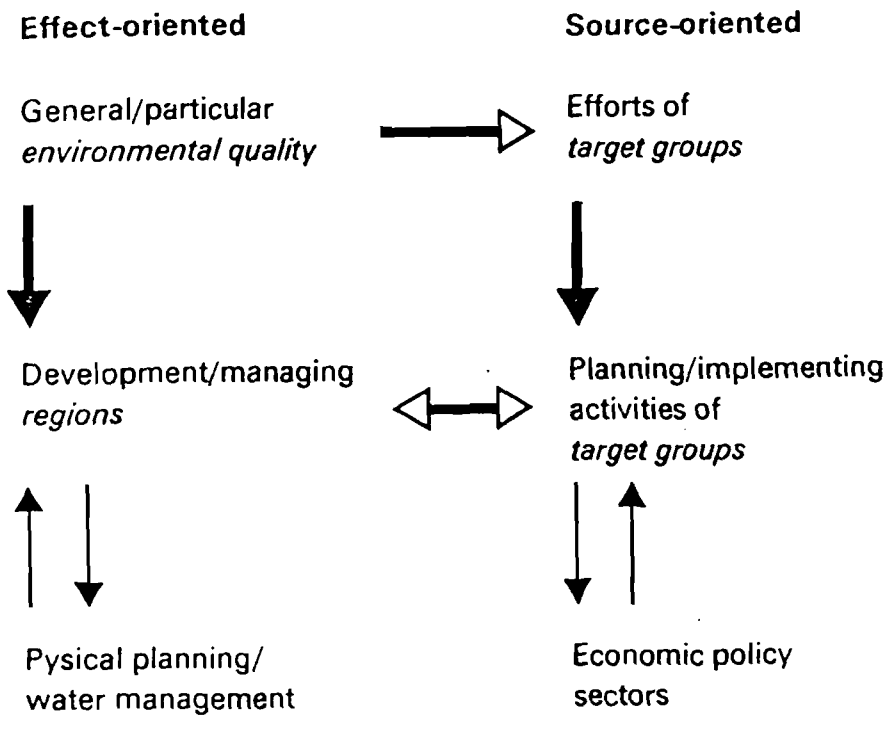
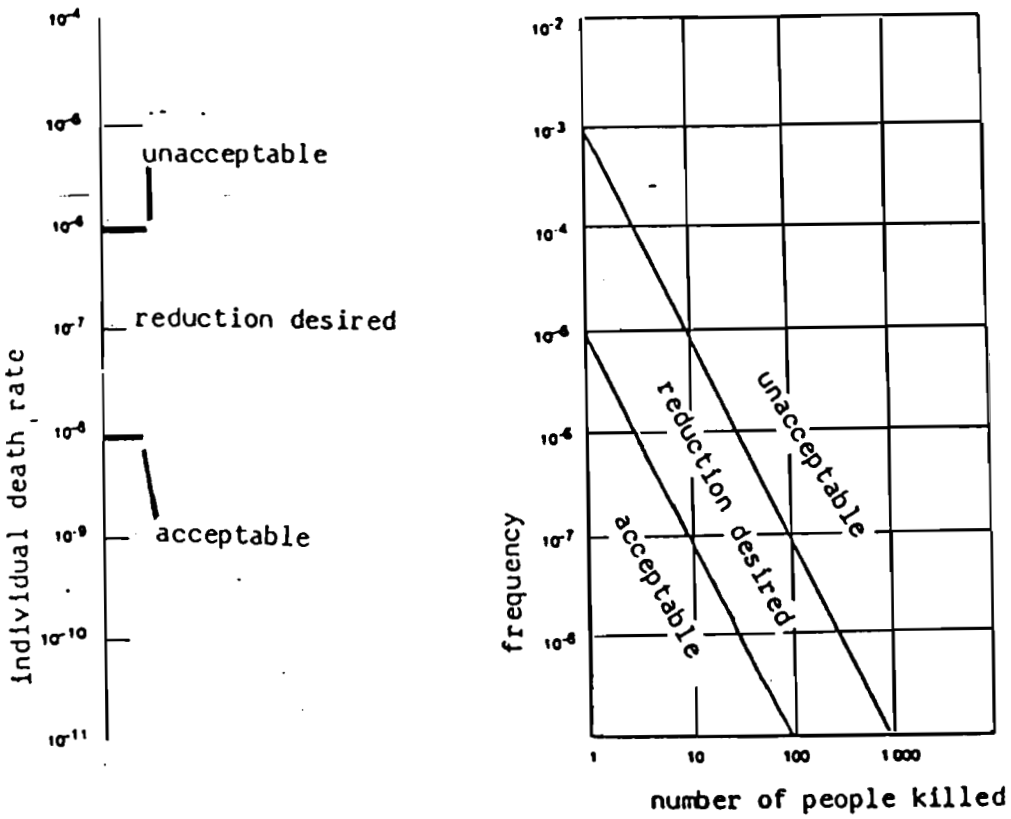


FIGURE 2

RISK CRITERIA FOR THE POLICY ON EXTERNAL SAFETY IN THE NETHERLANDS



INDIVIDUAL RISK GROUP RISK

FIGURE 3

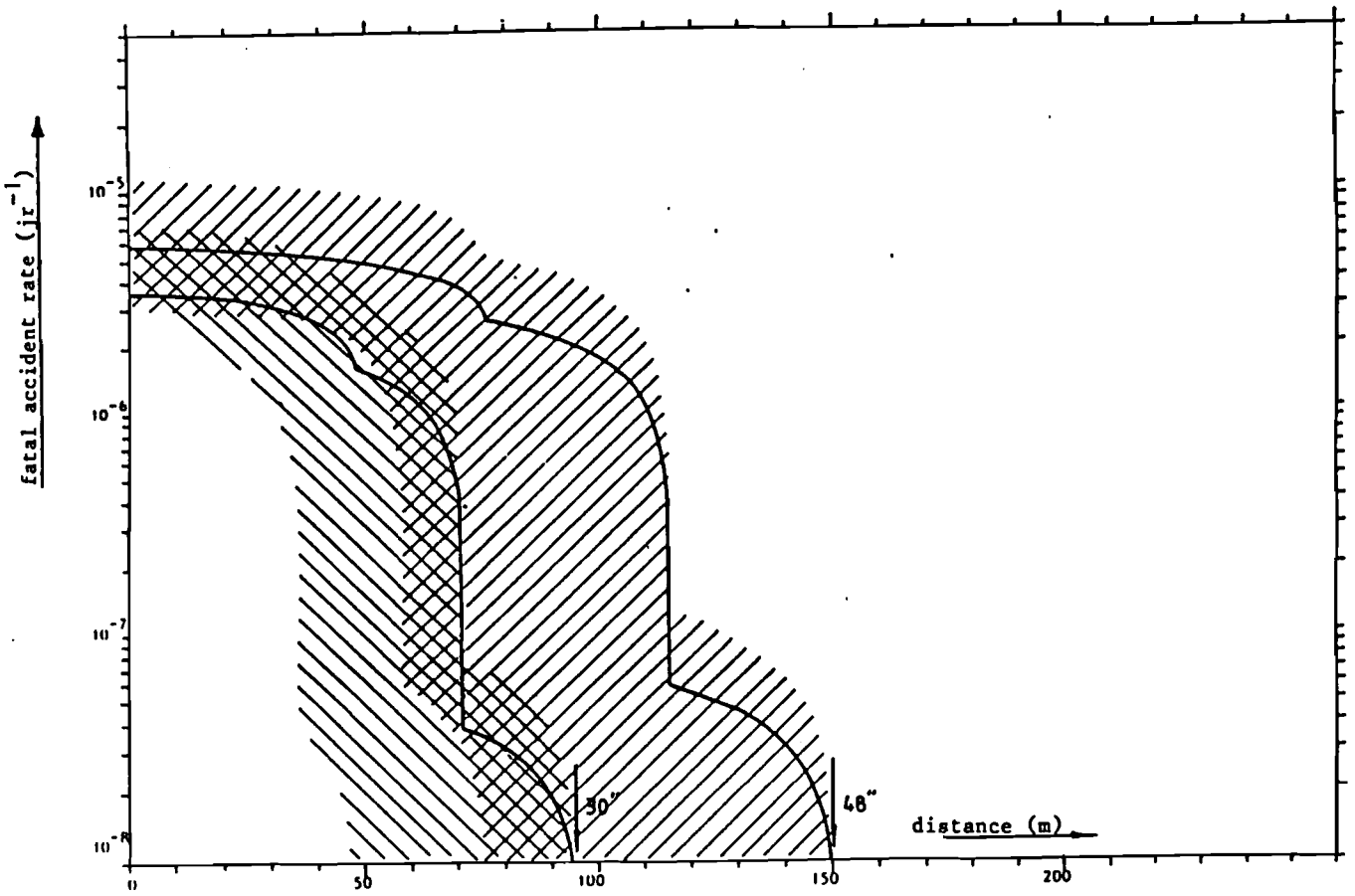


Figure 4: Fatal accident rate as a function of distance from a main transmission line for natural gas (pipe sizes in inches). The hatching gives a rough indication of the area of uncertainty.

RISK CONTOUR PLOT FOR THE WHOLE SITE OF DSM FIGURE 5

1.5. WAYS TO IMPROVE NUCLEAR POWER SAFETY: USSR POINT OF VIEW

V. Demin, I. Kuzmin, and V. Legasov
Institute of Atomic Energy,
Moscow, USSR

In the current century, the development of industrial power in the USSR as in many other industrially developed countries took place with a notable increase of oil, gas condensate and gas share, and a relative decrease in the share of coal. For example, oil and gas share in the national energy balance in 1961-1980 exceeded 80%. The USSR organic fuel reserves are the largest in the world. The USSR natural gas reserves are the largest; more than half of the known world coal resources are in the Soviet Union. The USSR takes the first place in oil production (including gas condensate) and the second place in coal production in the world. Thus, the USSR power development is secured by national natural resources for a long-term period. Moreover, oil and gas are exported to Eastern and Western Europe. Nevertheless, we are confronted with the necessity of changing the structure of the USSR fuel and energy balance to decrease the share of organic fuel. The necessary changes are caused not by resource depletion, but by the ever increasing geographic disproportion in fuel production and consumption locations.

A major factor determining the prospects of USSR power development is a continuous transition of its raw materials base into Eastern regions of the country. The organic fuel reserves located close to consumers in the European part of the country are being depleted. Most of the organic fuel reserves are situated in the Asian part of the country, but 80% of their consumption takes place in the European part. As a result, the average fuel transportation distance is constantly increasing. For example, the gas transportation distance increased from 530 km in 1956-1960 to 2400 km in 1981-1988, and will further increase in future. The gas main length reaches 150,000 km, and the total capacity of gas pumps at compressor stations is 23 GW. About 40% of the Soviet railway freight turnover is due to the transportation of fuel (mainly coal) from Eastern regions to the European part and to the Urals. It should be noted that to use new resources of organic fuel, it is necessary to develop vast remote areas with severe climatic and complex geological conditions. As a result, the specific cost of organic fuel production increase in the 1980's will be on average three times higher than a decade ago. For oil, the cost will be still higher.

Thus, the remoteness of organic fuel deposits from energy consumers in the USSR, large capital investments, long lead time, and large labor requirements will limit the prospects of this energy source.

Nuclear power opens a way to a practically inexhaustible energy source that is not connected with a geographical region of fuel extraction. Its large-scale introduction into the national fuel and energy balance enables large economic savings and considerable reduction of disproportions in increased fuel production and fuel consumption.

The energy program of the USSR provides for an accelerated development of nuclear power. In order to have a better national fuel and energy balance, it is planned to increase at least 5 times the electricity production at nuclear power plants by the end of the century. Electricity production increases in the European part and partially in the Urals will be provided mainly by nuclear power plants alone. As a rule, it is planned to build large nuclear power plants with the electrical power of several GW(e).

The serious accident at the Chernobyl nuclear power plant that occurred on April 26, 1986, has made us once more critically review both our plans of nuclear power development and measures to ensure its safety.

I will not go into details of causes and consequences of the accident; detailed information in all its aspects was presented by Soviet specialists at the special IAEA expert meeting in Vienna and other international conferences and discussed by international specialists and the general public.

Naturally, the Soviet Union studied very carefully the lessons of Chernobyl. We have drawn the following main conclusions:

1. The reasons that caused the accident are primarily related to mistakes of nuclear power plant personnel and violations of the plant operating regulations. These reasons are not specific for a nuclear facility, and therefore they cannot be considered fatal for nuclear power development.

2. The accident analysis did not identify any physical phenomenon which had not been previously studied within safety analysis either theoretically or experimentally. The analysis showed that the safety of nuclear power facilities of all types could be further improved by well-known physical and technical methods and a more accurate account of the human factor.

3. The analysis of the Chernobyl accident showed that, though its consequences are rather large from the point of view of both the number of fatalities and the economic damage, these consequences are comparable with other analyzed large industrial and transportation catastrophes.

4. If nuclear energy sources are replaced by traditional ones, the risk to human health and environment will increase by an order of magnitude if we do not consider radio-chemical

reprocessing of spent fuel, and it will be several times higher still if we include the risk of the whole nuclear fuel cycle.

5. The motives that forced the Soviet Union to develop nuclear power have not disappeared; on the contrary, they will manifest themselves even more strongly in future. The necessary modernization of industrial plants in the European part of the country requires increased electricity generation, naturally along with its more efficient use. Town development in our Northern climatic zone is impossible without nuclear-based electricity and heat generation; otherwise, we will be unable to solve ecological and transportation problems.

Thus, the analysis of our attitude to nuclear power after the Chernobyl accident does not lead to any changes in our principle position. We remain convinced of the necessity of its development for the benefit of the economy of the USSR and of the world as a whole. Our plans for nuclear power plant introduction did not change.

However, the Chernobyl accident as well as other nuclear power plant accidents in many countries demonstrate that nuclear power safety problems have not been fully solved. The lessons of these accidents for us and for the world community are that safety and reliability of new complex technology as a result of scientific and technological revolution requires a very careful attitude and that the technology does not forgive negligence.

After the Chernobyl accident, the Soviet Union realized a number of measures of organizational and technical nature aimed at a substantial increase in nuclear power safety.

First priority technical measures were developed and implemented to exclude the possibility of a Chernobyl-like accident reoccurring at RBMK-type reactors.

Based on the accident analysis, a complex set of measures was developed to improve the safety of nuclear power plants of all types. This includes implementing measures that have been developed earlier as well as ones developed as a result of recent advances in science and technology; accumulated operational experience, for example, to improve the diagnostics of tube and equipment metal state, and to use more widely automatic control devices in technological processes. A critical analysis of nuclear power plant siting problems is underway.

Calculations and experimental results on nuclear power safety were revised and assessed; measures were developed for their improvement and more comprehensive application.

Computer programs for nuclear power plant safety analysis have been updated for all possible transients and accidental

conditions, including hypothetical accidents; simulating systems and components are under development.

Studies have been intensified on the feasibility of a reactor with passive safety systems -- the so-called inherently safe reactor, the core of which cannot disrupt in any accident.

More efforts ill be directed towards quantitative probabilistic safety analysis, nuclear power risk analysis, development of a conceptual and methodological base for radiation safety optimization and comparison of radiation danger with other dangers in industrial activities.

The existing Soviet regulatory system covers all main aspects of ensuring nuclear power plant safety and continues to be improved. In 1985, under the auspices of the State Committee on Supervision of Safety in Nuclear Power, a combined list and plan of regulations development in nuclear power was created, which coordinates and directs all ministries in developing and systematizing relative scientific and technological documentation.

The existing safety regulations basically do not require revision. However, their practical implementation should be monitored more carefully. It is necessary to improve the quality of personnel training and retraining, to strengthen the designer verification activities of equipment quality, assembly, and start-up operations and their responsibility for subsequent efficient and safe operation of nuclear power plants.

In order to improve the administration and responsibility for nuclear power development and for plant operation, an All-Union Ministry of Atomic Energy has been established.

A number of measures have been taken to strengthen the state supervision of safety in nuclear power as well as the responsibility of personnel for the quality of nuclear power plant operation.

One of the critical problems in nuclear power as in other modern technologies is the optimization of man-machine interactions. The task of improving the personnel skills and training techniques is closely related to the task of developing more easily controlled reactors and ensuring optimum working conditions for operators.

In the process of mitigation and elimination of consequences of the Chernobyl accident, Soviet specialists and authorities are confronted with many particular scientific, technical and organizational problems. We have learned lessons from Chernobyl. This experience is very important from the point of view of decision-making regarding nuclear power safety. We are ready to share the experience with the international community. We are sure it will be useful, particularly in the area of nuclear power plant de-commissioning.

At present, the activities to eliminate the consequences of the Chernobyl accident have been almost finished.

The accident unit has been encased. Its encasement is a unique engineering structure with all the necessary equipment, diagnostic and monitoring devices. About 300,000 m^3 of concrete and over 6000 tons of metal structures were used during its construction.

The plant territory has been decontaminated. The radiation situation has been normalized.

The units No. 1 and No. 2 of the Chernobyl nuclear power plant have been put into operation.

The population has been provided with continuous medical supervision. Medical examination of all persons in the contaminated zone showed no new cases of disease, and there is now no danger of radiation sickness for anyone.

The country provided significant material assistance to the population; compensation for the damage is being paid. The total amount of money for this purpose is about 800 million rubles. Moreover, much money has been invested in the construction of homes and social and cultural facilities.

We continue to believe that a wide introduction of nuclear power into the world economy may have a stabilizing effect on international economic and political relations due to a sufficiency of its required raw material base and the possibility in principle to reach a high level of safety and ecological cleanliness.

However, besides the benefits in the area of energy generation and natural resources preservation, the world nuclear power development is accompanied by dangers of international character. These include trans-boundary radioactivity transport, in particular, as a result of large radiation accidents, the problem of nuclear weapons proliferation, the danger of international terrorism, and the specific danger of nuclear facilities during military conflicts. All these factors necessitate deep international cooperation in developing nuclear power and ensuring its safety.

The establishment of an international regime for the safe development of nuclear power, proposed by the Soviet Union at the special session of the IAEA General Conference in September 1986, will contribute to deepening international cooperation in peaceful uses of atomic energy and to making it more systematic. The proposed program provides to establishing material, scientific and technical bases for nuclear power safety development, accompanied by international legal norms and agreements. We are convinced that the realization of our proposals will contribute to achieving the common goal of the international community -- to

exclude the possibility of peaceful atomic energy doing harm to anyone.

We are satisfied to note that an essential part of the system of an international regime for the safe development of nuclear power is already operating.

It includes, for example, international conventions on early notification of a nuclear accident and on assistance in case of a nuclear accident or radiological emergency that have recently come into force.

The experience of the draft conventions development within a limited time shows that with good will complicated problems of international cooperation can be solved quickly and effectively. It is necessary to make every effort for the early implementation of other elements of the international regime for the safe development of nuclear power.

An important element of the system should be the creation of an international data bank on radiation background levels in some agreed upon geographic points. These data could be used for the purpose of comparison.

It is necessary to agree internationally on standards of emergency radionuclide concentrations and on land radioactive contamination levels. Such international norms and standards could be used by all countries to take protective measures and to justify claims relative to damages as a result of trans-boundary radioactivity release.

Another component of the regime could be an agreement that while developing, designing, constructing and operating nuclear power plants and other nuclear facilities, all countries shall follow IAEA recommendations, containing a minimum set of principle requirements for the safety of nuclear facilities. To give practical assistance in safety assessment and improvement, the IAEA could intensify its activities by sending to member-states at their request groups of highly qualified experts in nuclear safety.

An important element in the system of measures aimed at accident prevention is the collection, processing and exchange of information on nuclear power plant accidents, their causes, sequences, and consequences. The IAEA information system on incidents at nuclear power plants forms a good basis for a data bank on nuclear accidents. It is necessary to further widen and improve this system.

We should cast a new look at the safety of nuclear power based on present reactors and find ways to improve both the nuclear reactors themselves and all stages of the nuclear fuel cycle. This necessity was summarized by M. Gorbachev, Secretary-General of the Central Committee of CPSU, in his proposal on

international cooperation in the development of a new generation nuclear reactor.

What is the conceptual basis of the reactor?

It is now impossible to present a specific reactor design which will satisfy all the requirements of a "completely safe reactor," though some work in this area has already been done by different research teams in our country and abroad. Active international cooperation at this stage can largely contribute to these studies.

The following principles for such studies can be formulated:

1. The studies should deal not only with reactor design, but with its fuel cycle. Otherwise, the "total" safety of the system might not increase; on the contrary, it could decrease. For example, should a safe reactor require an increased volume of fuel reprocessing and refabrication, its transportation could create large quantities of radioactive wastes.

2. The reactor system to be developed should ensure an effective nuclear fuel utilization, i.e. its fuel cycle should meet modern requirements on uranium reserves.

3. The economic aspects of the nuclear power system should not be worse than those of coal power. Economic comparisons should be carried out taking into account the costs of general and ecological safety.

As far as the safety criteria of the reactor itself are concerned, the following aspects could be underlined even now:

a) minimum burn-up reactivity margin;
b) optimum of all reactivity effects;
c) rejection or limited use of chemically active materials, exclusion of the possibility of exo-thermal reactions;
d) wide use of passive safety features such as natural convection in all circuits, external cooling-down of vessels, etc.

Naturally, the list is not complete; it may be supplemented by joint efforts of specialists from all over the world.

Taking into account the concerns of the general public about the consequences of nuclear power development and the experience obtained as a result of analyzing the consequences of nuclear power plant accidents over the last years, work on developing the new generation reactor should be accelerated.

The Chernobyl accident as well as other accidents with radioactivity releases demonstrated once more the dangerous consequences of a possible intentional destruction of nuclear facilities. In this connection, the Soviet Union proposes to develop a reli-

able system of measures to prevent attacks on nuclear facilities. It is necessary to finalize an appropriate international convention according to which all states will undertake not to attack nuclear facilities.

A reliable system of measures should be developed against all forms of nuclear terrorism. Radiation danger and high toxicity of nuclear materials require their reliable protection against criminal encroachment. The possibility of utilizing stolen nuclear materials to create a simple nuclear explosive device with an aim to subversive and terrorist acts cannot be excluded. We are ready both to reach a separate agreement and to solve this problem within the framework of a general struggle against international terrorism.

We believe the delay in ratifying the convention on physical protection of nuclear material is unjustified. It is necessary to make additional efforts for early entry into force of this important convention. The Soviet Union was one of the first to sign and ratify the convention. We call other states to do the same in the near future in order that the convention can begin to act as one of the factors to ensure nuclear safety.

The problem of liability for nuclear damage should not be neglected. Despite efforts aimed at international legal regulation in this area, up to now the problem of material and moral-political damage in case of accidents at nuclear facilities has not been sufficiently resolved; this leads sometimes to attempts to use nuclear accidents to create tension and distrust in relations between states. A possible multi-lateral international legal document could provide for the liability of states both for the damage as a result of trans-boundary nuclear accident consequences and for inflicting moral and political damage as a result of unjustified actions carried out under the pretext of protection against nuclear accident consequences (distribution of unconscientious information, introduction of unjustified limitations, etc.).

In establishing the regime for the safe development of nuclear power, the leading and central role should undoubtedly by played by such an organization as the IAEA. It is necessary to use its experience in nuclear safety activities more widely, to increase its role and capabilities.

As essential contribution to establishing such a regime could be made by other UN specialized agencies and naturally such organization as the Council of Europe.

The following coordinated studies and exchange of experiences in different areas of ensuring nuclear power development should be carried out with the active participation of states and international organizations:

* development of methods for accident prevention and elimination of their consequences;

* analysis of events initiating accidents and the development of emergency situations, including probabilistic analysis;

* development of robots, machines and equipment to be used to eliminate nuclear accident consequences;

* creation of effective decontamination techniques, machines and devices for this purpose, reliable means for protecting people from radiation;

* development of medical preparations, means and methods to cure radiation sickness;

* development of a methodology for training personnel operating nuclear power plants.

It should be remembered, however, that in our interdependent world besides the problems of the peaceful atom, there are the problems of the military atom. Nuclear safety on our planet is unthinkable without stopping the material preparation of nuclear war and completely eliminating warfare means.

The Soviet Union will continue to do everything possible to implement the proposed program of complete and comprehensive eliminate of nuclear weapons. The twentieth century should end under the sign of nuclear disarmament and with the creation of a reliable basis for a safe world in which safe and reliable nuclear power will play an increasing role in satisfying the energy needs of mankind.

1.6. INDUSTRIALIZATION, INFRASTRUCTURE, RISK MANAGEMENT: THE CASE OF THE CUBATAO AREA IN BRAZIL

C. Costa-Ribeiro
Centro de Tecnologia Promon - CTP
Rio de Janeiro, Brazil

L. A. Mello-Awazu
Companhia de Technologia de Saneamento Básico - CETESB
São Paulo, Brazil

1. INTRODUCTION

The selection of Cubatão, in the early 50's, as the site for building an industrial district was due mainly to its favorable geographic location near a bay and close (50km) to the São Paulo Metropolitan Area with its present population of 10 000 000 people. Old and new infrastructures like roads linking the coast to the highlands where the city of São Paulo is located, a residual estuarine formation which allowed the construction of a port to serve the new industrial facilities and the availability of abundant and cheap hydroelectric power and fresh water were the main parameters considered in the selection of that site to house the first modern industrial complex in the recent history of the country.

Following the investments made by the Federal Government through its major state owned companies, other industries both national and multinational were attracted to Cubatão as well as workers seeking job opportunities.

Today, Cubatão has over 23 industrial complexes with 110 units for production of chemicals, petrochemicals, fertilizers and steel products clustered in an area of less than 20 km^2 with a

population of 100 000 people living between chimneys, polluted streams and zones subjected to periodical tidal flooding. The area is a narrow strip of land lying between the foothills of the Brazilian coastal ranges covered by tropical forests and the ocean. Industries, urban, commercial and administrative facilities as well as residential areas and illegal squatters settlements are jammed in this strip of land.

Apart from the unsuitability of the microregion of Cubatão to house all its present industrial plants, particularly with respect to the adverse meteorological conditions prevailing there, the enforcement of pollution control legislation was not duly considered when most of these units were erected. Furthermore, none of the major plants operating there incorporated in their design stage the necessary equipment for pollution abatement and other risk prevention measures. As a consequence, risk to human health, to the environment and to property reached unacceptable levels in Cubatão.

2.
MAJOR RISKS AT SITE LEVEL

In the late 60's air pollution levels in Cubatão where already well above those set up by the World Health Organization - WHO. Brazilian pollution control legislation which followed WHO standards went into effect only in the 70's when systematic measurements of air pollutants began. Fluorides, ammonia, sulfur dioxide, nitrogen oxides and particulates were identified as the main air pollutants in Cubatão.

The combination of a weak wind dispersion pattern due to the unfavorable topographic conditions in the Cubatão area, high levels of atmospheric contamination and heavy rainfall promoted a continuous and massive fallout of phitotoxic pollutants, such as fluorides, on the steep scarps of the coastal range around Cubatão, causing disruption of the fragile subtropical ecosystem

prevailing there. Thus, scattered destruction of the vegetation cover totalized, in the early 80's, an area of 60km^2 of dammaged forest. That fact, combined again with the local heavy rainfall put at risk extensive areas down at the foothills of the mountains where a network of pipelines, petrochemical and chemical storage tanks and industrial units are located, due mainly to the risks of land and mudslides and flooding.

Figure 1 shows a map of the Cubatão area with the main watersheds formed by creeks comming down the mountains encircling the area. These watersheds, numbered in the map as sectors, have been individually investigated to assess their potential risks for mud and landslide with disastrous consequences to the industrial facilities located down at the foothills of the mountains.

Figure 2 exemplifies the extension of damage to the vegetation in one of the watersheds. The uncovered soil of this old geologic formation became a potential risk for sudden and uncontrolled mud and landslides.

The interdependence among several of the 110 industrial units which form the Cubatão complex, relaying on the supply either of chemicals, water, energy or byproducts produced by other units on the site increased the risks for some of them in the event of a sudden and partial shutdown of a particular unit compromising the safe operation of a downstream plant.

Furthermore several of the existing large storage tanks of toxic compounds like ammonia and chlorine scattered in and around the facilities add to the overal risk for major accidents.

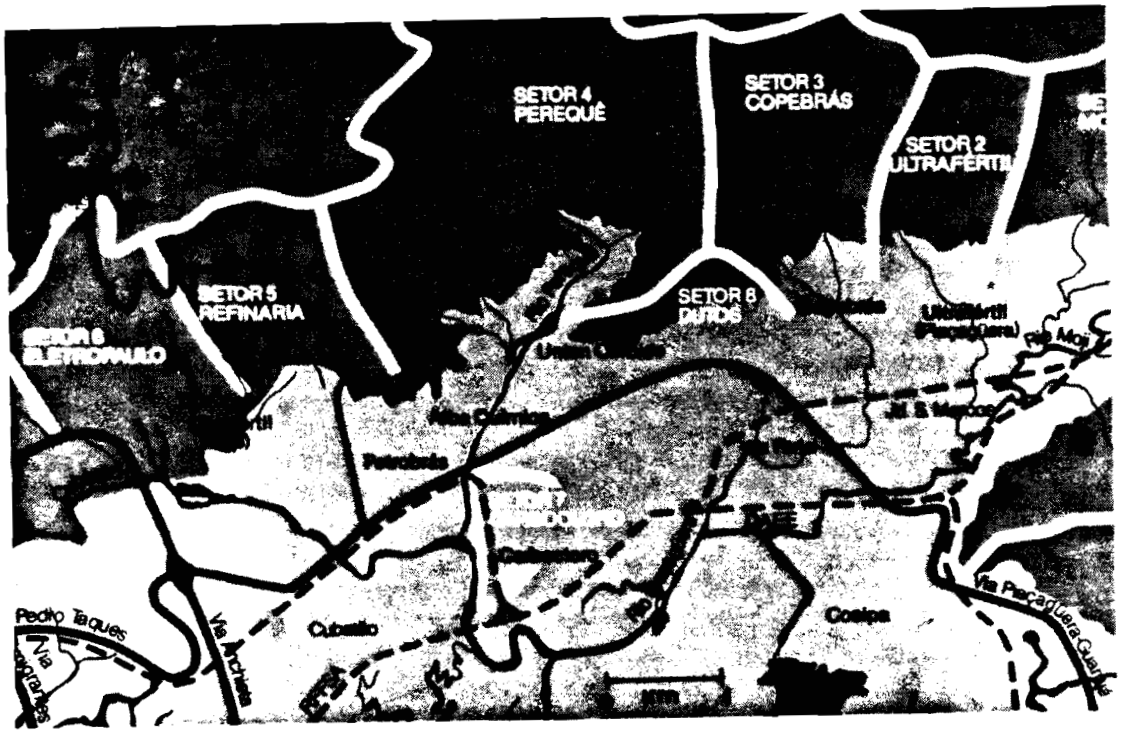


FIGURE 1
THE CUBATÃO AREA SHOWING MAIN WATERSHEDS DIVIDED BY SECTORS.

FIGURE 2
THE SCARPS OF THE MOUNTAIN RANGE AROUND CUBATÃO SHOWING THE AREAS WHERE DAMMAGED VEGETATION BY PHITOTOXIC FALLOUT IS NOW SUBJECTED TO LAND AND MUDSLIDES.
REF.: (2)

3.
EMERGENCY RISK MANAGEMENT PLAN

To cope with all those potential risks to human health, to the environment and to property (Cubatão contributes with 2,5% of the Gross National Product of Brazil which is presently at US$ 290 billions) the government of the State of São Paulo through its environmental control agency (CETESB), launched, in 1983, a crash risk management emergency plan based, among others, on the following key points:

- air pollution emissions reduction program at plant level;
- special program for building dams along the main drainages of the local watersheds to hold mud and other debris from landslides; dredging of brooks down at the valley to reduce the flooding risks near each industrial plant;
- recover the affected forest through a long range reforestation program to minimize the intensity of landslides;
- strengh local Civil Defense bodies through installation of modern communication systems and a network of automatic meteorological and hydrological stations to monitor rainfall levels in each sector and waterflows in every major brook.

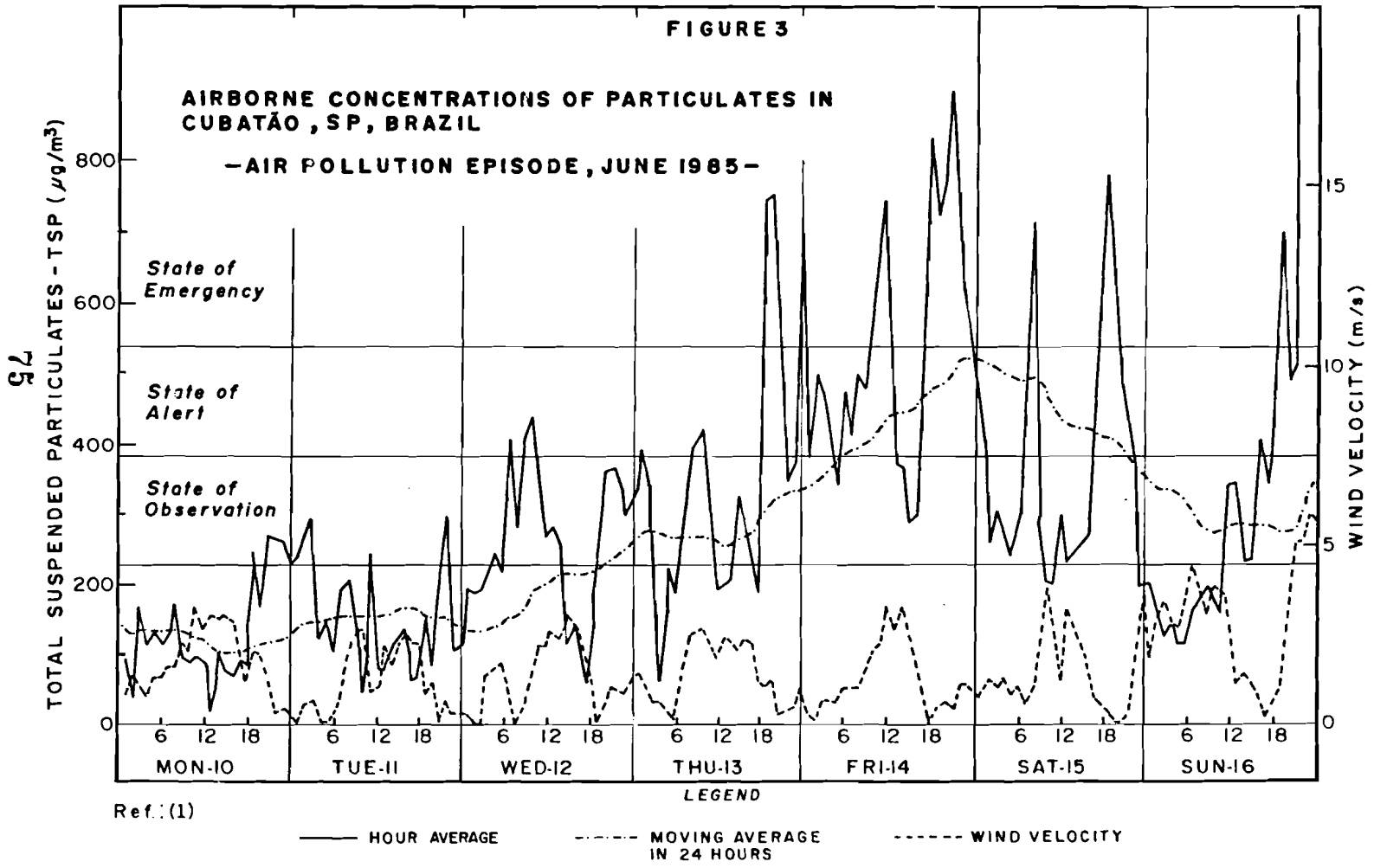
3.1
Air Pollution Abatement Program

Due to the unfavorable dispersion conditions prevailing in Cubatão there is a high probability of occurrance of critical episodes of air pollution particularly in winter time. Anticyclones associated to natural thermal inversions make it difficult for pollutants to disperse Figure 3 shows the recording of a typical air pollution episode which took place in June 1985 (1).

FIGURE 3

AIRBORNE CONCENTRATIONS OF PARTICULATES IN CUBATÃO, SP, BRAZIL

–AIR POLLUTION EPISODE, JUNE 1985–



Ref.: (1)

The air pollution abatement program set forth by CETESB established that each plant should take the responsability for preparing its own emission control plan based on the following items:

- adoption of the best practical technology;
- observance of pollutant emission standards;
- submission to CETESB of a schedule with implementation deadlines;
- respond with its own capital resources to the needs for implementing the control systems.

After individual control plans were approved goals have been set up for emissions reduction. Figures 4 through 8 present the results of the emissions reduction schedules for fluorides, ammonia, sulfur oxides, nitrogen oxides and total particulates for the entire area of Cubatão.

Table 1 shows the frequency of air pollution episodes which ocurred in Cubatão during the 1984/86 period. The data on Table 1 indicate the positive results of the program reflected in the reduction in the frequency of such episodes.

Table 2 presents the standards adopted by CETESB for classification of the severity of each episode.

3.2
Land and Mudslide Control Program

Recognizing the impossibility of quickly reverting the critical situation created by the long term effects of the phitotoxic fallout of pollutants on the vegetation cover of the mountains scarps,CETESB initiated plans for construction of mud holding dams along the main drainages of the mountain range. The capital

FIGURE 4

EMISSIONS REDUCTION SCHEDULE: FLUORIDES

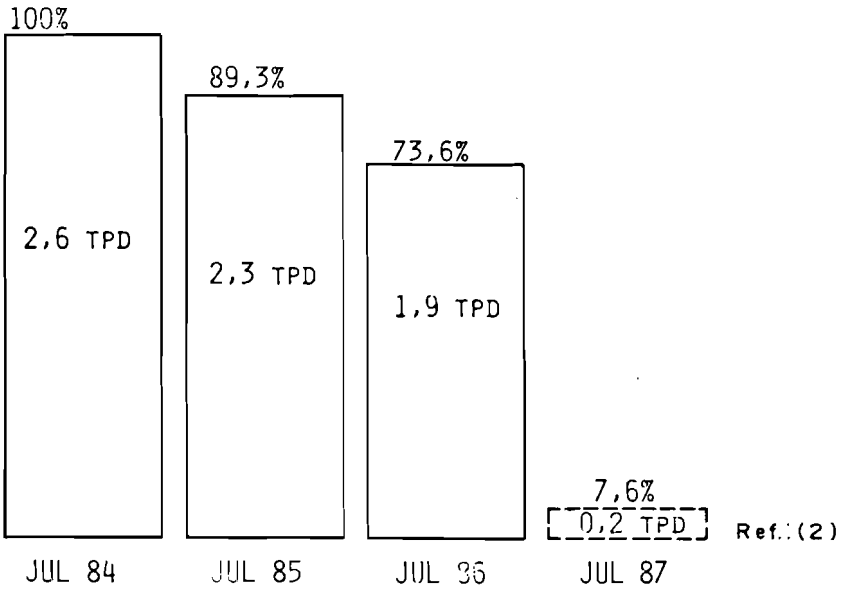


FIGURE 5

EMISSIONS REDUCTION SCHEDULE: AMMONIA

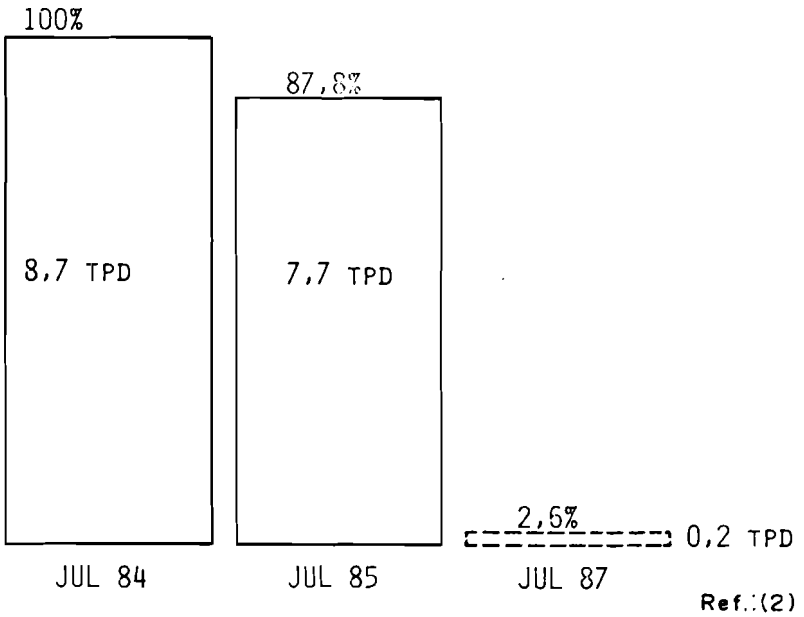


FIGURE 6

EMISSIONS REDUCTION SCHEDULE:
SULFUR FROM SULFURIC ACID PLANTS

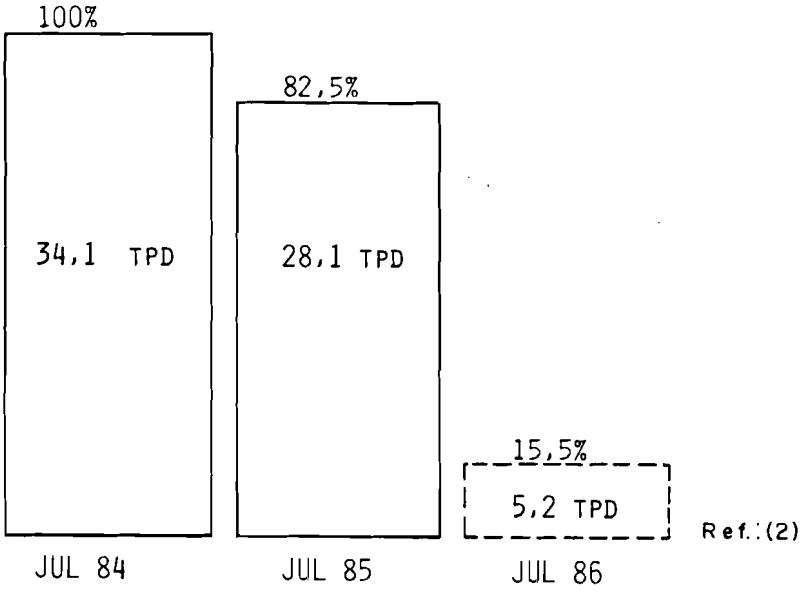


FIGURE 7

EMISSIONS REDUCTION SCHEDULE:
NITROGEN OXIDES (NO_X)

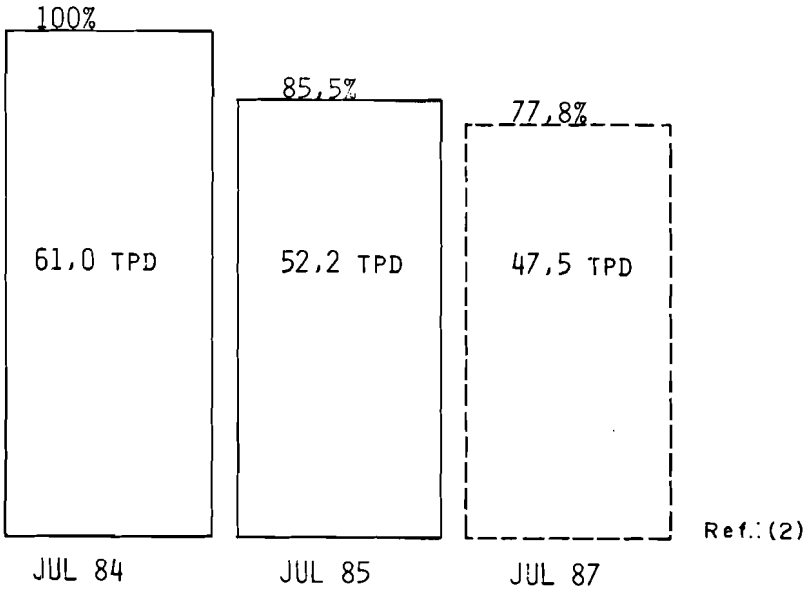
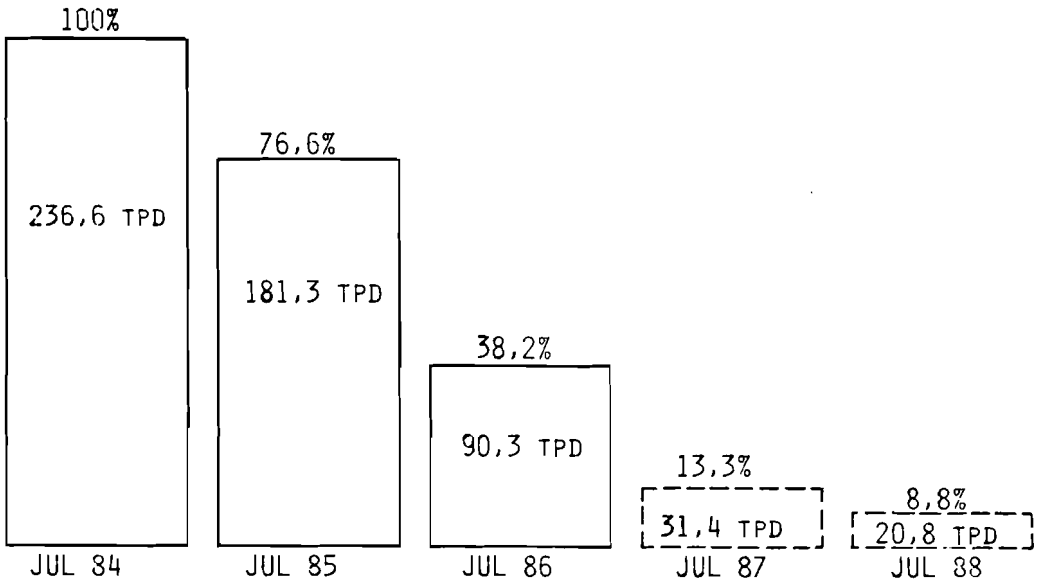


FIGURE 8

EMISSIONS REDUCTION SCHEDULE: TOTAL PARTICULATES



Ref.:(2)

TABLE 1
FREQUENCY OF AIR POLLUTION EPISODES
- Cubatão, SP, Brazil -

YEAR	N OF EPISODES		
	ALERT	EMERGENCY	TOTAL
1984	12	1	13
1985	8	1	9
1986	1	0	1

Ref.: (1)

TABLE 2

STANDARDS FOR CLASSIFICATION OF AIR POLLUTION STATUS

- CUBATÃO, SP, BRAZIL -

PARAMETER	UNIT	STATE OF		
		OBSERVATION	ALERT	EMERGENCY
SO_2	$\mu g/m^3$ (24h average)	800	1600	2100
PARTICULATES (a)	$\mu g/m^3$ (24h average)	375	625	875
SO_2 x TSP	-	65×10^3	261×10^3	393×10^3
CO	$\mu g/m^3$ (8h average)	17×10^3	34×10^3	46×10^3
O_3	$\mu g/m^3$ (1h average)	200	800	1200

NOTE:

(a) - As Total Suspended Particulates - TSP

Ref.: (1)

cost for implementing the program was obtained from the companies whose plants were at risk at each particular location. Figure 9 exemplifies the extent of the civil works in one of the major problem areas.

3.3
Reforestation Program

A reforestation program for the affected mountain scarps was initiated in 1985 using seeds of a special resistant gramineous (Brachiaria). The pilot experiment demonstrated a recovery efficiency of 40% in test plots. In a second phase, initiated in the second semester of 1985, native arboreous species have been planted. Preliminary results show encouraging response since most of the tested species sprouted.

Nevertheless, it is still to soon to evaluate if this ongoing program will be successful in reducing the impact of rainfall in the renewed forest cover.

3.4
Strenghtening of Civil Defense Bodies

Within the scope fo the crash risk management emergency plan launched by the State Government of São Paulo the program for strenghtening the Civil Defense system of Cubatão received special attention.

Among the key issues of that program the relocation of people living in illegal squatters settlements build around some of the plants was the one of greatest impact. The affected communities refused at first to move out the area. Although negotiations are still under way most of the more exposed people agreed to settle elsewere in new housing developments provided by the local government.

FIGURE 9
MUD HOLDING DAMS ALONG ONE OF THE MAIN DRAINAGES OF THE MOUNTAINS ENCIRCLING CUBATÃO
REF.: (2)

To anticipate the necessary steps to be followed by civil defense personnel the event of severe flooding, some main criteri have been established for switching levels of action during the rainy season. Figure 10 presents a summary of those criteria which were divided in two categories namely hydrological and geotechnical.

Depending on the degree of seriousness of the expected flooding consequences (i.e. observation, attention, critical or emergency) civil defense personnel would act at two distinct levels:

- Plant level action

  - Order partial or complete shutdown of plants. Decision is taken considering each one of the sectors in which the area of Cubatão was divided (See Figure 1);
  - Closing of pipeline valves;
  - Reduce inventory of main storage tanks of dangerous products;
  - Activate emergency energy supply systems.

- Population level action

  - Organize and conduct pre-prepared evacuation plans to withdraw plant personnel and people from endangered areas;
  - Provide transportation, health assistance and shelter to affected people.

4. FUTURE PROGRAM TARGETS

Figure 11 presents a summary of an integrated approach for risk assessment and management in highly industrialized regions in a country. Inspection of that figure shows what has been completed in Cubatão and what is still in progress or should be initiated in order to further reduce risks in the area.

FIGURE 10
MAIN CRITERIA FOR SWITCHING LEVELS OF ACTION DURING RAINY SEASON
- CUBATÃO CIVIL DEFENSE PLAN - (NOV-MAR) -

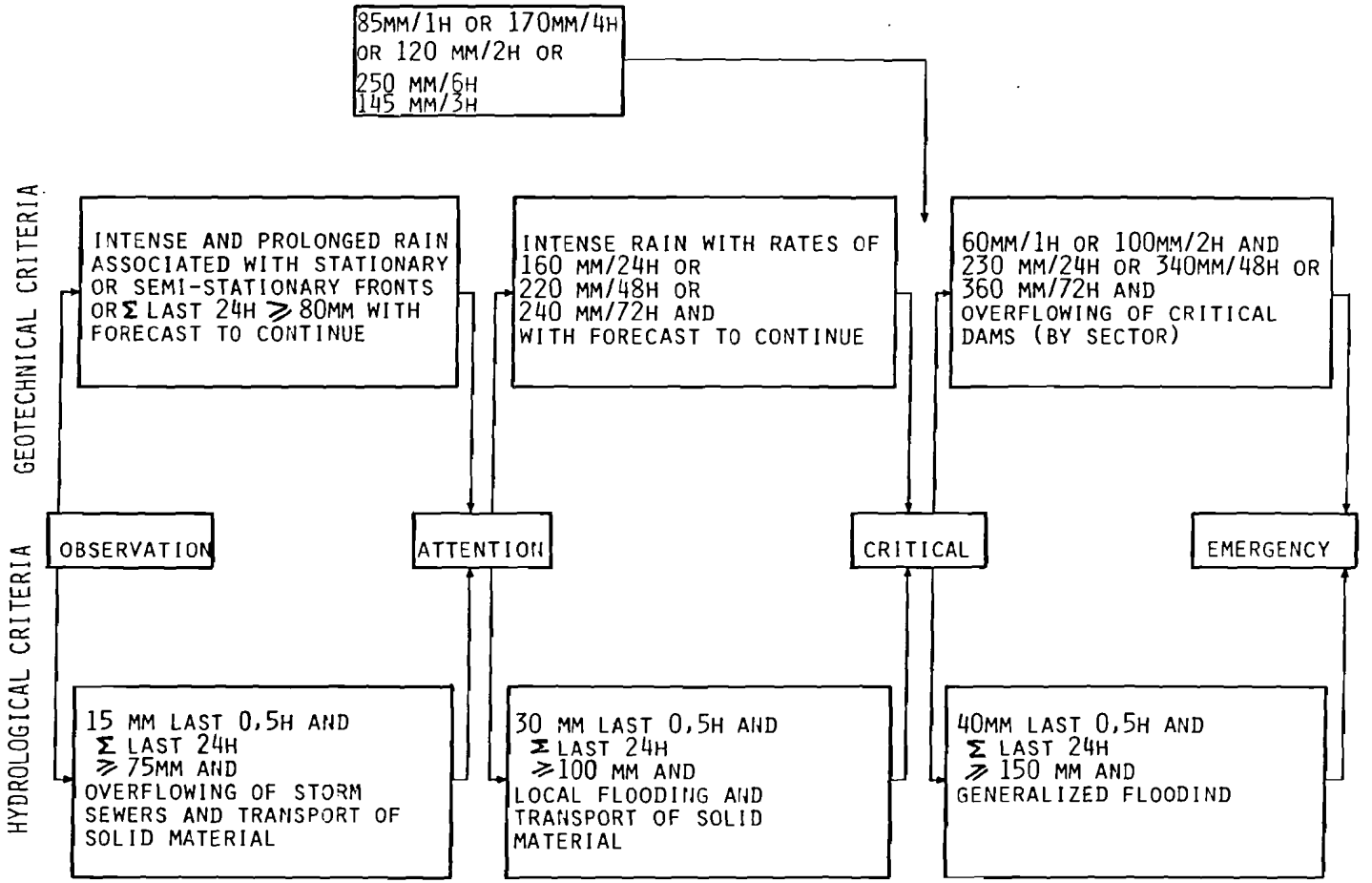
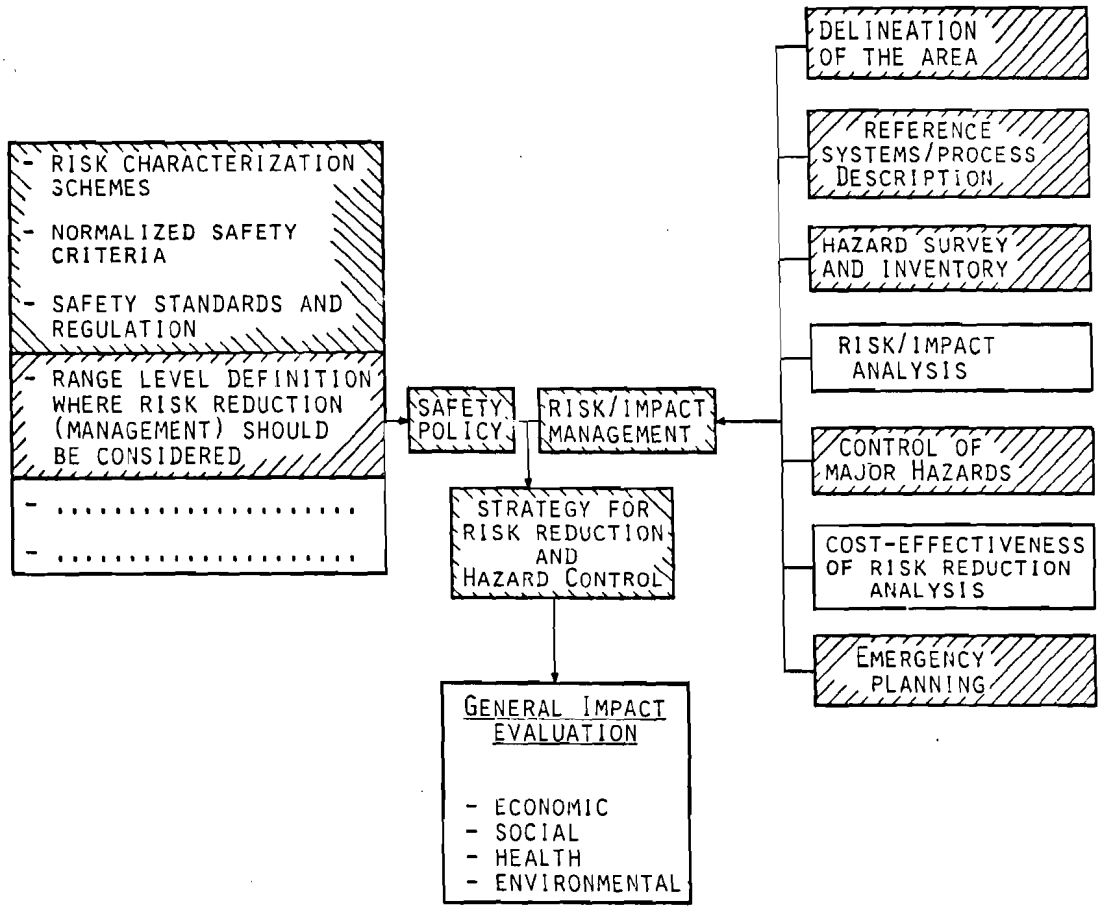


FIGURE 11

INTEGRATED APPROACH FOR RISK ASSESSMENT AND MANAGEMENT IN HIGHLY INDUSTRIALIZED REGIONS IN A COUNTRY



REF.: (3)

LEGEND:

COMPLETED

IN PROGRESS

Among the future targets of the plan conventional risk assessment and management studies at individual plant level will be conducted.

References:

1.
CETESB - Companhia de Tecnologia de Saneamento Ambiental; "Environmental Pollution Control in Cubatão"; Results Report; July 1983 to July 1986.

2.
CETESB - Companhia de Tecnologia de Saneamento Ambiental; Comissão Especial para Restauração da Serra do Mar; "Ações para a Restauração da Serra do Mar". 1986.

3.
Novegno, A. "Summary Description of Planned Joint WHO, UNEP, ILO, IAEA Project on Assessing, Controlling and Managing Health and Environmental Risks from Energy and Other Complex Industrial Systems"; Doc. No. 2001 d; IAEA, 1985.

1.7. THE ACCIDENT OF CHERNOBYL: ISSUES IN LOCAL RISK MANAGEMENT

M. Deicher, G. Lindner, E. Recknagel (Department of Physics, University of Konstanz, FRG), A. Ernst (Department of Biology, University of Konstanz, FRG), H. Hofsäss and C. Hohenemser (Clark University, Worcester, Massachusetts, USA)

Fallout in the days after the accident at Chernobyl reached levels 30 to 40 times natural background at locations as far as 1500 km from the accident. In the absence of coordinated government responses, spontaneously generated risk management was undertaken in many places. Described here are risk management efforts in a locally "hot" region of southern West Germany. Based on the achievement of high credibility with the local population, and the establishment of effective local countermeasures, it is argued that decentralization of risk management is a key to coping with future radiological disasters.

The reactor accident at Chernobyl in the Soviet Ukraine on April 25-26, 1986, led to the largest release of radioactivity ever recorded in one technological disaster. The event involved a "worst case" accident scenario in which a large reactor with a mature fuel inventory breached containment and released several percent of its radionuclide inventory.

Dry weather, favorable siting, evacuation of 130,000 people, and the dispersion of early releases to high altitude all contributed to holding prompt casualties to a small number -- 31 at last report [1]. Air concentrations and ground deposits as far away as 1000-2000 km, however frequently exceeded protective action guidelines applicable to the ingestive pathway. Since European risk management institutions were unprepared for an accident of the magnitude and transnational character of Chernobyl, it was necessary to improvise appropriate responses to the fallout.

In some countries, such as Sweden [2] and the Netherlands [3], improvisation was prompt because radiation monitoring laboratories coupled quickly to relevant public officials. In other cases, such as West Germany, established monitoring stations took many days to map the fallout, publish the results, and institute adequate public information campaigns and appropriate countermeasures. The spectrum of immediate response ranges from Switzerland, which established no early protective actions with respect

to food, to the West German state of Hessen, which set a standard for ^{131}I in milk at the extremely low value of 20 Bq/l.

If anything is clear from the European experience, it is that protective action planning at large distances from a reactor accident is an issue whose time has come. The need for such planning is not only driven by public fear and confusion, but also by estimates which place the collective dose in Europe at about 80 million rem [4]. Although for most individuals Chernobyl will impose an epidemiologically undetectable incremental cancer risk of 0.01% or less, it is predicted that the worldwide burden of cancer mortality will reach thousands to tens of thousands [1,4,5]. Thus, there can be little question that the public will demand appropriate protection.

We review here what is now known about the physical characteristics of Chernobyl fallout, and describe our experience in developing a response in the Konstanz area -- a locally "hot" region in southern West Germany. We also compare the responses of local, state, and federal governments in West Germany and the United States, and discuss optimal risk management designs for future radiological disasters.

1. PHYSICAL CHARACTERISTICS OF CHERNOBYL FALLOUT

The accident has been described in some detail at a review conference sponsored by the International Atomic Energy Agency (IAEA). According to Soviet scientists [1], the accident occurred during a series of tests designed to establish whether the reactor's turbines could provide emergency power to cooling pumps after a sudden loss of steam. To simulate this situation, operators ran the plant at 700 MWth prior to a sudden planned shutdown. In the course of the test, they inadvertently dropped to 200 MWth, where they encountered instability due to xenon poisoning.

Instead of shutting down altogether, as required by safety regulations, operators continued the test. Since the reactor has a positive reactivity coefficient at low power, the instability triggered a "runaway" condition in which local temperatures shot to over 2000 C in a few seconds. This resulted in a steam explosion that severed the tops of most of the 1661 vertical pressure tubes, and dropped the fuel changing crane onto the core. The steam explosion was followed by a second (hydrogen) explosion and a vigorous fire that burned for several hours.

The initial explosions and fire began at 1:23 am on April 26, and carried radioactive debris to an altitude of 2-5 km. Release of radionuclides continued for over nine days, and reached peak values during the first and ninth days. The first peak was caused by the initial explosion, the second originated from heat accumulation in the destroyed core, which had been covered with 5000 tons of sand, clay, boron, and lead to contain the fire.

The release of activity was ultimately stopped by pumping liquid nitrogen into the destroyed core.

According to Soviet scientists [1], radionuclide deposits in the Soviet Union measured 50 MCi as of May 6. Not included are about 40 MCi of gaseous ^{133}Xe and 0.6 MCi of gaseous ^{85}Kr, as well as activity deposited outside the Soviet Union. Since the reactor core contained about 1400 MCi of radionuclides on May 6, the ground deposits in the Soviet Union amounted to 3.5% of the core. Adding gaseous fission products brings the release to 6.4%; adding surface deposits outside the Soviet Union may place the total release fraction as high as 8-10%.

The release fractions for various isotopes differed substantially from those expected in a worst case pressurized water reactor (PWR) accident. In particular, owing to the initial explosion, Chernobyl had a lower fraction of some volatile fission products and a higher fraction of less volatile fission products than a corresponding TWR accident involving core melting and loss of containments [6,1]. To illustrate, Fig. 1 depicts the release fractions as a function of volatility class for the two cases.

Exposure rates, E, expressed as a multiple of normal background, are plotted as a function of the distance, r, from Chernobyl in Fig. 2. Results for Soviet locations are from the Soviet report to the IAEA [1]; other data are from our own compilation [7]. As indicated by the straight line, the dispersion may be fitted by the relation $E \sim r^{-1.4}$. Despite scatter in the data, caused by timing of the cloud's passage, non-uniformity of release and dispersion, Fig. 2 permits a rough interpolation for non-measured stations.

The data fall into two families -- those involving fallout deposition by rain and those representing dry deposition. At a given distance, rainfall locations have exposure levels 15-20 times higher than dry locations. Because dispersal was dominated by long-range transport of small particles, considerably further fractionation of radionuclides occurred during dispersal. Thus, fallout in Western Europe showed a marked relative deficiency in alkaline earths (Ba, Sr) and transuranics (Np, Pu), implying that Western Europe was largely spared the most dangerous radionuclides. The same can, unfortunately, not be said about regions of the Soviet Union close to the accident.

2. EVOLUTION OF LOCAL RISK MANAGEMENT IN THE KONSTANZ REGION

In the days immediately following the accident, the concise technical description of the fallout we have given was, of course, beyond the reach of anyone. To track how risk management developed in this context, we recall the situation in Konstanz, a city of 100,000 on the West German-Swiss border.

2.1. Early Discoveries

When Sweden announced the arrival of radioactive cloud on Monday, April 28, few of us were concerned. We discussed making fallout measurements on Tuesday, April 29, when the Soviet news agency TASS announced a serious reactor accident in the Ukraine. Despite prevailing easterly winds, we were quite skeptical that significant quantities of radioactivity could be measured 1500 km from the accident.

On Wednesday, April 30, thunderstorms and heavy rainfall occurred along the northern frontier of the Alps, including the Konstanz region. Out of curiosity, we carried a portable geiger counter outside after the rain had stopped. The counter, which read 8-10 counts/s inside the building, jumped to 250-400 counts/s outside. After some checks, we concluded that we had been showered with radionuclides in amounts equivalent to 30-40 times natural background.

By nightfall, we had begun measuring with a high resolution Ge counter, and by morning, we had a "textbook" gamma ray spectrum from which we could identify more than 15 well known fission products (see Fig. 3). It became clear that environmental contamination was at levels, which, had it occurred inside our building, would have required closing the laboratory on legal grounds. For example, we found combined concentrations of ^{131}I and ^{132}Te in rainwater of 90,000 Bq/l, and surface concentration of ^{137}Cs of 8,000-12,000 Bq/m^2. The latter exceeded by a factor of 10-15 the ^{137}Cs deposition in the peak year of weapons testing fallout [7].

In the first few days after April 30, almost all detailed information about the Konstanz fallout came from our own measurements. Fallout constituents were identified with a Ge detector; food contamination was checked with NaI detectors; ground activity was determined with portable geiger counters designed for detecting gross beta activity; contamination of persons was checked with a stationary personnel monitor. These measurements were supplemented by gross-beta measurements conducted by the Konstanz fire department.

We were puzzled because our results indicated much larger radionuclide burdens than given in scattered press reports for other regions of West Germany. The situation was finally clarified on May 8, eleven days after the accident, when the state government of Baden-Württemberg published a composite map of gross-beta activity measured by local fire departments. As seen in Fig. 4, this sows radiation levels near Konstanz as much as a factor of 15 higher than in Stuttgart and the northwest part of the state. Subsequently, we were able to explain this through a strong correlation of radiation levels with rainfall, as also shown in Fig. 4.

Our information during the first week was far from complete. We had no data on radioactivity of air, size and composition of fallout particulates, and the abundance of the most dangerous pure beta and alpha emitter (e.g., ^{89}Sr, ^{90}Sr, and ^{239}Pu). Our conjecture that these radionuclides were largely absent was confirmed only a month later [8].

2.2. The Structure of Local Risk Management

According to the West German constitution, state and local governments have the legal responsibility for setting protective action standards and establishing emergency management. Evacuation planning for West German nuclear plants is conducted by the affected county (Landkreis) under the supervision of the state. The federal government sets evacuation guidelines, but has only advisory power in this context. At the time of Chernobyl, emergency plans existed only in counties with nuclear plants, whereas "non-nuclear" counties, like Konstanz, had made no plans or preparations.

In this policy vacuum, the structure of local risk management developed spontaneously and independently of state and national authorities. During the first three days, the local daily newspaper, Der Südkurier, and our group at the University of Konstanz dominated local action. On May 2, the county commissioner (Landrat) formed an advisory committee, which subsequently became the center for decision-making and information exchange.

We interpreted our measurements in terms of the "minimum principle" (Minimierungsprinzip) of federal radiation protection guidelines [9]. Freely translated, this demands that efforts be made to keep exposure "as low as reasonably achievable" (ALARA). In the West German regulatory context, the ALARA principle is intended to guide licensing of new nuclear facilities and has no specific role in establishing emergency management. In the novel situation confronted in Konstanz, the principle effectively guided our search for countermeasures.

The first contact with the state government came on May 5, a week after the beginning of the crisis in Konstanz. At that time, we were asked officially to monitor radiation in food, as we had been doing for a week. Subsequently, there was no significant change in the self-evolved local decision-making, though contact with higher levels of government and trans-regional media increased. Financial support from the state government eventually made possible expansion of monitoring capacity.

2.3. The Content of Local Risk Management

Our public statements made during local risk management efforts were guided by three themes: (1) rapid publication of data; (2) description of physical phenomena in terms understan-

dable to the public; (3) warnings to avoid ingestion and breathing of radioactivity. In this way, it became possible for people to self-design protective actions. For example, with information about radio-isotope levels in food and knowledge of annual intake standards (Grenzwerte), citizens could decide what to eat and what to avoid.

Guidelines published during the first week are given in Table 1. Many of these were supported by specific experiments. Thus, we found washing removed only 10-20% of activity from shoes, asphalt, and vegetables; hence, we advised that shoes be removed on entering houses and that locally grown vegetables be avoided. We found air filters had high radio-particulate content, and thus recommended that children minimize outdoor play. Via experiments, we learned that the bulk of activity lay on the ground, whereas only about 20% adhered to growing vegetables. For this reason, we suggested decontamination be achieved by plowing under the crop, rather than by harvesting and disposing of contaminated vegetables.

The most significant intervention in Konstanz was the monitoring and control of milk. Consistent with an annual ^{131}I limit of 1800 Bq [9], raw milk collected from dairy farmers was sampled and accepted for processing only if it measured below 100 Bq/l. Because dairy farmers heeded local and state warning to avoid releasing cattle to pasture and to feed only stored hay, raw milk levels remained, for the most part, under 100 Bq/l. In contrast, the neighboring canton of Thurgau, Switzerland, experienced milk levels that peaked at 1500 Bq/l, because it instituted no countermeasures. Despite low levels of ^{131}I, milk demand in Konstanz dropped drastically during the crisis.

A second important intervention in Konstanz concerns locally grown vegetables, of which the environs of Konstanz are a major regional supplier. Due to information distributed via the newspaper, citizens knew early in the crisis that leafy vegetables had ^{131}I contamination well above the eventually announced federal guideline of 250 Bq/kg (See Fig. 5). As a result, the vegetable market had already collapsed by May 4, when an official ban on vegetable sales was instituted by the state. With no market available and the hope of federal compensation, farmers accepted local recommendations to plow under their crop. Over 2 million heads of lettuce, 65,000 kg of spinach, and 1.3 million kohlrabi were destroyed. The vegetable market was reopened on May 20, and after some weeks demand returned to normal levels.

In addition to milk and vegetable controls, the county commissioner and his advisory board opened special repositories for contaminated grass cuttings, issued guidelines for handling contaminated air filters, and took actions to prevent the use of contaminated sewage sludge in the community composting plant.

Not all proposed control measures were feasible. For example, we knew that the first hay cutting in May would be con-

taminated and issued an early warning to that effect [10], but our advice to cut and dispose of grass before maturity was unworkable because a large enough disposal area was unavailable. As a result, a second period of milk contamination occurred in Winter 1986-1987, when contaminated hay cut in May reached milk cattle. Its effect turned out to be less severe than expected, since our group's feeding experiments with contaminated hay established hay-milk transfer factors as a factor of 4 less than reported in the literature [11].

2.4. Risk Communication

After the first reports of the accident, the population developed an almost insatiable appetite for information. The most important means for communication with the public was the local newspaper, Der Südkurier, which opened its pages to extensive and accurate discussions of the situation. To help the paper in its effort, we contributed considerable material ourselves, including composite answers to 500 letters of inquiry, as well as articles on the accident sequence, the radio-isotopes in food, and the risk of radiation.

Public meetings, sponsored by a wide range of interest groups, were a second key source of information. These meetings featured individuals involved in measurements, risk assessment, and public policy, and generated a high level of public confidence. The first occurred on May 2, and attracted over 2000 townspeople. Our group eventually presented more than 100 public programs on radiation risk, with many talks given by graduate students involved with the measurements. The public generally had many questions and demanded a high level of technical detail. Throughout the process, we were repeatedly amazed by people's willingness to confront complex and ambiguous issues, e.g., the problems involved in extrapolating high dose data to low dose.

Telephone communication, conducted through a special "hot line," was a third means of reaching the public. In our responses, we sought to calm fears with specific suggestions for reducing exposure or explanations of the rather small individual risks of local fallout. As the work proceeded, regional and national media showed in increasing interest in Konstanz and became a fourth outlet for our results.

2.5. Evaluating Local Risk Management

Whereas it seems clear that local people felt satisfied with the local risk management effort, a number of criticisms of the effort have been aired. Most often heard is that local risk managers over-reacted, that guidelines and interventions were too numerous and far-reaching, and that they failed to consider economic losses. On the other hand, some say that we were too lax and did not do justice to the ALARA principle. Though it is hard

for us to judge our own activities, we can respond to these issues.

An important source of concern was the paucity of early information. In the first week of May, we did not know whether to expect further emissions from Chernobyl. It was also unclear whether ^{90}Sr or Pu were present in the local fallout. Our concern was heightened by our use of federal radiation protection guidelines [9], which set forth annual isotopic organ dose-limits based on expected cancer incidence. This approach is more conservative than the concept of "effective equivalent dose" used by the International Commission on Radiological Protection [12,13]. For example, the ICRP approach weighs organ doses with factors that reflect expected cancer fatalities and accordingly gives thyroid doses a nearly negligible weight of 0.03.

A specific case of caution which has been questioned concerns the recommendation that pregnant women avoid eating local fish, which in July 1986, surpassed the $^{137}Cs/^{134}Cs$ import standard of 600 Bq/kg set by the European Community. Even though this is relatively low compared to the annual intake limit of 21,000 Bq, we justified our caution because fish from Lake Konstanz often forms a large part of the diet, and because the further increase in cesium levels was expected. As it turned out, fish contamination stabilized in late summer at $^{137}Cs/^{134}Cs$ levels of 300-600 Bq/kg.

The discovery in late May that the fallout contained particulates with high specific beta activity [10,14] suggests that we may not have exercised sufficient caution in relation to inhalation dose. Thus, it might have been wise to warn more extensively against open air activities and to recommend more intensive street washing efforts.

Finally, our information campaigns provided the means for autonomous decisions by citizens. This, in turn, created a powerful market mechanism for ensuring radiation protection, albeit with some losses for affected merchants and producers -- losses which were eventually almost fully compensated by the federal government.

3. THE IMPACT OF THE STATE AND FEDERAL ACTIONS

It is interesting to compare the actions of state and federal governments to the local risk management just described. As seen in Table 2, the Bonn government adopted import limitations on the first day after the cloud and protective action guidelines (Grenzwerte) for milk and leafy vegetables on the third and fifth day. Early in the fallout episode, however, it announced that there was no reason to limit outdoor activity. In contrast, citizens in Konstanz were warned to limit outdoor play of children. This recommendation was based on local radiation levels which the federal government did not consider when it issued its statements.

The state government in Stuttgart converted the non-binding federal guidelines into concrete emergency actions. On the day of the cloud, it warned against iodine tablet use, and three days later, it warned against open pasture feeding of milk cattle and recommended washing of leafy vegetables. On the fourth day, it warned against sale of unprocessed milk, and on the fifth day, with the recognition that washing was futile, it banned the sale of locally grown leafy vegetables altogether.

Compared to state actions, local risk management in Konstanz moved more rapidly and effectively. Local warnings against consumption of leafy vegetables were published on the third day after the cloud so that by the time the state banned sales on the fifth day, the market had already collapsed. Local warnings about vegetables recognized the ineffectiveness of washing and thus avoided the confusion created by the state's washing directive. Finally, local efforts established milk control at one fifth of the federal standard, suggesting that the federal standard was locally inconsistent with the ALARA principle.

Some states set standards that were considerably stricter than federal guidelines. For example, whereas Bonn advised an ^{131}I milk standard of 500 Bq/l, the state of Hessen enforced a local standard at 20 Bq/l. This apparently large inconsistency was a source of confusion for the public and has been interpreted in terms of attitudes toward nuclear power, which are "pro-nuclear" at the federal level and "anti-nuclear" in the state of Hessen. An equally reasonable explanation, however, is that in a federal system different radiation environments naturally imply different local standards under application of the ALARA principle. For the small state of Hessen, which was spared heavy fallout, 20 Bq/l was a reasonable standard; in Konstanz, with much heavier fallout, 100 Bq/l could be enforced without serious losses; and in southern Bavaria, where the heaviest fallout occurred, a value approaching the federal standard of 500 Bq/l may have been necessary.

Individuals also set their own standards. For example, despite the fact that milk ^{131}I content was nearly everywhere below the federal guideline, milk sales dropped precipitously during the crisis. In the case of ^{134}Cs and ^{137}Cs, Bonn set no guideline. As a result, a variety of implicit guidelines were expressed through the market behavior of the public. In Konstanz milk, $^{134}Cs/^{137}Cs$ levels higher than 30 Bq/l were found unacceptable for small children, whereas berries up to 200 bq/kg and meat up to 600-1000 Bq/kg were marketable.

Perhaps the largest point of contrast between federal and state actions and the local work in Konstanz was the absence of quantitative data in early state and national pronouncements. Instead, central authorities made qualitative statements which had the apparent intent of minimizing the danger of the crisis. This approach may have been counterproductive, leading directly

to the loss of credibility that occurred -- particularly among individuals who have the ability and tools to form their own judgement. In any case, we attribute the high credibility of local risk management in Konstanz to early publication of quantitative radiation data for food, and comparison of these to federal annual intake guidelines. We also note that, in contrast to the early days of the crisis, the state government recently has been more forthcoming with specific data, presumably in recognition of the fact that this enhances its credibility.

4. LESSONS FOR THE FUTURE

The most important lesson of Chernobyl is that large scale toxic releases to the atmosphere can have extensive transnational impacts. For disaster management, this is a major insight which is currently fuelling an effort to develop systems that can cope with comparable future events. An obvious approach to such an event is immediate and complete exchange of information, coupled with aid to countries that require it. Such responses are best assured through prior international agreements, which are currently under discussion at the International Atomic Energy Agency, the World Health Organization, the Commission of European Communities, and the World Meteorological Organization. Individual nations are also taking steps to improve their planning.

A second key lesson of Chernobyl is that atmospheric transport disasters lead to highly variable impacts that are strongly dependent on local weather and terrain. Details of such impacts are largely unpredictable via existing atmospheric models, which at best provide general dispersion patterns [15]. At this time, the lessons for risk management are still being absorbed. In our view, one implication is that detailed local exposure data must rapidly be made available to local risk managers. This suggests that successful management must have a largely decentralized structure.

4.1. West German Planning

In West Germany, the delay and confusion associated with Chernobyl have served as impetus for significant action. In particular, the need for improving food chain protection outside established emergency zones is widely recognized. The fact that West Germans regard their reactors as safer and better than those of other countries plays little role here, largely because West Germany is surrounded by numerous nuclear power plants in neighboring nations.

The first major institutional response to Chernobyl came at the federal level when Bonn established a new Ministry for Environment, Nature Conservancy, and Reactor Safety. The next step, taken in October 1986, was federal legislation to provide improved radiation protection for the public [16]. The new law

is intended to deal with the problem of conflicting state and local standards in the recent crisis. It foresees centralized collection, analysis, and evaluation of data via an expanded monitoring system capable of accommodating local variability. State and local governments are to monitor and, if necessary, take action on local food chain problems. At the same time, they must follow federal guidelines and refrain from independent commentary and interpolation of data. In effect, the new law places the federal government into the role of "chief risk communicator," even while state and local authorities retain their constitutional responsibility for emergency management.

Bonn's de facto exclusion of autonomous local action reflects the government's concern with establishing a uniform standard. For at least three related reasons, such an approach may not be optimal. First, it is in conflict with the highly variable distribution of fallout, which by itself demands a localized response. Second, the danger exists that decision-making will be delayed because it is difficult to deal with local complexity from a national platform. Third, and most important, there is little hope that a centralized response will lead to the kind of risk communication success that is possible when local officials are informed locally and communicate directly with local constituents. Overall, it is likely, therefore, that the new law will create more problems than it solves.

4.2. United States Planning

Like West Germany's, the U.S. risk management system is constitutionally decentralized. Under federal guidelines issued through the Nuclear Regulatory Commission (NRC), reactor licensing requires state and local governments to develop an emergency evacuation plan over a 16 km radius emergency zone around each nuclear power plant. In addition, states are required to develop emergency plans for controlling exposure through the food chain in an 80 km radius ingestion pathway planning zone.

In the aftermath of Chernobyl, questions surfaced at the state level (e.g., in Massachusetts and Ohio) whether the existing 16 km emergency evacuation zones and the 80 km ingestion zone should be enlarged. So far, these questions have not been translated into action, and in contrast to West Germany, there is no plan to institute a nationwide monitoring system having a sufficient density to deal with the kind of local fallout variability experienced in the aftermath of Chernobyl.

If anything, the dominant reaction in the United States has been that "Chernobyl can't happen here," because U.S. light water moderated reactors are fundamentally safer than Soviet carbon moderated types [17,18]. In fact, in one state, New Hampshire, the utility and the state are currently seeking to reduce the emergency evacuation zone to 1.6 km radius, so that the zone lies entirely within the state [19]. At the root of this proposal is

a political conflict with neighboring Massachusetts, which would contain a significant fraction of the 16 km zone. Massachusetts has declared that effective evacuation to 16 km is unfeasible because of inadequate roads, and therefore will not participate in the emergency plan or assent to the licensing of the new reactor. If successful, the New Hampshire initiative may trigger similar initiatives elsewhere in the U.S.

Thus, the issue in the United States is not centralization vs. decentralization, but whether the existing decentralized system needs improvement. At the moment, the dominant view seems to be that improvement is unnecessary; and there is a change that through the New Hampshire initiative, emergency planning will be weakened. In this situation, one can expect that a major nuclear reactor accident, even with a release much smaller than Chernobyl, will produce at least as chaotic a result in the United States as occurred in most of Western Europe in the aftermath of Chernobyl.

4.3. Extended Emergency Planning

Based on the experience in Konstanz, we think it desirable for all countries involved with nuclear power to plan beyond emergency evacuation zones around nuclear power plants. Part of this planning should include the establishment of monitoring stations at sufficiently close intervals to permit rapid assessment of local fallout variability. The issue is not whether Chernobyl can recur, but whether any significant nuclear reactor accident can occur. Even a release equal to 1% of Chernobyl may, in the case of rain, require food-chain protection at 100 km. This can be seen from Fig. 3 by noting what happens if the line describing rainfall locations is moved downward by a factor of 100.

For coping with radiological protection beyond evacuation zones, we recommend establishing extended emergency planning zones managed by local government commissions who should handle most issues confronted in Konstanz during the recent episode. Local government should directly receive information from monitoring stations, report in detail to the public, and make decisions about local countermeasures. General guidelines, distribution and financing of standardized monitoring equipment, and handling of predominantly state and national issues, such as import limitations, should remain the responsibility of regional and national governments.

Because we can expect significant food chain problems out to 100 km, even for relatively small nuclear reactor accidents, extended emergency planning should cover all regions in which nuclear reactors are sited. Based on the observed variability of Chernobyl fallout, we estimate that the optimal size of these zones is larger than present evacuation zones, but not much larger than a few thousand square kilometers.

The advantages of local government commission managing local zones lie in their capability to respond rapidly and flexibly to exposure patterns with high spatial and temporal variability. An additional advantage is that local commissions can provide rapid and accurate communication with locally affected populations. This will forestall the loss of credibility that so often accompanies the delays of centralized organizations that attempt to handle too much complexity in a short time.

In establishing local commissions, thought should be given to the notion that universities and other organized centers of learning are among the best places for making unbiased measurements and analyzing risk management options. Alternatively, monitoring might be done by meteorological stations, as in the Soviet Union.

An important condition for the success of local zones is a framework for establishing protective action guidelines within each of several exposure regimes. The framework should rest on national or international guidelines that define annual intake limits. In the case of unavoidably large exposures, in which annual limits must of necessity by surpassed, prior planning should identify a series of emergency exposure regimes, within each of which the ALARA principle of the radiation protection guidelines can be applied. That different local zones may establish different protective guidelines is to be expected and is a logical consequence of applying the ALARA principle to a highly variable radiation environment. The public should be informed in advance that this is an expected and desirable result which deals in an optimal way with a complex situation.

5. SUMMARY AND CONCLUSIONS

Chernobyl constituted the largest release of radioactivity ever recorded in a single technological accident. It produced a highly variable pattern of fallout, strongly correlated with local rainfall. Even at 1500 km, fallout in some places far exceeded the peaks recorded in the 1960's during the period of atmospheric weapons testing.

Chernobyl demands reconsideration of emergency planning for nuclear power stations. Even if one assumes that accidents as large as Chernobyl will not recur, our experience with local risk management in West Germany suggests that response to large radiological accidents should involve a strong decentralized component with sufficient autonomy to make local measurements, conduct local risk assessments, inform the local population, and design effective local countermeasures.

Although both the U.S. and West German federal systems are ideally suited for establishing decentralized risk management efforts, it is doubtful whether either nation will be successful if it continues on its present trajectory. West Germany, with

most of the rest of Europe, has accepted the need for an extended monitoring system, but is in the process of strengthening centralized authority at the expense of local government. The United States, through its several states, is discussing the need for better monitoring systems outside established evacuation zones, but is moving very slowly toward adoption.

In this situation, we can predict that future nuclear accidents -- even if they are much smaller than Chernobyl -- will reproduce the chaos and confusion that Chernobyl brought to Western Europe in the spring of 1986.

REFERENCES:

[1] USSR State Committee on the Utilization of Atomic Energy. The Accident at the Chernobyl Nuclear Power Plant and its Consequences. A report compiled for the IAEA experts' meeting, 25-29 August 1986. (IAEA, Vienna, 1986).

[2] M. Jensen and J. C. Linhe, Activities of the Swedish authorities following the fallout of the Soviet Chernobyl reactor accident. A report of the Swedish National Institute for Radiation Protection, Box 60204, S-10401 Stockholm, Sweden, May 14, 1986.

[3] Rijksinstituut voor Volksgezondheit en Milieuhygiene te Bilthoven, Samenvattend voortgangsrapport radioactiviteitsmetingen in verband met het nucleaire ongeval Tjernobyl over de periode 1-12 Mei 1986, (RIVM, Bilthoven, the Netherlands, May 13, 1986).

[4] "Chernobyl doses across the continent," Nuclear News 30 (1), 62 (1987).

[5] F. von Hippel and T. B. Cochran, "Estimating long-term health effects," Bulletin of the Atomic Scientists, 43 (1), 18-24 (1986).

[6] H. W. Lewis, et al., "Report to the American Physical Society by the Study Group of Light Water Reactor Safety," Rev. Mod. Phys. 47, suppl. 1, S1-S123 (1975).

[7] C. Hohenemser, M. Deicher, A. Ernst, H. Hofsäss, G. Lindner, and E. Recknagel, "Chernobyl: an early report," Environment 28 (5), 6-13, 30-43 (1986).

[8] Gesellschaft für Strahlen- und Umweltforschung, Umweltradioaktivität und Strahlenexposition in Südbayern durch den Tschernobyl-Unfall. GSF-Bericht 16/1986. (Gesellschaft für Strahlen- und Umweltforschung GmbH München, Ingolstadter Landstrasse 1, D-8042 Neuherberg, West Germany, 1986).

[9] Verordnung über den Schutz vor Schaden durch ionisierende Strahlen, Bundesgesetzblatt no. 125 (Federal Government of West Germany, Bonn, October 13, 1976).

[10] C. Hohenemser, M. Deicher, H. Hofsäss, G. Lindner, E. Recknagel, and J. I. Budnick, "Agricultural impact of Chernobyl: a warning," Nature 321, 817 (1986).

[11] G. Lindner, M. Deicher, R. Eckmann, H. Hofsäss, S. G. Jahn, W. Müller, D. Petermann, W. Pfeiffer, S. Teufel, U. Wahl, S. Winter, and E. Recknagel, "Überregionale Aspekte der Tschernobyl Radioaktivität im Bodensee-gebiet," Symposium on radioactivity measurements in Switzerland after Chernobyl, and

their scientific interpretation, (Bundesamt für Gesundheitswesen, Bern, October 20-22, 1986).

[12] International Commission on Radiological Protection, Report 38, (Pergamon Press, Oxford, 1979/80).

[13] D. A. Baker, G. R. Hones, K. J. Soldat, Food - An interactive code to calculate internal radiation doses from contaminated food products, Report BNLWL-Sw-5523, (Brookhaven National Laboratory, Upton, NY, 1976).

[14] L. Devell, H. Todedal, U. Berström, A. Appelgren, J. Chrysslet, and L. Andersen, "Initial observations of fallout from the reactor accident at Chernobyl," Nature 321, 192-193 (1986).

[15] H. ApSimon and J. Wilson, "Tracking the cloud from Chernobyl," New Scientist 111 (1517), 42-45 (1986).

[16] Federal Government of West Germany, "Entwurf eines Gesetzes zum vorsorgenden Schutz der Bevölkerung gegen Strahlenbelastung," Drucksache 428/86, (Federal Government of West Germany, Bonn, 1986).

[17] H. W. Lewis, "The accident at the Chernobyl nuclear power plant and its consequences," Environment 28 (9), 25-27 (1986).

[18] R. Wilson, "Chernobyl: assessing the accident," Issues in Science & Technology, 3 (1), 21-29 (1986).

[19] L. Tye, "Seabrook seeks OK to shrink zone," The Boston Globe, December 19, 1986.

Acknowledgements: We thank our students and colleagues at the University of Konstanz, who participated in many fruitful discussions and extensive measurements, some still underway. We also thank friends and colleagues all over the world who helped us with advice and information. The effort in Konstanz owes a great deal to the local newspaper, Der Südkurier, and its assistant editor, H. Appenzeller. The effectiveness of local action depended on the intelligent response of local citizens, as well as several units of local government, particularly the county commissioner's office, headed by R. Maus. The final manuscript benefitted from extensive comments by R. Goble, A. Hohenemser, J. X. Kasperson, and O. Renn. Flexible financial support was received from the University of Konstanz and the state government of Baden-Württemberg.

TABLE 1: SUMMARY OF SPECIFIC RECOMMENDATIONS MADE BY LOCAL HAZARD MANAGERS DURING THE FIRST FEW DAYS OF THE EMERGENCY.

1.	Dairy cows should not be permitted to graze on open pasture.*
2.	Vegetables should be washed; later prohibition of vegetable sales, and that all vegetables be plowed under rather than harvested.*
3.	No rainwater collected on April 30 should be consumed.
4.	Children should be kept indoors as much as possible.
5.	Children should wash thoroughly (especially the eyes) after being outdoors.
6.	Kindergartners should avoid sandbox play.
7.	Sporting events on hardtop surfaces should be curtailed because of dust formation.
8.	Schools should monitor children during recess in order to avoid injuries. Schools should consider indoor sport.
9.	Sidewalks should not be swept.
10.	Street cleaning with sprinkler trucks should be increased.
11.	Lawn mowing should be postponed. Later recommendation to mow and follow instructions for disposal of grass cuttings.
12.	Children should not engage in gardening chores in order to avoid injury and dust build-up.
13.	People should not wear street shoes indoors.
14.	Hunting season should be postponed.*

* Also recommended by the state government of Baden-Württemberg.

TABLE 2: CHRONOLOGY OF THE FIRST TEN DAYS

DATE	INTERNATIONAL	FEDERAL	STATE	LOCAL
4/26	Explosion at Chernobyl, emission begins			
4/27	Evacuation at reactor			
4/28	Detection of radiation in Sweden, USSR announces accident	Activation of monitoring		
4/29	Emission continues	Issuance of public statement	Activation of monitoring	Article in paper on accident
4/30	Radioactive cloud crosses West Germany	Formation of working units	Formation of working units	Activation of monitoring, rainwater measured
5/1	Continued emissions in Chernobyl	Import quotas & border control established	Press release, establish research program	Monitoring of ground contamination
5/2	No further fallout in South Germany	Radiation protection guideline for iodine-131 set at 500 Bq/l in milk	Recommend no open grazing, wash vegetables	Publication of monitoring results in press warn against leafy vegetables, open form at University
5/3	Continued emissions		Warn against direct milk sale, advise dairies hold to federal iodine standard	Press report on leafy vegetable contamination
5/4	Continued emissions	Guideline for iodine-131 for vegetables set at 250 Bq/kg	Prohibit sale of leafy vegetables	Begin control of milk at local dairy
5/5	Emission at Chernobyl terminate		Universities asked to make measurements	Monitoring vegetables, state measuring begins

FIGURE CAPTIONS

Fig. 1 Release fraction under three conditions as a function of volatility class. The solid curve (1) described a theoretical reference accident for a pressurized water reactor. The broken line (2) describes the Chernobyl release. The dotted curve (3) describes the radioactivity measured in Konstanz normalized to Chernobyl at Class 3. Volatility classes are defined as follows: 1-noble gases, 2-iodines, 3-cesiums, 4-telluriums, 5-alkaline earths, 6-volatile oxides, and 7-nonvolatile oxides.

Fig. 2 Exposure levels due to Chernobyl in Eastern and Western Europe, measured 7-10 days after the accident. The open symbols describe dry deposition whereas the closed symbols describe rain deposition. The exposure, E, is measured as a multiple of the natural background, assumed to be 0.01 mrem/h.

Fig. 3 Gamma spectrum obtained from a grass sample in Konstanz on May 9, 1986, showing gamma ray lines of numerous fission products.

Fig. 4 Illustration of the correlation of activity level with rainfall. The numbers indicate ground level ^{131}I contamination in the state of Baden-Württemberg on May 8, 1986, in Bq/cm^2. The shading scheme indicates rainfall in mm during the period of April 30 to May 3, 1986.

Fig. 5 Time dependence of ^{131}I in lettuce in Konstanz. The bars indicate scatter of daily measurements, the heavy line the daily average.

Fig. 1

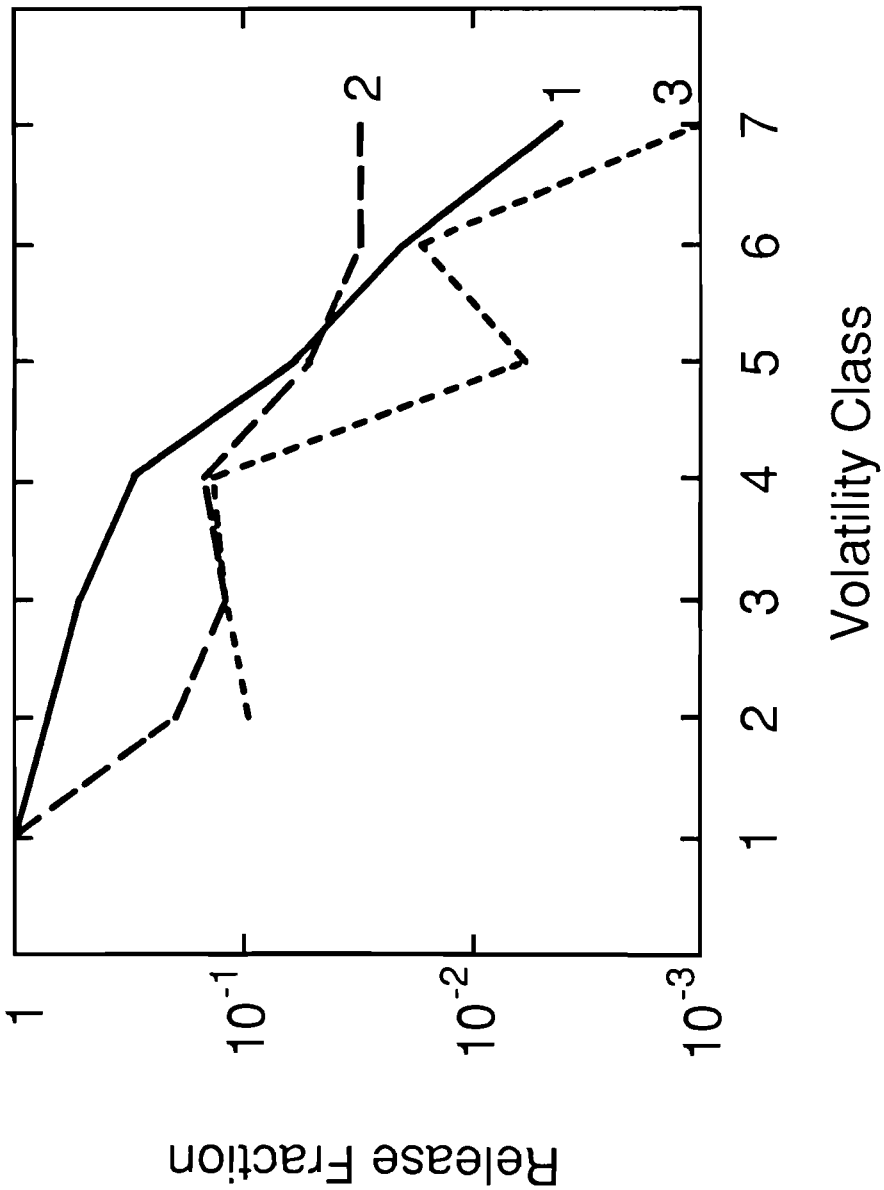

Release Fraction
1
10^{-1}
10^{-2}
10^{-3}
1 2 3 4 5 6 7
Volatility Class
1
2
3

Fig. 2

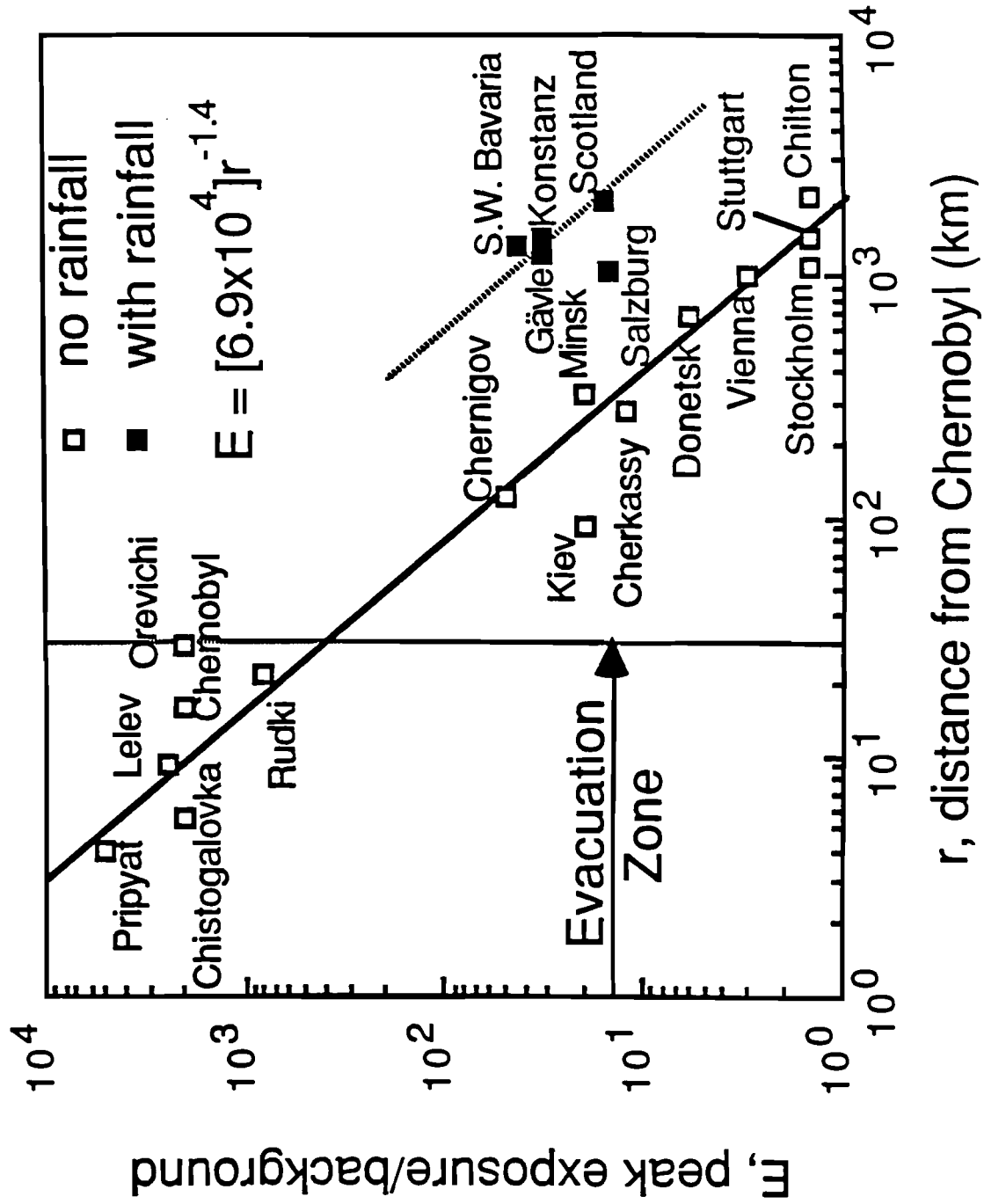

no rainfall
with rainfall
E = [6.9x10^4]r^-1.4
Pripyat
Lelev
Orevichi
Chistogalovka
Chernobyl
Rudki
Evacuation
Zone
Kiev
Chernigov
Cherkassy
Minsk
Gävle
S.W. Bavaria
Konstanz
Scotland
Salzburg
Donetsk
Vienna
Stuttgart
Stockholm
Chilton
E, peak exposure/background
r, distance from Chernobyl (km)

Fig. 3

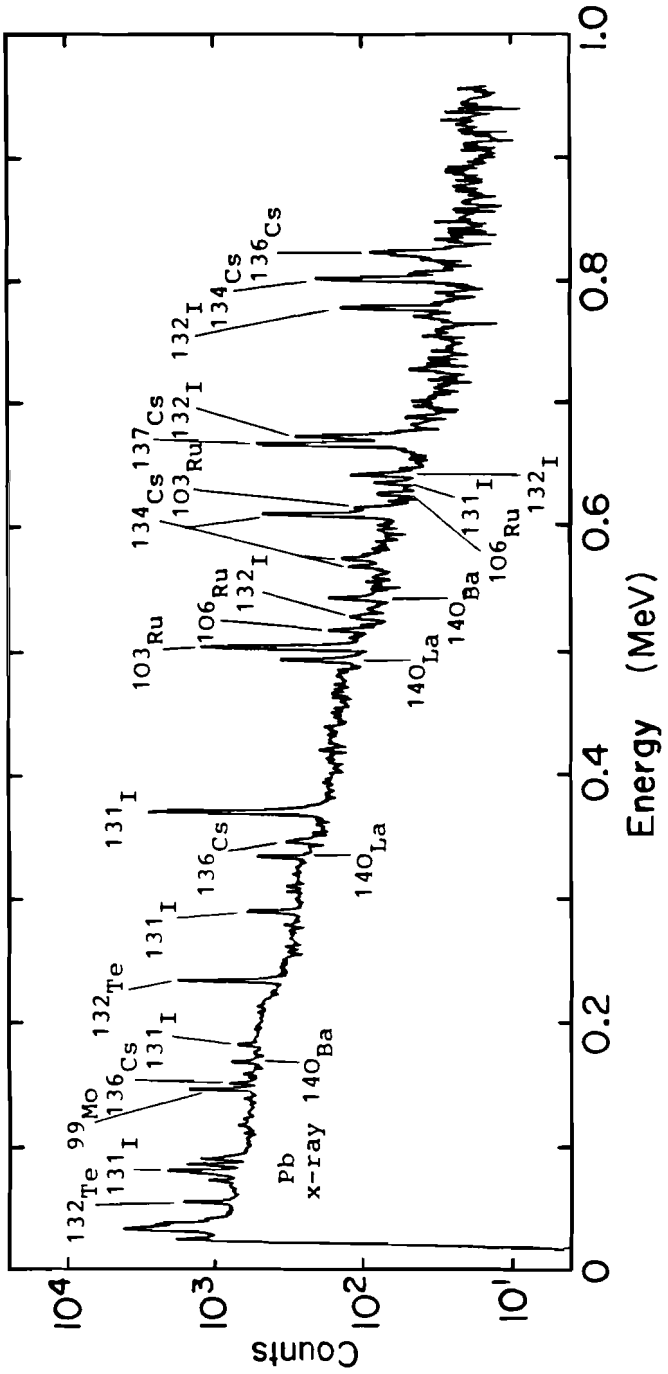

Counts
Energy (MeV)
0
0.2
0.4
0.6
0.8
1.0
10^4
10^3
10^2
10^1
^{132}Te
^{131}I
^{99}Mo
^{136}Cs
^{131}I
^{132}Te
^{131}I
^{136}Cs
^{131}I
Pb x-ray
^{140}Ba
^{140}La
^{103}Ru
^{106}Ru
^{132}I
^{134}Cs
^{137}Cs
^{103}Ru
^{132}I
^{132}I
^{134}Cs
^{136}Cs
^{140}La
^{140}Ba
^{131}I
^{106}Ru
^{132}I

Fig. 4

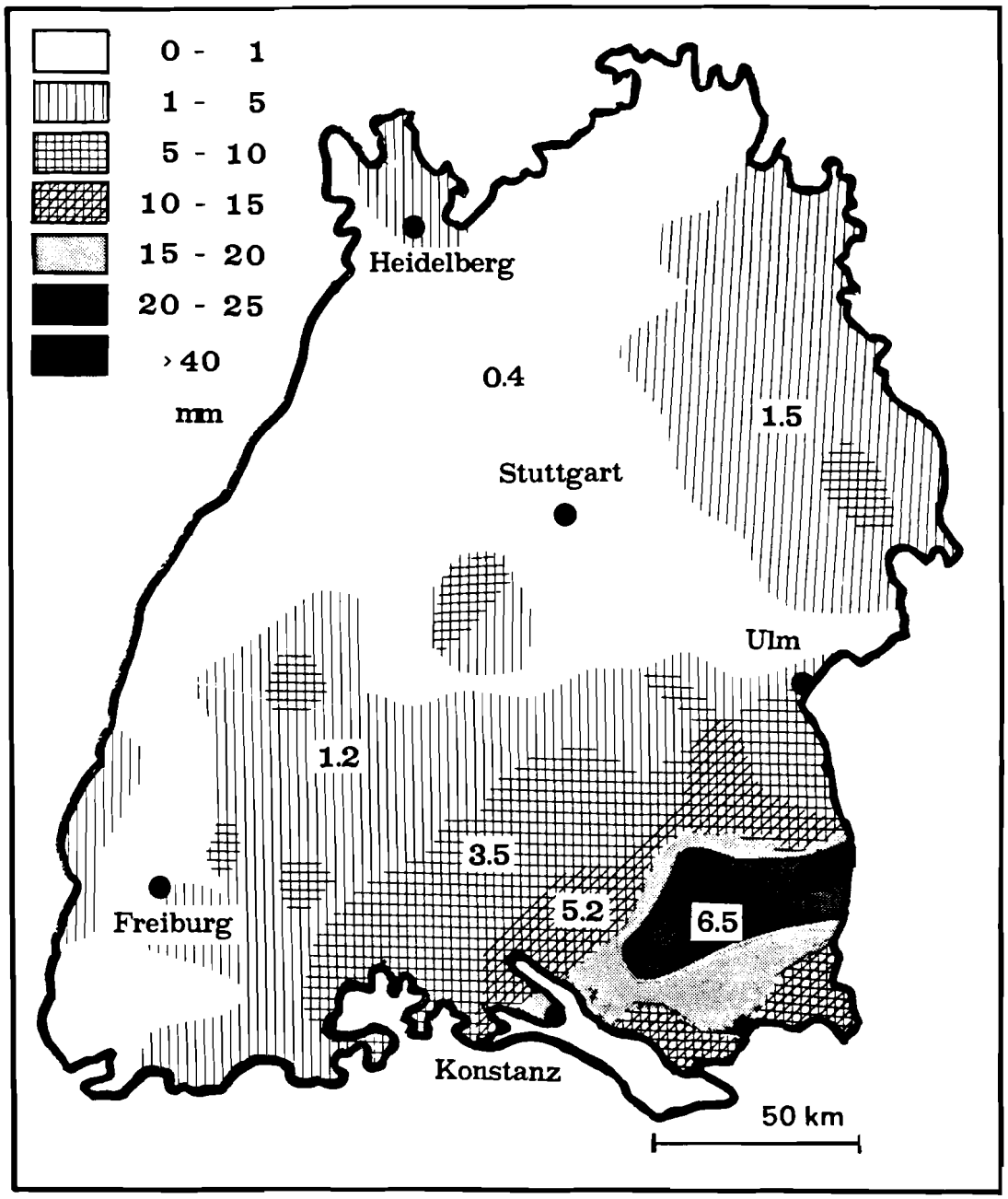
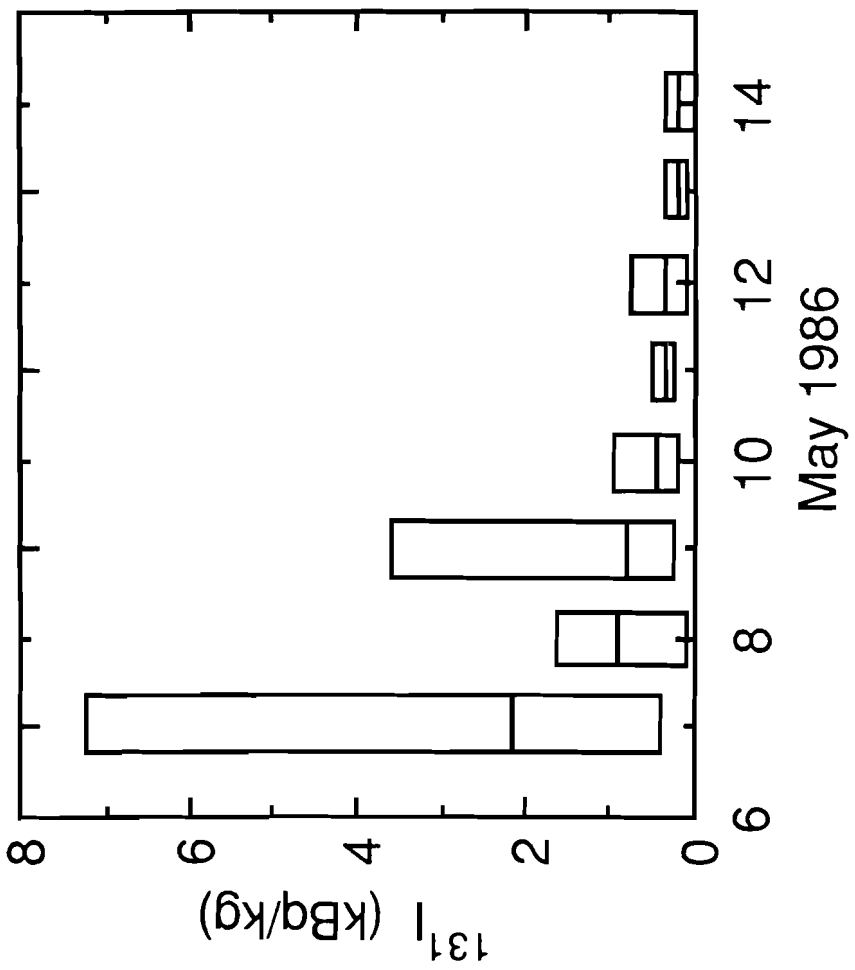

0 - 1
1 - 5
5 - 10
10 - 15
15 - 20
20 - 25
› 40
mm
Heidelberg
0.4
1.5
Stuttgart
Ulm
1.2
3.5
5.2
6.5
Freiburg
Konstanz
50 km

Fig. 5



2. MANAGEMENT OF ENVIRONMENTAL CONSEQUENCES

2.1. RISK STRUCTURES AND PERCEPTION PROBLEMS

Prof. Boris Segerståhl
IIASA, Laxenburg, Austria

Introduction

"Bhopal", "Chernobyl", "Basel", to name a few of the serious technological accidents of the last decade, have become symbols of the destructive and catastrophic potential of modern technology. In addition to pollution risks, these accidents have generated a credibility gap over the risk associated with several modern technologies. An early topic in risk research was quantifying the probability of environmental and public harm from technological activities, and ordering risks and priorities for their reduction. The problem of main concern today seems to be how societies can cope with the large scientific uncertainties in the consequences of their actions. The numbers estimating risks are important for technical design purposes, but of limited relevance for policy setting.

Risks are far reaching in the world of today. Accidents such as those at Chernobyl or in Basel have created an acute need for international cooperation on risk and crisis management. Traditional organizational procedures are not adequate in handling large-scale emergencies. Too many organizations are involved; no common command structure can be established; common goals are vague or nonexistent; the time frame involved is too large; economic, political and social conflicts emerge; the dynamics and structure of the event as a whole is not understood.

Our purpose here is to draw a preliminary sketch of the systemic structure of a large-scale crisis management system. We don't give a recipe for a management system design. That would be futile as all new disasters are unique. We try, however, to point out a few basic facts about the structure and interactions in a typical, more or less ad hoc, crisis management system with special emphasize on the characteristics of risk perception.

Dimensions of the system

We start with a few definitions to indicate how the total system can be structured and analyzed. There are many dimensions to the problem and no commonly accepted terminology exists. The terminology used in this paper is not in any way definite. It is, however, an effort to create internal consistency in this presentation. We will look at three different dimensions of the system - time, type and actors.

Time. The event which is the object of our investigation is called a **disaster**. Over time a disaster goes through different stages:

- Pre-catastrophe
- Catastrophe
- Crisis
- Reconstruction
- Monitoring

The first stage - pre-catastrophe - is often neglected in crisis management systems. The reason is simple: you never know about a catastrophe before you are in the middle of it. One common fact should, however, be noted. In many cases the transfer from normal operating conditions to a catastrophe is not direct. The prelude to a disaster is often a period of maintenance, testing, changes in operating procedures, or other activities which cannot be considered as an integral part of the steady state operation of the plant. In Chernobyl the accident was triggered by badly planned tests and ignorance of safety requirements. In a recent train accident in Sweden the accident was preceded by maintenance of the safety and signal system.

To use an analogy from the military environment; instead of either having normal operating conditions - complete peace - or a catastrophe - war - a military organization uses a sequence of alert levels. This is routinely done on airports when a plane has to land after having reported abnormal operating conditions. A system of alert levels automatically introduces a system of checks and clearances for non-routine activities in an industrial plant. This type of pre-catastrophe alertness can eliminate the accident in some cases. When an accident occurs the preparedness would be better and consequently the damages should be smaller.

Pre-catastrophe conditions are easy to identify when an accident with possible but avoidable catastrophic consequences has occurred. One well known case is the Mississauga evacuation in Canada. The accident itself never reached the proportions of a catastrophe, but the evacuation of more than 220,000 people took on all the characteristics of a crisis.

The catastrophe stage ranges over anything from ten seconds to several days. The border line to the next stage is fluid. One way to identify a transition from catastrophe to crisis is to judge whether there is any immediate unavoidable danger for loss of life caused directly by the original catastrophe. Another indicator showing that the catastrophe has mutated into a crisis is that outside agencies and organizations become involved and the geographical dimensions of the event have grown beyond what can be controlled by plant management. In the case of Chernobyl the crisis continued less than three months and was preceded by a catastrophe period ranging over five to fifteen days.

Reconstruction is on one hand technical and economic reconstruction of damaged property and structures and on the other hand rehabilitation of destroyed credibility including introduction of new regulations and standards. Part of the reconstruction after Chernobyl (excluding local work) was the passing of two international conventions prepared by the IAEA (International Atomic Energy Agency). These conventions define procedures and guidelines for early notification and emergency assistance in the event of a nuclear accident or radiological emergency - specifically, in the event of "a release of radioactive material which occurs or is likely to occur and has resulted or may result in an international transboundary release that could be of radiological safety significance" (4). Draft agreements on the conventions were signed in September 1986. The convention on early notification entered into force on 27 October 1986 and the convention on emergency assistance entered into force on 26 February 1987.

Type. There are many ways to classify technological risks. One of the more ambitious efforts to generate a taxonomy was done by Hohenemser and his colleagues (3) at Clark University. Risk taxonomies which order risks according to causes of hypothetical accidents, are not suitable for classification of disasters. For this purpose we suggest a classification which puts most of the emphasis on the physical and chemical characteristics of the catastrophe itself. One of several possible classifications according to type is:

- Contamination of large areas
- River and lake pollution
- Gas releases
- Explosions and fires

It should be noted that a particular disaster can exhibit, simultaneously or sequentially, characteristics from several of these types. In addition the characteristics of a specific disaster are different depending on the geographical position of your point of reference. In Chernobyl the catastrophe was an explosion and fire. In other European countries the crisis emerged as a consequence of large scale contamination.

The main reason for including a typology as one dimension of a crisis management system is that it puts the system on a fast learning curve. A complete classification system has to include several stages of refinement. After an indication that gases have been released a need arises to determine whether the gases are heavy or light and what the concentrations and toxicity levels are. This information guides protective measures for the crew working on the site of the catastrophe. Combined with meteorological data the information gives a basis for the team which has to make the most difficult decisions of all in an emergency. Should an evacuation be ordered? And if so: when, how, and what scope?

Actors. A minor or "routine" emergency is taken care of by the plant or company being affected. In a major disaster it is inevitable that several different societal actors become involved. The main actors are:

- Plant and company staff
- Fire departments, police, military, hospitals
- Industry, insurance companies
- Government and local agencies
- Regulatory agencies
- Press and TV
- Political system and general public

To organize coordination and communication between these actors is a formidable task. In many cases the structures are semi random and nondeterministic. It is natural that nobody is completely in control in a large-scale crisis management system. The control function is with the plant staff during the first stage of the catastrophe. This control will be transferred as soon as fire departments and police are on site. After a crisis has replaced the initial catastrophe, events can occur rather randomly depending on the power structure in society as a whole and on the regulatory framework. The importance of a well designed regulatory framework is not in its ability to provide exact rules but in its ability to create predictable patterns for interaction among different actors in the crisis management system.

System structure

The general structure of the system is shown in Figure 1. The system is driven by the case specific information available. The structural behavior of the system is influenced by earlier experience, the general knowledge base available, and by the regulatory framework within which the activity takes place. As a vertical structure the system is straightforward:

- Identification
- Assessment
- Decisions
- Communication
- Perception
- Actions and reactions

It is, however, clear that the system behaves in a nonhierarchical manner. Connections between levels are created, bypassed, and destroyed depending on the dynamic changes in the overall situation. The situation is further complicated by the fact that analysis and management of a large-scale disaster cannot be based on the assumption that only one system is in operation. In cases where several countries are affected, each country has its own system. The connections between national systems is one of the main problems for efforts

to manage a disaster efficiently. These connections between parallel systems exist mainly on the communication level. It is obvious that coordinated connections on several levels might be preferable in an ideal case. In reality temporary, and often informal, links between national systems are created for coordination of decisions and actions.

Identification and assessment

Identification of the characteristics of a major disaster range from the immediate and trivial to the vague and confusing. The first indication that a nuclear accident might have happened came in western Europe when increased radiation levels were measured at the end

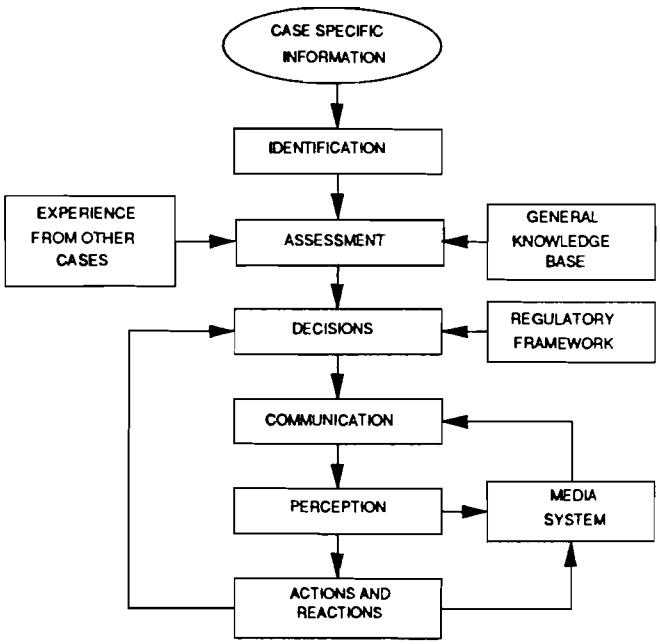


Figure 1: Structure of a risk management system

of April, 1986. At that time there was no clear information available from the USSR on what the source for this radiation might be. The identification process proceeds in parallel with emergency actions. Its main purpose is to serve as input for the assessment process which in turn creates a base for decision-making. The identification process is in the case of a nuclear accident to a large extent based on measurements. In addition, atmospheric transport models can be used to design an optimal monitoring strategy.

It became very clear after the Chernobyl accident that many countries in Europe were unprepared for monitoring of nuclear contamination on the scale required. Two problems dominated: a need for immediate information which lead to an overload on measurement systems and laboratories, and unforeseen problems with big local variations in contamination levels. The effect of rain on fallout was much higher than expected and lead to big local variations in contamination levels. A lot of confusion and distrust emerged as the system was unable to cover these aspects of the situation adequately.

From a management point of view two requirements are important for the identification process. National and international consistency have to be ensured. Varying standards and very uneven quality of instruments and professional skills in different countries have lead to repeated arguments concerning real radiation levels in different countries. The second requirement is, that the relevant substances are monitored and measured. In the case of the recent fallout in Europe this was no problem. From past experience it was known that cesium and iodine were the important substances to monitor.

We will not discuss the scientific aspects of risk assessment or the methodological problems and technical priorities, but concentrate on the problems which arise when this activity enters the emergency management process.

Experts are in a very difficult position with respect to their credibility during an emergency - real or imagined - as has emerged in the last years. As pointed out by Krohn and Weingart in a recent paper (5), the expert has to represent a scientific "consensus" which has to be presented in the political context as fixed, irreversible, and final. This is the expert's chief contribution to the transformation of probabilistic knowledge into knowledge for political decision-making.

The situation is contradictory and clearly impossible. How can an assessment be fixed, irreversible, and final, when it has to be based on information which is vague, contradictory, and constantly changing. It is not possible to escape this dilemma with the knowledge we have today of the overall crisis management system. A serious effort is needed to create procedures which would enable us to harmonize the entire process.

Communication

The communication process and its deficiencies are at the core of much of the confusion and many of the conflicts which emerge during and after a catastrophe. Let us first separate between "professional communication" and "public communication". Professional communication is taking place between organizations and units collaborating in the rescue and salvage operations during a catastrophe and crisis. This type of communication follows established rules and procedures. It can be predefined, organized and rehearsed. This does not

ensure that the professional communication system functions properly in all situations. Incompatible equipment; confusion with radio frequency usage; overloaded switchboards which prevent telephone communication; conflicting terminology and many other problems create serious communication problems within the professional system.

The real quagmire is in the field of communication with the general public. This communication process changes with time and is dependent on local circumstances and culture. The public broadcasting systems can be included in the professional communication system during the initial stage - the catastrophe - of a disaster. Instructions to the public and unedited news bulletins from the management center are transmitted without distortion. This means in many cases that the messages are also transmitted without clarification.

The dialogue between crisis management staff and the public can break down within a few minutes when the mode of communication reverts to the traditional style where the media are expected to be the watchdogs and deliverers of the "real truth" . To this is added the confusion generated by the use of "concerned scientists" and other sources which see as their main objective to correct the disinformation spread to the public by the officials in charge.

Credibility and consistency are the two main requirements on communication to the public. It is often impossible to fulfil these requirements completely. Information becomes available gradually and leads to reassessment of the situation. As a consequence a need will arise to upgrade or downgrade the level of alertness which is required by the public.

Harry Otway (6) has made an important point in differentiating between two kinds of communication. The first is intended to persuade people to accept policies or technologies and the risk they imply; in essence it encourages passive compliance with the intentions of those providing the information. It is fundamentally manipulative. The second tells people how they can avoid or mitigate risks, or gives information which helps them to form their own opinions; it supports the needs of the audience rather than those of the communicator. The difference is subtle, perhaps sometimes more a question of intent than content, but with this choice between a technocratic or a democratic path, risk analysis stands at a crossroads.

After the Chernobyl accident, situations were observed where the intent of communication fell into the second category -- efforts to help the public form their own opinions; but due to several factors and specific circumstances the communications were interpreted as manipulation and turned out to be counter-productive. After statements by specialists on television that there was no need to take iodine pills, pharmacies were crowded with people buying these pills. The technical and professional implementation of communication strategies is still far from adequate and often looks like a sequence of trials and errors.

The public was at the center of what is sometimes called the "Chernobyl experiment." Assumptions about its behavior, however vague and unfounded, were also the basis for all measures planned and implemented after the accident. These assumptions should now be tested and conclusions drawn.

Perception

The way people perceive, order and react to risks is often a mystery both to scientists trained in the natural sciences and to decision-makers with a professional involvement in the control and management of a crisis.

While scientists rely on risk assessment to evaluate hazards and risks in an objective way, the majority of people rely on intuitive, subjective risk judgments. We use "subjective" and "objective" not as a way of indicating any superiority of one compared to the other, but as a way to stress the point that we deal with two different views of reality and of the relationship between scientific abstractions and real societal phenomena.

The difference between risk assessment and risk perception is often considered as being equivalent to the difference between knowledge (based on assessments) and belief (based on perception). The solution to this problem suggested by experts is to change belief into knowledge through a process of communication. Real world efforts in this direction have, however, a consistent tendency to fail.

Let us first make a few short comments on the philosophical foundation of this dichotomy. In philosophy the standard approach is based on the so-called *possible-worlds* approach first proposed by Hintikka (2). The idea is, that besides the true state of affairs, there are a number of other possible states of affairs, or possible worlds. Some of these possible worlds may be indistinguishable from the true world. A person is said to *know* or *believe* a fact if this fact is true in all the worlds he thinks possible. Possible-world semantics fail to model human reasoning in an adequate way because it assumes that a person is so intelligent that his knowledge is complete and closed under implication, so that if he knows fact *a*, and knows that this fact implies *b*, then he must know fact *b*. Hintikka calls this the problem of *logical omniscience*.

People are certainly not omniscient in real life. Possible-worlds proponents stress that this approach assumes an ideal and rational reasoner, with infinite computational power. Various approaches have been proposed to the theoretical problem stemming from the fact that our world is inhabited by non-ideal mortals. One approach is syntactic: a person's beliefs are described by a set of formulas, not necessarily closed under implication, or by the logical consequences of a set of formulas obtained by using an incomplete set of deduction rules.

Fagin and Halpern (1) have pointed out that previous efforts to solve the problem of logical omniscience have failed because they have ignored the fact that it arises from several different sources. Some of these are:

- Lack of awareness
- People are resource-bound
- People don't always know the relevant rules
- people don't focus on all issues simultaneously

The practical implication of work done in logic and philosophy is, that truth can be a multivalued function depending on where you stand and depending on your set of possible-worlds.

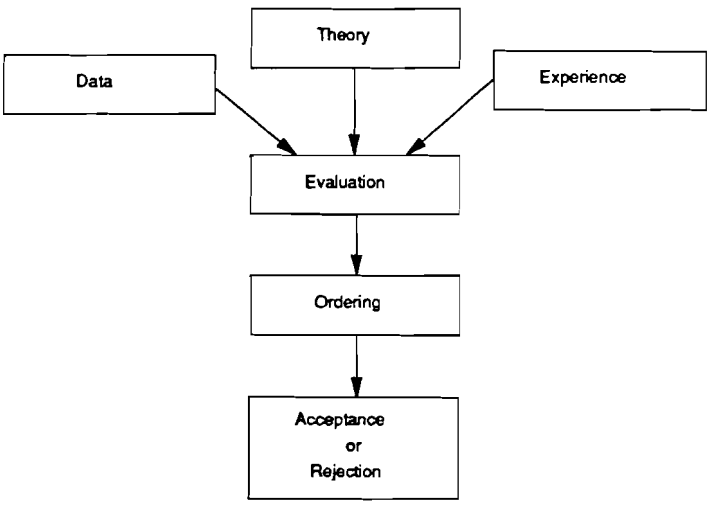


Figure 2: Model of evaluation process

Perceived risks are real phenomena. Even in cases where there is a substantial difference between assessments and perceptions there are valid reasons to take perceptions seriously. Let us mention one example. The value of land around a planned chemical plant is determined not by the outcome of probabilistic risk assessments, but by the perceived risk of the plant. It is difficult to imagine that a promotional campaign aimed at communicating results of risk assessments could have any noticeable influence on what developers are willing to pay for land in the immediate vicinity of the plant.

Research on risk perception is shedding more light on what people mean when they say that something is risky, and on what factors and processes underlie those perceptions. The basic motivation for this work lies in the fact that both for regulation related to health and safety and for crisis management, a better understanding of the risk perception process is needed.

The basic process leading to ordering, acceptance, or rejection of risks is indicated by the flowchart in Figure 2. In a risk assessment exercise done by experts evaluation is equivalent to e.g. probabilistic risk assessment. Risk perception is a more intuitive process of evaluation. It should be noted that even if assessment and perception are functions of data, theory, and experience, both the structure of the function, and the sources and structure of the inputs are different.

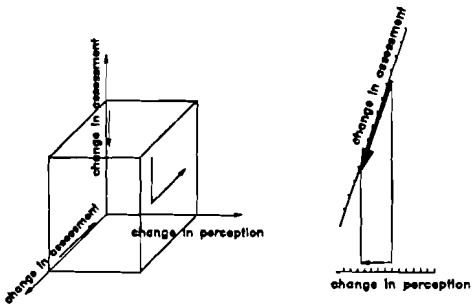


Figure 3: Assessment space and perception space

In **assessments** the generating function is based on theories derived from natural sciences and technology. Data is generated through experiments and statistics on component failures. Experience is imbedded in data and theory. In most cases it does not influence the assessment directly.

In **perception** we deal with a very fluid and to a large extent subconscious theory about society and technology. Perceptions are to a high degree invariant to data for the simple reason that the conceptual theoretical model used is more qualitative than quantitative. As a consequence of the structure of the imbedded theory, perceptions are very much dependent on experience - direct and indirect.

The facts mentioned above lead to a rather pessimistic conclusion. The theory behind risk assessment is quantitative while the theory behind risk perception is qualitative. An assessment is highly dependent on data while data is of minor relevance to the formation of a risk perception. Risk assessments use experience indirectly while risk perception is strongly influenced by experience and personal, empirical evidence. As a consequence evaluation

and ordering based on assessments can be expressed as vectors and semiordered sets in an assessment space while evaluation and ordering based on perception are vectors and semi-ordered sets in a completely different perception space.

Substantial movements in the assessment space can go unnoticed in the perception space. This is illustrated by Figure 3. Risk communication can according to this model be considered as a transformation of dimensions and movements in the assessment space to corresponding dimensions and movements in the perception space. In an extreme the assessments and perceptions form orthogonal hyperplanes. This is equivalent to a manifestation of mutually excluding concepts of rationality in the group representing assessments and the group committed to perceptions. It should be emphasized that the words "assessment" and "perception" in this case have to be interpreted as labels of identification for different approaches without indicating superiority of one over the other. What has been stated here is to vague and intuitive to offer more than a starting point for more thorough investigation. It is, however, obvious that a firm fundament of theory is required before the relationship between assessment and perception is well understood.

The situation is recognizable in work on risk perception. Risk analysis describes the impact of an event in terms of direct or indirect, short- or long-term harm to the population. Risk perception seems to be more concerned with what Slovic (7) calls the signal potential of an event. The signal potential of an event, and thus its potential social impact, appears to be systematically related to the characteristics of the hazard and the location of the event within a factor space defined by one factor labeled "dread risk" and one factor labeled "unknown risk."

Slovic is actually working with a multidimensional perception space which he then tries to reduce to a two-dimensional hyperplane in the way described above. A more complete list of words describing the (not orthogonal) dimensions in this example of a perception space is: *observable, known to those exposed, effect immediate, old risk, risks known to science, controllable, not dread, not global catastrophic, consequences not fatal, equitable, individual, low risk to future generations, easily reduced, risk decreasing*. At the other extreme on the scales of these dimensions we find the opposites of the expressions listed.

Slovic gives a list of thirty risks ordered by four different groups. The list is given for reference in Appendix 1. Figure 4 shows in graphical form the variety of ordering given by the four groups. It is obvious that different groups give very different evaluations of relative risks. It can be seen from the chart that a broad trend exists. This means of course that the ordering is not completely random but is based on a common rationality expressed by the implicit use of theory, data and experience as mentioned earlier.

One important interpretation of the signal concept is that effort and expense beyond levels indicated by a cost-benefit analysis might be warranted to reduce the possibility of a "high-signal accident". Another important implication is that a reduction in the potential impact of an accident does not influence its position in the signal-factor space. If the wrong conclusions are drawn from these two implications, we are in danger of promoting policies which lead to very low accident probabilities while the impact of one of these very improbable accidents could be enormous.

The important implication for the crisis management framework into which we put risk perception is that communication is a translator between the "assessment space" and "per-

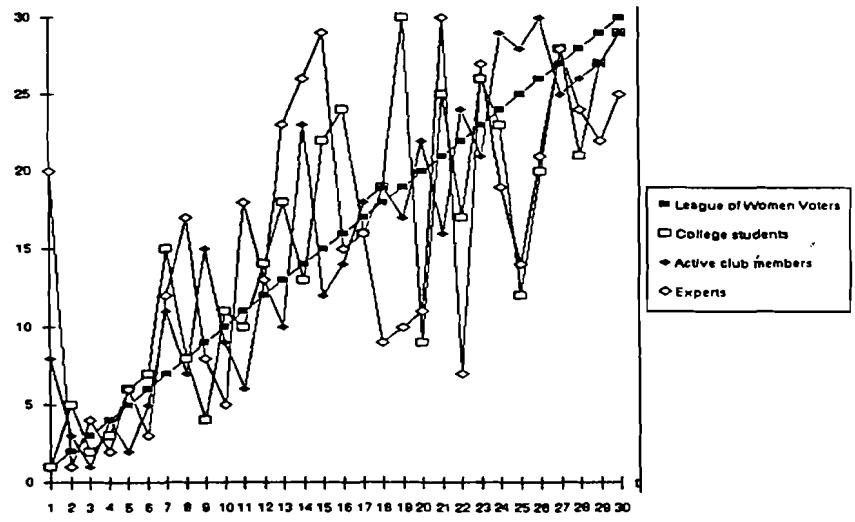


Figure 4: Ordering of risks by four groups according to Slovic (7)

ception space". If we learn how to do this translation, many of today's communication and credibility problems could be, if not eliminated, at least reduced to manageable proportions.

Actions and reactions

Actions and reactions occur as an integral part of the decision-making process when decisions are made and actions taken in the same organization. These actions are not being discussed here. Problems arise when a decision-maker has little or no control over the organizations or groups that should act (or refrain from acting) in accordance with his decisions. The general public can not easily be forced to act according to decisions unless

these decisions are perceived as being in the best interest of the individual person. If an evacuation is ordered the implementation depends to a large extent on the level of credibility transmitted through communications to the public. Unpredictable and counterproductive actions can follow on instructions from the authorities if there is a lack of credibility. The earlier mentioned example of pharmacies crowded by requests for iodine pills is a typical example of a situation where a reaction instead of a non-action followed a specific communication.

In extreme cases the reactions generate perturbations which affect the whole crisis management system. Staff changes and transfers of responsibility can be initiated through a political process driven more by demands from the public than by a need to minimize the effects of the disaster. All this boils down to the earlier mentioned need for consistency, clarity and credibility in communication.

References

[1] Fagin, R., Halpern, J.Y.: Belief, Awareness, and Limited Reasoning. *Proceedings of the Ninth International Joint Conference on Artificial Intelligence(IJCAI-85)*, Los Angeles, 1985.

[2] Hintikka, J.: Knowledge and Belief. *Cornell University Press*, Ithaca, NY, 1962.

[3] Hohenemser, C., Kates, R.W., Slovic, P.: The Nature of technological hazard, *Science*, **220** (1983), pp. 378-384.

[4] International Atomic Energy Agency: *IAEA Newsbrief*, Volume **1**, No. **1**, October 1986.

[5] Krohn, W., Weingart, P.: Nuclear Power as a Social Experiment - European Political "Fall Out" from the Chernobyl Meltdown, *Science, Technology, & Human Value*, Volume **12**, Issue **2**, pp. 52-68.

[6] Otway, H.: *Experts, Risk Communication and Democracy*, (Commission of the European Communities, Joint Research Center, Ispra Establishment, November 1986).

[7] Slovic, P.: Perception of Risk, *Science*, **236** (1987), pp. 280-285.

Appendix 1

Table 1. Ordering of perceived risk for 30 activities and technologies. The ordering is based on the geometric risk ratings within each group. Rank 1 represents the most risky activity or technology (from Slovic, 1987).

Activity or technology	League of Women Voters	College students	Active club members	Experts
Nuclear power	1	1	8	20
Motor vehicles	2	5	3	1
Handguns	3	2	1	4
Smoking	4	3	4	2
Motorcycles	5	6	2	6
Alcoholic beverages	6	7	5	3
General (private) aviation	7	15	11	12
Police work	8	8	7	17
Pesticides	9	4	15	8
Surgery	10	11	9	5
Fire fighting	11	10	6	18
Large construction	12	14	13	13
Hunting	13	18	10	23
Spray cans	14	13	23	26
Mountain climbing	15	22	12	29
Bicycles	16	24	14	15
Commercial aviation	17	16	18	16
Electric power (non-nuclear)	18	19	19	9
Swimming	19	30	17	10
Contraceptives	20	9	22	11
Skiing	21	25	16	30
X-rays	22	17	24	7
School and college football	23	26	21	27
Railroads	24	23	29	19
Food preservatives	25	12	28	14
Food coloring	26	20	30	21
Power mowers	27	28	25	28
Prescription antibiotics	28	21	26	24
Home appliances	29	27	27	22
Vaccination	30	29	29	25

2.2. ELEMENTS OF A NATIONAL EMERGENCY RESPONSE SYSTEM FOR NUCLEAR ACCIDENTS

Marvin H. Dickerson
Lawrence Livermore National Laboratory, California, USA

INTRODUCTION

The purpose of this paper is to suggest elements for a general emergency response system, employed at a national level, to detect, evaluate and assess the consequences of a radiological atmospheric release occurring within or outside of national boundaries. These elements are focused on the total aspect of emergency response ranging from providing an initial alarm to a total assessment of the environmental and health effects. Elements of the emergency response system are described in such a way that existing resources can be directly applied if appropriate; if not, newly developed or an expansion of existing resources can be employed. The major thrust of this paper is toward a philosophical discussion and general description of resources that would be required for implementation. If the major features of this proposal system are judged desirable for implementation, then the next level of detail can be added.

The philosophy underlying this paper is preparedness — preparedness through planning, awareness and the application of technology. More specifically, it is (1) establishment of reasonable guidelines including the definition of reference and protective action levels for public exposure to accidents involving nuclear material; (2) education of the public, government officials and the news media; and (3) the application of models and measurements coupled to computer systems to address a series of questions related to emergency planning, response and assessment. It is the role of a proven national emergency response system to provide reliable, quality-controlled information to decision makers for the management of environmental crises.

EDUCATION

Clearly defined reference and action levels should exist for various dose pathways expected from an accidental release of nuclear or toxic material. These levels should represent values below which there is no health concern, values above which there are health concerns, and an area in-between where discretionary actions may be appropriate depending on the circumstances of the accident and exposures. An example of these levels is given for nuclear accidents by the International Commission on Radiological Protection publication (ICRP) 40–which suggests 0.5 Rem whole body dose as the lower limit number where no action is required and 5.0 Rem as the upper limit above which protective actions would be required.

Once the reference and protective action levels have been established then the educational process should begin first with government officials not directly involved in establishing the reference and protective action levels, followed by the news media and then by the general public. The absolute values of the reference and protective action levels are not as important to convey to the public in the beginning as is the methodology used to develop the guidelines and plans for implementation during an accident.

As part of an education and training process the national center can be used to help plan and execute exercises and drills that test the components of the system. This process will help various government agencies to communicate with each other and interpret the advisories produced by the center.

TECHNOLOGY APPLICATIONS

Radiological Measurements

Three levels of ground based environmental monitors used for measuring airborne and deposited radioactivity are suggested for the emergency response system. These levels are national, regional and local.

a. National System. This is a real-time continuous measurement system with a centralized data collection, interpretation and data basing facility. The major purpose of this system is to provide a "first alert" for either a national or international incident that releases nuclear material. Through the use of modeling, climatology, land use and terrain studies a limited number of measurement stations can be located near facilities within the country that have a potential for an atmospheric release of nuclear material and in other areas for intercepting nuclear material crossing international borders. A minimal number of stations should be deployed and the number of parameters measured should be limited to a selected group to identify and initiate an alarm.

b. Regional System. The next level should be designed to supplement the national system, provide more spatial resolution, and quantify the measurements more than would be practical for a national real-time system. The regional systems should be developed and implemented by laboratories, universities or other responsible agencies under the supervision of a central governmental agency. These regional offices would be responsible for purchasing instrumentation, calibration and distribution to groups or individuals charged with making the measurements. Should an accident occur these regional centers would be responsible for monitoring the measurements, collecting the data, quality control and transmission to the central agency for further interpretation and inclusion in a master data base.

c. Local System. These systems would be designed to address local concerns particularly as they relate to more detailed definition of the space and time variability of material on the ground. The point of contact for calibration and data dissemination should also be under the control of but not necessarily in direct contact with the regional center. The path for information transfer between these measurement systems and the national agency in charge of the technical evaluation should

involve the regional centers. The national agency should insure that a standardized protocol is established for all radiological measurements e.g., time intervals, calibration, etc.

In addition to these ground based systems an airborne monitoring system supported and administered by the central authority should be available to (1) directly measure airborne material emitted from nuclear facilities within the country and (2) measure ground contamination caused by etiher an accident within or outside the country. Through a combination of these systems the environmental measurements aspect of emergency response can be handled efficiently.

Meteorological Measurements

Two levels of meteorological measurements are suggested for an effective emergency response system. These levels are national and local.

a. National System. This system is normally in-place and is managed by a national or federal meteorological service. In most cases hourly or 3 hourly surface wind speed and direction, temperature, pressure, humidity, visibility and cloud cover observations are reported through the national network to a central office. In addition, 6 or 12 hourly vertical profile measurements of windspeed and direction, temperature and moisture are reported through the national network. A computer link from the national meteorological service to the central government agency responsible for estimating public health effects would be required. Agreements and procedures should be developed to increase the measurement frequencey, if required, for an accident assessment.

b. Local System. Each nuclear facility within a given country should provide a meteorological measurement system located near the facility to provide wind speed and direction and temperature data. In case of an accident these data would be used to define the path and diffusion characteristics of material as it moves away from the nuclear facility into a regional transport and diffusion regime defined by the national meteorological network. Data from these local sources would be required at the government facility responsible for assessing public health and safety as well as the local facility changed with implementing immediate actions to protect public health.

Modeling

The intent of the atmospheric transport and diffusion modeling aspect of this proposal is to act as a planning, real-time response and assessment tool (analysis) when effectively integrated into the national emergency response system.

a. Planning. For areas around specific facilities, e.g. nuclear power reactors, modeling can be used in conjunction with land use and climatology studies to define measurement locations that have a high probability of intercepting material released from a particular nuclear site, thus limiting the number of instruments required. (e.g., the state of Illinois, USA, has an excellent monitoring system around each nuclear power plant site in the state). In addition, if the same or similar model is used for the emergency response, then emergency response managers and staff

members have the benefit of familiarity with the techniques employed for assessments. This planning activity also can help insure a compatibility between models and measurements, e.g. averging times of measurements that are suitable for comparing to model calculations. A similar study, on a larger national scale, can be used to define measurement locations for intercepting material, released in other countries, that has crossed the border and poses a potential threat to public health and safety.

b. Real-Time Emergency Response. Models should be developed or transfered to a central agency's computers that can provide the following functions to the emergency response manager or decision member during an emergency:
   - Determine the amount of material escaping into the atmosphere (source term).
   - Provide guidance to measurement teams as to where measurements should be made.
   - Bracket potential consequences using normalized calculations.
   - Check consistency of measurements to determine possible extremes due to either measurement errors or unrepresentativeness of the measurements.
   - Interpolate and extrapolate measurements.
   - Provide updated time integral for total dose.
   - Help implement protective action guidelines; if needed.

c. Assessments. After an accident has terminated the government and the public need to know (through the news media) the total effects of the accident on public health and safety, and the economic impact. To help estimate the impact on public health and safety a combination of dose modeling and measurements is needed for a creditable assessment. The credible assessment should be made public by a single-government decision maker (e.g., Mr. Harold Denton, USA Nuclear Regulatory Commission, during the TMI accident). For a radiological accident this assessment amounts to estimating both individual and person-rem doses for the affected public.

Computers and Data Handling Systems

To integrate the components of a national emergency response system into a reliable service for public health protection requires the development and implementation of a computer network devoted to data collection and analysis, model simulations and the publishing of health and safety advisories. Such a system could be developed and implemented largely through the use of technology that is presently available from commercial computer and research and development organizations. Attributes of such a system should include:

- Real-time Data Transmission
- Data Basing Techniques
- Quality Control Measures
- Analysis Techniques
- Model Simulations

This system should focus on the integration of modeling and measurements through the use of modern analysis and graphical techniques.

ADVISORIES

The major output of such a national emergency response system is a series of health and safety and economic advisories regarding impacts associated with an industrial accident that releases radioactive (or toxic) material to the environment. These advisories should be easily understood by government officials and the public. They should be based on the established reference and guidance levels and provided to the public through the governmental agency charged with protection of public health. Close cooperation between governmental agencies responsible for the technical evaluation and those relaying the assessments to the public will ensure a consistent and informative information flow to the public sector through a single voice of authority.

OTHER USES

The national emergency response system can be used for other related purposes to enhance its utility beyond nuclear accident assessments. A natural extention of this system involves the direct inclusion of toxic chemical releases in the emergency planning, response and assessment aspects of the system. Although many features of toxic chemical releases are different than those for nuclear releases, many similiarities also exist. The release and atmospheric disperison of some chemicals can be modeled in a manner similar to that employed for nuclear material while other toxic substances, e.g. heavy gases, could require different modeling techniques depending on the particular physics/chemistry of the release conditions. On the other hand measurement techniques for detecting an array of different toxic chemicals is considerably more complex than techniques used to measure radionuclides.

Another extention includes monitors for measuring air concentrations of conventional pollutants which could be co-located with the national monitoring system. These measurements could be used to establish a baseline (background) for conventional pollutants, and then can be used in conjunction with models for future industrial planning and implementation studies.

The data base established by this system can be used for managing responses to other emergencies, e.g. earthquakes and fires. These data bases can also be used for the design and analysis of railways, communication systems and other studies requiring a knowledge of terrain, climatology, geography and river flow rates.

Acknowledgment

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

2.3. MANAGEMENT OF THE CONSEQUENCES FOLLOWING THE CHERNOBYL ACCIDENT IN AUSTRIA

Franz Schönhofer
Federal Institute for Food Control and Research,
Radiation Protection, Vienna, Austria

Summary:
========

The surveillance systems in Austria are described and a survey of data which were collected after the Chernobyl accident is given. The countermeasures taken by the Austrian Ministry of Health and Environmental Protection are shortly reported. Some aspects of the actual management and difficulties are discussed.

1. Surveillance Systems

In Austria two networks for surveillance of the environment with respect to radioactivity exist. One ("early warning system") is based on measurement of the γ-dose rate, the other one ("surveillance system") on nuclide specific analysis of aerosols, precipitation and other media.

1.1. "Early Warning System"

All over Austria 336 permanent measuring γ-dosemeters are spread (Fig.1). The measuring range is from natural acitivity (in Austria approximately 10 μR/h) to over 30R/h and is divided into eight distinct ranges. The actual range of the γ-dose rate is reported on line to "warning centers" in the respective county and to a "federal warning center". By this system information about the approximate distribution of the contamination of the country can be obtained and the external doses received by the population can be estimated.

1.2. "Surveillance System"

The fallout associated with the nuclear weapons tests in the late fifties and early sixties gave rise to the installation of a surveillance system for environmental radioactivity. In 1979 nuclides specific measurements were introduced for routine analysis. The aim of this system is to monitor the level of artificial radioisotopes in the environment on a long term basis, but also to detect any emission from nuclear power stations in the vicinity of the Austrian border and emissions from installations of nuclear medicine or Austrian research reactors. One important task was to be prepared for nuclear accidents or explosions of nuclear devices - which can only be achieved when having laboratories doing surveillance work continously on a routine basis.

The location of the sampling stations for aerosols and precipitation is given in Fig. 2, for surface water in Fig. 3.

2. Situation in Austria - first measurements of contamination

On the evening of April 28th, 1986 first informations about a nuclear accident at Chernobyl were spread by Austrian radio and TV. In the morning of April 29th first authentic informations about the contamination of air and ground in Finland and Sweden were obtained from the respective radiation protection institutes. Since information was given that the reactor was burning, contamination was likely to occur also in Austria at a later time and some kind of "first alarm" was given for increased alertness. In the early afternoon a small but significant rise of the dose rate in Vienna and north-eastern Austria was noticed as well as fresh fission products were detected in high concentrations in aerosols both in Vienna and Seibersdorf (south of Vienna).

2.1. Time dependency of contamination of the Austrian territory and regional distribution

Fig. 4 and Fig. 5 show the regional distribution of γ-dose rates in Austria from April 29th, 16 h until April 30th, 22 h. Since the dosemeters are nearly exclusively located in the vicinity of more densely populated areas and therefore mostly in flat land and valleys, the contamination situation in the mountains is not reflected. It can be easily seen that contamination starte on April 29th afternoon in the north eastern part of the country, heading to the south and then turning to west. Local showers during early morning on April 30th caused in several small areas in the south and south west heavy contamination. A second wave arriving on April 30th covered mostly the north and north west of Austria and added more contamination. Fig. 6 shows the observed daily maxima of the dose rates from April 28th to May 1st. (Note that the dose rate values for different grey

shades differ from those of Fig. 4 and 5 considerably. Heavy showers on May 1st in the northwest (in the county of Oberösterreich - Upper Austria) lead to the highest contaminations in Austria. Though more contaminated air masses conquered Austria the following days, the amount of radionuclides deposited was low compared with the decay of short lived fission products. After a maximum on May 1st and 2nd dose rates dropped and had reached values of less than 50 µR/h at all stations by May 25th.

From the data and the time dependency obtained it is obvious that high contamination of soil and grass occurred when the passage of contaminated air masses coincided with heavy rainfall. A comparison of the map of precipitation shows fairly good agreement with date from the "early warning system".

Fig.7 shows the dose rate at a station in north-eastern Austria. There no rain occured and only a small rise was observed. Two distinct passages can be seen as the result of dry deposition. In Vienna (Fig. 8) also two distinct passages of contaminated air caused rises, followed by a sharp rise on May 1st after a very brief rainfall. Overall only a four fold rise occured in Vienna though on April 30th the highest contamination of air in whole of Austria was observed (see 2.2.) - but it did not rain during the critical time. A different pattern is exhibited at the station on top of the mountain Sonnblick - 3105 m high, in the south-west of Austria (Fig. 9). After a sharp rise on April 30th another clear peak is observed on May 3rd and a small but significant rise on May 7th corresponding to passages of contaminated air masses at high altitude (see 2.2.).

2.2. Concentration of fission products in air

Already in the first test run of a high volume aerosol sampler on April 29th early afternoon in Vienna fresh fission products were detected in high amounts. In Seibersdorf south ov Vienna the concentration of gaseous radioiodine was determined to be about twice the aerosolbound one. In Fig. 10 the concentrations of J-131 and Cs-137 in aerosols in Vienna is shown. Clearly several distinct peaks can be distinguished,

the most prominent ones occurring on April 29th and 30th (the latter one was the highest value observed in Austria) and smaller ones on May 3rd and 7th. In Klagenfurt (Fig. 11), south of the Alps a completely different pattern was observed with a rise on April 30th, a much slower decrease and a small rise on May 7th.

2.3. Precipitation

Fig. 12 shows the concentrations of I-131 and Cs-137 in precipitation. The reference date is May 1st. The ratio of these radionuclides is in Bregenz, the most western sampling station completely different from the others. Due to lack of time more than 100 samples of a precipitation sampling network have not yet been measured.

As it has been shown above in the case of dose rates at the Sonnblick mountain (2.1.) the pattern of contamination was in the mountains different from that in the valleys and in flat land. This was confirmed by measuring rain and snow samples collected from different heights. Fig. 13 shows a logarithmic dependency at Rax, a mountain about 80 km south of Vienna. In other cases it could be observed that the contamination level rose with hieght, but decreased after a maximum again.

3. Conclusions from environmental data

During the passage of the radioactive clouds data on the contamination of air at eight sampling stations were available (with some delay), but information on the dose rate levels in and near the more densely populated areas was available at any moment. These data showed that the surface contamination of the Austrian territory was extremely inhomogeneous. The dose rates in excess to the natural background varied in Austria between 10 µR7h to 260 µR7h at maximum on May 1st. From both sorts of data inhalation and external doses for the population could be calculated.

4. Countermeasures

Soon it became evident that the by far highest contribution to the dose absorbed by the population was to be expected from ingestion of contaminated food.
At the time of the radioactive fallout grass had already grown in most parts of the country as well as the grazing season had started. Contamination of grass (or hay) results very quickly in contamination of milk especially concerning J-131 and (slower) in contamination of meat with radiocesium. Also fresh vegetables like spinach and lettuce were contaminated heavily by direct fallout and rainout.
According to the Austrian radiation protection law any needless exposure to ionizing radiation has to be avoided. The maximal permissible dose due to artificial radionuclides to the public is limited to 167 mrem per year. The Ministry of Health and Environmental Protection aimed in the first days after starting of the fallout to limit the dose by quick countermeasures toward values below this limit, though the radiation protection law is not strictly applicable in such a given situation. This was achieved in the first, socalled "iodine phase", by forbidding the sale of fresh vegetables and rigorous control of milk to ensure distribution of milk which was below the limit of 10 nCi/l for J-131 (370 Bq7kg). After about a month this problem was over because J-131 had decayed, but two weeks after fallout had started the concentration of Cs-137 and Cs-134 rose in milk. Due to direct contamination of leaves and transport within the plants, vegetables and fruits were contaminated. Different pathways as well as extremely inhomogeneous geographical and height distribution made extensive controll of food stuff necessary. Limits were set. Difficulties in export arose and with respect to some fruits and part of food a part of the production exceeded the given limits. All the following measurements and results on environmental and food samples as well as description of all problems arising cannot be discussed here and are not the aim of this paper, because what can be regarded as the acute crisis was over after about two to four weeks.

5. Management of the consequences - difficulties

(The following remarks reflect the personal view of the author who has been involved partly in compilation of data and providing basis for decisions of the Ministry of Health and Environmental Protection as well as performing measurements and has compiled the official report on the impact of Chernobyl on Austria.)

From the description above it can be seen that some unofficial warning from other countries was obtained, that the contamination situation was very quickly known, that lots of data were available on the distribution of various radionuclides in environmental samples as well as in foodstuff. Excellent equipped laboratories existed with enough capacity to handle large numbers of samples. One problem was that all laboratories were situated in the east and south and transport of samples provided difficulties. For handling the consequences of the Chernobyl accident, this was only a basic requirement which was not at hand in all affected countries. Not lack of measuring capacity or too little information and data caused severe difficulties but a great variety of factors in the field of communication, data transmission, evaluation and political problems, not at least public opinion and psychological problems. In order to analyse this some basic aspects of the consequences of the Chernobyl accident have to be considered.

Reacting to a given situation involves several steps and many preconditions have to be fulfilled for effective management of a crisis. Both national and international aspects have to be considered in a case like the Chernobyl accident.

In order to react one has to find out first of all, what the situation is like. After careful analysis and assessment of possible consequences in all respects there has to be decided whether countermeasures are necessary and justified - not only health aspects have to be considered, but also aspects like public opinion, economical and political consequences. In case of a decision for countermeasures, the

most difficult step is to decide w h i c h ones have to be taken. The same aspects as above apply in this step. A fourth step is to cover all problems which arise from countermeasures and to decide when they should be abandoned.

5.1. Aspects at international level

The Chernobyl accident showed that an international warning system would have been of great advantage - concerning information about the fact that a severe accident occurred as well as regarding the necessity of more accurate information about the circumstances. Consequences could have been estimated to some extent for other countries in advance and more time for preparing for decisions would have been available. Informations about the contamination of Scandinavian countries were available soon, but informations came first via massmedia (so many scientists did not believe them .....) or via private channels from collegues. Even if data were transmitted by official channels the question is whether the competent authorities were reached quick enough.

It can be concluded that at an international level the most important thing would be very quick and as comprehensive as possible information to the competent authorities or persons.

International cooperation could be imagined in the field of quick calculation of dispersion and deposition.

5.2. Aspects at national level

The existence of alarm systems, equipment and trained personnel provides a necessary precondition at a national level, but many more factors influence how a crisis like Chernobyl can be managed. Som of the factors which caused troubles not only in Austria should be mentioned.

All emergency plans which may exist can only assume certain types of accidents. In Austria emergency considerations were mainly directed towards an accident with a single release in a nuclear installation near the border or the case of a nuclear attack, both resulting in high contamination either in a limited area or a uniform high contamination

over the whole country. It was not possible to foresee a situation like Chernobyl - continous (and varying) releases over about two weeks, uncertain future weather conditions, which made any precise prediction of the development of contamination of air, soild and food impossible and as a result an extremely ununiform deposition all over the country. In this respect the lack of a rigid detailed emergency plan which could have been followed strictly was no drawback. The number of radiation protection experts within the authorities was too low, because no nuclear power station is operating in Austria and naturally the probability of a severe accident like Chernobyl had been regarded as too unlikely to build up a big emergency organization with continous preparedness only for a purpose like this. This lack could be overcome by special efforts of the people involved. But everybody has a limited capacity for work and simply needs some rest after days of continous work, not to talk about the difficulties which stess puts for personal communication and ability to judge a situation correctly. More "human factors" like several personal interests of people involved occurr. Data transmission and evaluation provided difficulties - simply because telephone lines were blocked by the public and because too many data were transmitted by too many people and organisatons it was difficult to sort out the relevant ones. By giving information to the public analytical work on important samples was hindered.

Difficulties with public opinion were clearly caused also by reports in the mass media, which gave the impression that risk was much higher than the authorities admitted. Easy to follow recommendations of the authorities to limit exposure to even lower levels were misinterpreted in the way that the situation was really very dangerous. The absolut correct mean values of contamination published by the authorities were doubted by several newspapers presenting data of selected samples from highly contaminated ares.

Different opinions of experts published by papers led to even more confusion of the public. "Experts" presented measurement results which were achieved with absolute unsufficient methods and instruments.

It can be concluded that the management of the acute phase during May 1986 was possible due to several circumstances: There was no acute danger, but it was even possible to reduce the absorbed dose considerably by rather simple countermeasures. Most difficulties could be overcome by the flexibility and personalefforts of the motivated and unselfish persons involved.

It is the authors point of view that avoidance of r i s k from radioactivity was only one part and aspect of the considerations which had to be taken into account. At least a similar important role played also economic, political and psychological considerations.

Fig. 1: Location of γ-dosemeters of the "early warning system"

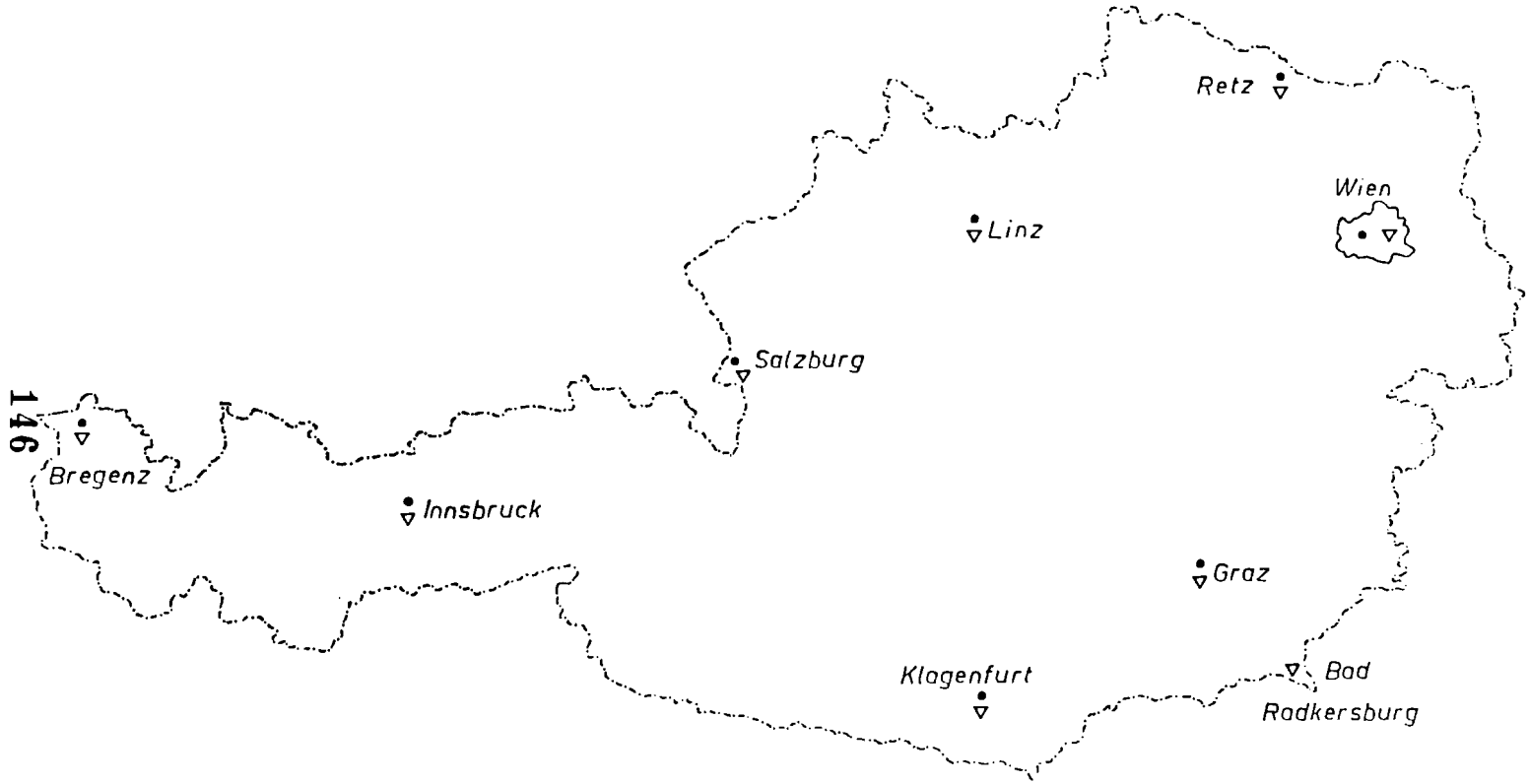


Fig.2: Location of sampling stations for aerosols (△)
and precipitation (•)

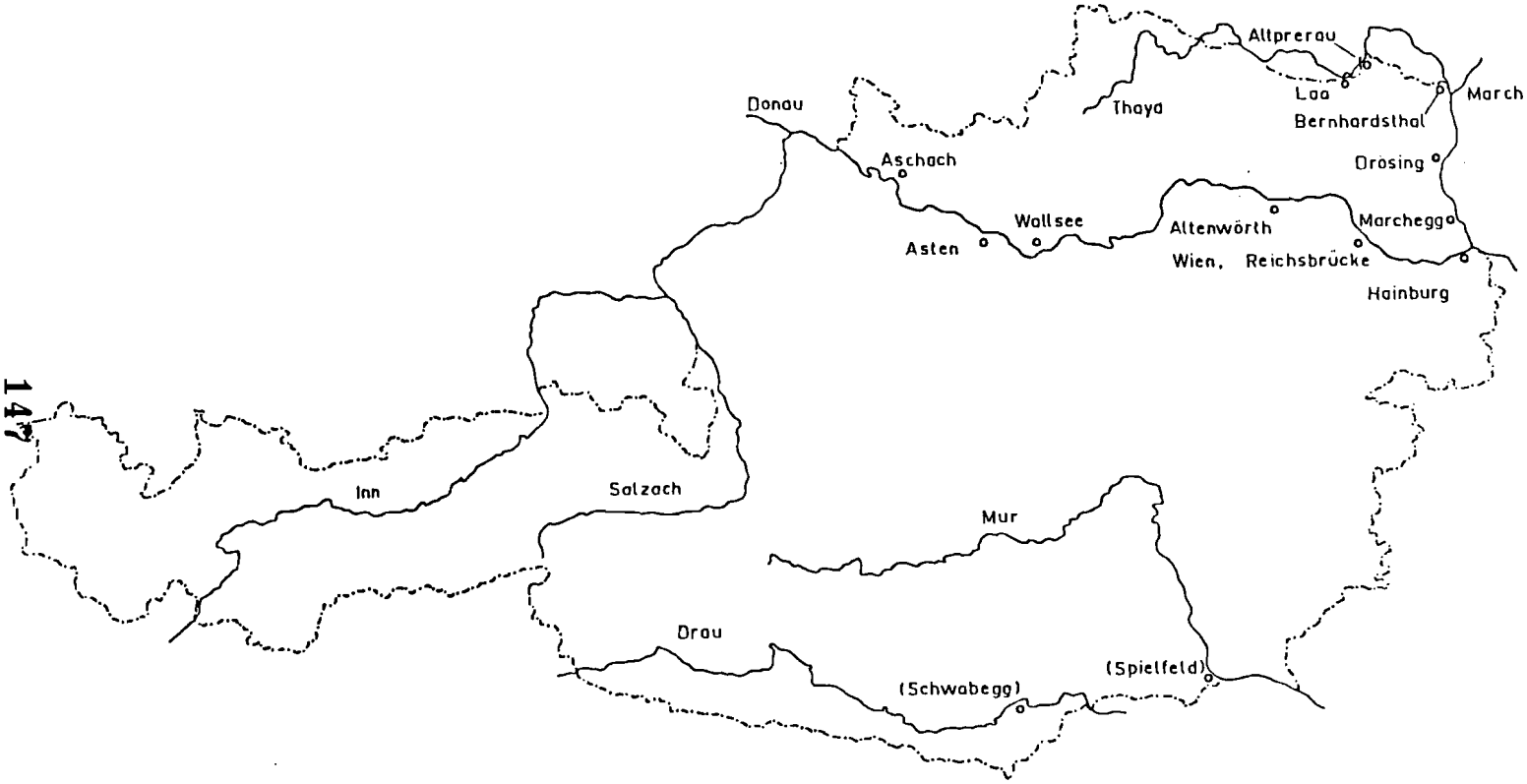


Fig.3: Location of sampling stations for surface water;
stations in brackets: not in operation since May 1985

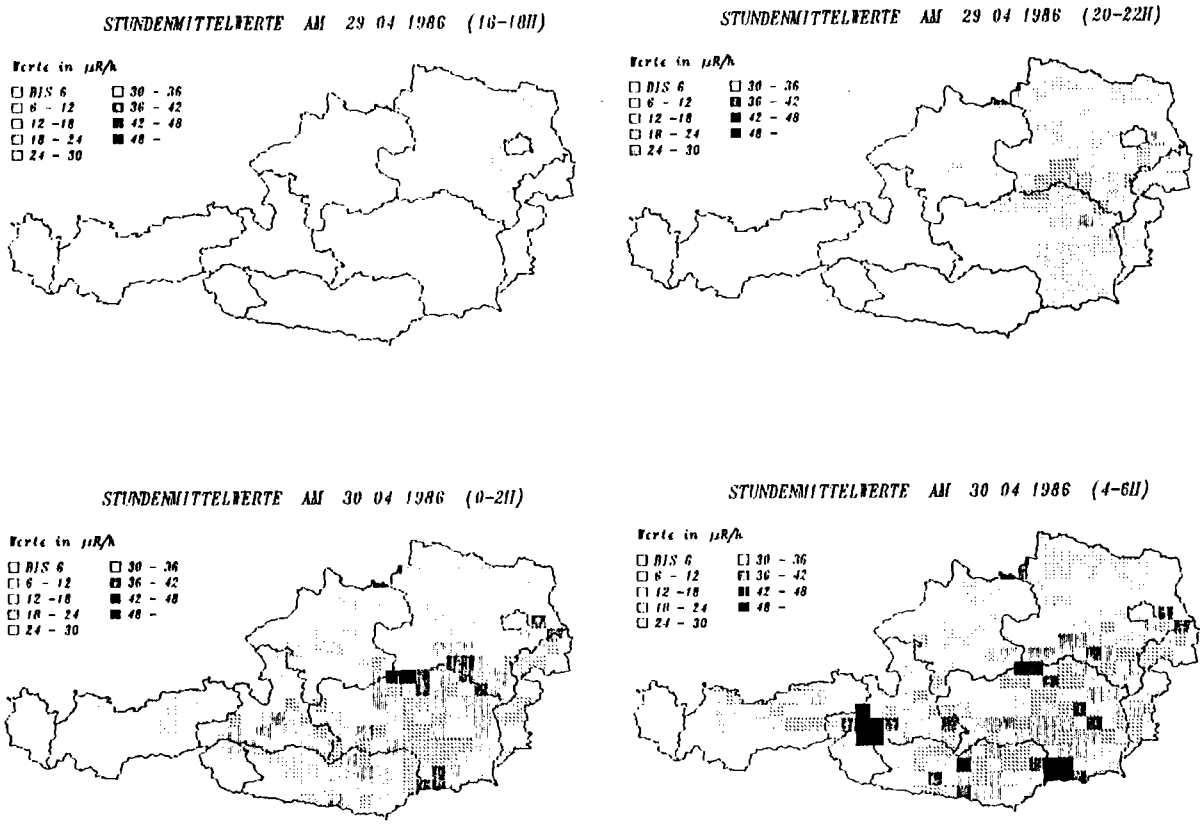


Fig. 4: γ-dose rate distribution in Austria,
April 29th, 16h until April 30th, 6h

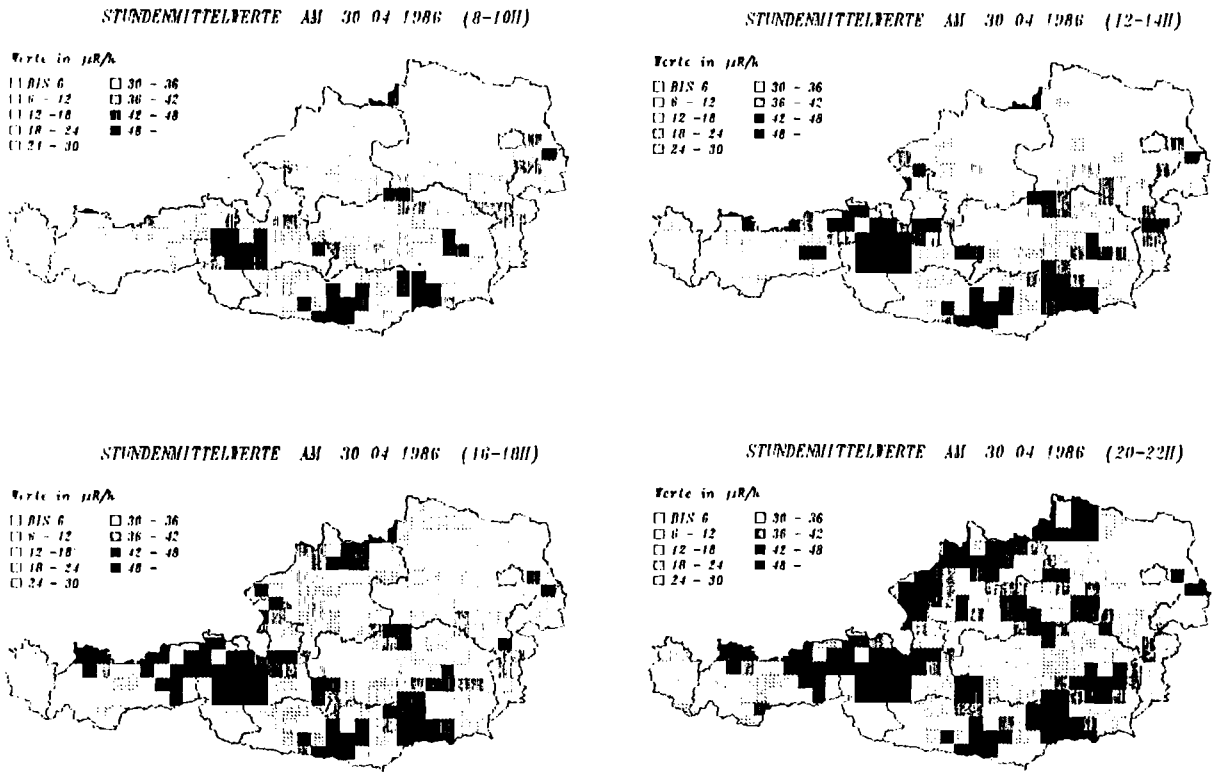


Fig. 5: γ-dose rate distribution in Austria,
April 30th, 8h until April 30th, 22 h

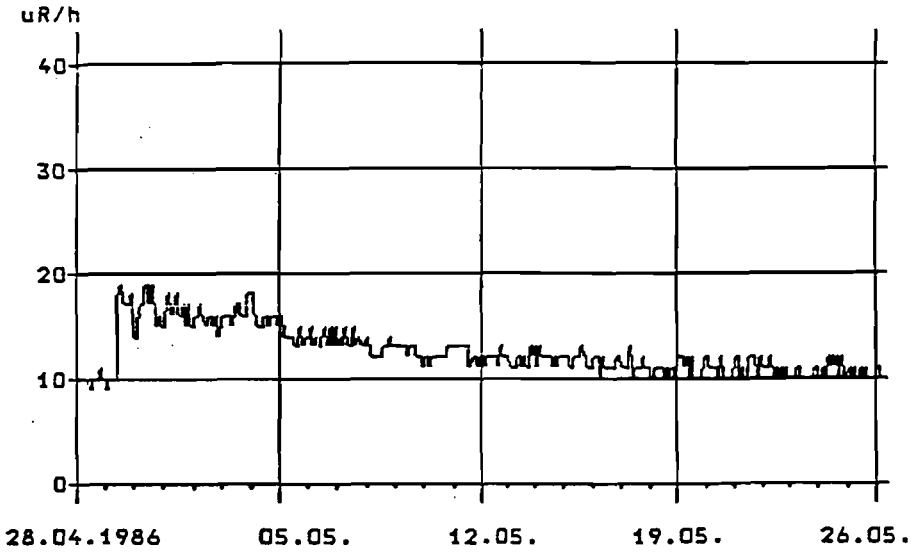


Fig. 7: Time dependency of dose rates at Poysdorf, north eastern Austria

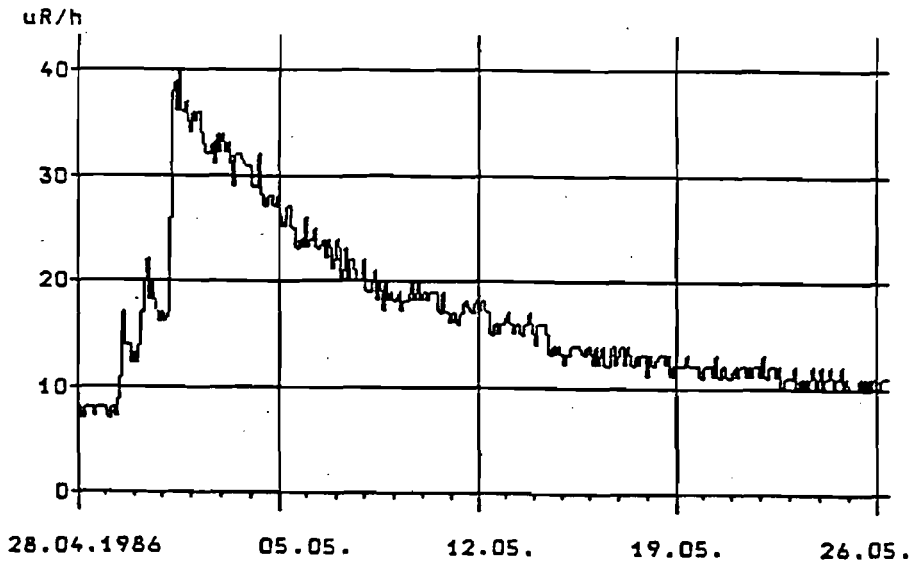


Fig. 8: Time dependency of dose rates in Vienna

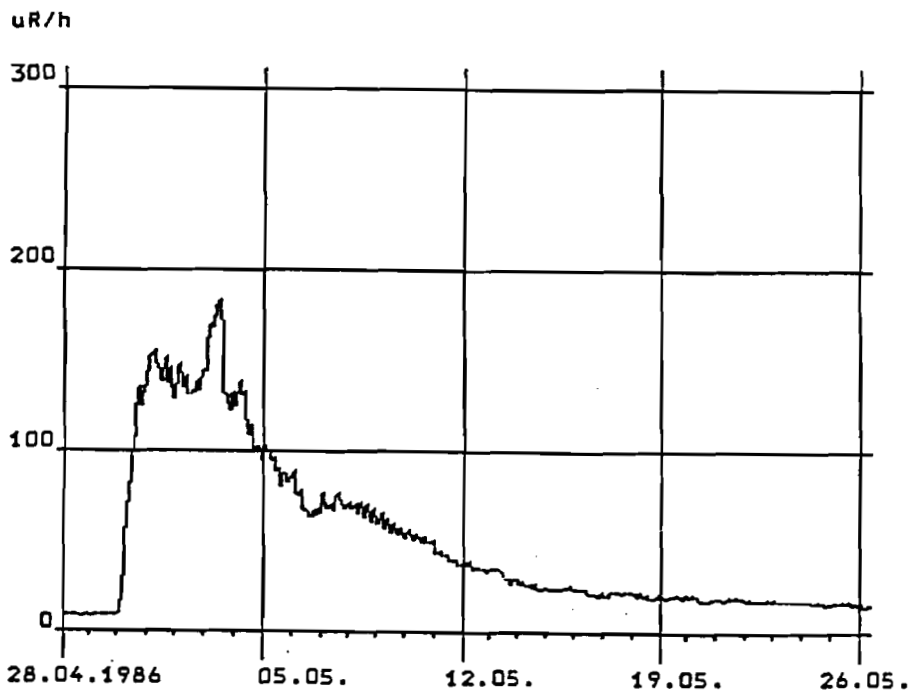


Fig. 9: Time dependency of dose rates at the mountain Sonnblick, south west Austria, 3105 m altitude

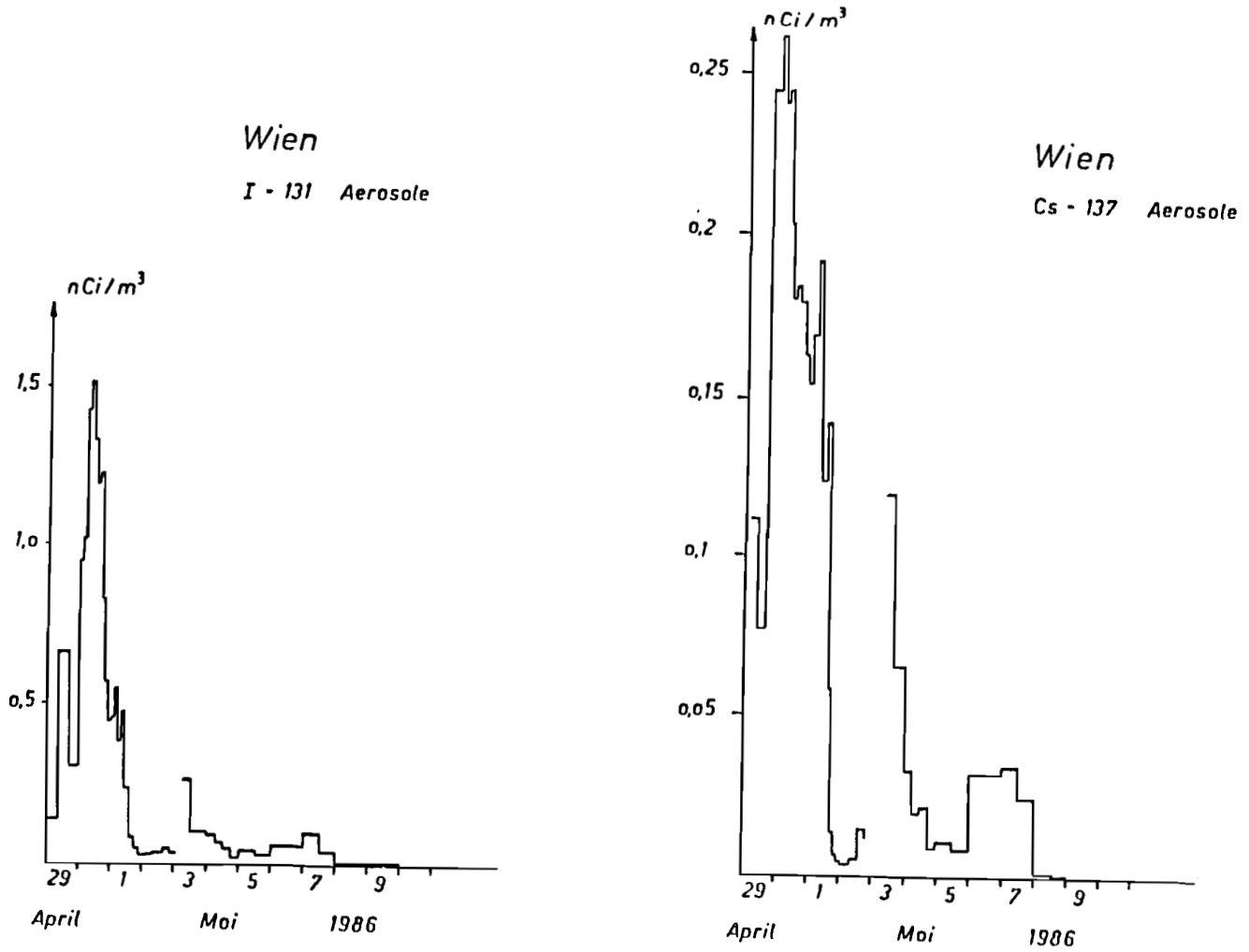


Fig. 10: Concentration of J-131 and Cs-137 in aerosols, Vienna

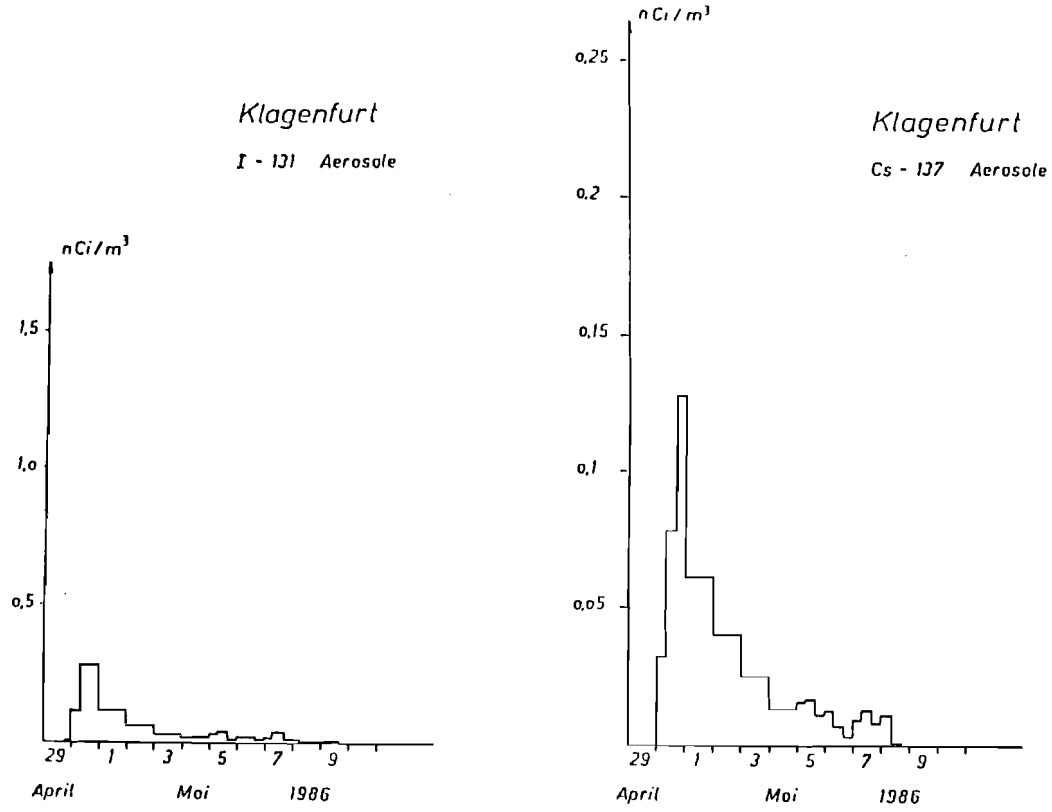


Fig. 11: Concentration of J-131 and Cs-137 in aerosols, Klagenfurt

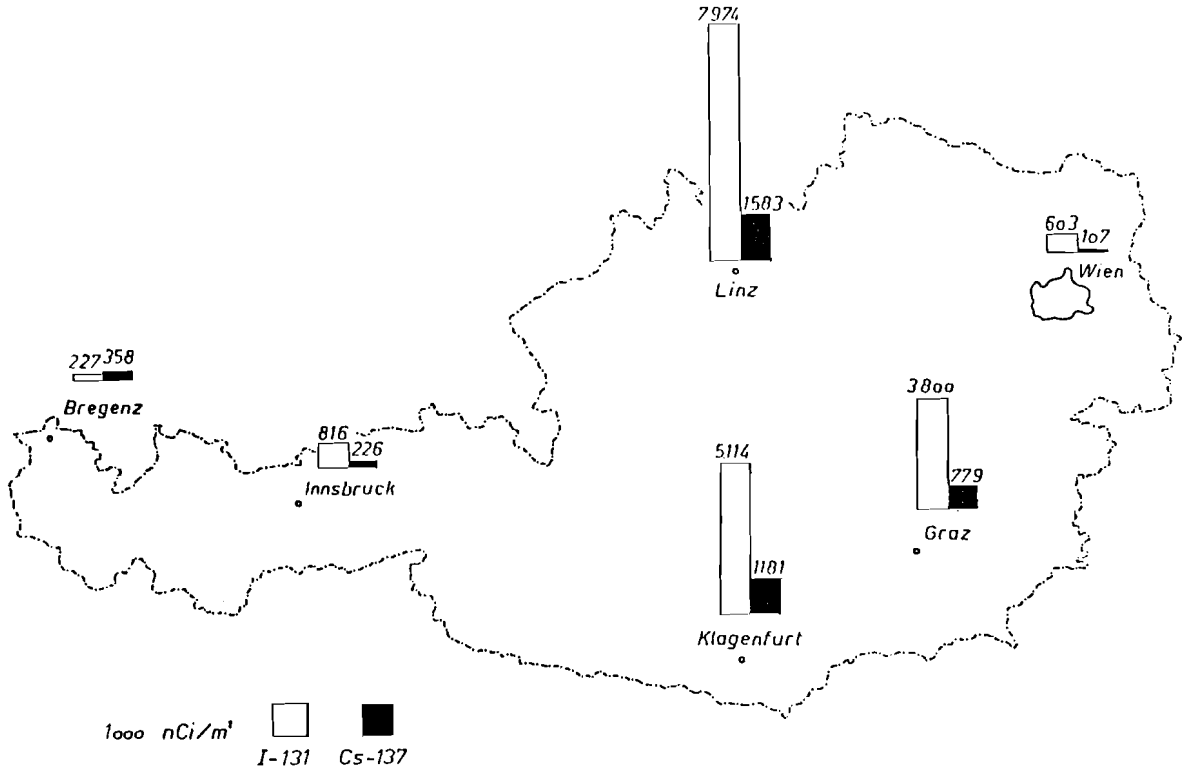


Fig. 12: Concentration of J-131 and Cs-137 in precipitation in nCi/m^2; reference date May 1st

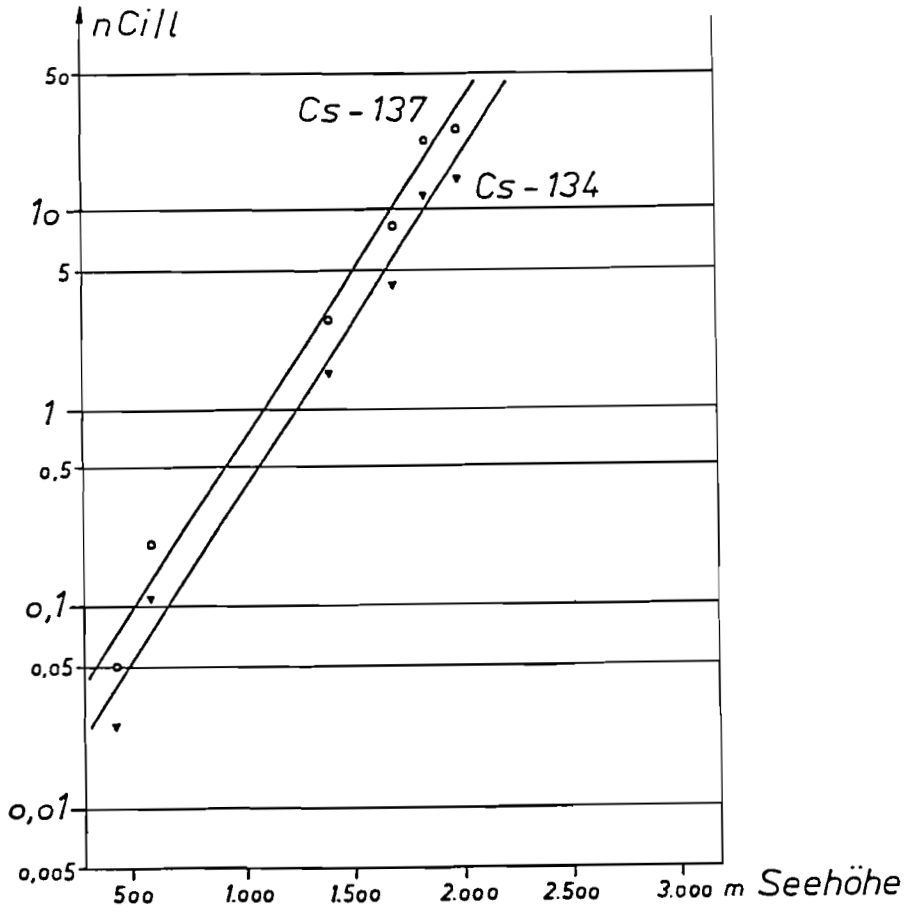


Fig. 13: Dependency of radiocesium contamination on height, Rax, May 4th, 1986

2.4. ENVIRONMENTAL ASPECTS OF NUCLEAR POWER

L. B. Sztanyik
"Fréderic Joliot-Curie" National Research Institute for Radiobiology and Radiohygiene, Budapest, Hungary

Introduction

Mankind was ever exposed to various harmful factors of the environment. He had to contend not only with natural catastrophes, but also with nutritional deficiencies, natural air and water pollutions, poisonous chemicals in mushrooms and many other foodstuffs, allergies to such agents as ragweed pollen, infectious and parasitic diseases. Technological development has brought some additional undesirable effects. The grim factory towns of the industrial revolution consumed men just as surely as the cotton fields and coal mines did /1/.

Every age has its own typical hazard.

Radiation is one of the modern environmental contaminants to arouse a general public anxiety. It is an unfamiliar threat that is unseen and unfelt, and worldwide in its distribution. It is a factor capable of causing acute deaths, inducing cancer in twenty or thirty years later, and even hereditary harm which may be expressed for many generations to come /2/.

This public anxiety is the main reason why the nuclear energy industry has paid an exceptional and exemplary - for other branches of industry - attention to the task of ensuring adequate safety and environmental protection from the very beginning of its development.

1. Acceptable risk of radiation effects

Risk is defined as a measure of the probability and severity of harm to human health. Nothing can be absolutely free of risk. A thing is safe if its risks are judged to be acceptable. This definition implies that two different activities are required for determining how safe things are: measuring the risk, an objective

but probabilistic persuit; and judging the acceptability of that risk, a matter of personal and social value judgement.

In radiation protection practice, acceptability of risk has been defined by the International Commission on Radiological Protection as follows:

"The Commission believes that for the foreseeable future a valid method for judging the acceptability of the level of risk in radiation work is by comparing the risk with that for other occupations recognized as having high standards of safety, which are generally considered to be those in which the average annual mortality rate due to occupational hazards does not exceed 10^{-4}."

"From a review of available information related to risks regularly accepted in everyday life, it can be concluded that the level of acceptability for fatal risks to the general public is an order of magnitude lower than for occupational risks. On this basis, a risk in the range of 10^{-6} to 10^{-5} per year would be likely to be acceptable to any individual member of the public."

In its basic form, the risk approach to setting radiation protection standards may be formulated as follows:

$$\text{Exposure limit} = \frac{\text{Acceptable risk}}{\text{Risk per unit exposure}}$$

Up to the end of the 1960's, it was established that some radiation effects /acute mortality, skin burns, impairment of fertility, etc./ had a genuine threshold so that they could be completely prevented by setting dose limits below this level. These are now referred to as non-stochastic effects, the severity of which varies with dose. No true threshold could be established for some late somatic and hereditary consequences for which the probability of occurrence rather than severity was regarded as a function of dose. The latter are referred to as stochastic effects. Of these, carcinogenesis is considered to be the chief somatic risk of irradiation at low doses and, therefore, the main problem in radiation protection.

The risk of stochastic effects per unit exposure has been adequately studied and established in human epidemiological studies over the past 25-30 years /3/.

The dose limits recommended by the competent international bodies are defined to provide absolute safeguards against all immediate, non-stochastic effects of radiation and to reduce the probability of delayed, stochastic consequences /cancer, leukemia, genetic harm/ to the level believed to be acceptable for workers as well as for members of the public.

2. Risk under normal operational conditions

In operation, a nuclear power plant produces huge quantities of radioactive substances. In order to limit the risk caused by these substances and their radiation to a level which is acceptable both for the workers in the plant and for the public at large, every measure must be taken to ensure that -

- the installation design provides adequate barriers to contain the radioactive substances produced and sufficient shielding to absorb the radiation emitted;
- the site selected is capable of receiving radioactive discharges without appreciable risk for the public;
- the construction and manufacture are in keeping with the design specifications and accompanied by appropriate quality controls;
- the safety requirements are carefully fulfilled during commissioning and maintained throughout the entire operation /4/.

The most important measures to be taken are:

- setting up protection standards,
- licensing of facilities and processes,
- regulatory control of activity,
- monitoring and maintaining surveillance,
- education of workers and the public.

In Hungary, dose limits for workers employed in nuclear energy applications and for the population at large have been established by the Ministry of Health with due account given to the fundamental principles of radiation protection laid down by the ICRP in its recommendations of 1977 /5/ and by the IAEA, ILO, OECD NEA and WHO in the Basic Safety Standards for Radiation Protection in 1982 /6/. Based on the dose limits, releases of radioactive effluents from the nuclear power plant into the environment have also been regulated. According to these regulations "external and internal exposures of any individual member of the public to radioactive substances released under normal operational conditions from a nuclear power plant of 1000 MW/e/ installed capacity must not result in an annual effective dose equivalent exceeding 0,25 mSv, of which 2/3 may be the contribution of airborne and 1/3 of liquid releases.

This approach relates the level of exposure /i.e. risk/ assumed by individual member of the public to the production of electric energy /i.e. benefit received by the society/ and also makes allowance for future developments /7/.

Monitoring of radioactivity in the effluents and the environment is the responsibility of both the nuclear power plant and the appropriate authorities. Of these, airborne discharges are controlled by the National Bureau of Environmental Protection and Nature Conservation, liquid discharges by the National Bureau of Water Economy, radiation levels and radioactivity concentrations in the environment by the Ministry of Health, concentration of radioactive substances in agricultural and food products by the Ministry of Agriculture and Food Industry. This state control is in fact independent of that of the operator and its primary aim is to ensure that operational controls are effected and to check that the results are satisfactory.

Data provided by the nuclear power plant itself, and by the competent authorities are collected and collated, processed, evaluated and stored by the Data Collecting, Processing and Evaluating Centre operated by our institute for the Environment-

al Radiation Protection Surveillance System of the Authorities /ERPSSA/.

According to the monitoring results of 1985, the total airborne release of radioactive noble gases, and particulates containing iodine and strontium isotopes constituted less than one per cent of the authorized limit. Gross beta activity of liquid releases did not exceed 10 per cent of the authorized limit. Release of tritium with liquid effluents amounted to about 9 TBq, which is somewhat more than 50% of the authorized limit /15 TBq/.

Maximum annual whole body doses received by individual members of the population in the surrounding area due to the radioactive discharges from the nuclear power station into the environment were calculated on the basis of monitoring data, prevailing meteorological parameters and with the use of the AIREM programme. The maximum individual dose of less than 0,35 uSv received at a distance of about 0,5 km from the site is a negligible increment in the annual dose of about 1 mSv received from natural environmental sources. The collective dose of the population living in the area of 30 km radius was found to be less than $0,55.10^{-3}$ man-Sv /8/.

Because of the system of control applied to environmental releases from nuclear power installations, doses to individual members of the public are generally well below the relevant dose limits and correspond to low levels of risk. Individual dose levels decrease rapidly with distance from a given source, therefore, values of collective effective dose equivalent per unit of electrical energy generated thus remain low /9/.

3. Risk in accidental situations

Despite all the precautions specified and imposed, the possibility of accidents arising from human error or defects in the equipment cannot be excluded by absolute certainty. During operations, nuclear plants can give rise to accidents of a perfectly conventional character. For instance, account must be taken of the risk connected with the handling of large

masses of water and steam at high temperatures and pressures. The specific feature of nuclear plants, however, is the possibility of damage caused by radioactive contamination of the environment from a serious failure /4/.

In the case of accidents and environmental contamination, when exposures may not be subject to control, the concept of dose limits ceases to be meaningful. Instead, other considerations arise, such as the need to balance the risk from radiation against the risks from particular countermeasures or interventions. The type of action which is effective in reducing the exposure of the population in these circumstances varies widely depending on local situations. The mitigation of exposure from environmental radioactive contaminants might require, e.g. sheltering, stable iodine administration, evacuation, or reorganisation of food supplies. In some circumstances such actions might have far reaching effects and impose new risks on the community, that could be predicted only very approximately in advance of their implementation /10/.

Temporary intervention levels for nuclear accidents were introduced in Hungary in 1980 and amended in 1985 /12/.

In a recent accident at the Chernobyl nuclear power station large quantities of radioactive substances have escaped from the damaged reactor and caused a significant environmental contamination over almost all of Europe. Some of the experiences obtained by us in the aftermath of this accident are summarized here briefly /11/.

In connection with the atmospheric nuclear weapon tests after the 2nd world war, an environmental monitoring network was set up in Hungary at the beginning of the 1960s. Since that time, airborne radioactivity has been measured by the National Meteorological Service, surface and drinking waters monitored by the National Water Authority, agricultural and food products by the Ministry of Agriculture and Food Industry, environmental levels of radiation and radioactivity in general by the Ministry of Health. Separate environmental monitoring systems were established around the Central Physical Research

Institute in 1959 and the Paks Nuclear Power Station in 1980. All these components and subsystems resulted in a nationwide monitoring network that is capable of detecting and measuring levels of radiation and radioactivity in the environment both under normal operational conditions and in accidental situations.

The radiological consequences of the Chernobyl accident were followed and assessed by this network under the supervision of a governmental committee made up of representatives of the competent national authorities and its advisory body /12/. The results of the environmental monitoring were regularly communicated to the IAEA, the Regional Office for Europe of WHO, and to the governments of the neighbouring countries since the 1st of May, 1986.

Trace amounts of I-131, I/Te-132 and Cs-137 radioisotopes were first detected in aerosol samples taken in the morning of 29 April. In the period of 30 April to 10 May, three subsequent peaks in aerosol activity were detected: between 30 April and 2 May, on 3-4 May and 7-9 May. In the area of Budapest, maximum concentrations of I-131 in aerosol and vapour were found to be about 4 and 10 $Bq.m^{-3}$ in the first peak, and about 2 and 7 $Bq.m^{-3}$ in the third peak, respectively. The second peak was only significant in the southern part of the country.

A fraction of airborne particulates and radioiodine vapour settled down to the ground surface by wash-out and dry-out. In accordance to the rainfall patterns of that period, significant fall-out activities were detected in the northern and north-western regions between 29 April and 3 May, while somewhat lower activities is the southern parts of the country on 8-9 May. From 10 May, the fall-out activity decreased to a negligible level. Correspondingly, the ground contamination levels as well as the gamma dose rates measured in free air at 1 m above the ground surface were the highest in the northern and north-western regions.

No significanct contaminations were detected in surface

and drinking waters. About 40 stations of the nationwide monitoring network and 10 specially equipped laboratories of research centres and universities participated in the control of agricultural and food products, particularly of milk, meat, fruit and vegetables. Similarly to the experiences obtained from the atmospheric and ground surface measurements, various regions of the country could clearly be distinguished from the point of view of contamination levels of food-stuffs. Maximum activity concentrations on vegetables were found on 3 May. In milk, the activity of I-131 reached maximum values between the 2nd and 12th of May, depending on the region concerned. Highest activity concentrations of Cs-134 and Cs-137 in milk were observed towards the end of May.

Based on the results of environmental monitoring of radiation and radioactivity levels, the following measures were taken and advices to the population given:

- the use of surface water from the Danube as a drinking water supply for Budapest was stopped,
- grazing of cows was prohibited for the large state farms and agricultural cooperatives,
- potassium iodate tablets were prepared and stockpiled,
- people were advised that intake of stable iodine preparations was unjustified and unnecessary,
- people were advised to consume milk and milk products collected, blended, controlled and put on the market by the dairy industry,
- people were informed that work and entertainment outdoors were safe and sheltering was unjustified,
- pregnant women were informed that the levels of environmental radiation and radioactive contamination were not high enough to justify artificial interruption of pregnancy.

Preliminary estimates of exposure show that radioactive contamination of Hungary from the Chernobyl accident has resulted in an average total /external and internal/ effective dose equivalent of about 1 mSv. This value may vary by a factor of 2 in both directions, depending on the age and location of the people concerned.

Conclusions

1. It must be kept in mind that not all hazards are manmade. Humankind was always exposed to natural threats, but it is true that technological development may bring some additional danger.
2. Risk is inseparable from life. It is important, however, that societal benefit attributable to a given practice should exceed the dimension of risk.
3. Further use of nuclear power as a major source of energy is dependent on the actions intended to maintain the highest possible level of safety under normal operational conditions and to improve capability for the prevention of accidental situations.

References

/1/ Lowrance, W.W.: Of Acceptable Risk - Science and the Determination of Safety. W. Kaufmann, Inc., Los Altos, California, 1976.

/2/ Pochin, E.E.: Man's exposure to radiation. In "Ecology, The Shaping Enquiry - A Course given at the Institute of Contemporary Arts." ed. by J. Benthal. Longman Group Ltd., London, 1972, 271-292.

/3/ Sztanyik, L.B.: Significance of human epidemiological studies for setting radiation protection standards /In press/.

/4/ Nuclear Energy and the Environment. EP/GE.4/R.27, 1979. A report drawn up by a Group of Experts on the Relationship between Electricity and the Environment. UN ECOSOC Economic Commission for Europe.

/5/ Recommendations of the International Commission on Radiological Protection. ICRP Publication 26. Annals of the ICRP, Vol. 1, No. 3 /1977/.

/6/ Basic Safety Standards for Radiation Protection 1982 Edition. Safety Series No. 9. IAEA, Vienna, 1982.

/7/ Sztanyik, L.B. Bojtor, I.: Experience in the application of the new ICRP recommendations in Hungary. In "The Dose Limitation System in the Nuclear Fuel Cycle and in Radiation Protection." IAEA, Vienna, 1982, 605-612.

/8/ Report of the Environmental Radiation Protection Surveillance System of the Authorities /ERPSSA/ on the year 1985. /in Hungarian/.

/9/ Ionizing Radiation: Sources and Biological Effects. UNSCEAR 1982 Report to the General Assembly, with annexes. UN, New York, 1982.

/10/ The evaluation of risks from radiation. ICRP Publication 8. Pergamon Press, Oxford, 1965.

/11/ Biró, T., Fehér, I., Sztanyik, L.B.: Radiation consequences in Hungary of the Chernobyl accident. Hungarian AEC, Budapest, July 1986.

/12/ Sztanyik, L.B.: Involvement of the public health authority in emergency planning and preparedness for nuclear facilities in Hungary. In "Emergency Planning and Preparedness for Nuclear Facilities." IAEA, Vienna, 1986, 159-167.

2.5. SOCIAL AND ECONOMIC ASPECTS OF SYSTEM SAFETY

Russell R. Dynes
Co-Director, Disaster Research Center
Professor and Chair, Department of Sociology
University of Delaware, Newark, USA

In modern societies, there is increasing attention given to the analysis of and the planning for emergencies. Emergencies, simply defined, are those events which cannot be dealt with by ordinary measures or routines. The notion of planning for emergencies has been more recently extended to disruptions in the socio-technical structures within societies. A good case can be made that such events derived from technological risks will become the "natural" disasters of the future. Even with the increasing concern with technological risks, however, there is still a tendency to examine them only as failures in the technical systems rather than to see them as embedded in various social systems, particularly those of the work force and of the community context of plants.

There currently exists a considerable body of knowledge accumulated over the last several decades which has been concerned with the social and behavioral aspects of emergencies. Even when the "causes" of the precipatating event differ, there is considerable uniformity in the response of social systems. Some of those uniformities will be identified here in

relation to response to technological risk. Of particular importance are assumptions which are made in planning. The whole notion of emergency planning, although oriented toward significant changes in the physical and material environment, is based on actions and activities in the social environment. Given that premise, there are certain persistent problems and principles which apply.

1. Planning for emergencies should be based on patterns of everyday routines. Most emergency planning anticipates new dramatic and unfamiliar situations. It also assumes that "emergencies" will be characterized by new and dramatic behavior and by significant social disorganization. In fact, the differentiation between emergencies and non-emergencies is often slight and requires social definition, not simply the observation of simplistic physical clues. Physical indications are initially usually "normalized" and discounted. Suspicious dial readings are attributed to malfunctioning of the dials, rather than to an accurate reading of internal malfunctioning of production. This also suggests that planning documents which make subtle distinctions between degrees of emergencies will often eventuate in attention being given to taxonomy rather than to the continual monitoring of threat.

A derivative of the principle is that, planning should be based on what people are likely to do in an emergency, rather than trying to get people to behave according to plan. By contrast, a careful examination of planning documents usually reveals that assumptions are built in to create radically new and unfamiliar behaviors. In addition, most organizational plans are oriented toward making the emergency most convenient for the planning organization.

2. Current models of emergency planning contain a number of problematic assumptions. Much emergency planning is predicated on the assumption that emergencies create severe disruptions in the social systems which reduce their capacity to effectively respond. Planning efforts then focus on the development of mechanisms to control maladaptive behavior and to create ad hoc structures to replace natural ones. Much of that effort is directed toward "strengthening" authority, since it is assumed that disaster agents severely weaken social structure and this needs to be overcome. The outcome usually created is some version of what is termed command and control. These structures are created to locate centralized communication and information systems to collect information which will allow for centralized decision making.

A more realistic behavioral assumption than the disintegrating effects on behavior by emergencies is the continuity of behavior. This means that the easy resolution of existing complexities in authority patterns will not be easily accomplished; that the centralization of communication may lead on the one hand to cause significant information to be lost in the new system and, on the other hand, to insure a rather meaningless information overload. In effect, a command and control model insures a "command post" view of the emergency which is more likely to be isolated from reality than it will be buffered from diversion. The fact that command and control models do not work well is usually attributed by their designers to the stupidity of the participants rather than to question the design. In the technological systems, just as in the complex environments of community systems, the focus would be on the design for coordination by feedback to various elements in the system, rather than by one directional information flow toward one isolated location.

3. It is important to give attention to a distinction between emergency planning and emergency management. It may be important to make this distinction even though there is an obvious relationship between planning and management. While poor planning inevitably leads to poor management, good planning does not necessarily lead to good management. The distinction intended here is similar to the one military makes between strategy and tactics. Strategy, in general, has reference to the overall approach to a problem, but tactics refers to situational adjustments which have to be made to achieve the objective. Most tactical elements, however, can also be anticipated. Of particular importance is a difference between agent-generated demands and response-generated demands. Not all problems stem from the effects of the "causal" agent, but many problems emerge from the response itself. Almost all major responses are multiorganizational, so this means there are a number of rather predictable emergency management problems with regard to the communication process, the exercise of authority and the development of coordination. Only one aspect of those response-generated demands will be mentioned below.

4. What is useful organizational information is not necessarily useful public information. Many organizations which have responsibility for industrial processes which can create risk, often see and plan as if the "public" were outside the emergency system. Consequently, they often issue public statements and official information which is devoid of relevant information for the public. The statement to evacuate a particular geographical area is often lacking with ideas about the extent of the danger, what is required in evacuation, and where it is safe to relocate.

While that type of information may exist in the notifying organization, the public is often forced to develop that information on their own to make relevant decisions for their own behavior. The issue shifts from "why don't people pay attention to my messages," to "how can we communicate messages which provide meaningful and useful messages to stimulate action" on the part of the public. While a plant can be seen as a system, it is also part of a number of other systems, some of which include the public.

Summary

The notion of emergency planning for technological risks is increasingly important in the modern world. Such planning should be based on a problematic assumptions.

It is important to make the distinction between emergency planning and emergency management. This is particularly important since many of the management problems are not related to the "agent" but to the response itself. It is also important to see the "public" as a part of the social system for the response and thus to emphasize the difference that might exist between public and organizationally-relevant information.

2.6. LARGE SCALE ACCIDENTS AND PUBLIC ACCEPTANCE OF RISK

George Yadigaroglu
Swiss Federal Institute of Technology, Zurich

Hector A. Munera
Tecnicontrol Ltd, Bogota, Colombia

"As the length and quality of life have increased, and thereby its value, society has become increasingly concerned with avoiding risks, particularly those imposed without offsetting benefits to the risk taker" (Rowe, The Anatomy of Risk). The public seems to be particularly sensitive to the consequences of large-scale technological accidents. The fact that the expected average number of fatalities or other probabilistic measures of damage from large accidents could be much smaller than those from numerous small accidents does not seem to be an important factor in the public mind. Indeed, what determines whether a technology is acceptable from the standpoint of risks to public health seems not to be the expected average number of fatalities or injuries that it will cause, but rather the potential for unlikely, but very-high-consequence events. In fact, the public mind has no good perception of very small probabilities and is not convinced from probabilistic arguments advanced to prove the safety of technologies. The controversy regarding nuclear power and its acceptability proves well this fact.

Since, in democratic societies, the public is the final decision maker, and public opinion cannot be ignored, this particular aspect of public perception of risks must be taken into account in decision making, even though there may be no "rational" thinking behind it. We adopt here the point of view that risky alternatives cannot be compared on the basis of the expected value of their consequences only.

In a recent study (Munera, in Risk Analysis as a Decision Tool, G. Yadigaroglu and S. Chakraborty, editors), the risk was dissociated into two components: the frequency of undesirable events and the probability distribution function (pdf) for the number of fatalities conditional upon the occurrence of such an event. (Within this framework a lower cutoff

line for consequences is needed; only accidents with a number of fatalities larger than 10 have been considered).

It was found that if one plots these conditional probability distributions (obtained from historical data) for various types of technological accidents (marine, aviation, explosions and fires, etc.) as well as for natural disasters (hurricanes, floods, earthquakes), one obtains some clustering of the cumulative complementary probability distribution functions (ccpdf) in two distinct regions separated by a gap: The ccpdf's for natural catastrophes lie an order of magnitude above the ccpdf's for technological accidents.

The public considers the large natural catastrophes as particularly dreadful, but they have to be accepted as "acts of god". Since "ordinary" technological accidents seem to be at least tolerated by society, one is tempted to propose the upper envelope of the cluster of conditional ccpdf's for the technological-accidents as a regulatory limit line for maximum tolerable technological accidents. Thus one essentially limits the damaging potential of technological accidents to levels that have been historically observed at least, independently from the accident rate. One can associate to this criterion a second criterion limiting the absolute frequency of technological accidents.

It is believed that adoption of such criteria limiting the maximum potential damages from various technologies will facilitate rendering these publically acceptable.

It is hoped that discussion of this thesis, presented here more like a proposal for discussion rather than a firm conviction, may lead to some useful conclusions.

2.7. OUTLINES OF A MANAGERIAL APPROACH TO RISKS

Gustaf Östberg
University of Lund
Sweden

Abstract

The intention of this contribution is to outline a basis for improvements of risk management against the background of Bhopal, Challenger, and Chernobyl. The treatment of this subject covers first some philosophical principles of dealing with incompatibilities in complex systems. Particular attention is called to the role of non-technical factors which can be handled only by the proper application of such non-scientific disciplines as sociology, psychology, and business administration. This leads to a plea for the development of a certain managerial approach.

BACKGROUND, SCOPE, MESSAGE

It is nowadays widely recognized that the reliability and safety of materials are multidisciplinary phenomena. What this means in practice and in theory will be illustrated by consideration of two aspects of the behaviour and performance of materials. One is an interpretation of actual events - notably the Three Mile Island accident and the Chernobyl catastrophe - and the other is an analysis of the nature of knowledge about relationships between the structure and composition of materials, on the one hand, and on the other hand their properties and performance.

Most of the experience on which this treatment of safety and reliability is based comes from nuclear technology. The confidence in nuclear power, based on the progress made by the early scientists, has largely disappeared, thanks to the subsequent poor performance of the technology. It may be easy then to put the blame on the practitioners of this technology only. The point I want to make through this lecture, however, is that scientists developing the principles and designs of early schemes for technical products may also lay the foundations for later failures of the technology in question.

FOUNDATIONS IN PHILOSOPHY OF SCIENCE

At this point you might ask yourselves what this lecture really is about. Does it concern your work as scientists or is it just one of those talks about the dangers of uncontrolled development of technology? In order to place the issue in its scientific context, I want to call your attention to some fundamental problems of science that I have met in my attempts to find reasons why science often fails to serve its purpose to develop technology.

In essence I think we have to realize that the systems we are dealing with in complex technologies contain incompatibilities to an extent that we are usually not aware of. Our ability to overcome such problems is developed already at school. Take the calculation of the circumference of a circle, for example. No school teacher tells his or her pupils about the irrationality or the transcendental nature of π. The result of a calculation of the length of the circumference is considered to be an exact number.

A similar case is the calculation of the length of the hypotenuse from the length of the catheses. Again we are induced to think that there is no conflict between this calculation and, for instance, the physicist's or the crystallographer's views about the exactness of the measure of the distance between atoms along diagonals in a cubic lattice.

In the same way we are accustomed in school to accept equivalences between different physical phenomena, for instance between mass and energy, between change of energy and the frequency of the corresponding wave motion, between mass and acceleration etc. It is only when we learn about statistical mechanics and quantum physics at the university that we might realize that such relationships are indeed very puzzling. But even then few students care about the philosophical questions involved in the understanding of incompatibilities in our systems for explaining complexities.

COMPLEXITY OF TECHNOLOGY

In conventional physics and chemistry, our ignorance and lack of interest in the nature of relationships are usually of little importance. We can deal with irrational and transcendental numbers without difficulty, and the same is true for the proportionality constants we apply to make up equations and models. In technology, however, we have to consider relationships which extend beyond our theoretical and practical experience. In new developments, the validity of our projections cannot always be proved but has to be estimated on the basis of our judgement.

For materials, this kind of uncertainty becomes critical when we proceed from relationships between structure and properties to performance. We then move from one level of complexity to a higher one. This means not only that new and different factors are introduced, but also that new rules may take over.

The philosophical framework that I have now outlined is the basis for my views on failures and risks associated with the development and application of technology in general and of engineering materials in particular. The problems I address are those that occur at the stage when fundamental discoveries under simplified or strictly controlled conditions are to be applied in circumstances which cannot easily be predicted or handled using rules and methods for less complex situations.

There are numerous examples of failures due to the effects of factors others than those prevailing during the early stages of development. To mention just one typical case, corrosion is a factor which is simultaneously often overlooked and difficult to predict with respect to its causes and consequences - if ever recognized.

NON-TECHNOLOGICAL CONTEXT

So far I have considered only the scientific and technological aspects of failure of materials under practical conditions. Experience overwhelmingly demonstrates, however, that it is lack of understanding of - or rather respect for - the non-technical context which is the ultimate cause of failure of materials. In recent years we have witnessed such failures on a grandiose scale in cases like Challenger and Chernobyl, but we can find the same basic principle of non-technical causes of failure behind the majority of so-called technical materials failures.

Now I come to the core of my message to you. When faced with arguments about the role of factors other than those considered in their textbooks, most scientists and technologists tend to draw a demarkation line between the technical professions and other non-scientific or non-technological professions or disciplines, such as sociology, psychology, business administration etc. The natural tendency of most scientists and technologists or engineers is to dissociate themselves from the outside world when it intrudes.

PSYCHOLOGICAL BARRIERS

In fact, as far as I can understand from several years of studies of practical cases of materials failures, the root of the problem is not primarily the complexity of materials performance but the reluctance of those responsible for the technology to consider and handle the relations between technical factors and other non-technical conditions affecting the performance of the materials in question. Furthermore, behind this reluctance and negligence there is often a lack of respect for other things in life than those which can be quantified or expressed by equations and models.

At this point I would like to call your attention to a paradox. The interpretation of the ultimate cause of materials failures I have now given - based on an analysis of practical cases using arguments from systems theory and the theory of science - suggests that scientists and technologists are rationalists and positivists. But at the same time they seem to cultivate opinions about their own professional work that stress the importance of other qualifications, such as intuition, imagination, creativity etc. When one scientist is thought to be superior when compared with his colleagues, therefore, it is mainly his non-scientific, non-rational abilities that are stressed.

THEORETICAL AND PRACTICAL SOLUTIONS

When considered from the point of view of systems incompatibilities, the intriguing problem of materials failures appears to be associated with our ways of dealing with relationships between science and technology on the one hand, and on the other hand social and psychological realities. One popular argument is to refer to the development of artificial intelligence, AI. In view of the critical role played by non-rational factors, including tacit knowledge, AI may lead us to partial solutions only.

The views on materials failures that I have presented up to now seem rather pessimistic. There is nevertheless some hope of resolving the dilemma of systems incompatibilities using concepts developed by philosophers and applied by practioners in quite a different field, namely that of management. In simpler terms, the philosophical principle in question can be illustrated by the problem of blowing up a balloon from inside. The difficulties involved in dealing with incompatibilities in technical systems can be solved only by means from outside or, in systems terminology, by consideration from another level or from another contextual point.

Actually, this is what Pythagoras did when he solved the problem of irrational numbers. He transferred the problem from the linear dimensions of the hypotenuse and the catheses to their squares. Such a move can be made in simple geometry with no violation of logical rules. If you go to higher orders of complexity, however, the derivation of relationships on a higher level cannot necessarily be based on the rules or language developed for the lower level. This is, by the way, another limitation of AI in addition to its inability to consider non-rational factors.

Management, the practical parallel to this philosophical principle, also operates from a point outside the system of non-compatible elements. In a company, the manager's position above everybody enables him not only to view the different activities from a less egocentrical perspective than those of the different units making up the organisation. Since one of his major tasks is to direct and govern the work, he is also in a position to establish goals and to make these goals understandable to all parties, including the shareholders and the board. Furthermore, a manager has to integrate the particular interests and professional peculiarities of the different units, such as purchasing, sales, design, production, administration etc.

ROLE OF MANAGEMENT

Now you might ask yourselves what this has to do with materials failure. The reason why I have made the analogy between management of business and management of materials failure problems is not to suggest that scientific and technological research and development should be organized and administered like commercial companies. My point is related to the establishment of goals. Successfully managed companies have one thing in common, namely a well-defined goal in terms of a so-called business idea. This is what I want to suggest as the conclusion of my reasoning and arguments about materials failure: that in projects involving complex materials systems, there should be not only a scientific and technological idea, but also a clear idea about how to handle failures associated with materials.

RISK HANDLING

Finally, I will say a few words about risks. In common usage, failure is in principle associated with risks. For the purpose of this lecture it is then appropriate to make a distinction between different categories of risks. There are certain risks for which we know both probabilities and consequences fairly well, for instance traffic accidents and normal failures of electronic components. In both these cases there are statistics on which we can base our considerations about how to handle the risks in question.

On the other extreme, there are risks of which we know very little, if anything. One example is AIDS. Before the outburst of the present epidemic, there was practically no possibility to foresee its development.

The failures associated with materials that I have had in mind in my previous discussion are those that may be foreseen in principle, but not necessarily in probabilistic terms. From my experience as an analyst of failures of components in nuclear reactors I can cite numerous cases of failures that should have been foreseen, although not on the basis of probabilistic assessments. It is in order to find the means of handling such failures - or rather to avoid them - that I have developed the arguments for management just suggested.

As you certainly know, risk is nowadays the subject of systematic, scientific studies from a number of points of view. In a brief review like the present one, the following aspects of risk can be identified:

- risk recognition
- risk imaging
- risk perception
- risk assessment
- risk evaluation
- risk acceptance
- risk distribution
- risk management

The list ends with the key-word of this lecture. Only by means of proper management can a coherent and comprehensive handling of risks of materials failure work to the satisfaction of those ultimately concerned, the end-users of the technical systems and those who make decisions on their behalf.

For your consideration as topics for the discussion I want to close by adding the following phenomena or concepts involved in the management of risks:

attitudes
bureaucracy
context
creativity
fragmentation
holism
imaging
inconceivable events
mentality
paradigm
soft factors
surprise
surrealism
tacit knowledge
two cultures

2.8. QUANTITATIVE RISK ANALYSIS AND REDUCING THE RISK

Dr. B. J. M. Ale
Ministry of Housing, Physical Planning and Environment
Leidschendam, Netherlands

ABSTRACT

Since the beginning of this decade the dutch government has spent much effort in the development of quantitative techniques that could assist in making the siting and zoning decisions for and around chemical complexes.
In its present form these techniques are aimed large, relatively long range effects. Incorparation of short range effects is necessary to support a fully balanced risk reducing strategy.

INTRODUCTION

The chemical accidents in te mid seventies together with the EEC directive nr. L230, "the Seveso directive" led the Dutch authorities to carefully consider risk bearing activities. This was even more important since large industrial complexes and heavily populated area's were located close together already.
It was and still is of vital importance to the dutch economy that industry and population can coexist in harmony. It was decided fairly early that zoning was one of the instruments to be used and that the extent of the safety zones should be based on quantitative considerations. Unfortunately at the time no coherent methodology existed for quantitative risk analysis of chemical plants as opposed to for instance nuclear facilities.
The Public Vulnerability Model of the US Coast Guard was as close one could get to the quantification, and that was quantification of effects only. It is noteworthy that this PVM still forms the backbone of the harbour safety policy of the US Coast Guard and that a lot of the modelling principles still are used even in the Safeti package to be described below.
The techniques since than developed rapidly. The publication of the "Yellow Book", the report describing agreed methods of calculating effects was a first mile stone in this development.
The Yellow Book is still available, now in a recently updated form, including the recommendations of the DIERS working party.
The next milestone was the COVO study. As fase as we know is the first integral complete risk analysis of chemical installations (2).
It was from this study that the Dutch authorities learned that a lot of the calculational effort that comes with performing a quantified risk analysis can be automated and the Directorate General for Environmental Protection together with the Rijnmond Authority embarked on a project to develop what is now known as the Safeti package.

COMPUTER ASSISTED RISK ANALYSIS

A suite of computer programs was developed by Technica to form a package now known as SAFETI [3]. It consists of some 35 separate programs that assist the risk analyst in the quantification of the risks of chemical plants and the associated transport. From a data base of vessels, and process conditions for a particular plant a set of potential failure scenario is generated. The frequency of these accidents is derived from a data base which contains information on the frequency of failure of process plant components. The consequences are calculated using a built in physical property data base for the substances involved. These consequences can result from outcomes of accidents such as fires, explosions (including BLEVES) and toxic vapour clouds. An ellaborate set of models to calculate the various phenomena that occur as the initial accidents scanario develops is available. The results of the consequence calculations are combined with data on the local weather conditions, population distribution, ignition source locations to calculate the final impact of the scenario's on the population. These results are finally aggregated into the individual risk contours around a plant or a site and the group risk lines. The use of advanced computing techniques allowed the incorporation of an appropriate level of complexity in the modelling at each stage in the risk quantification procedure. This results in enhancing the precision of the calculation when compared with methods used previously [4]. The current estimate of the uncertainty in calculating the consequences is about a factor of 2. [5].

The uncertainty in the frequency numbers is largely due to the limited availabity of historical data and is currently estimated as a factor 3(better or worse) than the best estimate.

THE POLICY

While techniques to estimate the risks evolved decisions on risk bearing activities had to be taken. In this daily proces of managing risks a general risk management policy emerged which was laid down as a policy statement of the dutch central governement in the multiyear plan for the environment 1986-1990 (1).

Here risk management is formulated in a four stage cyclic process. The four stage being indification, quantification, reduction and controll as in figure (1).

In the identification phase it has to be established whether there is a threat and what is it's nature. This is done on the basis of established or suspected ill effects. At the present state of environmental policy these threats usually are aimed directly or in directly to humans. The incident with the river Rhine showed that treats to the environment itself need attention as well.

In the estimation stage the magnitude of the risk is established, preferably in quantitative terms. It is clear that risks associated with the frequent incidents can be more readily estimated than rare events, be it with large consequences.
These large consequence-low probability risks however are the most difficult and sometimes the most important in the risk decision process. The dutch government has chosen to apply quantitative risks analysis in those cases as well. This week the concept general administrative measure to implement the post Seveso directive together with a positive advise form the central Environmental counsil will be sent to parliament. It is expected to be in force in the first half of next year. It will demand from those industries that fall under the terms of article 5 of the Seveso directive to submit a quantitative risk analysis to the competent authorities.

After this stage a decision has to be taken whether to accept a risk or do something about it.
The environmental plan distinquistes between group risks or F-N curves and individual risks or risk contours. The group is defined as the chance of exceding a certain number of casualties, and the individual risks a defined a the change of exceeding a lethal level at a certain place.

For these two measures of risk limits are indicated below which a risk is deemed to be acceptable, limits above which a risk is deemed to be unacceptable and between those limits a so called grey area in which the decision merely is influenced by economical, social and other factors. The numerical values of these limits are given in fig. (2).

Then a decision has been taken whether measures are required to reduce the risk or the risk is accepted.
In the last phase of the process the established situation of acceptable riks is maintained by inspection, zoning requirements etc.

REDUCING THE RISK OFF-SITE

The policy as described above itself reduces the off site to people, or at least does limit it to a politically accepted level. However one can go beyond zoning and try to find measures on the plant to reduce the offsite risk. It is an easy task to sort the contributing events in order of their contribution to the risk. In practice one can sort with respect to the contribution to the group risk of a certain magnitude to the individual risk at a certain place. It is quite a common result that only a few possible events are dominant in a broad range of accident sizes and in the individual risk as well. It is thus possible to seek for the parts of the installation from which these incidents might emerge and consider risk reducing measures there. An example.
From the risk analysis of the whole of the DSM site in the south east of the Netherlands the conclusion resulted that the risk for the population was caused mainly by the ammonia ringline, a system to supply various installation with pressurised liquid ammonia. From the analysis at proved to be worthwile to study measures for this line in more depth including the technical feasability of closing down a section of the line closest to the population. These studies are presently underway.

BALANCING ON-AND OFF-SITE RISK

The techniques described above are explicitely aimed at larger range effects and therefore not suited to quantly the whole of the one site risk without addition of shortrange effects. However the on-site risk has to be considered even when developing an off-site risk policy. There is a distinct class of meassures that reduce the offsite risk of toxic vapours that increase the onsite risk namely enclosure. These containment type constructions have to be considered very carefully even if the effect on the offsite risk is beyond discussion. As has been stated elsewhere, it is impossible to develop objective, technical criteria to weigh the risk to employees against the risk to the popuplation especially if the former are killed one at the time and the latter in larger groups at the same incident, as is usually the case. This weighting is a political decission. At this stage of development of safety policies it is not clear whether a generalised policy can be the developed or that case to case decission making is the maximum achievable.

CONCLUSION

Quantification techniques are now accepted in the Netherlands as a common basis for siting and zoning policy.
Their usefullness in finding risk reducing measures on the plant is increasing with the increasing capabilities of analysis of the details of the risk picture. However care must be taken where the proposed measures reduce of site risk while increasing onsite risk.
When this is born in mind however quantitative techniques can be of great beneficial value in reducing the risk.

REFERENCES

1) Environmental plan for the Netherlands 1986-1990, Tweede Kamer der Staten Generaal 1985-1986, 19204 nrs. 1-2, the Netherlands.

2) Report on the COVO study to the Rijnmond Authority 1979, Reidel.

3) Zonering langs hoge druk aardgastransportleidingen, Minister van Volkgezondheid en Milieuhygiëne 1981.

4) Integrale Nota LPG, Tweede Kamer der Staten Generaal, vergaderjaar 1983-1984, 18233 nrs. 1-2.

5) Risk analysis of the DSM site. Report to the province of Limburg 1985.

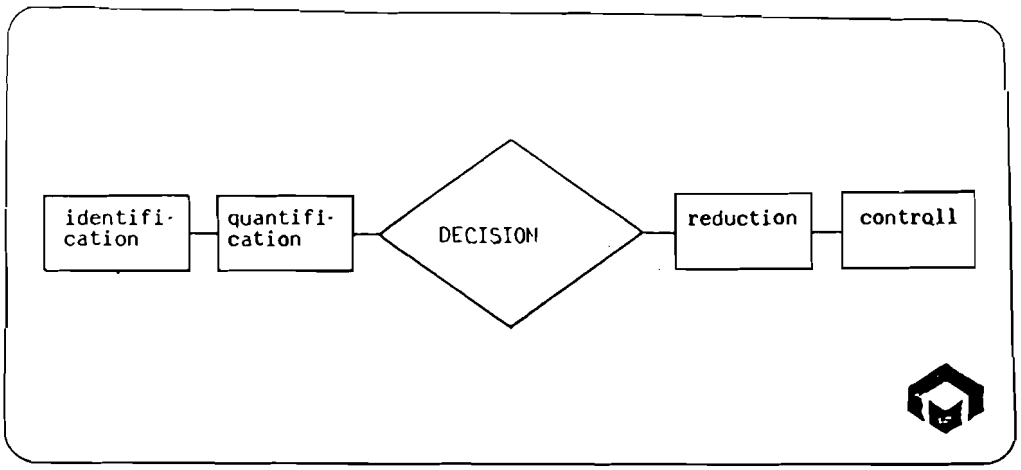


figure 1. Risk managment cycle

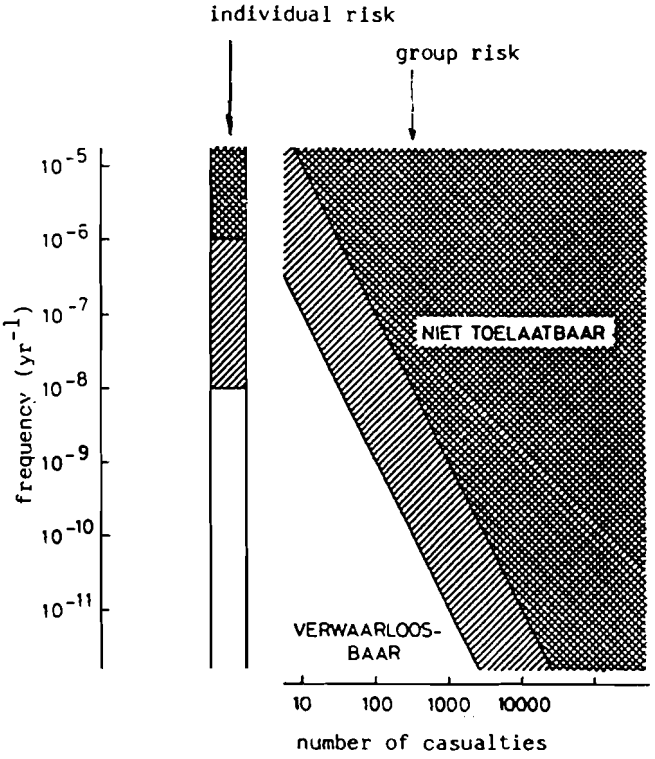


figure 2. Risk limits

2.9. COMPARISON OF DECISION ALTERNATIVES WITH REGARD TO RISK AND SAFETY CONSIDERATIONS: METHODOLOGICAL PROBLEMS

O. I. Larichev
VNIISI, USSR Academy of Sciences, Moscow

1. INTRODUCTION

The evolvement of large-scale technologies gave rise to a problem of choice between complex technological projects with regard to risk factors. The problem is quite specific and is commonly referred to as risk analysis. A partial case of this problem is the siting of a complex engineering system such as a nuclear power plant, a chemical factory, liquefied gas terminal, gas pipeline, and the like.

The problem of site selection with due account of the risk factor has been studied in many papers. IIASA approached it from the descriptive standpoint (how the choice is exercised) by conducting four case studies into the selection of sites for liquefied gas terminals.[1] Some papers[2] treated the problem from the normative standpoint. G. Ford et al[3] compared a number of methodological approaches to the nuclear power plant siting. The comparison ended with selection of the two best methodologies. In line with the latter and following the elimination of clearly unacceptable alternatives, the quantitative method of utility function construction was used to evaluate each alternative.

We believe the methodological specifics of the considered problem require some other approach. Further, we shall consider the distinguishing features of the problem of complex technological system siting.

2. SPECIFICS OF THE CONSIDERED PROBLEM

According to the descriptive research, subject to analysis is the multiple participants (many active groups) and multi-attribute problem. What is more, the multiple criteria estimates are highly uncertain and the opinions of the experts producing the estimates are often conflicting. The decision process as such comprises several steps resulting both in an acceptable decision or no decision at all.[1] Besides, there are the following specifics:

1) Inhomogeneous Criteria: Of course, there are many criteria characterizing the preferable alternatives for different decision choice participants. The additional complexity is that the criteria are inhomogeneous. They characterize economic, social, ecological, and organizational aspects of each decision alternative.

2) Criteria Estimates are in a Different Form: It is worth pointing out that because of the different nature of criteria, the criteria estimates are in different languages. Some of them may be quantitative (cost, distance estimates, etc.), others qualitative (environmental impact, earthquake probability). The lack of precise probabilistic estimates implies elicitation of the expert information only in the form of verbal event probability statements. What is more, the lack of necessary information sometimes results in relative rather than absolute criteria estimates. Thus, in comparing the gas pipeline alternatives with respect to the safety criterion, use was made only of qualitative methods,[4] i.e. which alternative is the safest for the population.

   We believe that the primary language the estimate is formulated in is very important for all subsequent stages of alternative evaluation. Only the language customary for experts may ensure the measurement reliability. Of course, more often than not the measurements are conducted on strong quantitative scales. Nevertheless, the transition from the primary qualitative estimates to the secondary quantitative ones is methodologically incorrect as it engenders an unjustifiable arbitrariness.

3) Difficulty of Comparing Estimates by Some Criteria: Apart from the usual difficulties relating to comparing inhomogeneous estimates, there are additional complexities such as the comparison of the amount of electric power generated by a nuclear power plant and the number of casualties in case of accident. One can hardly imagine a manager capable of finding an explicit trade-off between the estimates by the above criteria. The assignment of criteria weights is psychologically incorrect.

4) Necessity of Accounting for Criteria Relating to Different Moments in Time: In making decisions on siting the complex technological systems, three groups of estimates must be taken into consideration:

   a) estimates of the area and place of location;
   b) estimates of the operating system's environmental impact;
   c) estimates of an accident's implications (highly unlikely, though).

The three groups of estimates relate, in effect, to different projects: the one under construction, a normally operating project, and a damaged one.

5) Difficulty of a Reliable Assessment of the Decision Implications: The book[1] convincingly shows that the expert estimates of probabilities of different events relating to the future can vary considerably (the probability of an aircraft hitting a liquefied gas terminal, probability of liquefied

gas-carriers colliding, etc.). The variance is probably due to the fact that people perceive poorly and assess very low probabilities.[5] The low probability estimates (10^{-4} and the like) are, therefore, hardly informative for accidents, both trivial and disastrous, which do take place from time to time. More informative is the matching comparison (quantitative and qualitative) of different safety control systems.

6) Difficulty of Harmonizing Conflicting Estimates: Of course, harmonizing opinions of different active groups is a complicated process. Even if all of them strive toward an acceptable decision, the alternative estimates of individual criteria and on the whole may vary considerably.

3. REQUIREMENTS TO DECISION TECHNIQUES

The above specifics make it possible to formulate several requirements on evaluating technological system siting alternatives. First, practice shows the desirability of approaching the choice problem from a more general standpoint: not to be confined to comparing the available alternatives, but to look for new ones and compare (sometimes modify) them with the existing alternatives. In other words, it is a consistent specification of requirements for the complex project siting by analyzing the available alternatives, determining the range of alternative estimates, searching for new sites (if necessary), etc.

Second, each active group must be able to verify any estimate. Hence, the latter must be easily understood and formulated in an adequate language.

Clearly, the axiomatic techniques based on quantitative scales, comparison of all criteria, and construction of the decision-maker's utility function do not meet the requirements.

4. THE SUGGESTED METHODOLOGICAL APPROACH

The first characteristic of the suggested approach is the search for a dominant alternative. The psychological research[7] indicates that in selecting the best alternatives, the decision-maker first pinpoints a preferable alternative and then tries to substantiate its superiority over the others.

It is possible to develop a normative method also oriented toward the search for domination. In comparing the decision alternatives, one has first of all to remove the inferior ones. Then, in the course of a pair-wise comparison, one looks for superiority of one alternative over the other.

There is, as a rule, a small number of decision alternatives (not more than 10). The suggested approach implies a pair-wise comparison of project siting alternatives. The three aforemen-

tioned groups of estimates (those of site, of environmental impact, and of accident implications) are not compared with one another. The estimates of only two alternatives in each of the three groups are subject to comparison. The purpose of comparison is to determine which alternative is preferable and by what criteria group. With this in mind, use is made of the compensation techniques and the improvement of some estimates of some estimates at the expense of others. The second feature of the approach is that the decision alternatives are not viewed as fixed and invariable, but rather as a type of alternative with possible modifications within the limits of the type. The point is that in designing certain projects (industrial buildings,[6] gas pipelines,[4] cities), it is possible to improve some criterion estimates at the expense of others. Thus, with additional investments we may improve the quality of a nuclear plant site. By installing a new power line, we may place the plant farther from settlements, etc. In case the alternatives are incomparable, it makes sense to define requirements to an alternative which is superior to the two available alternatives by all criteria. Account must be taken of the opinions of different active groups. The decision-maker's job boils down to a search for the required alternative and to demonstrating the lack of an opportunity for developing one.

The pair-wise comparison may end up in the selection of an alternative acceptable to all active groups or in a lack of accord between the active groups if no best alternative can be found. In the latter case, however, there arises a host of requirements for the project design and the desirable site which is in effect a guide to future actions.

We employed this approach in comparing the alternative routes of a gas pipeline.[4]

At the preliminary stage of research, three variants of pipeline route have been selected: maritime, median, and piedmont. The comparison of variant was made on criteria given in the table.

Of the parties involved in the actual pipeline selection procedures, four major participants can be singled out. First, there is the customer organization which determines the design task and performs pipeline maintenance; secondly, the organization that designs the pipeline; thirdly, any project has to be agreed upon with the regional authorities which represent the interests of the local population; and finally, the route selection is influenced by the contractor who will actually construct the pipeline.

When comparing the routes, each participant in the selection process is primarily concerned with a definite subset of the given criteria. For example, the project organization draws attention to criteria C, C1, C2, IN, R, and S; regional authorities are concerned with criteria RP, IN, S, R, and C2; and the customer is naturally interested in criteria C, M, R, and S.

Finally, the contractor gives primary consideration to criteria T_{min} and S.

The selection procedures adopted are as follows. The project organization analyzes all possible pipeline routes. Using the initial basic outlines, the route direction in each version is then specified as that minimizing the presented costs. Then the project organization selects a version and transfers this proposal together with information about all the other versions to the customer and then to the regional authorities for approval. The contractor's representatives also take part in these discussions. In this example, the project organization preferred the maritime version. When considering the various versions, the regional authorities pointed out the comparison between the far superior evaluations of the median version on criteria C2, RP, and R and the "best" evaluations of the maritime version on criteria IN and S. During the analysis, the regional authorities asked the customer and the project organization to find new technical solutions to improve the evaluations of the median version on criteria IN and S in order to bring them nearer to the maritime version evaluation. As a result of investigations towards this end, the project organization suggested the possibility of cutting down the guarding zone, combined with an increase in reliability effected by increasing the thickness of the pipe wall. It was found that with such an improvement the number of buildings requiring demolition would be considerably reduced and the presented costs of the median and maritime versions would become closer, despite the increase in the amount of metal required and in the cost of the pipeline. In the table, evaluations of the versions after incorporating this improvement are given.

With these improvements, all the participants in the selection process chose the median version as the most acceptable, and so this version was selected.

The example given above is typical in gas pipeline route selection. Each active participant in the procedure is at first guided by his own subset of criteria, working through from the more to the less important ones. This is characteristic of a satisfactory decision search according to Simon. We must point out that usually no single version is superior on all criteria; it is almost always necessary to look for a compromise. A typical feature of an actual comparison process is a series of attempts to revise some of the versions, in order to improve their assessments on particular criteria.

5. CONCLUSION

We believe that the successful selection of a project site depends on the following factors:

1) understanding by all active groups of the necessity to solve the problem the technological project is being built for (e.g., additional power supply);

2) opportunity for all active groups to elicit information about all feasible alternative ways to solve the problem; a joint selection of one of the ways is desirable;

3) opportunity for the joint assessment and comparison of the project sites;

4) development of a convenient and effective tool for comparing the alternatives; a man-machine collective decision support system best serves the purpose.

TABLE

	Criterion	Designation	Order of Preference		
			Maritime	Median	Piedmont
1	Presented costs (million roubles)	C	8,9	9,5	10,8
1A	Cost of laying the main route (million roubles)	C1	31	40	46
1B	Cost of laying prospective pipeline branches to consumer (million roubles)	C2	9,5	5	5
2	Construction time	T_{min}	Second best	Best	Worst
3	Convenience of maintenance	M	Inferior	By far the best	Inferior
4	Reliability of maintenance	R	Best	Inferior	By far the worst
5	Influence on the environment	IN	Best	Inferior	By far the worst
6	Connection with regional development plans	RP	Second best	By far the best	Worst
7	Construction conditions	B	Second best	Best	By far the best
8	Population Safety	S	Best	Inferior	Inferior

REFERENCES

1. Kunreuther, H., Linnerooth, J. et al. Risk Analysis and Decision Processes, Springer-Verlag, 1983.

2. Keeney, R. L. Siting Energy Facilities, Academic Press, 1980.

3. Ford, C. K.; Keeney, R. L. and Kirkwood, C. W. "Evaluating Methodologies: a Procedure and Application to Nuclear Power Plant Siting Methodologies," Management Science, Vol. 25, No. 1, 1979.

4. Larichev, O. I. et al. "Main Gas Pipeline Route Selection Problems, Taking into Consideration Risk and Uncertainty Factors," in: H. Kunreuther (ed.) The Risk Analysis Controversy, Springer-Verlag, 1983.

5. Kahneman, D.; Slovic, P. and Tversky, A. (eds.) Judgement under Uncertainty: Heuristics and Biases, Cambridge University Press, 198.

6. Larichev, O. I. et al. "The Interactive Procedure of Industrial Building Projects Choice," in: Proceedings of Multicriteria Objects Estimations, VNIISI Proceedings, No. 9, 1984.

7. Montgomery, H. and Svenson, O. "A Think Aloud Study of Dominance Structuring in Decision Processes," in: R. Tleitz (ed.) Aspiration Levels in Bargaining and Economic Decision Making, Berlin: Springer-Verlag, 1983.

2.10. SYSTEM APPROACH TO RISK PREVENTION AND UNIVERSITY EDUCATION

Eng. J. Hadas
Informatics Center of the Hungarian Industry, Budapest

Dr. I. Kiss
Bureau for Systems Analysis, State Office for Technical Development, Budapest

In our industrialized society, the hazards and risks of accidents and other undesirable occurrences are omnipresent: at work, in traffic and even at home, during leisure time. According to general opinion, factories and plants belong to the most dangerous places from the viewpoint of accidents and damages. It is somewhat contradictory that the frequency of home injuries is higher compared with occupational and traffic ones. For instance, in Hungary only one third of the yearly 7000-7500 fatal accidents originate at work or in traffic. Nearly the same rates can be found in social insurance statistics, too.

Facts show that the consequences of industrial accidents and catastrophes are more serious than others. This is connected with the complexity of new technologies, the substantial concentration of production and the several kinds of hazardous technologies and materials. This is strikingly apparent in the process industries.[1]

The purpose of occupational safety and work planning in general is to minimize accidents. Special attention is, of course, draw to the well-educated engineers and other specialists. In Hungary, the Budapest Polytechnical University was one of the initiators and founders of instructing university students in labor safety (Prof. V. Wartha, 1870) and in "professional diseases" (Prof. K. Müller, 1879). In compliance with a decree issued by the Ministry of Education, instruction in labor safety in every Hungarian institute of higher education has been universal and obligatory since 1963. The subject called labor safety is taught for one semester at every Hungarian university and college of technology, and the students have to take an examination, too. But instruction on labor safety is not confined merely to this independent subject, for it is also taught within the framework of the different subjects, exercises and practice sessions in the laboratories and workshops. This compulsory subject cover a wide field in system-approach from the classical tasks of organization to the risk analysis methods.

---

[1] Insuring and Managing Hazardous Risks: From Seveso to Bhopal and Beyond. IIASA Executive Report 11, Laxenburg, April 1986. Editors: Kleindorfer, P. and Kunreuther, H.

Connected with this, ergonomics takes part in the labor safety teaching programme. We have a recent Hungarian Standard on ergonomic principles in the design of work systems,[2] which substantially correspond to the international ISO standard.[3] This constitutes the basis of exposition of such topics as, for example, the main factors in the person's environment, the stresses and conflicts between the man and his organizational environment, increasing human performance, the hazards of stressful events and work overloads, the dangers of repetitive machining work, monotony and tiredness, consideration of human information processing,[4] and possibilities of automation, cybernetic systems, etc.

We use multi-variate analyses to suggest socio-technical design and generally system-approach risk prevention methods for future engineers and participants of post-graduate courses. The system analysis is one of the background materials,[5] but the role and significance of this must be increased.

There are monetary interests at the industry and insurance companies to decrease accidents and damages. The economic effects of these are unnecessary expenditure, production losses of the manufacturing organization. In consequence of accidents and damages, the profit of a productive organization in Hungary decreases, the atmosphere of the plant becomes impaired, and the reputation of the institution vitiated. For this reason, the industry makes new demands on institutes working in the discussed fields. We hope that the new demands will raise the resources for further research, on which both modern education and prevention can be based equally.

---

[2] MSZ 17 235-82.

[3] ISO 6 383-81.

[4] Hadas, J.: Cybernetic Model of Human Perception and Observation; Information-channels for Sampling. First prize winning competition study, 5th National Labor Safety Competition, Miskolc, August 1973.

[5] Kiss, I.: Systems Theory - Systems Technics. NIM IGÜSZI, Budapest, 1970.

2.11. TECHNOLOGICAL RISK AND THE POLICYMAKER

Ing. Jan Neumann
Energy Commission
Czechoslovak Academy of Sciences, Prague

The policy-maker who is responsible for decisions concerning construction of large energy complexes (for example, coal burning or nuclear power stations with capacities of several thousand MW) must be aware that he is deciding about the development not only of energy, but also of economics for the next 50 years, that he is deciding about great changes of the area where the construction will be situated, about future influences of the environment. The risk of his decisions must be minimized by scientific knowledge, by respecting the interests of the whole society and international obligations of the state. He should never be influenced by local interests or possible pressure from political or economic groups.

Experiences concerning the centralized economic planning that has been applied in Czechoslovakia during the last 40 years confirm that. We passed several peripetias of scientifically non-justified decisions, leading to difficulties in energy supply, and seemingly economically advantageous burning of cheap brown coal had a serious impact on ecology. But it seems this is not only our problem; in our country prevailing west winds carry more sulphur dioxide from our Western neighbors than from us to them.

Czechoslovakia, as a state with advanced industry and intensive agriculture, consumes a considerable amount of primary energy resources. In 1985, the total consumption reached 104.2 mil tce, or 6.7 tce per capita. Approximately 60% of this consumption is solid fuels (brown and hard coal), 35% liquid and gaseous fuels (crude oil and natural gas) and 5% primary electricity (from hydraulic and nuclear power stations). While the consumption of solid fuels is covered in a great majority by Czechoslovakia's own mining, a preponderant majority of liquid and gaseous fuels are imported from the Soviet Union. Crude oil is transported by the pipeline "Druzba," which leads from the east border of Czechoslovakia to all Czechoslovakian oil refineries and further to the west border to the petrochemical works near the city of Most. The natural gas is transported by a whole system of gas pipelines, constructed not only for Czechoslovakia's own consumption, but also for the transport of Soviet natural gas to neighboring countries. At present, the transit of natural gas across Czechoslovakia is as high as 50 Gm^3 per year and is continuously increasing.

The production of electricity in Czechoslovakia in 1985 reached the level of 80.63 TWh, or 5200 kWh per capita. Eighty percent thereof were produced in thermal, 5% in hydraulic and 15% in nuclear power stations. In 1985, the import of electricity to Czechoslovakia was higher by 3.54 TWh than the export, so that

the Czechoslovakian consumption of electricity was 84.17 TWh, or 5430 kWh per capita. The installed capacity of the power stations in 1985 was 20.3 GW.

The production of electricity, steam and hot water for large systems of the centralized heat supply were covered until 1980 mostly by Czechoslovakian brown coal and by heavy heating oil. Both those resources contain sulphur: brown coal on average 1.7% (1.7 b $S.MJ^{-1}$) and heating oil about 3% (0.8 g $S.MJ^{-1}$). Combustion of these fuels has led to the significant pollution of the whole Czechoslovakian territory by emissions of fly-ash and sulphur dioxide, and consequently causes acid rain and water and soil pollution, dangerous for the whole biosphere. Especially the forests have been seriously damaged. Particularly affected are industrialized and densely populated areas: North Bohemia, Prague, and others.

The state is solving this problem by various means. The most important is decreasing brown coal mining from the level of 100 million tons in 1985 to 80 million tons by the year 2000 and changing the processing of crude oil. The residual oil with high sulphur content will be partly cracked and partly gasified for further use in the chemical industry; at the same time, sulphur will be produced as an accessory product. Two large cracking units are under construction at present, and one gasification unit already works producing water gas and hydrogen. The import of crude oil will slowly decrease between the years 1985 and 2000.

The whole increase of electricity and heat production will be covered until the year 2000 by the increased import of natural gas and especially by the construction of nuclear power stations. In accordance with the approved conception, the installed capacity of the nuclear power stations should reach 11,000 MWe by the year 2000, and nuclear energy should cover more than 50% of Czechoslovakian electricity consumption by the same time. All nuclear stations will be equipped with pressurized light water reactors of 440 MWe and 1000 MWe capacities according to the Soviet projects; the majority of equipment at these power stations will be produced by the Czechoslovakian machine industry.

Another means to decrease the negative influence of brown-coal-burning power stations on the environment is the absorption of sulphur dioxide from combustion waste gases. At the power plant "Tusimice" in North Bohemia, a de-sulferization unit is under construction for a 200 MW unit. The principle of sulphur removal is a wet absorption and regeneration method, using magnesium oxide connected with the production of sulfuric acid. The technology was developed in the Soviet Union and the plant equipment was delivered by Czechoslovakian and Soviet machine works. the de-sulferization unit should be in operation by 1988. If the tests are successful, the technology will be used for the next three units of this power plant. In this case, the Tusimice power plant should produce in addition to 3.5 TWh an additional 200,000 tons of sulfuric acid annually. It is also considered

that the power plant "Prunerov" in North Bohemia with its five 200 MW units will be equipped with a similar de-sulferization technology. The more simple additive limestone method will be tested in already operating power plants with 100 MW units. Using this technology, the majority of sulphur bound to calcium leaves the boiler as a component of ash.

By the year 2000, brown coal ought to be used to a great extent for producing heat both for industry and for communal and house-building (in the form of steam or hot water). Therefore, steam boilers equipped with a fluid-bed gasification generator or a fluid-bed furnace are being tested. Both types, each with a capacity of 25 tons of steam per hour, are in operation. The additive limestone technology is being tested for the steam boiler with a fluid-bed furnace. Negotiations have been started with several German and Swedish firms concerning the possibilities of buying the equipment and know-how for producing steam boilers with fluid-bed furnaces and limestone de-sulferization at a capacity between 100 and 200 tons of steam per hour.

An important measure, leading to a decreased negative influence of energy installation on the environment and at the same time to a substantial increase in power plant efficiency, will be the reconstruction of condensation power plant, both coal-fired and nuclear, on the combined production of electricity and heat. In such a way, all large power plants situated in the North Bohemian coal basis will be reconstructed, and a large system of centralized heat supply for all big cities will be formed. Prague's atmosphere will also be significantly improved. The heat delivered from the power plant "Melinik," 30 km outside Prague, will allow a decrease in the consumption of coal and heating oil in the city's heating plants. In the historical center of the city, the coal used for local heating will be replaced by natural gas and electricity. All the working and constructed nuclear power stations will provide hot water into a network of centralized heat supply to distances as much as 50 km from the source. The hot water pipeline from Jaslovske Bohunice to Trnava is already under construction; the others, from Mochovce to Nitra, from Dukovany to Brno, from Temelin to Ceske Budejovice, are projected.

The gradual conversion of the energy supply structure from a coal basis to the nuclear one will represent a significant decrease in negative influences of energy production on the environment. Czechoslovakia is aware, however, of certain risks connected with developing nuclear energy, especially from the standpoint of radiation exposure of the biosphere. Therefore, the state is paying an extraordinary amount of attention to the problems of safety and reliability of the whole nuclear energy complex. Responsible for the safe operation of all units of this complex are operators - national enterprises, supervised by the Federal Ministry of Fuel and Energy.

Under the corresponding laws, the following state authorities supervise the construction and operation of nuclear power plants:

a) Offices of Labor Safety of Czech and Slovak socialist republics, responsible for supervision of technical safety for all pressurized systems and transport devices;

b) Ministries of Health of Czech and Slovak socialists republics, supervising radiation safety inside and outside the enterprises of the nuclear energy complex;

c) Czechoslovakian Commission of Atomic Energy, supervising nuclear safety of nuclear power plants and of transportation and disposal of nuclear fuels and radioactive wastes.

Czechoslovakia pays a great deal of attention to human factors in nuclear energy. It represents, above all, the choice and training of qualified engineers, technicians and skilled workers for the nuclear energy complex, especially for projection, construction, equipment production and operation of nuclear power stations.

In particular, operators and shift-leading engineers in attendance at nuclear power stations have to undergo a demanding system of training. They are all graduated from technical universities and take part in a special post-graduate course, completing a practical and theoretical state examination using the simulating machine VVER-440 at the training center in Trnava. Their constant ability at their function is verified every two or four years by a repeated state examination before the state examination commission.

As present, great attention is devoted to caring for the psychological and physical condition of operators and shift-leading engineers. On the initiative of the Czechoslovakian Atomic Energy Commission, a research project for the Medical Faculty at the Charles University in Prague has been included in the State Plan of Research, concerning research of risk factors during specific psychological stress of operators and shift-leading engineers, especially the factors influencing their cardiovascular system.

At present, the responsible planning authorities in Czechoslovakia are elaborating a prognosis of economic and social development through the year 2000. This work aims to increase the national income by more than two-thirds in comparison with 1985. This means that the growth rate of the national income should be 3.5-4.0% per year. An important question is what growth rate of consumption of primary energy resources, necessary for the economic growth mentioned above, would be optimal. The value of the coefficient of the national income energy elasticity (i.e. the ratio of the annual growth rate of consumption of primary energy resources to the annual growth rate of national income in percent) in Czechoslovakia was 0.9 between 1950 and 1960, and 0.5 between

1960 and 1980. For the period 1985-2000, the value of 0.2 has been determined. This is a very important decision, limiting the investment expenditures for the development of the complex including fuels and energy to approximately 30-35% of the total industrial investment; the risk connected with this decision is balanced by the extensive state program of fuel and energy consumption rationalization. This program demands a decrease of specific energy consumption for all branches of the national economy.

The Czechoslovakian state, as the "policy-maker" in energy policy, leaning on contemporary scientific knowledge, cares that the future development of the energy base be in harmony not only with the development needs of the national economy, but also with the principles of the present struggle to protect and preserve the environment.

2.12. RISK MANAGEMENT IN JAPAN AND THE UNITED STATES: A COMPARATIVE PERSPECTIVE ON PRACTICES AND APPROACHES

Saburo Ikeda
Institute of Socio-Economic Planning, University of Tsukuba, Sakura, Japan

Kazuhiko Kawamura
Management of Technology Program
Vanderbilt University, Nashville, Tennessee, USA

This paper is principally based on the study conducted by the "Joint U.S.-Japan Workshop on Risk Management in the U.S. and Japan," funded by the U.S. National Science Foundation, U.S. Environmental Protection Agency, and the Japan Society for Promotion of Sciences

1. Introduction

The management of technological risks has emerged not only just as science/technology policy but also as one of the most important policy issues in public policy confronting all industrial nations. While the technical challenges of regulating risks are often similar in most industrial countries, each country may have a different management approach and practice due to a different context of cultural, political, and institutional backgrounds in which regulation process must operate. A cross-national perspective in approaches or practices of risk management may provide a wide spectrum of knowledge from which we can compare the strengths and weaknesses of various approaches to technological risk management issues (1,2).

In 1983, the US National Science Foundation (NSF) supported a twenty-month exploratory research project on a cross-national comparison on technological risk management between US and Japan, which was conducted by Vanderbilt University, USA, with a cooperation from the University of Tsukuba, Japan. Later in 1983, the Japan Society for Promotion of Science (JSPS) announced a support to the University of Tsukuba for Japan-US joint workshop on "Comparative Study of Risk Management in Japan and the US" under the bilateral science cooperation with the US counterpart, the NSF.

This joint workshop was an important working event in conducting the study which was held on October 28-31, 1984, at Tsukuba Science City, Japan. The meeting was organized in such way that both Japanese and the U.S. risk professionals (about 30 experts) were allocated in equal number to working groups to discuss a selected number of technological risk cases, provided the background data and information prepared by the joint study team from both countries (3).

The criteria of selecting the technological risk cases were:

- simplicity of the issue in both countries,
- representativeness of risk management practices,
- sufficiency of the issue duration time,
- extensiveness of the issue to other risk problems, and
- availability of the data and information.

Based on these criteria, we chose the following four topics which have the different risk characteristics as shown in Table 1:

1) environmental risks from chemical detergents;
2) human health risks from exposure to airborne lead;
3) human and ecological risks from agricultural chemicals; and

4) human and societal safety risks from the nonusage of seat belts.

This paper summarizes the findings of both the NSF Study (4) and outcomes of the joint workshop focussing on those four cases. The major objectives of our comparative study were:

i) to conduct a systematic comparison of risk management on the basis of "structural characteristics" of risk problems in terms of scientific knowledge, technological options and societal perceptions, and finally of decision processes in conflict arena;
ii) to suggest possible cross-cultural lessons in improving the risk management practices which cover information gathering, monitoring, regulatory decision making as well as communication among interested groups, taking account of different historical, socio-economic,and cultural background in both countries.

2. Framework for The Study

For the past two decades, major changes have been taken place in Japan and the U.S. in the nature of technological risks, as well as in the practices of managing such risks in the different context of social, political and cultural conditions. For example, in both countries the leading causes of major death or fatal accidents have been shifted from infectious epidemics or from natural hazards to chronic degenerated diseases of cancer, brain stroke and heart disorder or to automobile accidents including other high-speed transportations that are highly associated with the development of modern technological society.

In addition, there have been dramatic increases in the number of health, safety and environmental laws and regulatory agencies in charge of managing those increased risks. The increase of national or federal involvements in regulating technological risks, despite the recent tendency of de-regulation in both countries, has shown a broad array of the factors has to be taken into consideration in the current risk management policy. Beside socio-cultural factors such as a rise of environmental consciousness, a decline of public confidence in business practice of dealing with economic externality and emergence of public interest movements, some of specific science/technology-oriented factors which lead to the continued national regulatory involvement are:

- an accelerating rate of technological change in terms of physical and temporal scale and complexity of risks;
- a shorter time lag between scientific discovery or

- an increased role of public sectors as a producer of risks through its sponsorship of scientific and technological research and development;
- a rising cost of risk control and damage compensations (5).

In this context, it is reasonable to use a kind of policy research framework which consists of four major components in analyzing the risk management: They are "Science", "Technology", "Society" and "Politics" (6). Figure 1 illustrates our framework for analysis of the issues in managing technological risks.

For example, in environmental risk problem, "Science" provides the data and findings on items such as:

- types of risks and their sources,
- pathways, and climatic and topographic impacts on transportations,
- dose and exposure vs responses of living organisms,
- health and ecological effects to human and fauna and flora, and
- Factors and judgemental criteria of uncertainty.

"Technology" provides information and evaluation on items:

- technical options for abating or mitigating risks,
- institutional or administrative options for regulating risks,
- monitoring or surveillance schemes for identifying risks,

together with consideration of economic costs and benefits, resource constraints, and ecological or biological capacity.

"Society" transmits:

- experiences on hazardous events and catastrophe,
- perceptions, values and attitudes on risk issues.

Finally, "Politics" of environmental arena, interpreting either objectively or subjectively the inputs from "Science", "Technology" and "Society" in view of such political feasibility and acceptance as:

- urgency of the problems,
- efficiency of resources allocation and utilization,
- equity of distribution in benefits and damages,
- accommodation to a existing legislative and administrative framework,

will make a decision how to institute a new action or to remain in status quo.

Next step of the comparative analysis is to look at the dynamics of risk management process in which actual decision practices have been developed in the following three stages of:

i) risk acknowledgment,
ii) risk engagement,
iii) risk resolution.

Figure 2 shows a two-dimensional scheme of generic risk management (7). The dynamics of generic risk management are represented by the specified actions of four actors: activists, secondarilly engaged social groups, primary producer and user network, and legislative system.

3. Findings in Four Case Studies

Given the study framework in the preceding section, a broad array of literature and data have been surveyed and summarized as background reports to the workshop participants for their discussion and comparison. All cases show that there are a number of complicated chains of dynamic interactions among actors that have different perceptions, beliefs and decisions, in each phase of risk management process. Generally speaking, most cases demonstrated a large degree of common features in risk assessment (risk acknowledgment, and engagement), but several important differences in risk management (risk resolution) were found.

Detergent

In this particular case, both countries have shared a number of close similarity in risk acknowledgment and engagement, although Japanese responses as to reducing the phosphorus contents in detergents were largely learned from U.S. experiences in 1960s and 1970s: The issues have been how to manage aesthetic, eutrophication and health risks in bodies of water which might be increased by the intensive use of synthetic detergents.

The emergence of synthetic detergents in 1950s had compelled natural soaps because of efficiency and conveniences as well as of economical advantage in cleaning laundry and dishes. The first issue came up from the use of alkyl benzene sulfonate (ABS) in detergents which had been acknowledged as the major causes of unpleasant foaming in waterways due to slow degradability in sewage treatment facilities. In 1963, Wisconsin became the first State in U.S. to ban the use of "non-biodegradable" detergents. In early 1960s, the detergent industry responded by substituting another chemicals of linear alkylbenzene sulfonate (LAS) for ABS in detergents which are more rapidly biodegradable in water.

This substitution, however, brought the second issue of eutrophication of water bodies, in particular, in the large lakes and reservors. The excess eutrophication of increasing phosphorus content in water originated from LAS detergents stimulates algae blooms, and subsequent decay, depletes oxygen in water, and finally deteriorate aquatic ecosystem. But, the next industry's response to water eutrophication problems in 1970s of introducing non-phoshorus detergents (nitrilo tri-acetic acid: NTA) has encountered with the third issue of health safety problem, that is, possible carcinogenic risks from the NTA used in substituted detergents.

The U.S. management response has indicated a variety of efforts to regulate sources of phosphorus beyond detergents including other sources of nutrients loadings into waters, but

most of the attention has been focussed primarily on detergents because of quick and effective solution for reducing the level of phosphorus content in water. To date, a comprehensive consensus on the appropriate regulatory strategy on these three issues has not emerged.

Japan also responded to the eutrophication problem by focussing primarily on phosphorus in detergents, but rather in different ways. In particular, eutrophication of surface waters has affected greatly the water quality problem for municipal water supply in urban area. The issue of phosphorus-bearing detergents has become one of the major pollution problems in environmental politics in late 1970s.

For example, the Lake Biwa, the largest lake in Japan which supplies drinking water to more than 12 million people, suffered frequent outbreak of "algae blooms" and subsequent deterioration of water quality in the late 1960s. Mostly because of construction delay of secondary treatment facilities for waste water, it was regarded as reasonable and feasible for pollution control to directly reduce the phosphorus load from household use of detergents which accounted for 18 % of total contribution to the lake water.

The political outcomes resulted in local legislation in 1979 to ban the sale and use of domestic detergents containing phosphorus which was strongly assisted by the local women and consumers movements. Since then, non-phosphorus detergents have become dominant in Japanese market even in areas where there is no such regulation requiring non-phosphorus detergents, together with the industry's response of reducing zeolite of NTA as much as possible in their substitute (8).

Table 2 summarizes the comparison of risk management approaches in the U.S. and Japan as uncovered by the working group of detergent case study at the Tsukba workshop (9).

Lead

The approach of risk management of lead additive in gasoline may illustrate some differences in more drastic way. In 1970, the Ushigome-Yanagicho incident in one of the busiest intersections in Tokyo made it clear that there exists the risk of exposure to lead, when the mass media revealed the data of elevated blood lead levels in the residents monitored by local political and environmental groups. Although health officials found later no significant evidences for the direct causal relationship, the issue became one of the most important environmental pollution problems in the early 1970s.

The progress of reducing lead contents in gasoline in both countries is shown in the following figures (unit: grams Pb/liter):

Year	Japan	U.S.
1968	8.96	
1970	3.28	0.61
1975	0.21	0.29
1977	0.05	--
1985	unleaded	0.13
1986	--	0.026

The governmental council for promoting the use of unleaded gasolin set up in 1970 called for a immediate lowering of high lead content in gasoline from 8.96 to 3.28 grams Pb/l in 1974. Later the expert committee outlined a schedule for reduction of lead content to the level of 0.15 grams Pb/l in line with the U.S. target level by 1975 with heavy administrative regulatory guidance ("gyousei-shidou") to the oil refinery industries to increase the production of less-leaded or unleaded gasoline. A total ban of lead in gasoline was finally adopted in 1976. Beside health safety, this decision was also supported by the additional requirement in compliance with the exhaust gas regulation from automibiles with catalytic converters.

In the U.S., the Environmental Protection Agency was sued in 1975 for its action to list lead as a pollutant under the Clean Air Act. This action was challenged, but eventually listed as a pollutant, and the air quality criteria and standards for lead additives were developed. The energy crisis in 1974 and subsequent economic recessions delayed the reduction of the lead content in gasoline in comparison with the Japanese case.

Table 3 summarizes approaches of managing risks from lead additives in gasoline in the U.S. and Japan conducted by the task group in Tsukuba workshop (10).

Beside the very similar process in risk acknowledge process, there is a clear distinct characteristic in risk engagement and resolution processes. The U.S. system of evaluating risks appears to be more open, with greater transfer of information promotes a lengthy process with the opportunity for different views to be heard. By contrast, the Japanese system does not seem to provide an opportunity for such a variety of information to be made available to the outside groups or interested individuals. Rather such information is restricted to the expert committee for their scientific evaluation of risks.

Pesticides

The use of synthetic pesticides increased rapidly in both countries since the late 1940s. Partly because of geographical and climatic differences, the magnitude of pesticides use in Japan has been markedly larger than that in the U.S. in terms of average consumption per unit arable land. During the 1970's Japanese farmers were using some 31 pounds of pesticides per hectare; by comparison American farmers were using an average 1.19 pounds per hectare, though total annual consumption of pesticides amounted to 350 million pounds by 1980 in the U.S.

This fact has added additional acute and chronic health or accidental safety problems to Japanese farmers besides a number of well known environmental pollution problems such as toxic residue formation in crops and soils, acute and chronic toxicity in wild life and other ecological organisms.

The contents of technical studies undertaken in each country's management process is largely same in terms of testing procedures (acute and chronic studies), and evaluation criteria and methodologies that are now internationally standardized. Each country utilizes basically a two-step management system. Prior to commercial sale in market, pesticides are subject to registration review and assessment. Secondly post-monitoring assessment continue as warranted. For examples, registration status and conditions may be revised or ultimately cancelled as new evidences on effectiveness and adverse impact of the use in fields become available.

Instead, the management process in each country has different approach which has been deeply embedded in the political and cultural landscape. Strong pro and con interests and conflicts among various actors contend in a different way for influence on pesticide policy formulation. Foremost among the differences is the formal procedures of risk assessment which is accorded to so-called risk-benefit studies in pesticide assessment. In the U.S., the special review procedure of quantitative risk-benefit studies is required as a formal process in the management practice. There is, however, no such legal and administrative procedure in Japan. Rather such analyses, when conducted informally in advisory committees, tend to be judgmental in character.

Table 4 summarizes the outcomes of task group discussion as to approaches to risks from pesticides problems in terms of risk acknowledgment (assessment), risk engagement (policy formulation), and risk resolution (technology development) (11).

Seat Belt

Traffic fatalities in both countries increased during the 1960s. By 1970, Japan hit an all-time high of 16,765 as Japan moved into a highly motorized society. The number of cars registered had trippled between 1965 and 1970. The number of traffic fatalities in the U.S. passed 50,000 in the middle of the 1960s and reached an all-time high of 54,589 in 1972. Both figures have decreased in the subsequent years, but not substantially in numbers, and again began to increase slightly in the early 1980s.

Although wearing seat belt is perceived as one of the most effective means of reducing the traffic fatalities, seat belt usage in both countries has been low until the time of the study in 1984: average usage in both countries was under 20 percent. Despite successful mandatory seat belt law in most European countries, neither the U.S. and Japan had passed an enforceable mandatory seat belt law by 1984.

Japanese development of seat belt began in the mid 1950s with initial attention of seat belt concept by assessing its effectiveness in vehicle safety systems. By the mid 1960s, the standards for seat belt designs and associated joint mechanisms were developed, and mandatory installation of seat belts in Japanese cars began in 1968. While seat belt equipped cars, later expanded to rear-passengers and even trucks, have become standard in Japan, it has been left to individuals whether they use the seat belts or not. Although the compulsory use of seat belts on the express highways was added in the Road Traffic Regulation Law (RTRL) in 1971, there was no penalties specified for enforcement.

In 1977, the National Public Safety Commission proposed a revision of the RTRL to include the mandatory usage of both helmets for motorcycle riders and seat belts for automobiles passengers. The matter of mandatory use of seat belts on all roads was postponed by 1986 mainly because of low public acceptance for mandatory usage with any penalties.

In the U.S., the government responses to reducing traffic fatalities began in the mid 1960s including a requirement for safety devices on automobiles. The first federal standards for automobile seat belts and a requirement for installation of seat

belts in new cars were issued in 1968, and the first proposal for mandatory automatic restraints of seat belts emerged in 1969. A strong, negative public reaction, however, resulted in simple requirement for presence of manual seat belt.

Since that time, an array of legistlation, regulatory standards, and industrial proposals have been tried for acceptance or rejection, and often replaced by further legislation, standards and proposals. In general, the U.S. has avoided federal laws or regulations for mandatory usage of seat belts in nationwide, except for child safety seats now required in all 50 states.

Table 5 summarizes the approaches taken to seat belt usage by the major actors involved in management system in both countries by the members of the task group in Tsukuba workshop (12).

There exists obvious parallels in the attitudes and activities of government police and traffic safety agencies against the passage of legislation for mandatory use of seat belts. This reflects the public reluctance of restricting individual freedoms in spite of increasing public concern over traffic safety as seen in various recent polls. The insurance and legal systems have not been significant sources of motivation for increased seat belts usage in both countries. In Japan, auto liability system which imposes a heavier burden of liability compensation on the lesser-injured party who actually wear seat belts. The mixed insurance system of the U.S. carries no great motivation for higher usage of seat belts as well.

4. Concluding Remarks

All four case studies of risk management practices in the U.S. and Japan suggest a strong similarity on scientific studies for risk acknowledgment, but a substantial difference on regulatory approaches in the process of risk engagement and resolution processes. It would be too easier to attribute major reason that has made such distinctive differences in regulatory approaches, to cultural differences rooted in both countries. Nevertheless, in the area of risk management in which regulatory decisions have to be made under high public involvement and high uncertainties in risk assessment, political and cultural factors are the ones dominated among others.

Governmental bureaucracy and agencies in Japan still retain a strong paternalistic character (13). Given such a deep cultural tradition of keeping legitimacy and authority in overseeing broad social interests of society as a whole, their policy making has tended to a centralized process and closed to influences outside the point of view held by the governmental bodies. This credibility and accepted responsibility are underlied in their ways of orientating the concerned parties toward consensus building in decision makings with emphasis on non-legal approaches in implementing policies or achieving conforming social behaviors. Japanese approaches of risk management draw heavily on these traditions (6).

By contrast, the U.S. government and agencies are more formal and open, but viewed with some suspicion by the interested groups. This attitude, along with the belief in the underlying social rationality of adversarial competition among idears and interests, promotes open and adversarial ways of political decision making process in which contention and disagreement are often aggressively pursued. Technological risk management process of acknowledgment, engagement and resolution is fought in this political and cultural background. Because of this institutionalized processes, government policy making is often subject to the decentralized influences and is prone to intense advocacy and fragmentation in outcomes, and resulted in a coercive and legal bent of political relationship between "gainer" and "loser".

The followings are the some of the important recommendations that were agreed in workshop participants for improving current practices of technological risk management in the U.S. and Japan (4):

1. The use of full and open disclosure when investigating scientific data relating to a risk. Such an open atmosphere allows for the input of all affected parties and the examination of scientific data.

2. The use of cooperation and consensus rather than antagonism and conflict. After the data has been examined, the use of consensus would reduce the lengthy process between recognition and action as exists in the U.S. This could manifest itself in compromise for a common goals.

3. The use of incentives as opposed to enforcement. Economic incentives and non-regulatory incentives may be more effective than regulation and enforcement. Incentives may also require less administration.

4. The development of risk assessment techniques, such as cost-benefit analysis. Because Japan does not have formal risk assessment procedures, these techniques should be explored in a cultural context. Risk assessment in the U.S. is not a standardized process and requires additional investigation, especially in the case of hazardous wastes.

References

(1) Lave, L.B. and J. Menkes: Managing Risk; A Joint U.S.-German Perspective, Risk Anlysis, Vol. 5, No.1, 17-23, 1985.

(2) Brickman, R., et al.: Controlling Chemicals: The Politics of Regulation in Europe and the United States; Cornell Univ. Press, Ithaca, 1985.

(3) Kawamura, K ans S. Ikeda (eds.): Proceedings of the First U.S.- Japan Workshop on Risk Management, Tsukuba Science City, Japan, October, 1984.

(4) Kawamura ,K., M.Boroush, S.Ikeda, P.Lynes & M.Minor: Risk Management in the U.S. and Japan, Final Report to the NSF, Management of Technology Program, Vanderbilt University, May 1986.

(5) Covello, V., K. Kawamura, P. Lynes and M. Minor: A Historical Perspective; in Proc. of the First U.S.- Japan Workshop on Risk Management, ibid (3), 1984.

(6) Ikeda, S.: Managing technological and Environmental Risks in Japan; Risk Analysis, Vol. 6, No.4, 389-401, 1986.

(7) Kawamura, K: Risk Management and Assessment in the U.S.: Perspective on the state of the arts; in Proc. of the First U.S.- Japan Workshop on Risk Management, ibid (3), 1984.

(8) Morioka, T.,: Risk Management of Household Detergent in Japan; in Proc. of the First U.S.-Japan Workshop on Risk Management, ibid (3), 1984.

(9) Vlachos, E. and T. Seishi: Summary Conclusions from Detergent Task Group of Tsukuba Workshop, ibid (3), 1984.

(10) Parker, F. and M. Tanaka: Summary Conclusions from Lead Task Group of Tsukuba Workshop, ibid (3), 1984.

(11) Boroush, M. and S. Ikeda: Summary Conclusions form Pesticide Task Group of Tsukuba Workshop, ibid (3), 1984.

(12) Kasperson, R. and N. Sakashita: Summary Conclusions from Seat Belt Task Group of Tsukuba Workshop, ibid (3), 1984.

(13) Sueishi, T. and Nishimura, S.:The State of the Arts in Risk Assessment in Japan; in Proc. of First U.S.-Japan Workshop on Risk Management, ibid (3).

Figure 1 Study framework for Technological/Environmental risk management

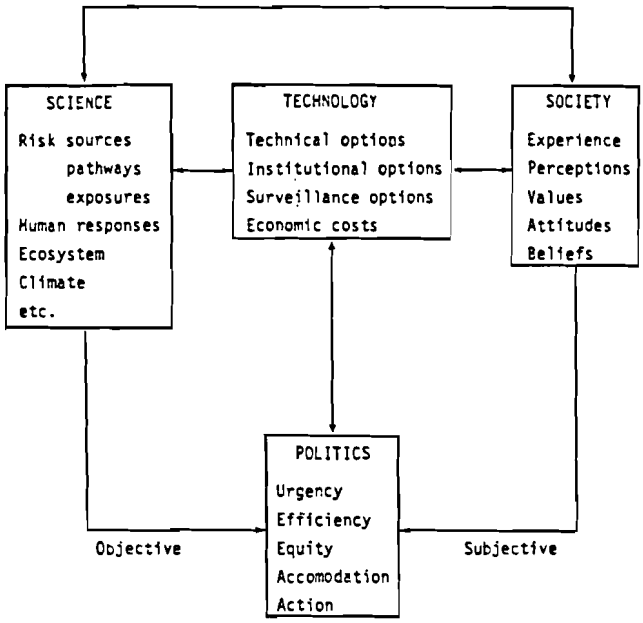


Figure 2 Dynamics of generic risk management processes

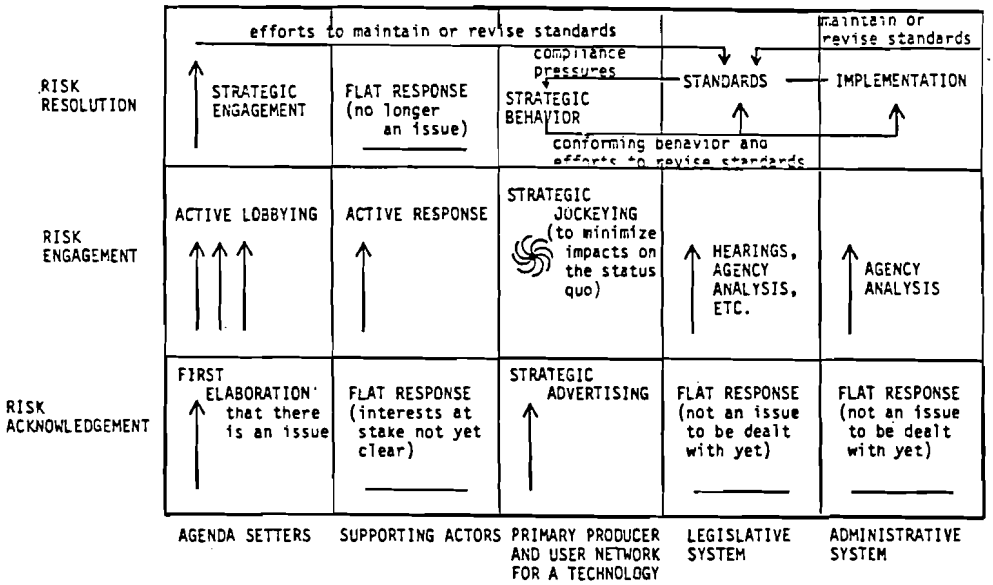


Table 1 Case study topics and risk types

Case Study	Risk Type	Nature of Inference Task
Detergent	Long-term environmental	Direct, originally from visual evidence
Lead	Chronic human Point source	Indirect, from human measurement, monitoring
Pesticides	Acute human Long-term environmental Non-point source	Indirect, from human and other measurement, monitoring laboratory testing
Seat Belts	Acute human	Direct, from experimental evidence

Table 2 Comparison of approaches to technological risk from detergents

Detergents	U.S.	Japan
1. Regulation	Law	Administrative guidelines
2. Levels of Gov't	Federal, state, local	Mostly central
3. Laws	Broad--water quality & human health	Nonexistent or narrow
4. Agencies	Strong	Weak
5. Industry Role	Increasing	Not significant
6. Public Role	Large, Secondary	Large, Primary
7. Scientific Community Role	Large & improving	Selectively applied
8. Interaction & Info-sharing	Large & increasing	Limited; even restricted
9. Risk Assessment	Emerging	Not clearly focused
10. Risk Management	Separate	Focussed
11. Source of Data	All	Limited; no industry
12. Media	Reflector/detractor	Major actor

Source: E. Vlachos and T. Sueishi, "Summary of the Detergents Task Group", Proc. of the First U.S. Risk Management Workshop, Tsukuba Science City, Oct. 1984.

Table 3 COMPARISON OF APPROACHES TO TECHNOLOGICAL RISK FOR LEAD PROBLEMS

Phase	U.S.	Japan
Acknowledgment/ Recognition	Local citizen group Large citizen group Respond to problems directly affecting individuals	Local citizen group Mass media important Respond to broadly implied problems
Engagement/ Measurement and Evaluation	Adversarial Open Formal Risk Assessment	Committee system Closed, Ad Hoc No Formal Risk Assessment
Resolution/ Control	Standards Legal Enforcement Encourage regulation Compliance vs. problem solving	Directives Guidance Non-punitive Co-operative Consensus

Source: Parker, F. and M. Tanaka, "Summary of the Lead Task Group," Proceedings of the First U.S.-Japan Risk Management Workshop, Tsukuba Science City, Japan, October 28-31, 1984.

Table 4 Comparison of approaches to technological risk for pesticides problems

	U.S.	Japan
Scientific Studies and Risk Assessment	Proper interpretation of animal toxicological data	Proper interpretation of animal toxicological data
	Better identification of differential exposures among populations groups	Conduct of risk assessment studies--particularly for very low level exposures
	Knowledge of mechanisms of pesticide biodegradation	Assessment and communication of appropriate precautions to users of household and garden pesticides
Process and Policy	Determination of acceptable exposure levels	More extensive review and use of toxicological data
	Priorities for assessing pesticides that are contaminating ground waters	Achievement of a better balance between technical assessments and political needs in policy formation
	Improvements in the speed and effectiveness of the operation of the regulatory system	Generation of greater public awareness of toxicological information
		Shift of the dominant cultural orientation for "safety" assessment more toward toxicity assessment
Technology Development	Development of pesticides with acceptable performance and environmental characteristics	Development of more effective pesticides --particularly to meet the needs of small land areas
	Capabilities for effective management of pesticide run-offs into water	

SOURCE: Pesticide Task Group discussion at the U.S.-Japan Workshop on Risk Management.

Table 5

Summary of Approaches to Seat Belt Management
in the United States and Japan

	U.S.	Japan
GOVERNMENT	Avoid regulation	Avoid regulation (but follow the lead of foreign countries)
	Periodic information campaigns	Periodic information campaigns
	50 State child restraint laws	No child restraint laws
	State + local initiative	Prefecture + local initiative
INSURANCE/ LEGAL	Mixed: No fault 3rd party	If fault unclear, assign liability to lesser injured
	Lower rates for passive restraints + air bags (but small savings)	No preferential rate but some higher damage awards (for death)
	Some higher compensation awards	
INDUSTRY	Resist regulation	Initial reluctance, then neutrality
	No marketing initiative	No marketing initiative
INDIVIDUAL	High perception of effectiveness	High perception of effectiveness
	Opposition to mandatory use	Opposition to mandatory use
	Conflict with individual freedom	Conflict with individual freedom
	Relatively flat use rates (10-15%)	Slightly increasing (?) use rates (5-10%)

Source: R. Kasperson and N. Sakashita, "Seat Belt Usage in the United States and Japan. A Summary of Conclusions from the Seat Belt Task Group,"

3. MAN–MACHINE INTERACTION

3.1. MAN-MACHINE INTERACTION

Björn Wahlström
Technical Research Centre of Finland
Espoo, Finland

1. INTRODUCTION

There has recently been a number of spectacular incidents where human errors have been an important contributing factor. At the Three Mile Island nuclear power plant in 1979 the operators did not completely understand the state of their plant and they made a number of errors, which resulted in a loss of coolant accident and a partial melt down of the reactor core. In Bhopal in 1981 a series of operations led to the release of toxic gas that killed about two thousand and injured several thousand people. Later investigations have indicated that the safety management of the plant was not at a satisfactory level. The Challenger accident in 1986 killed the crew of astronauts and was caused by a leaking seal known to produce trouble in weather conditions like those the morning of the launch. The Chernobyl accident in 1986, which killed about thirty persons and caused a large fallout in Europe, was caused by a number of deliberate violations of safety rules. The release of toxic substances from the Sandoz factory into the Rhine should have been possible to avoid by appropriate fire protection equipment and a consideration of the possible consequences of a fire.

The accidents may seem different but they all have in common a breakdown of same aspects of interaction between man and the technical system. The investigations of the Three Mile Island incident identified control room design, emergency operating procedures and operator training as the main contributors to the human errors. At the Bhopal plant there had been a deterioration of the operational staff and no

actions had been taken on identified safety threats. In the space shuttle programme the problem with the leaking seal had been identified several years earlier, but a redesign had been considered too difficult to carry out without a serious delay. The Chernobyl operators were apparently not aware that their actions were dangerous and they were too eager to carry out the tests they had been assigned to do. The Sandoz management should have been aware of the risks with the storage of chemicals but they chose not to fund improvements in fire protection.

The incidents have brought out a distrust of the technical systems and the decision-making process leading to the construction and operation of such systems. This distrust has been most clearly seen in the nuclear power field, where decisions not to commission even ready built nuclear power plants have been taken. Some of the distrust is clearly based on emotional feelings, but the more objective opposition is based on a consideration of the risks associated with complex technology. Any human activity will involve different kinds of risks and the use of a technical system is justified only if the benefits of its use outweight the risks. The decision either to adopt or abandon a technology should therefore be based on an assessment of benefits and risks associated with that technology. The risks for a technology in use should naturally be brought to a level as low as is reasonably achievable. This means that requirements have to be put on the systems also with respect to how the human and system interactions are arranged. The question here is whether or not it is possible to build complex systems which are safe enough.

2. INTERACTIONS BETWEEN MAN AND MACHINE

Man will interact with the machine in several different ways in a complex technical system. The following general roles for the human in the system may be identified

- the decision maker
- the designer
- the constructor
- the safety analyst
- the operator
- the maintainer
- the manager

The construction of any large plant will be preceeded by a detailed analysis of the technology, the resources needed, time schedules, costs, staffing, etc. In that process a number of decision makers have to make up their minds on the size of the plant, the site of the plant, vendors etc. The construction of the plant is often also connected with different permits granted by authorities. A safety analysis is usually carried out as a part of the predecision assessment. As the decision makers are human, it is possible that they make suboptimal decisions with regard to the technology, the vendors, the site selected etc. The decisions will also have a large influence on the requirements placed on the design of the completed plant.

The designers are usually working with a fixed budget and a fixed time schedule. The design of a complex industrial plant is always based on earlier design, where the proof of principles have been obtained. The earlier designs are then changed in the design project and scaled to get a better performance for the new plant. Design in general can be very complicated where a satisfactory solution has to be sought in response to several conflicting requirements. To improve the quality and efficiency of design, a number of design guides have been developed. Considering the human in the system, the design project should be able to arrive at an acceptable solution with respect to eg. control room design, procedures and operator training.

The construction of a large plant can require the cooperation of thousands of people and involve millions of drawings. During the construction process deficiencies in the design may be detected and they should be corrected without disturbing the overall schedule of the construction. It should be possible to check the quality of the components and the work done in all phases of the construction project. All design solutions should also be documented as the plant is constructed. When the construction has been completed, then the plant should be started up section by section after the completion final of tests for the components, subsystems and systems. When the start-up has been completed, a period of test operation is initiated, this aiming at identifying all the operational characteristics of the plant.

Any potentially dangerous industrial installation should go through a systematic safety assessment procedure. Depending on the size and type of plant, the procedure will be carried out by one or several safety engineers.

During the procedure, hazardous process states and sequences of events are identified. The likelihood of the different safety threats are then assessed and barriers are then built into the process, the automation, the control room and the procedures.

The operation of an industrial plant is usually carried out on a regular shift basis, the size of the shift depending on the type of plant and the selected level of automation. The operators are usually hired in due time before the start-up of the plant, and they are given both theoretical and practical training. In modern automated plants the operations are usually carried out from a centralized control room with only a few tasks in the plant performed by rowing operators. The main tools of operation in the control room are control boards and panels equipped with different kinds of displays and controls. Today most new plants use computers in the control room. In addition to the technical equipment, the control room operators have access to different kinds of plant documentation such as procedures, system descriptions, drawings etc.

Test and maintenance is carried out as a regular activity at all industrial plants. When safety is a specific concern, preventive maintenance is adopted as a policy ie. a component is maintained or changed either regularly or when regular tests indicate that maintenance is necessary. Test and maintenance at a complex plant will require coordination with the control room to ensure that correct components are worked on etc. Maintenance of the very many different components and systems will require good documentation and procedures.

The management will ultimately be responsible for the performance of the organization. This means that management should be able to motivate the personnel to use agreed procedures to insure the safety in all stages of design, construction, operation and maintenance. The management should also be able to detect degradations in performance

and to rapidly bring the organization back to the required performance level. The management should also be sensitive to weak signals of approaching problems to initiate development or training programmes sufficiently early.

3. HUMAN ERRORS

Any error, human or technical, can be seen as one point in a chain of events. This means that the error will have different causes and it can lead to different consequences. A search for the causes helps to identify places where remedies can be applied. A search towards different possible consequences of one or a combination of errors will indicate the importance of the errors with respect to plant safety.

A human error can be defined as an act outside some range of acceptability. A human error should never be accepted as an explanation, rather different contributing causes should be sought in the same way as for technical errors. This means that explanations should be sought where remedies could be inserted, eg. control room design, procedures and operator training. The system design should aim at solutions where untolerable errors can be avoided.

In order to improve system design one has to aquire some understanding of human behaviour. Human errors can be said to be a part of human nature, trial and error providing the basis of human learning. Where errors can not be tolerated, barriers have to be built in, either by providing procedures for a correct operation or by building interlocks to prevent incorrect operation. Collection and analysis of human errors can give a more accurate picture of different causes of human errors.

Considering different human errors, one has to isolate errors of intention, sabotage and cheating being examples. A human being incapacitated by alcohol or drugs is another case where the error could be considered intentional. For nonintentional errors the division between slips and mistakes has been suggested. A slip is then a case where the human did know better, but made an error which was immediately recognized. A slip will then be observed from the outside only when the slip can not be corrected before the plant has been

driven to a point of no return. A mistake in this connection is an error committed in considering the act as a correct one although a thorough analysis would have revealed it as incorrect. A mistake will then indicate deficiencies in understanding the plant, which again could be due to deficiencies in control room design, procedures, training, etc.

Human errors can be committed in all phases of design, construction, operation and maintenance. As human errors can not be avoided completely, the crucial thing is to detect errors committed before they influence the safety of the plant. One possibility in this connection is to include different checks to ensure that everything has been done according to standards before the plant is started up. This should be done as a regular quality control procedure where independent checks are introduced. In a similar way the safety assessment should be carried out as an independent procedure to search for possible weak points and to introduce improvements where weak points are found. One type of human error, which actually points towards deficiencies in management, is connected with deterioration of quality control and safety assessment functions.

Organizational deficiencies can be introduced as a separate category of human errors where the interaction of several individuals is considered. In this connection one may see cases where information is not distributed in the organization in a proper way. One also finds cases where safety has short-sightedly been traded in favour of economic considerations. Maintaining preparedness for unexpected events is also an important task of the organization.

4. THE MAN IN THE SYSTEM

There are many different and often conflicting requirements placed on an industrial plant. The requirement to take the abilities and limitations of the human into account in system design is actually derived from the more general requirements of the plant economy and safety. The design process is supposed to arrive at a technical solution which is a satisfactory compromise between the different requirements. This means that the technical solution will reflect some

requirements better than others, where the designer has given an order of priority for the requirements. It is important, however, that all relevant requirements are included in the original design specifications to be considered.

The requirement to also take the man into consideration seems to have been forgotten in many of the plants, in their maintenance procedures and management systems. Man is clearly fallible, though as a system component can be very ingenious when given appropriate tools and a nonhostile environment. The objective in the system design is then to be able to build in the barriers against intolerable human errors, but at the same time give the humans in the system the possibility to do their best. This objective places requirements both on the plant and the organizational design.

Automation has been one of the means by which the harmonization of man and machine has been pursued. Early automation tried to a large extent to remove the man from the system as a response to the need for improved working conditions, and to observed human shortcomings in the operation of the processes. Automation has been developed by control engineers, who have not always had an understanding of human behaviour. Some of the problems have, however, been identified and different guidelines for the design of man machine systems have been developed. The problem, however, seems to be to integrate such guidelines into the actual design projects.

The design of the control and instrumentation of a plant embraces the definition of the automation concept, the control room design and the design of the instrumentation and the plant computer systems. The exact division of the different design activities depends on the country and company tradition. The man-machine guidelines developed have to a large extent concentrated on control room design. The guidelines are often written in the form of a check-list of questions, to which it should be possible to answer with a yes in order to meet the requirement. The guidelines seem, however, to reflect at the same time both requirements and specific design traditions. This makes it difficult to utilize the guidelines in one place, if they have been developed somewhere else.

Guidelines for writing procedures have also been developed and similar problems in how they are used can be observed as for other guidelines. The correctness of the procedures in all possible operational conditions of the plant is the main problem and this cannot be solved using the guidelines. Recommendations for training operators of a plant have also been developed. Training simulators are commonly accepted as being very efficient tools for operator training and this approach is used regularity in the aerospace and the nuclear industries.

With regard to what is known about the principles for how to account for the man in the system, the main problem seems rather to be how to integrate that knowledge into system design than to generate new knowledge. This is also reflected in a commonly seen attitude that improvements of the design process are unnecessary and difficult if not impossible to carry out. The striving for efficiency has also implied that the subsystem designers do not usually have the broad overview of system and human behaviour necessary if somewhat general design rules are used. The problem seen here involves the need to cope with the complexity of a modern industrial plant, where very strict financial limits for all activities are given.

The only way of coping with the complexity of a large industrial plant is to build up several independent feedbacks in the design, construction, operation and maintenance of the plant. The feedbacks should directed to detecting and correcting errors observed at different levels. This means that in the design project there should for all design activities be an independent checking and authorization mechanism by which the quality of each activity is maintained. Feedbacks should also be built at different hierarchical levels to ensure that performance on a system level is a satisfactorily result of accepted subsystem performance. Similar systems of feedbacks should also be built on a national and international level where a continuous evaluation of the performance of the system takes place and necessary actions are initiated when degraded performance is identified.

One of the main problems in the consideration of humans in the system is associated with the difficulty of making predictions regarding their behaviour based on system characteristics. This means that it is very

difficult to include the human actions in a systematic safety analysis. The methods developed so far can give qualitative guidance for the relative importance of some of the sequences of events, but all quantitative estimations will be very unreliable. A possibility here is to adopt a safety management approach, where experience on system behaviour is collected at each level and compared with available safety analysis. In this approach all events will be analysed to decide if they are expected within the normal variability of the technical system or the human. If an event is accepted as being something normal, then no action will be taken. If the event occurs too frequently then it should lead to a change in the system. The safety analysis should always be living in the sense that changes in the process, the instrumentation or the organization should be updated in the safety analysis and its assumptions.

5. TECHNOLOGICAL RISKS AND THE SOCIETY

Technology will undoubtedly bring with it new risks, which have not been a part of the life in a pretechnical society. The motives behind the introduction of technology are the benefits which are considered to be larger than the costs. The problem with introducing new technology is that some but not all risks are seen in the beginning. This is clearly due to the fact that new technology can have drawbacks and can affect the society in many different ways which are not immediately seen and the persons responsible for the development of new technology cannot have the required broad overview to consider all secondary and tertiary effects. The introduction of new technology often occurs gradually, which means that it is possible to adapt it with respect to risks observed later.

The risks associated with the utilization of technology have been raised as a political argument in many countries. The risks are in some cases based on new experience and in other cases problems which experts have been aware of for a considerable time. In the case of new experience it may take a considerable time to develop new solutions, if the new technology has to be abandoned. If experts have been aware of a problem associated with new technology, then usually at least a partial solution exists. In both cases, however, the decision regarding how to

cope with the risks will be based on economic considerations. Economic considerations are usually brought into a framework of political decision making where costs and benefits are calculated and the priorities are set.

A political decision taking position on a question concerning risks should be based on a systematic analysis. This means that decision alternatives should be assessed within a common framework with respect to different scenarios of events. The difficulty, however, is to create a reliable model of all possible scenarios together with a valid quantification of risks, costs and benefits. The problem is also to be able to utilize available experience in all the different fields of knowledge. Another problem is to communicate the results of the risk analysis to the decision-maker in a comprehensible form.

The handling of the problems of complex technology in political decision-making depends on the interaction between experts and laymen. As no single person can manage the knowledge needed to understand all aspects of any specific technology, the decisions have to be made by a group, where each individual has his own field of expertise. To render the decision acceptable it has to be possible to scrutinize it independently, which means that it should be possible to communicate to laymen. Here an understanding between experts and laymen is needed and this requires trust of another person's judgement. This trust can be maintained only if reasons for the judgement can be communicated together with an account of one's own motives in a comprehensive form.

One of the problems regarding new technology is associated with the beliefs and expectations arising from it. When a new technology is introduced it is very common that it is marketed with optimistic expectations. The expectations create beliefs in the benefits of the technology and if the expections cannot be fulfilled in a certain timeframe a feeling of frustration can be created. If such a frustration is combined with fears of something unknown and is accompanied by a superior attitude on the part of the experts, it is very likely that an earlier positive attitude may be changed into one of opposition. Taking into account the tendency of humans to build their beliefs on evidence and to collect new evidence only in support

of old beliefs, it is easy to understand, that a polarization can occur. The deadlock over the debate of the pros and cons of nuclear power can at least partly be explained by such a model.

To arrive at a balanced view in society with respect to new technology, it has to be supported with popularization, which enables an enlightened layman to understand it. This means, that simplified models should be developed to explain how technology works. The models should be supported with a clear explanation of the limits of their validity in order to avoid their abuse. Models should also be developed to provide a better understanding of how technology and society interact to be able to support the political decision-making. Also those models should be popularized to provide a basis for debate on the goals for social development.

6. CONCLUSIONS

Man will always be a part of any technical system as a designer, constructor, safety assessor, operator, maintainer and manager. Man is also fallible, which means that provisions should be built into the technical and the managerial systems to detect errors before anything serious occurs. The problem of today is not what we do not know, but to utilize what we do know. A part of this problem can be solved by adapting the existing tools to specific design and work practices, while another part can be solved by training and education. There is, however, a generic problem in the design of complex processes, which is connected with the managerial system in use. This problem concerns the development of new tools for the design, because the cost of such a development cannot be justified without a construction project, but when such a project has been started, there is no longer time to develop the tools needed.

The importance of the man in the system as an operator and a maintainer is well understood today. The importance of the designer, the constructor and the safety analyst is also well understood, although human errors in those tasks are seldom analyzed in the same way as operation and maintenance errors. The importance of the management is still less understood and organizational errors are usually not even

used as a category in analyzing events. The idea that the layman in society has an important role in decision-making regarding new technology's adoption or abandonment is something new in the society of today. The idea that politicians are fallible humans with their own goals and ambitions, working in an unstructured decision-making environment has to come if we want to avoid costly human errors in the social decision making process.

One of the crucial things in avoiding human errors will be how well we are able to handle the complexity of the systems. The decision-makers have to support their own understanding with different kinds of models provided by their training and the decision support systems used. The requirement of human understanding within the span of control for the decision maker may actually set a limit on the manageable complexity of a system.

Looking at the records of high-risk industries, one may get the pessimistic impression that the accidents are necessary before any system is improved. It is true, that many of the problems revealed in accidents have been realised, but this fact rather points towards a possibility than a problem. If we are able to solve the managerial problems of utilizing available knowledge and if we are able to allocate enough resources then it should be possible to create safe systems before accidents force us to do so. With an understanding of the problems together with an effective collection of experience, it should also be possible to create sufficiently safe complex systems. Manpower with a background both in systems engineering and behavioural sciences will have to be available for this to be achieved.

3.2. NEW DISPLAY AND CONTROL TECHNOLOGIES AS SOURCES OF DIFFICULTY FOR THE HUMAN PROCESS OPERATOR

L. Bainbridge
Department of Psychology
University College London
London, England

INTRODUCTION

Computer generated display-control interfaces and computer based automatic control systems give us interesting new potential for supporting the human operators of high risk industrial processes. They can also pose new difficulties, causing slow and error-prone activity. The new equipments and working methods are usually designed in ignorance of the factors which affect human error rates, although many of these factors are well understood, and it is possible to design to minimize human error (e.g. Rasmussen & Rouse, 1981; Rasmussen et al, 1987). The main problem is one of "technology transfer," of drawing designers' attention to the relevant principles and data. Therefore, this paper outlines aspects of human factors which are well known and indicates how to design to reduce error, emphasizing issues which have not been widely discussed elsewhere. It is not possible to remove human error altogether, but it is possible to:

1. reduce human error by an order of magnitude through appropriate design of equipment;

2. use our understanding of human error and recovery to design error tolerant systems (e.g. giving rapid feedback about the results of actions, making actions reversible).

If our knowledge of what affects human error is not used in design, then this raises serious questions about the attribution of responsibility for human error. If an operator makes a mistake, but the equipment is designed in such a way that it is difficult not to make a mistake, then the responsibility lies with the designer of the equipment, not with the maker of the error (see e.g. Malone et al, 1980; Reason, 1987).

This whole area of designing equipment and work for human beings is a technical discipline in its own right. In this paper, we will look briefly at two main aspects:

1. New display technologies: computer generated displays ironically can display both greatly extended and greatly reduced information to the human operator.

2. New control, decision, and advice-giving technologies: decision-making by computer allows increasing amounts of the process operators' task to be done automatically, while

Expert Systems expand the possibilities for the operators to interact with intelligent advice-giving machines.

How should these two types of new technology be designed to enhance human operation, rather than to make it more difficult? We will outline some of the basic human information processing characteristics. Designs should take advantage of high capacity processes, and minimize the use of low capacity processes and time pressures.

The main human information processing characteristics are:

A. High parallel processing capacity for:
   1. Visual and sound patterns and semantic context;
   2. Skills.

B. Low serial processing capacity (which deteriorates further under distraction) for:
   3. Working memory;
   4. Time to translate from one form of representation to another (whether these are two different external displays or one external display which is not compatible with the viewer's mental representation of the task).

Reaction time shows a speed-accuracy trade-off. People can take a variety of lengths of time to do the same work. When we work slowly, we make minimum errors. But as we try to work faster, there comes a break point below which every increase in speed is paid for by an increase in errors. If people doing an easy task are put under pressure, they can work better. But when people doing a difficult job are put under pressure, their performance will deteriorate.

I. NEW DISPLAY TECHNOLOGIES

There are three important themes in the use of computer generated multi-plexed displays:

Expanded Information:

1. "Anything" can be displayed, so what should be?

Reduced Information:

2. Any VDU shows a narrow "window" onto the potentially available data about the process, so what information should be available at one time? There is a huge dynamic data-base of information about a process which the operator should keep track of.

3. The information on any one VDU frequently changes, so how can users keep track of where they are in relation to the other potentially available data, and how to navigate around this data-base to find other information?

1. Optimum Individual Display Formats:

People react more quickly and accurately to display codes (e.g. magnitude, color, shape) if the codes are salient and discriminable (both these depend on human sense organ characteristics, VDT contrast and resolution are usually inappropriate for the human eye), and if they are compatible, unambiguous and consistent (i.e. each code has one and only one meaning).

As an example of the effect of using a non-optimum design: Grether (1949) found that pilots made 17 times more errors and took over 4 times as long, when reading a "3-pointer" altimeter (the type to which many aircraft crashes have been attributed) than when reading the form of display which is now used. There are several US and European Standards and Guides for human aspects of control system design (e.g. Kinkade, 1984; Anon., 1985). The majority of these are oriented to conventional interface technology and hard-wired control, but are equally applicable to software based interfaces. They do no explicitly include the new problems posed by graphic or multi-paged limited-window interfaces, nor do they emphasize design for error recovery. But the information which we do have about human cognitive processes used in these tasks allows us to make strong design proposals for these new situations.

Visual patterns, which are possible on graphic displays, are good for tasks involving comparing or relating. Comparing and relating tasks can become trivially obvious on a well designed pattern/graphic display, compared with an alpha-numeric, or verbal, presentation.

Computer generated display technology means that information about any part of the process can be displayed in "any" format (compared with conventional hard-wired display-control interfaces, on which each variable is linked to one display). Therefore, it could be possible to produce many individual displays, each optimum for a particular part of the operators' task. There are therefore practical questions about the optimum format of these representations. This is a specialist topic, concerned with optimum representations for different types of information (see e.g. Bainbridge, 1987; Goodstein & Rasmussen, in press).

2. Multi-plexed Graphic Displays:

In multi-plexed display systems, only one (or a small number) of the potential display formats (which run to several hundred in some systems) is shown on each VDT at any one time. The others can be "called up" when needed. Practical questions are therefore concerned with how many different display formats there should be and with how many should be viewable at the same time.

Number of different display "pages:"

In assessing the number of different formats, remember that people take time and may also have difficulties of understanding when translating from one representation to another. For example, people given an item in one layout and asked to find its pair in another layout take about 4 times longer and make about 4 times as many mistakes if the two layout patterns are random, compared with when the two layouts are the same (Fitts & Deininger, 1954). This implies that people would work more effectively if the number of different layouts is minimized as this will minimize cross-reference problems.

Considering the ideal number of display pages, in summary we can say that increasing the number of pages (given a constant number of VDT's):

A. Reduces the user's:
   1. Need to remember process structure or functions;
   2. Time spent on individual problem-solving tasks (considered in isolation);
   3. Amount learned about relations in the process and how to solve problems.

B. Increases:
   1. The explicit task specific information;
   2. Coding and cross-reference problems;
   3. Problems of finding place in total data-base;
   4. Display accessing time;
   5. Software investment.

Number of VDT's:

If all the information that the operator needs is not all displayed on available VDT's, then the user must call up another page and compare the new page with memory of the previous one. The important cognitive limit here lies in the human ability to remember (numerical) information over short periods of time. This capacity is very limited (about 7 items) and is interrupted by doing other tasks. For example, if people have to do a classification task between being given a number to remember and being asked to repeat it back, then they forget about 12% of the original numbers after 5 seconds and more than 30% after 30 seconds (Posner & Rossman, 1965). This task is like using a VDT and having to interrupt thinking about the main task in order to remember how to and then carry out the actions needed to call up another display. To avoid this high rate of forgetting, all the information required in one decision should be available at the same time. This has strong practical implications for design.

In summary, the minimum number of VDT's which can be used depends on:

1. Size of the largest sub-unit in the process, all parts of which must be viewed at the same time. The method of dividing the process into functional sub-units is a question of process technology rather than of human factors.

2. Worst case scenarios (e.g. if the two largest sub-units of the plant fail at the same time).

3. Minimizing stress from not having immediate access to what is happening in all parts of the plant during fault management.

4. Permissable inter-sample interval.

5. Number of different types of information needed.

6. Reducing visual clutter.

Less: number of items which can be displayed on (high-speed) hard copy.

Increasing the number of VDT's:

A. Reduces the users'"
   1. Memory load;
   2. Distraction from accessing other pages;
   3. Time spent accessing other pages.

B. Increases:
   1. Visual and arm reach distances;
   2. Hardware investment.

3. Accessing the Data-Base

There are two main problems here:

1. Knowing what data and displays are potentially available and how to get from the current display to the next one wanted.

2. Using the interface controls to interact with the displays, both for navigating around the data-base and for controlling the process.

Knowing where one is in the data-base is a task involving relations: we have already mentioned that these are supported by pattern displays. New menu and summary map techniques are becoming available to help with this problem.

The main human information processing characteristic that we need to mention in relation to optimizing control design is the development of skill. "Skilled" behavior is very efficient: a skilled person has developed an "automatic" or "open-loop" way of doing something; there is no need to work out consciously what to

do or to monitor consciously that the task is being done correctly. This saves time and mental effort. The practical difficulty for design is that such skills can only develop in a consistent environment, one in which the result of a given action can be learned and then taken for granted. If actions will least interrupt the main task thinking when they are automatic, and this requires consistency, then this raises various questions for interface design.

Stable position is one of the advantages of conventional control rooms. This is lost on a multi-plexed interface, so it may be difficult to develop automatic skills of using it. For example:

1. When a given display or control is always in the same place, its location can act as an additional identity code, and the user can learn to aim eyes to a display or move hand to a control automatically. These are not possible with multiple layout VDT pages or with moving controls which change position, such as mice.

2. Using the same device (mouse or keys), both for data-base search and for control actions, means that there is no consistency either in the meaning of a given action or in its display-control ratio. So all actions must be monitored carefully before and during execution.

3. Using analogue controls, operators learn that a given size and timing of control movement has a given effect on the process. Using alpha-numeric keys to indicate size of control action, there is no mapping between the nature of the action and its effect. This raises questions about how effectively people can learn control skills when using keyboards.

The design implications are to maximize consistency, to use different devices for control actions and for interface actions, and perhaps to use analogue controls for analogue effects.

II. AUTOMATED DECISION-MAKING AND HELP FUNCTIONS

Modern control system development is concerned with automating decision-making as much as possible or with using "intelligent" expert systems to give the operator advice.

People, however, are usually retained in these automated systems to deal with un-anticipated situations. A key problem with automation is that the more the easy parts of an operators' task are automated, the more difficult the tasks which still have to be done by the operator become (Bainbridge, 1983). This is not only because when the operator takes over during fault management, the system which has gone wrong is more complex, involves

several technologies, and is less observable. It is also due to four further characteristics of human information processing:

1. Vigilance: it is humanly impossible to concentrate attention effectively on something which rarely changes; this sort of attention cannot be maintained by will-power. The rate of missing rare signals can double after about half an hour. The standard solution to this is to use audible alarms (see e.g. Rasmussen & Rouse, 1981).

2. Maintenance of Skills: Human beings not only need a consistent environment to develop automatic skills; we also need recurring practice to maintain them. This applied to "cognitive" skills of understanding what is happening, solving problems, making decisions, remembering things, etc., as well as to the perceptual-motor skills mentioned above. Therefore, the less an operator is involved directly in operating the plant, the greater the need for good training to maintain skills and knowledge. Also, it is important to design the equipment so that the operator can use familiar interface: using skills when doing infrequent tasks under the pressure of fault management.

3. Human beings work most efficiently in a known context of:

   a) the current state of the process. This awareness takes some time to develop and is not available to people who are expected rapidly to take over manual control from failed automatics.

   b) the current activities of other members of the control team (including the automatics) and the allocation of responsibility between them.

4. Maintaining attitudes: Much work in the area of "job satisfaction" shows that using skills, seeing how one's work makes a contribution to the enterprise, and being responsible for the final outcome, all affect both self-esteem and attitudes to work. These attitudes affect economic factors such as absenteeism, labor turnover, and rate of spoilt work.

Historically, approaches to automation have gone through a series of stages:

a. Automate everything.

b. Allocate function between people and machines according to whether person or machine is best at doing the task. This is the "Fitts list" approach, named after the first person to produce comparative lists of human and computer abilities.

c. The most recent approach is to allocate function and to design the work to take account of the human characteristics above, so ensuring that skills, attitudes and alertness are

maintained. For discussion, see Price (1985), Rouse & Morris (1986), Sage (1983).

This third approach represents a change from thinking in terms of removing the human operator to recognizing that:

a. in most economic systems, this is impractical or impossible;

b. a human operator will do tasks which have not been automated more effectively when working with the computer, in collaboration and for support.

Design for collaboration means thinking of computer and person as a team with interdependent responsibilities. The computer should be used especially to support the person when a task is too fast or accurate for a human being or poses too high a workload. Failures to consider collaboration and what the computer can best do for the enterprise are more well known in the area of office automation, e.g. Eason (1982).

Collaboration raises questions about the most effective use of Expert Systems in supporting the human operators' most difficult tasks (see Hollnagel et al, 1986). Expert systems and intelligent interfaces have been suggested for: alarm suppression, interpreting the process sate and diagnosing faults, giving explanations, and suggesting what to do in fault management. Most of these ideas come in the category of "blue sky optimism" compared with what is currently actually possible with a large complex industrial process. It would be useful, however, if expert systems could:

1. pull together large amounts of information about the plant and make inferences and explanations;

2. make decisions based on mathematically optimum use of limited information. There are many interesting biases in the way in which human beings make use of evidence in decision-making. Both interface design and training could be used to counter some of these biases, see Sage 1981, Moray (1986).

We will mention some of these biases of human judgement, as they affect the way in which people accept collaborative computer support systems:

1. Human beings tend to make judgements based on first experiences.

2. Human beings tend not to think in terms of probabilities, but assign events a "probability" of 1 or 0. If there is a very low probability of computer failure, operators will see no reason for maintaining adequate take-over skills. On the other hand, if there is a noticeable computer failure rate (the computer makes conclusions or suggestions which the operator knows are inadequate), then the operators will

ignore the computer's output and do all the task for themselves, which add to workload and communication problems.

These points suggest that it is important to introduce a good and fully working system, rather than an experimental one, to operators.

CONCLUSION

This short paper has introduced some of the main principles of designing complex industrial processes in a way which takes account of human operators, so that the combined person-machine system will give optimum performance.

REFERENCES

Anon. (1985) Guide to Reducing Human Error in Process Operation, Short Version. UKAEA Safety and Reliability Directorate, SRD R 347.

Bainbridge, L. (1983) VDT/VDU Interfaces for Process Control. in J. R. Wilson, E. N. Corlett, and I. Manenica (eds). New Methods in Applied Ergonomics. Taylor & Francis. pp. 97-105.

Eason, K. (1982) The Process of Introducing Information Technology. Behaviour and Information Technology, 1, 197.

Fitts, P. M. and Deininger, R. L. (1954) SR Compatibility: Correspondence among paired elements within stimulus and response codes. J. Exp. Psychol., 48, 483-492.

Goodstein, L P. and Rasmussen, J. (in press) Representation of Process State, Structure and Control. Le Travail Humain.

Grether, W. F. (1949) Instrument reading: I. The design of long-scale indicators for speed and accuracy of quantitative readings. J. Appl. Psychol., 39, 227-236.

Hollnagel, E.; Mancini, G. and Woods, D. D. (eds) (1986) Intelligent Decision Support in Process Environments. Springer-Verlag.

Kinkade, R. G. and Anderson, J. (1984) Human Factors Guide for Nuclear Power Plant Control Room Development. Electric Power Research Institute. NP-3659, Research Project 1637-1.

Malone, T. B. et al (1980) Human Factors Evaluation of Control Room Design and Operator Performance at Three Mile Island-2. NUREG/CR-1270. Nuclear Regulatory Commission, Washington, D.C.

Moray, N. (1986) Modelling Cognitive Activities: Human Limitations in Relation to Computer Aids. in Hollnagel et al, op cit., pp. 273-291.

Posner, M. I. and Rossman, E. (1965) The Effect of Size and Location of Informational Transforms upon Short-term Retention. J. Exp. Psychol., 70, 496-505.

Price, H. E. (1985) The Allocation of Functions in Systems. Human Factors, 27, 33.

Rasmussen, J. and Rouse, W. B. (eds) (1981) Human Detection and Diagnosis of System Failure. Plenum.

Rasmussen, J.; Duncan, K. and Leplat, J. (eds) (1987) New Technology and Human Error. Wiley.

Reason, J. (1987) The Chernobyl Errors. Bull. Brit. Psychol. Soc., 40, 201-206.

Rouse, W. B. and Morris, N. M. (1986) Understanding and Enhancing User Acceptance of Computer Technology. IEEE Trans. Sys., Man, Cyb., SMC-16, 965-973.

Sage, A. P. (ed) (1983) Special Issue on Control Frontiers in Knowledge Based and Man-Machine Systems. Automatica, 19, 593.

Sage, A. P. (ed) Behavioural and Organisational Considerations in the Design of Information Systems and Processes for Planning and Decision Support. IEEE Trans. Sys., Man, Cyb., SMC-1, 640-678.

3.3. PROBLEM SOLVING, RISK AND TECHNOLOGY

David D. Woods
Westinghouse R & D Center
Pittsburgh, Pennsylvania, USA

The Role of Human Related Issues in the Risky Technologies

Human-Technical Systems

There are two major perspectives on activities in the design, operation and regulation of various risky technologies: the engineered system, which can be subdivided into various pieces of the system or engineering points view such as thermodynamic, mechanical, electronic – typically called the "technical" system, and the human role in maintaining, operating, designing the engineered system, which can be subdivided into socio-behavioral points of view such as physiological, cognitive, organizational, motivational – the human systems.

The state of the technical process in question (e.g., nuclear power plant, chemical plant, etc.) changes in a series of interactions between the human and technical systems. In general, designers have been successful in reducing the exposure to catastrophic outcomes (given normal conditions to begin with, single failures cannot lead directly to significant radiation releases). As a result, accidents develop or evolve through a conjunction of actions/failures that involve a series of interactions between the human and technical systems. One of the two acts; the other responds which generates a Gxresponse from the first and so forth. The evolution towards different negative consequences can be broken at any point. Accident evolution points out that there is some initiating event in some human and technical system context, but there is no one clearly identifiable cause of the accident. However, points during the accident evolution can be identified where the evolution can be stopped or redirected away from undesirable outcomes.

The behavioral science view of this process emphasizes the demands and environment that the technical system creates around the human. The extreme view is that the technical system must anticipate all human deficiencies and compensate for them. The technical view emphasizes the pernisciousness of people in shortcircuiting an otherwise safe technical system. In the extreme the source of poor performance is the person who must be aided or eliminated. Svenson (1987) points out a Catch 22 that arises if there is a gulf between the human and technical views of the system: if the behavioral scientist/practitioner attributes the source of poor human performance to factors created by the technical side, then he is no longer an expert in how to correct the situation; similarly, if the physical scientist/engineer attributes the source of poor system performance to the human element, then he is no longer an expert in how to correct the situation. As a result each camp can fall prey to recommending/pursuing changes that are very general and non-professional, e.g., improve technical subsystem A/reduce the number of ..., or improve operator training/provide maintenance aids.

What this means is that effective research, development, and operation of complex risky technologies depends on a synthesis of how the technical and human systems interact. The NPP is not just a technical system, is not just a human system, and is not a simple addition of these two views. To date the purely technical view has dominated. Failures to conceive of the system as both technical and human has retarded the formulation of useful research questions and the transfer of results to the field in socio-technical systems.

TMI: A fundamental surprise -- technology alone is not enough

On March, xx, 1979 the nuclear industry and technologists wre rocked by the Three Mile Island accident. The consternation that resulted was only in small part due to the fact that it was the worst nuclear accident up to that time or due to the radiological consequences per se. Rather the accident is a case of what Lanir (1986) terms "fundamental surprise."[1] A fundamental surprise, in contrast to situational surprise, is a sudden revelation of the incompatibility between one's self-perception and his environmental reality. Examples include Pearl Harbor for the U.S. (Wohlstetter, 1962), the launch of Sputnik on the U. S., and the Yom Kippur war for Israel (Lanir, 1986) among many examples. The TMI accident was more than an unexpected progression of faults; it was more than a situation planned for

[1]See Appendix 1 for a short excerpt from Lanir, 1986 that graphically illustrates the concept of fundamental surprise.

but handled inadequately; it was more than a situation whose plan had proved inadequate. The TMI accident constituted a fundamental surprise in that it revealed a basic incompatibility between the nuclear industry's view of itself and reality. Prior to TMI the industry could and did think of nuclear power as a purely technical system where all problems were in the form of some enginnering technical area or areas and the solutions to these problems lay in those engineering disciplines. TMI graphically revealed the inadequacy of that world view because the failures were in the socio-technical system and not due to pure technical (a single equipment or mechanical flaw) nor pure human factors (incompetency or deliberate error). The pre-planning for emergencies had consisted of considering large equipment failures and not a series of small failures and interacting inappropriate human assessments of the situation and therefore erroneous actions. This kind of interaction between human and technical factors was inconceivable prior to TMI,[2] although all significant nuclear power plant incidents involve this interaction (e.g., Brown's Ferry; the incidents examined in Pew et al., 1981; Ginna; Davis-Besse; and others) and most significant accidents in other worlds also involve this interaction.

The post-TMI U.S. nuclear industry has struggled to cope with and adjust to the revelations of TMI. The process of adjustment has involved the phases associated with fundamental surprise described by Lanir. First, the *surprise event* itself occurs. Second, reaction spills over the boundaries of the event itself to include issues that have little to do with the triggering event – *social and epistemological crises.* Third, these crises can lead to *fundamental learning*, although this may be partial and ineffective. For example, the fundamental surprise often is denied by approaching the incident as if it were only a situational surprise that requires only a local response. Fundamental learning, in turn, produces practical changes in the world in question – *morphogenesis.* Finally, the changes are absorbed and a new equilibrium is reached.

The immediate investigations of the accident focused heavily on the mutual interaction between technical systems and people and proposed changes that addressed the basic character of the joint human-machine system (classic ways to cope with problem solving breakdowns such as multiple ways to represent the state of the plant (function oriented displays in safety parameter display systems),

---

[2]Chernobyl, although a more severe accident does not carry the same fundamental surprise, at least for the U.S. because TMI already revealed the nuclear power plant as a human/technical system. The Russians, and perhaps the Europeans had not been forced to confront TMI in the same way as had the U.S. Thus, they could deny its relevance, so that Chernobyl may have constituted a fundamental surprise for them.

institutionalize people with multiple views of the situation (shift technical advisor), symptom management as well as fault identification approaches to emergency response (new procedures).

However, in the process of carrying through on these and other "lessons learned" the industry began to treat the accident as a mere situational surprise and began to apply purely technological solutions. While the post-TMI changes clearly have improved aspects of the socio-technical system through such things as new sensors, new analyses of possible accident conditions, new guidance on how to respond to certain accident conditions, changes in emergency notification procedures, the basic socio-technical system for operating and responding to failures has not changed. Symptoms of this are the long delays and apparently uneven implementation of post-TMI changes such as new instrumentation, new procedures and computer based display systems (the SPDS), judging from the results of the NRC audits conducted to date. However, the revelations of TMI continue to re-occur in other major incidents (e.g., Davis-Besse, NUREG-1154; San Onofre, NUREG-1190; Rancho Seco, NUREG-1195; and most tragically Chernobyl).

The U.S. nuclear industry and other risky industries as well continue to treat a socio-technical system as if all issues are merely technical issues in some engineering discipline: if decision support systems are needed, the question is what language it should be programed in; if following guidance contained in procedures is important, then computerization in and of itself is the answer. All investigations of problems in complex technologies show that "human error" is a major source of difficulties (figures vary from 40 to 80%). In other words, human related aspects are a major part of virtually all issues. The temptation to treat socio-technical systems as purely technical is particularly seductive because the technical disciplines alone can create the system *at some level of abstraction.*

The behavioral sciences do not presently have all of the answers (or perhaps not even very many) that industry needs. However, the behavioral sciences do have knowledge and approximate models on human-technical systems that can in the short run begin to influence research, design and evaluation. Furthermore, the current base of knowledge needs to be stimulated and grown so as to able to provide stronger answers in the future. Knowledge from the behavioral sciences is needed because new technological disciplines are and will produce new systems for application in risky technologies that can repeat the errors of the past. What is clearly needed is research and application of research on socio-technical systems to complex risky technologies.

Complex Technologies as Problem Solving Systems

Introduction

Here I will cover some of the aspects of a socio-technical system considered a problem solving system[3] . When looking at a problem solving system one is concerned with what knowledge is used, the conditions under which it is accessed, and the ways knowledge is packaged and delivered.

At the center is the operational part of the technological world. This refers to all of the activities that people carry out that make direct physical contact with the components and systems that make up the technological process itself. This includes maintenance of equipment, test & calibration of systems and instrumentation, startup/shutdown, normal operations, detecting and responding to abnormal conditions. This area includes various kinds of people: technicians, supervisors, auxillary operators, licensed operators, those who staff auxillary facilities, engineering personnel (either on-site or with access to on-site personnel during some activity). This area applies to activities carried out at various locations in the plant, control room activities, and activities in auxillary facilities. Design, management, organization,and regulatory activities represent aspects that surround the operational plant. They are of concern in how they can affect the above activities. For example, how organizational factors affect the way that people on the operational front lines make decisions under risk.

What do operational people do? They work the front lines of socio-technical systems; they are the ones who must act on the system directly; they are the ones who see the system as an integrated whole rather than a bounded piece (e.g., a system designer) or a single point of view (e.g., regulatory). Those who direct, organize, regulate, and design for operational people, in one sense, deploy knowledge about the technical system to the operational personnel. Knowledge can be deployed internal to people (inherent capabilities, education, training, experience) or in external form (encoded in different media and organized for retrieval in different ways) and the knowledge can be available during task performance (via memory, another person, or a knowledge delivery system) or on call (a human engineering specialist or a special engineering analytical model).

---

[3] E.g., the view from the fields of cognitive psychology, cognitive science, artificial intelligence, decision theory.

Managing trouble

It is very useful to distinguish between coordination by pre-planned routines and coordination by resource management. In the former, knowledge is packaged in terms of what situations are to be recognized, what evidence signals that these situations have arisen, and what response should follow (Rasmussen's rule based behavior; e.g., Rasmussen, 1986). This knowledge is delivered in the form of education about the routines, training (exercise and drill) in carrying out the recognitions and responses, and on-line systems to help prompt and retrieve the guidance (either paper or computer based). When human behavior is to guided by pre-planned routines, human performance aiding is to teach the person about the knowledge encoded especially the background for the routines (Brown et al., 1982), to practice the person on the routines, and to provide retrieval aids so that the person uses the correct guidance for the current situation.

For example, the new emergency procedures that have been developed in response to TMI include new categories of situations to be recognized by operators, i.e., safety functions (this is not to say that operators never thought of emergency situations in these terms prior to the new procedures, but only that education, training and on-line retrieval mechanisms for these categories were increased), the evidence to recognize them was specified, and response strategies were planned should they occur.

However, coordination by pre-planned routines is inherently brittle (e.g., Fischhoff et al., 1986; Brown et al., 1982). When the pre-planned routines are rotely followed, performance breaks down in the face underspecified instructions, special conditions or contexts (boundary conditions such as in the incidents described in NRC Information Notice 83-30 or impasses where assumptions about the world in the routine are not true), human execution errors, bugs in the routines, multiple failures, novel situations (incidents not planned for or multiple failures). While some types of worlds or parts of worlds are more prone to these factors than others and the quality of the pre-planning effects the frequency with which these arise in particular worlds, research in a variety of worlds consistently has shown that these factors can never be completely eliminated by expanding and refining pre-planned routines (for both pragmatic and theoretical reasons) and that these factors are ubiquitous in actual serious accidents in nuclear power plants and other industries (see Woods et al., 1987).

The challenge is to develop problem solving architectures that are not brittle in the face of unanticipated variability, to define problem solving systems that function

well even when the exact nature of the problems to be handled are not known in advance. Usually, people think that the only alternative to coordination by pre-planned routines is creative problem solving (e.g., the Browns Ferry fire) but that operators are not selected for capabilities in this area. However, there is an alternative type of behavior which does fit within the scope of operational personnel. In coordination by resource management, an actor "at the scene of the crime" does more than deploy pre-planned strategies; he also monitors the response to see if it is going according to plan (e.g., are the relevant goals met?). Departures from plan (from expectation) signal that more knowledge needs to be brought to bear on the problem. What happens is that there is a gradual unfolding of more and more of the background knowledge behind the pre-planned material including the written background information for procedure steps, specialist knowledge about system design, specialist knowledge about accident analysis. In some cases the relevant knowledge is potentially available if a delivery path is known (i.e., the operational personnel must know enough to ask the right question and they must know where or who can provide answers); in other cases the knowledge must be generated , e.g., from engineering analyses. Aiding human performance in this aspect of operational knowledge addresses recognizing departures from plan, what additional knowledge is needed, and how to call on that knowledge.

Both kinds of coordination are necessary for effective human performance at the operational front lines: expanding and refining available guidance expands the amount of routine problem solving; supporting knowledge resource management addresses situations that have not been or cannot be completely anticipated -- a kind of cognitive defense in depth. In other words, after you have tried to think of and plan for all possible contingencies, plan for the fact that you have probably missed some things.

Research on how to manage trouble is essential in technological worlds that have proven again and again that not all factors can be anticipated in advance. This research will have a significant effect on how new computational technologies (e.g., artificial intelligence) should be utilized and on how to avoid errors in their deployment. It is essential for the both the operators of complex technologies and for those who design and regulate complex technologies. Psychologists are fond of discovering biases in human decision making. One judgemental bias is the overconfidence bias where people at all levels of expertise overestimate how much they know (e.g, Wagenaar, 1986). Sometimes we forget that these biases can apply to design problem solving as well as to operational problem solving. The

ovevconfidence bias means that the designer of a system is likely to overestimate his/her ability to capture all relevant aspects of the situations that can occur. For example, this has occurred often with the design of forms of automation and support systems -- the designer of the the system fails to appreciate all of the complexities of the operational setting so that the system fails to support or even hinders the operator in achieveing his/her goals. Again, provisions must be made about how to build problem solving systems that are robust in the face of unanticipated variability.

The cognitive system triad

One can think of problem solving situations in terms of interactions among a set of three mutually constrained factors (Figure 1): the world to be acted on, the agent or agents who act on the world, and the external representations through which the agent experiences that world. Each of these factors contributes to the performance of the agent in the relevant domain (cf., Edwards & von Winterfeldt, 1986, p. 669-677 for a particularly engaging demonstraton of the interaction of these factors). Understanding the interactions among these factors is the target of the psychology of human behavior in complex systems. When we better understand the nature of a broad sample of the problem solving situations people face, we can better understand the behavior exhibited when someone is confronted with a particular situation and how to support and improve performance.

Starting from the apex of the world itself, the characteristics of that world contribute various kinds of cognitive demands that must be handled to adequately perform domain tasks. There are four dimensions of problem solving worlds that define its cognitive demands: *dynamism, the number of parts and the extensiveness of interconnections between the parts or variables, uncertainty, and risk* (Woods, in press). All domains (or applications within a domain) can be characterized in terms of a position along these dimensions. In general, when a problem solving world is described in everyday terminology as "simple," it will place low on all four of these dimensions; while a world described as "complex" will place high on these dimensions (but remember complexity is a function of the interaction of all three apices).

When a world is dynamic, problem solving incidents unfold in time and are event-driven, that is, events can happen at indeterminate times and the nature of the problem to be solved can change (e.g., multiple failures). The result is cognitive demands associated with anticipation or prediction of the behavior of the world and the need to be able to revise one's assessment of the state of the world and

therefore one's tactical or strategic response (cf., Montmollin & De Keyser, 1985; De Keyser, 1986 for treatments of how dynamism affects cognitive demands). Failures to revise are one source of fixation errors (Figure 2).

When a world is made up of large number of highly interconnected parts (cf., Perrow, 1984; Rasmussen, 1986; Dorner, 1983; Woods & Hollnagel, 1987), one failure can have multiple consequences (produce multiple disturbances); a disturbance could be due to multiple potential causes and can have multiple potential fixes; there can be multiple relevant goals which can compete with or constrain each other; there can be multiple ongoing tasks at different time spans. In addition, the parts of the world can be complex objects in their own right. One typical error form is failures to consider side effects, requirements, or post-conditions (Dorner, 1983). Another problem solving error that occurs when a world is high on this dimension of complexity (particularly when it is simplified to cope with the complexity) is to mistake one factor related to the state of the world as the single explanation for that state. This becomes an error when the attribution to a single factor delays or prevents identification of the set of factors that actually contribute to the observed situation (Bechtel, 1982).

When data are uncertain, an inferential process is needed to go from data to answers about the state of the world. When uncertainty is high, some data always fail to fit together into the correct assessment due to red herrings, sensor failures, human reported data, perceptual judgements, irrelevant factors, or multiple failures. Not only does the inferential value of different data vary, the inferential value of a single set of data can vary with context. Furthermore, data gathering to reduce uncertainty can become necessary and can interact with effort and risk. A typical cognitive failure form is over-reliance on familiar signs (Rasmussen, 1986). See Cohen et al., 1987; Coombs & Hartley, in press; Einhorn & Hogarth, 1985; Sorkin & Woods, 1985; Schum, 1980; Dubois, in press for treatments of different aspects of uncertainty and its consequences for problem solving demands and activities.

When there is risk, possible outcomes of choices can have large costs. The presence of risk means that one must be concerned with the rare but catastrophic situations as well as with more frequent but less costly situations. When uncertainty is coupled with risk, situations of choice under uncertainty and risk arise. Current knowledge about human performance in risky decision making indicates that generalizations from research with non-risky tasks to risky tasks must be made very cautiously.

To illustrate how interactions among these dimensions affect cognitive demands,

consider a world that has high evidential uncertainty how this can interact with the other three dimensions. When a world is both uncertain and dynamic, strategies for acquiring data become important. All evidence is not available at once because it comes in over time or because it must be actively acquired with associated costs (effort and risk). As a result, situation assessment and evidence gathering interact, e.g., the information value of the data to be collected can interact with the effort that must be expended in order to collect it (e.g., Moray, 1984; Johnson & Payne, 1985), especially when there is a high workload. Uncertainty and risk interact when data gathering can be an action in the world of interest with attendant consequences for parts of the world. For example, medical tests can have negative consequences that must be balanced with gain of information (Cohen et al., 1987) or obtaining data from a location involves danger such as radiation exposure or fire (Klein et al., 1986). A common strategy in research and in building machine experts (Mycin) is to consider situation assessment/diagnosis independent from data gathering. However, this simplification obscures the interaction between these two and the cognitive demands generated by that interaction when evidence comes in over time or has associated costs in terms of effort and risk (Cohen et al., 1987). It is one example of failing to take the perspective of the problem solver in the situation when mapping cognitive demands.

The need to know when and where to look for evidence results in an attentional cognitive demand to focus in on the significant subset of data for the current problem context, given a large amount of potentially relevant data. In this significance of data information handling demand (Woods, 1986), the problem solver must decide what data is relevant to consider in determining a solution; thus, it is part of problem formulation. A large category of errors in worlds high on the dimensions of complexity can be described as failures of attention (Woods, 1984b), in that, from hindsight, data from which the solution could have been extracted were available but were not attended to or looked for at the right time or in conjunction with the appropriate set of data, given an erroneous assessment of the situation or an erroneous approach to the utilization of evidence. From the point of view of problem formulation, these attention failures are seen as errors of solving the wrong problem. Examples of breakdowns in this cognitive demand include disturbance management in process control accidents with conventional alarm systems (Lees, 1983; Woods et al., 1986) and intelligence failures in military history (Wohlstetter, 1962; Shlaim, 1976).

The position of a domain along these dimensions determines the cognitive demands and the cognitive situations that problem solvers can face in the world in question.

These demands can strongly affect what are effective or sensible reasoning strategies to adopt and the cognitive failure forms that will occur. The difficulty of meeting these demands varies depending on the processing characteristics of the relevant cognitive agents, the architecture of the various cognitive agents (Sorkin & Woods, 1985; Fischhoff et al., 1986; Woods et al., in press) and on the representation of the world that is provided to the problem solving agent (Rasmussen & Lind, 1981; Rasmussen, 1985).

For example, Fischhoff et al. (1986) discuss how risk interacts strongly with multi-agent architectures to influence the level of risk acceptance of the joint cognitive system and therefore the quality of problem solving behavior. Furthermore, they show how changes in the power and scope of centralized information systems (a change on the representation apex) can change the distributed decision architecture and strongly affect risk taking behavior, i.e., the decision criteria on the willingness to innovate or depart from doctrine at various levels of a hierarchical organization.

If one views the triad from the vantage point of problem representations, the effect of various possible representations depends on the cognitive demands imposed by the world and on the processing characteristics of the relevant cognitive agent. Any particular representation makes certain information or manipulations of information explicit at the expense of other information or manipulations which are pushed into the background. A simple example is notational systems such as numeral systems -- try multiplication and division in the Roman numeral system.

Human Error and Person-Machine Mismatches

Questions about human error -- what it is, what factors produce it, what forms does it take, how to measure the potential for error, how to predict its form or frequency or timing, where is a task vunerable to error -- are essential topics for risk identification and management. The level of effort devoted to these questions has accelerated recently (e.g., Moray & Senders, in preparation; Rasmussen, Leplat & Duncan, 1986).

There are several common themes in the recent work on human error (e.g., Rasmussen, 1986; Moray & Senders, 1986; Rasmussen et al., 1986; Reason & Embrey, 1985; Woods, in press). First, there is a distinction between error forms -- the likelihood of different kinds of errors given that an error occurs, and error emission patterns -- the statistics of how often will inadequate performance occur (e.g., Senders, 19x). Researchers have generally focused on the systematic error forms because these suggest potentially identifiable and correctable underlying factors.

Research on error today assumes error is the result of limited rationality -- people are doing reasonable things given their knowledge, their objectives, their point of view and limited resources, e.g., time or workload (Reason & Mycielska, 1982; Montmollin & De Keyser, 1986; Woods, in press) -- and that error analysis consists of tracing the problem solving process to identify points where rationality breaks down. This has been called an assumption of imperfect rationality or a cognitive existence theorem (there is some cognitive system which can be postulated which would rationally, i.e., within its knowledge and information processing capability, exhibit the behavior that has been observed).

A third theme derives from studies of actual incidents (e.g., Pew et al., 1981; Reason & Mycielska, 1982; Woods, 1982; Perrow, 1984; Montmollin & De Keyser, 1985). These studies reveal that there are a set of individually necessary but only jointly sufficient conditions for a disaster to occur; therefore, labeling any one the cause requires additional information (e.g., Mackie's [1974] point about a background causal field). For example, in an actual train derailment leading to a two train crash, one can refer to a large number of conditions but for which the accident would not have occurred -- such as, the information processing demands placed on the driver, the change in habits due to the end of the holiday period schedule, the speed of the train, the proximity of another track at the site of the derailment, the timing that another train was on this other track at nearly the same time, etc.

This observation has led to general agreement among the research community (but not necessarily in particular application communities) that it is more fruitful to think about person-machine system flaws than human errors (e.g., Perrow, 1983; Rasmussen, 1986). The label "human error" is often used as a residual category; it tends to imply responsibility and blame (punishment); it focuses changes on local, incident-specific responses (different people, better motivation). Error attribution is an exercise in hindsight judgement (a two state discrete dimension); whereas prior to the outcome there are only degrees of performance (a continuous dimension) and factors that make it more or less difficult to perform. In the train crash example, all the trains that day went too fast through the section of the track where the derailment occurred. Thus, once performance deviates from its target, it has the potential to be labelled erroneous. Whether it will lead to negative consequences depends on the presence of other necessary factors.

A more productive alternative is to focus on the factors that produce the behaviors underlying the disaster (as Perrow 1983 puts it, what forced the erroneous

behaviors). For example, an airplane crash into a mountain on a clear day was originally labeled "crew error." However, further investigation revealed that this seemingly irrational incident was actually the product of the interaction of a set of factors -- the flight computer course had been changed without notifying the pilot, the new course was visually quite similar to the old, and a dry air whiteout made the mountain invisible to the pilots (Mahon, 1981). Identifying how a set of factors converge in the genesis of a disaster leads to an emphasis on demand/resource mismatches, person-machine performance, multiple contributors to incidents, multiple responses, and failures as potential learning experiences. From this perspective we need to understand the relationship between human processing mechanisms (e.g., Arkes & Hammond, 1986; Edwards & von Winterfeldt, 1986) and the demands and resources actually present in complex problem solving situations such as flightdeck operations, emergency response in nuclear power plants, or marine safety. For example, one position is that human processing consists of relatively simple but normally quite effective mechanisms. Performance failures occur when designers unintentionally create excessively harsh cognitive environments due to the demands of the world itself and due to the primitive representations available (Perrow, 1984; Reason, 1986; 1987).

One path to approach questions about human error is to examine criteria for skilled or expert performance. One often noted aspect of skill or expertise is the ability to adapt one's response in light of changing circumstances in pursuit of a goal (Brown et al., 1982; Bainbridge, 1981; Woods & Roth, 1986). Adaptability depends on abilities to predicy or anticipate the behavior of the world and to to be sensitive to what might happen next (e.g., a field of attention). This definition emphasizes the ability of the skilled performer to compensate for environmental variability or disturbances. Error then becomes a breakdown in one's resistence to variability or disturbances, either failures to recognize the need to adapt (behavior persists in one path in the face of changing circumstances that demanded a shift in response) or erroneous adaptation (the need for adaptation was recognized but the attempted adaptation was inadequate due to incomplete knowledge). This view emphasizes the active role of any cognitive agent or set of cognitive agents in controlling a world and the need to treat performance failures through changes in the capabilities, resources and architecture within the cognitive systems triangle. This suggests that human participation often prevents the propagation of errors or usually works around error prone points (flaws) due to the flexibility, adaptability, "intelligence" of the human in the loop. For example, it is ironic that decision automation is often justified on the grounds of human incompetence, however it is

the same person who must compensate for the "brittleness" typically exhibited by machine agents in the face of unexpected situations (Woods et al., in press). This is in stark contrast to the view that the human is an independent source or contributor of errors, where system failures in which human actions played a role should be treated by increasing the role of machine cognitive agents in order to eliminate or reduce the human's role.

One source of mismatches within the cognitive system triad that contribute to performance breakdowns has been purely technology-driven deployment of new automation capabilities. When this occurs, there are frequently unintended and unforseen negative consequences in terms of new types of errors/accidents. Examples are multifold. Among the most dramatic instances are: cases of shifts from manual to supervisory control in process control where productivity actually fell from previous levels due to failures to support the new supervisory control demands (Hoogovens Report, 1976); cases of automation related disasters in aviation (e.g., Wiener, 1983; 1985),[4] a shift in power plant control rooms from tile annunciator alarm systems to computer based alarm systems that eventually collapsed and forced a return to the older technology because strategies to meet the cognitive demands of fault management that were implicitly supported by the old representation were undermined in the new representation (Pope, 1978); and shifts from paper based procedures to computerized procedures that have also collapsed due to disorientation problems again as a result of a failure to anticipate the reverberations of technological changes in the cognitive system triangle (Elm & Woods, 1985).

Consider a simple example of automation. You have a portable cassette tape recorder to record letters. In the manual recorder you must switch from one side of the tape to the other when you have filled one side. Now you purchase a new, more technologically sophisticated recorder that has an automatic reverse -- when you reach the end of one side, the machine automatically begins to record on the other side of the tape. You no longer have to take out the tape, reverse it, and reload it. Automation has produced positive impact, especially if you frequently record while your hands are busy at some other activity like driving a car. However, there are other consequences or effects of the new automation that introduce possibilities for new kinds of errors/inadequate outcomes if not addressed.

---

[4] A research program is underway to track the effects of recent changes in commercial flightdeck automation, cf., Curry & Wiener.

In our automated recorder example, consider what happens if on one day you record enough to fill the first side of a tape and part of the second. On the next day you want to add additional material to the tape; in other words, you want to resume recording where you left off the previous day. Notice what can happen. You do not remember where you left off – on side A or on side B and there is no cue in the configuration of the device to tell you which (because the tape is always in the machine on the same side – the machine switches for me). Thus there is the possibility that you will simply initiate the record mode and begin to speak without the second command needed to start on side B. As a result, a portion of the material you had recorded the previous day will be erased and recorded over. Note that this is a new error form/negative outcome; it is impossible with the manual machine – one always begins to record where one left off previously. The point is that new automation aids can have multiple effects on the human side and that some of these effects can be negative. In other words, there are post-conditions associated with new automation that must be met otherwise errors/negative outcomes can occur – in this example, some way to keep track of which side of the tape is unrecorded (a display or memory aid) or for the machine to be capable of resuming to record from the place where previous recording stopped (further automation). The point is not that new technology should be avoided – because the automation does make possible significant improvements. Similarly, the point is not that new technology is always beneficial – because there are post-conditions associated with its introduction that must be satisfied in order for the potential to be achieved and for undesirable consequences to be avoided or mitigated. Furthermore, these post-conditions will generally strongly influence the way the technology is used (or even the type of technology used). One strong example of this has ocurred in marine transportation (Perrow, 1984). Technology only driven increases in the machine power devoted to navigation and collision avoidance did not reduce marine accidents (Gaffney, 1982). This spurred the U.S. marine community to continue to increase levels of automation. However, the existence of automation related accidents triggered the european community to look at what we have called here the cognitive system and to use machine power to enhance total system performance (e.g., to reduce fixation errors by encouraging communication of task relevant information across cognitive agents).

One problem is to measure and predict human performance (or problem solving performance), especially as a function of changes in the man-machine system. PRA is sometimes offered as a candidate. However, as currently practiced, it cannot adequately fulfill this role for human related issues: among many deficiencies, it

cannot address cognitive factors, it cannot address the effect of changes in the man-machine system, it is basically a look up of cumulative experience but there is no experience with new technologies on which to base predictions, and the criterion of risk is too narrow for evaluating human performance.

To have effective man-machine systems in complex worlds requires sophisticated human-machine performance modeling capabilities. Significant research work has been done on human error and there are several research programs underway to use this data base to develop analytical models of human performance (Mancini, 1986; Woods & Roth, 1986).

Appendix

Excerpt from
"Fundamental Surprise"
by Z. Lanir

Webster's Anecdote

Fundamental to this theory is the distinction between two different types of surprise: situational and fundamental. One way to introduce this distinction is with an anecdote about Noah Webster, the well-known dictionary lexicographer.

One day, he arrived home unexpectedly to find his wife in the arms of his servant. "You surprised me," said his wife. "And you have astonished me," responded Webster. Webster's precise choice of words captured an important difference between his situation and that of his wife.

One difference between surprise and astonishment is the different level of intensity associated with the two: astonishment is more powerful and extensive than surprise. Indeed, Mr. Webster's situation possesses an element of shock. His image of himself and his relations with his wife were suddenly and blatantly proven false. This was not the case for Mrs. Webster who, although surprised by the incident, still could maintain her image of herself, her environment, her husband, and the relations between them. Indeed, even if Mrs. Webster had taken all the steps she viewed as necessary to prevent the incident, she had to assume that there was some possibility of her unfaithfulness eventually being revealed. Her feelings might be analogous to those of drivers who brakes suddenly fail. Although surprised and frightened, such drivers should have realized that brake failures are always a possibility. Thus, we are aware that failures occur in nature as well as in technical, social, and organizational systems, so that when they do occur, our belief in those systems is not completely destroyed, however surprised and upset we might be.

For Mrs. Webster, the failure was due to an external factor. Although she was uncertain about the external environment she was not uncertain about herself.

In contrast, Mr. Webster's astonishment revealed unrecognized uncertainty extending far beyond his wife, his servant, or other external factors. For him, comprehending the event's significance required a holistic reexamination of his self-perceptions in relation to his environment. Although this surprise offered Mr. Webster a unique opportunity for self awareness, it can at the price of refuting his deepest beliefs.

A second distinction between surprise and astonishment lies in one's ability to define in advance the issues for which one must be alert. Surprises relate to specific events, locations, and time frames. Their demarcations are clear. Therefore, it is possible, in principle, to design early warning systems to prevent them. In contrast, events providing astonishment affect broad scopes and poorly demonstrated issues. Mr. Webster's shocking incident revealed only the "tip of an iceberg."

Another distinction concerns the value of information. Mrs. Webster lacked one item of information which, had she had it in advance, would have allowed preventing her surprise: the information that her husband would return early that day. No single piece of information could have prevented Mr. Webster's astonishment. In most cases, the critical incident is preceded by precursors from which an outside observer could have deduced the state of the couple's relations. Such observers should be less prone to the tendency to interpret information in ways that suit one's own world view, belittling or even ignoring the diagnostic value of information that contradicts it.

A fourth distinction between fundamental surprise and astonishment is in the ability to learn from the event. For Mrs. Webster, the learning process is simple and direct. Her early warning mechanisms were ineffective. If given a second chance, she might install a mechanism to reduce the possibility of being caught in a similar situational surprise.

Mr. Webster might attempt an explanation that would enable him to comprehend it without having to undergo the painful process of acknowledging and alerting a flawed world view. For example, he might blame the servant for "attacking his innocent wife." If it were established that the servant was not primarily at fault, he might explain the incident as an insignificant, momentary lapse on his wife's behalf. In more general terms, we may say that Mr. Webster's tendency to seek external, incidental reasons reflects the human tendency to behave as though astonishment is merely a surprise and, thus, avoid recognition of the need to experience painful "self" learning.

We will refer to Mrs. Webster's type of sudden discovery as a "situational surprise" and Mr. Webster's sudden revelation of the incompatibility of his self-perception with this environmental reality as a "fundamental surprise."

3.4. THE DESIGN OF OPERATING PROCEDURES

Nelville Moray
Department of Industrial Engineering
University of Toronto, Canada

Human Factors North, Inc.
Toronto, Canada

The design of operating procedures must be a matter of a systems approach, in which engineers, operators, management, human factors specialists, writers and trainers must be involved. This is particularly true of Emergency Operating Procedures. A design aid, the Emergency Operating Procedure Procedure, EOPP, is suggested for this purpose.

Although the purpose of this paper is to provide a rational theory and design method for all operating procedures, I shall exemplify the method by considering the special case of emergency operating procedures (EOP). Recently, Feher, Moray and Senders (1987) have reviewed the design of EOPs, and the ideas to be presented here are drawn from their report.

In designing EOPs, the aim is to ensure that under the pressure of a hazardous incident the operators will both know what to do and also will be able to do it. It follows that the EOPs are not just a list of actions to be taken, but should also implicitly embody rational and integrated planning concerning manning levels, training, anthopometrics, shift work philosophy, etc. Without such an integrated approach the EOP, while correctly describing what actions, should be taken, cannot ensure that the operators will be able to carry out the actions.

For example, if the EOP is generated by the engineers responsible for the physics of process control, but without interaction with the architect-engineers who design the control room layout, a procedure which is correct in terms of engineering functions of physical chemistry might be written, but which required two controls to be operated simultaneously which are, say, 3 meters apart. If so, a single operator could not carry out the EOP. If the design of the control room is already frozen at the time the EOPs are generated, they will require at least a 2-person crew. If on the other hand, management has set the manning level of the control room, it will mean either the engineers will be constrained in how they allocate function in the EOP, or there will be an impact on the organizational hierarchy and training of the control room crew. For example, a decision will have to be made as to whether each member of the crew will be trained to carry out all functions, or whether they will specialize each on one part of the system (for example, one on the control of reactivity, another on the control of the cooling system, in a nuclear power plant). The allocation of function will in turn prescribe the

workload to be born by each operator. If operators must both read the procedures and carry them out, they will be more heavily loaded than if a supervisor reads out the procedures and the operators carry them out; but in that case the supervisor in turn may become overloaded.

In practice at present different industries take different approaches. At the IAEA meeting in Munich in 1986, for example, one group said that they first wrote the procedures and then decided on manning level, while another group apparently did the reverse. The overall impression was that nowhere was there a technique which could act as the core of the design procedure, around which rational design and integration could take place. The EOPP (Emergency Operating Procedure Procedure or Emergency Operating Procedure Philosophy) provides such a technique.

The EOPP diagram is a graphical representation of the flow of information and control during normal and abnormal operations (examples are shown in Figures 1-4). The box diagram shows the various activities by which the control room crew interact with each other and with the process. The flow graph below each box diagram shows a time-line of events.

Figure 1 shows a simple situation in which a supervisor and an operator manually control a process. In normal operation there is a cycle in which the operator Looks at the plant, the plant Shows the operator its state, and the operator Acts on the plant. (This normal cycle is shown in a dashed box in each flow chart.) when an incident occurs, the plant Shows an abnormality, and the operator Tells the supervisor. The supervisor consults the EOPs (shown by dashed parallel lines), Commands the operator to act, and Requests Confirmation that the action has been taken. He may also Request Data to help him chose or monitor the EOP, and the operator will Tell him the data. (Because of this cycle we have sometimes called this the "show and tell" model.)

If we compare Figure 1 with the other Figures, the value of the EOPP becomes apparent. It displays clearly and graphically the implications of the management's operating philosophy. Notice how an automated plant changes the flow of information and control. Notice what happens when two operators are used, and the difference between two operators with and without a supervisor. In the former case, the operators have an enormous burden of reading EOPs and also communicating each with the other. In the latter case, they are relieved of those burdens, but at the cost of a very heavy workload on the supervisor.

We have, in the report cited, considered a number of implications which these EOPP diagrams revealed. For example, consider how they are related. If in a Figure 4 type of system, the supervisor were to become ill suddenly, or, in an extreme case, be killed by a terrorist, the system would become a Figure 3. Would the operators be able to work with EOPs designed for a Figure 4, and when all their training assumed a Figure 4? This analysis

clearly shows that when designing EOPs, abnormal plant conditions are not only hardware conditions, but also crew conditions. As far as I know, no EOPs have ever been explicitly written with regard not merely to plant condition but also to crew condition. But considering the EOPP diagrams shows that EOP design, training, and manning must be integrated, and that a change in crew level or organization should be explicitly considered in an emergency, and EOPs written for those situations.

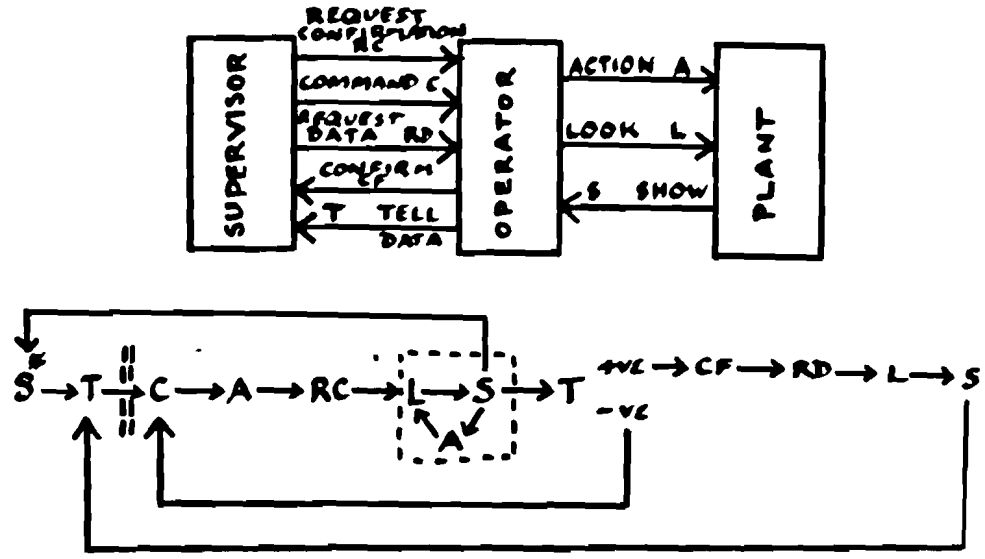
The workload on the various crew members can be estimated qualitatively in terms of the number of lines entering and leaving each box. It would probably be possible to quantify this to some extent by treating the graph as a time-line analysis for each EOP scenario, although we have not so far done this. We believe it is most important for the clear picture it provides of strength and weaknesses of communication among the crew. One particular point is related to the belief among many experts that an extra crew person is needed for emergency situations. There is abundant evidence that under pressure people are inefficient decision makers. In particular, they tend to commit themselves too early to a plausible diagnosis of the trouble, and monitor displays for evidence to confirm their hypothesis, and to assure themselves that their intervention is succeeding. The EOPP shows that the operators are likely to be completely taken up in the L-A-S-T-CF sequence, and the supervisor in reading the EOPs and his C-RD-RC-CF-T sequence. It is important that someone has time to monitor the overall plant condition, particularly looking for information which may reveal that the state of the plant is not actually what the operators believe it to be, or that disturbances are propagating to other parts of the system. The EOPPs support the contention that an extra operator, whose task is not to take part in the EOP but to monitor the plant and make independent state assessments, is desirable, since otherwise the supervisor or one or both operators would have to perform this task.

Developing an EOPP in detail also shows the impact on training. The particular L-A-S sequence performed by an operator depends on the training he has received, as does the structure of his communication with his fellow crew-members. If he has been trained to specialize in one part of the plant and communicate only with the supervisor, the flowchart will be different from its nature if all operators operate all parts of the plant. The advantages of specialization are reduced workload and a reduction or elimination of ambiguity about which operator will carry out which actions (obey which commands). Training is simpler. But the crew becomes heavily dependent on the supervisor for coordination and inflexible in their tasks.

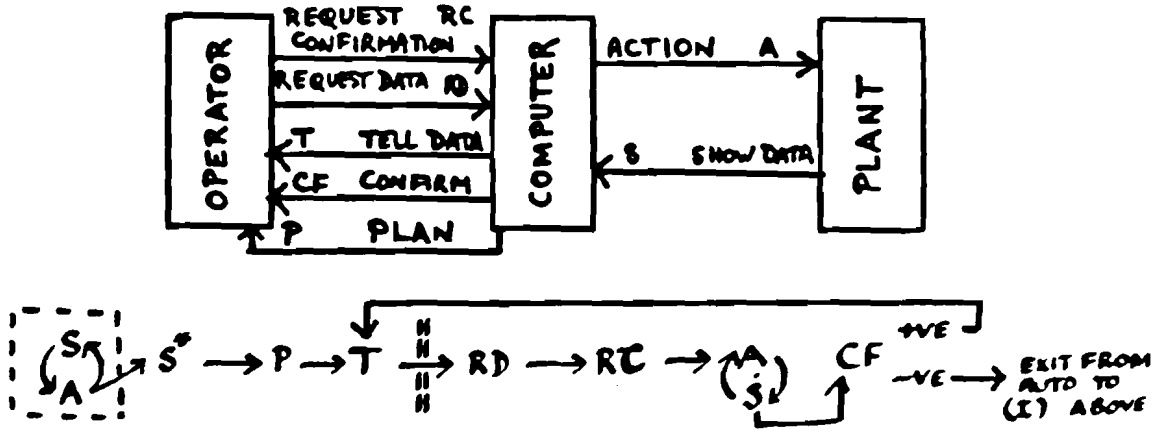
In summary, neither EOP generation, training, manning levels, operating philosophy (how much automation to use), or control room organizational hierarchy can be considered as separate operations. The first decision must be the operating philosophy. In the decisions which follow from the choice of an operating philo-

sophy we believe that the EOPP diagrams can play a useful role in integrating a systems approach to design for fault management.

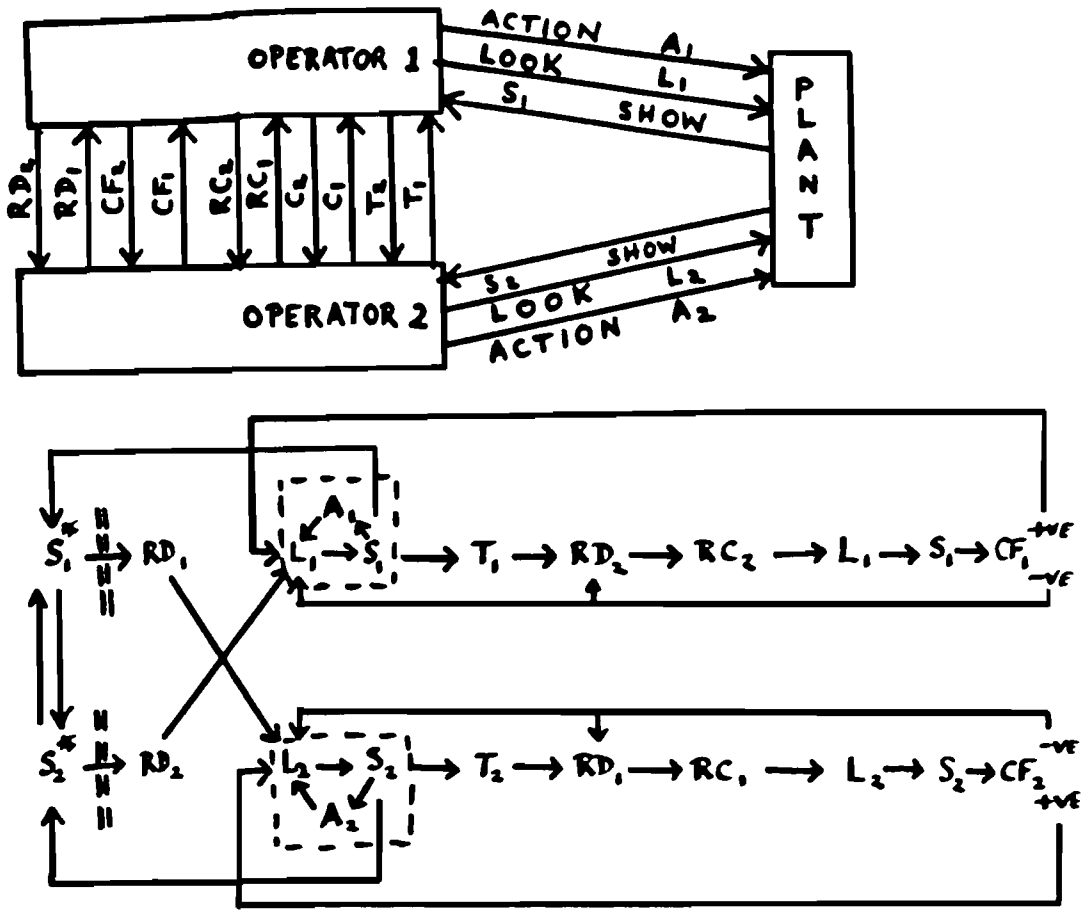
Feher, M., Moray, N., & Senders, W. 1987. The Development of Criteria for Emergency Operating Procedures. Atomic Energy Control Board. Ottawa, Canada.



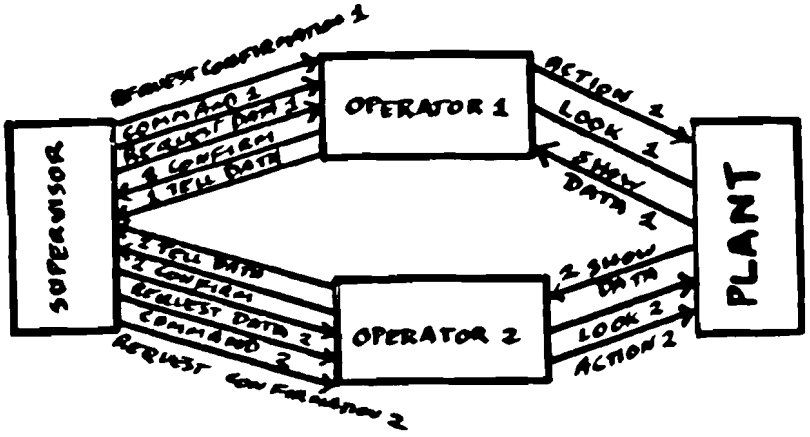
I. MANUAL CONTROL : HIERARCHICAL CREW

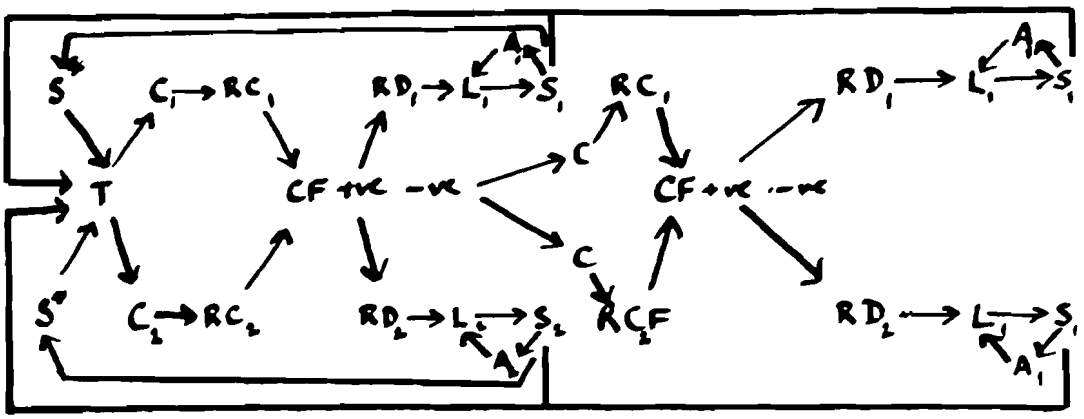


II. FULLY AUTOMATIC : HUMAN SUPERVISION



III. MANUAL CONTROL : HETERARCHICAL CREW.

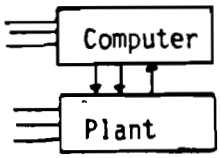




IV. MANUAL CONTROL: HIERARCHY WITH HETERARCHY.

Manual -

Semi-automatic -



Automatic -

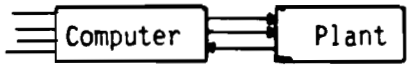
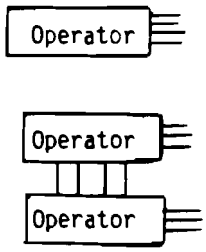


Figure V

Information Flow Diagram Building Blocks
Process Control Type

No Hierarchy -



Hierarchy -

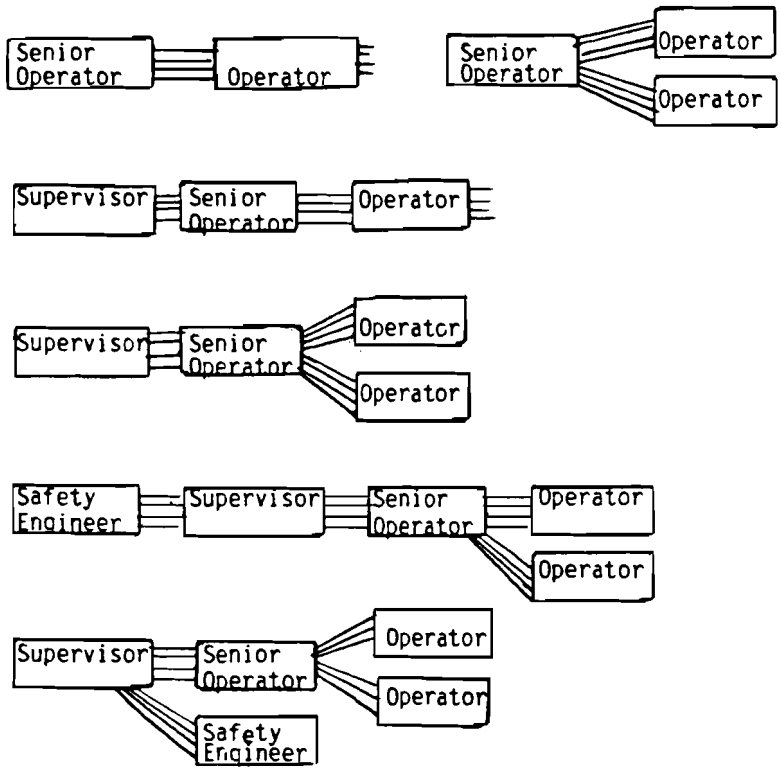


Figure VI

Information Flow Building Blocks
Crew Structure

4. TECHNICAL CONCEPTS

4.1. COMMENTS ON INHERENTLY SAFE TECHNOLOGIES

Prof. Boris Segerståhl
IIASA, Laxenburg, Austria

1. The Issues

Modern society has seen an enormous increase in scale and complexity of industrial activities. For a long period of time this development went unquestioned. An almost complete faith in the skill of managers and engineers prevailed. The situation has changed dramatically during the last two decades. There are three main reasons for this.

First. Nuclear power emerged in the fifties as the ultimate solution to the worlds increasing demand for electrical energy After the initial successes accompanied by a few but partly covered accidents the public became more and more concerned about the darker sides of this new technology.

Second. Environmental degradation and a growing concern for the quality of our physical living conditions lead to a more critical attitude to uncontrolled industrial expansion.

Third. Several spectacular industrial accidents like Seveso meant that public faith in the quality of industrial safety measures was destroyed almost overnight.

Public concern about the risks of industrial activities is reaching proportions which are almost beyond control in some cases. This is obvious in the case of opposition to nuclear energy. To a growing extent the same opposition can be seen in matters related to all handling of toxic materials or hazardous waste.

Political pressures from the public, and in some cases from the international community has lead to the establishment of new government agencies which have as their specific task to deal with regulation of industrial activities.

Industry is becoming worried about the present situation. The safety level of most industrial plants is without doubt good enough to answer any reasonable demands from regulators. This is, however, not enough in all cases. As can be seen from the nuclear industry, demands concerning safety leads to a destruction of the economic base for the whole industry. This can, with the exception of a few countries, ultimately lead to a disappearance of the whole technology.

The problem related to social and political acceptability of certain types of industrial activities is not independent of a country's overall cultural, political and economic situation. Without going into details we want to mention the fact that different policies related to nuclear power in countries like FRG, France, USSR, Sweden and USA does not depend only on the technical quality of their power plants or the overall economic situation in these countries. The general attitudes are a function of the population's total social and political awareness with the priorities following from this.

2. Definitions of Inherent Safety

Inherently safe technology is in the strictest sense of the word a system in which safety is based on physical properties of process design rather than on characteristics of technical components. A fail-safe system has to be designed with components which by no means can be considered as being fail-safe. Inherently safe properties of the system are triggered by malfunctioning components, instrumentation failures or operator errors. In extreme cases the definition of and insistence on inherent safety is absurd. It is a matter of demanding that "whatever happens nothing may happen".

It is essential to make a clear distinction between qualitative and quantitative demands. Qualitative demands imply that no causal paths from any type of malfunction or error may exist to a state where releases of energy or matter harmful to the environment and/or man take place. Quantitative requirements accept the possibility that in very improbable situation release levels might occur which are so low that they don't cause any harm.

If we take the case of a nuclear reactor. No causal path from any operating conditions to a core meltdown is allowed to exist in a system which is inherently safe *with respect to core meltdown*. Other accident trajectories, which might cause minor contamination or releases, can be constructed. As a relative concept we can however say that the plant is inherently safe due to the fact that its construction makes a core meltdown not only extremely improbable but *completely impossible*. This is one important property of inherent safety as it is generally understood. Inherent safety is a design concept related to broad scenarios defining what is considered as being unacceptable - e.g. core meltdown - while no claims are being made to elimination of all conceivable minor and major incidents in outrageously improbable situations.

Lawrence Lidsky (1987) has suggested that a useful way to classify nuclear plants would be to use four safety categories. In declining order of safety the classifications would be: "absolute" safety (no hazardous materials or confined energy sources); "inherent" safety (immune to major structural failures and operator error); "passive" safety (no immunity to major structural failure or operator error, but no need for active systems in the events of sub-

systems failure); and "engineered" safety (no immunity to major structural failure; positive response required to subsystem malfunction or operator error; in-depth defenses).

In the nuclear energy field all radically new development projects under way in different countries are probably concerned with the design of systems which fulfill the requirements of "passive" safety while "absolute" safety and "inherent" safety are concepts which require more theoretical and practical clarification before they can be accepted as a base for technical research and design activities.

3. Approaches in the Nuclear Industry

The focus of attention in the nuclear industry has been on ways to prevent loss of coolant accidents (LOCAs) with a potential for leading to core meltdowns in traditional reactor designs. The concept "inherently safe" stands for alternative reactor designs which have been proposed as radically safer alternatives to designs now used in commercial plants. As mentioned above the design concepts would lead to a classification of these concepts as passive safety design rather than inherently safe designs. From a practical point of view this is of course a minor point. What is essential is that work on radically new designs is under way.

Two heavily promoted alternative designs have attracted a lot of attention: the PIUS (Process Inherent Ultimately Safe) design proposed by ASEA and the HTGR (High Temperature Gas-Cooled Reactor) proposed by several companies in Europe and the USA. Of these two PIUS is more innovative and perhaps in a stricter sense inherently safe while the HTGR is more tested. Both designs are, however, commercially unproven experimental designs.

The PIUS reactor is a radically new LWR. The reactor core, primary cooling system and steam generators are immersed in a large pool of cold, borated water within a prestressed concrete pressure vessel. The pool and the primary cooling system are hydraulically connected, but under normal conditions the pressure developed by the coolant pumps is just enough to keep the pool water from entering the core. Any disturbance in the cooling system would upset the balance, and the borate solution would flood the core. The boron in the water would shut down the chain reaction, and the cold pool water would carry off the residual heat. Neither an operator nor an electromechanical device would be needed to set these events in motion (Lester 1986).

The European work on HTGRs will not be described in this paper as the topic has been dealt with in other papers in these proceedings.

Intensive development efforts are under way in USA. Three conceptual design programs were started in 1984. They include two LMR (Liquid Metal Reactor) concepts, the General Electric Power Reactor Inherently Safe Module (PRISM) and the Rockwell International Sodium Advanced Fast Reactor (SAFR), and the modular HTGR. Each reactor concept has adopted passive means of reactor shutdown and heat removal and thereby minimized the number of systems and components required for nuclear safety. In each of the designs, safety-related systems are limited to the reactor module. The rest of the plant and intermediate heat transport systems are decoupled from the safety systems.

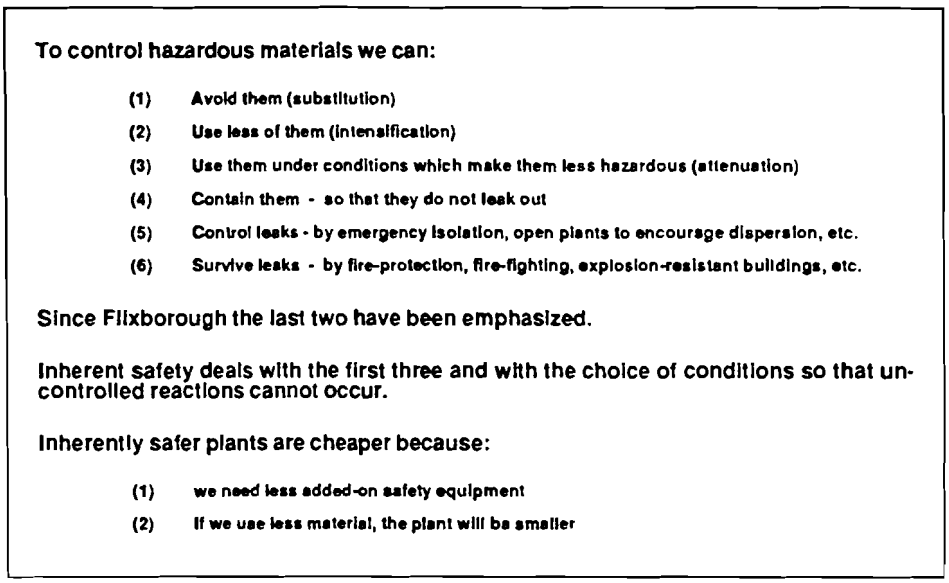


Fig. 1: The concept of inherent safety (Kletz 1984, p 6).

Safety of the LMR is based on natural laws such as gravity, thermal conductivity, thermal expansion, Doppler broadening, and sodium coolant density change to meet safety requirement and criteria. These properties are the basis for reliable shutdown and heat removal systems that function without electrical or mechanical support and are insensitive to station blackouts. Systems remain functional at all times, do not rely on operator action, and therefore cannot fail or be shut off.

Passive safety of the modular HTGR stems from the ability to effectively utilize inherent features of the concept including the inert coolant, the capability of the refractory coated fuel to withstand high temperatures, the high thermal inertia and high temperature stability inherent in the graphite core and support structures, and the strong negative temperature coefficient of the reactor core (Lester 1986).

4. Chemical Industry

Nuclear and chemical hazards are viewed and controlled differently. This reflects the different organizations of the industries and the different levels of public and political concern. The nuclear industry is a very small group of highly sophisticated large companies. Communication and coordination of development and safety activities is therefore efficient. This is true even in competitive situations. Also, the public hazard and acceptance aspect has been recognized since the beginning of the nuclear industry as a prerequisite for operation of nuclear power plants. As a consequence it has traditionally been possible to give high priority to the setting of safety goals valid for the industry as a whole.

The chemical industry is structured differently. It consists of a wide spread of company types, and analogous risks can be created by many whose use of hazardous substances is ancillary to their main business. The competition in the market for chemical products is different from the nuclear industry. There is a continuous need to minimize cost in many plants producing bulk chemicals for international market. The price competition in the nuclear industry has a completely different structure (if it exists at all).

The concept of inherent safety has no clearly established position in the chemical industry. Trevor Kletz (1984) has for a long time been advocating the concept as a design base for safer chemical plants. The approach taken by Kletz is a practical engineering approach. He does not bother with a scientifically consistent definition of inherent safety. In Figure 1 we reproduce his view of the concept of inherent safety.

Time is not ripe to even try to give an overview of the concepts and principles in the chemical industry. The situation is to unstructured and it is obvious that only marginal improvements will be achieved in the near future. The chemical industry is simply so constrained by economics, politics and tradition, that the development of new concepts and principles for chemical processes and plants will take a long time to come. Fortunately much work is being done on quantitative improvements to compensate for the slow progress in the field of qualitative innovations.

What can be said about the chemical industry is said very well by Kletz. It is, however, difficult to identify a generic concept of inherent safety in this approach. By following Kletz's guidelines it is in most cases impossible to state that one design is inherently safe while another is not. It is of course possible to compare the relative safety of different designs but this as such does not imply that there is a qualitative difference between designs in such a way that an inherently safe plant can be defined and identified.

5. Constraints

As Lester (1986) has pointed out, many people in the nuclear industry regard the idea of a major shift away from current technology as unrealistic. According to this view, it is better to improve existing technologies incrementally. This would enable the industry to draw on the enormous store of knowledge related to the LWR. Whatever the advantages offered by new systems, the revolutionary concepts would encounter many unanticipated problems. The critics are also worried about diverting development from the international mainstream of technological development.

The constraints on the chemical industry have been mentioned above. Many of the problems related to introduction of radically safer plants can be traced back to traditions of thinking in the industry and, on a more tangible level, to concerns for competitiveness, cost efficiency, and new risks created by untested processes.

Before an old and tested design is abandoned in favor of a radically new one there has to be, in the word of Norman Clark (1987), an alternative which shows promise of dealing with the pitfalls and puzzles experienced in the operation of existing technological practice, since in the absence of such a candidate it is likely that attempts will continue to be made to prop up the status quo - to regard 'anomalies' as 'puzzles'.

Constant (1984) states: "Old communities and traditions virtually never give birth to radically new technologies. No manufacturer of piston aircraft engines invented or independently developed a turbo-jet. No designer of conventional reciprocating steam engines independently developed a steam turbine.... When abrupt transitions in technological practice do occur, as happens from time to time, they almost always are the work of people outside, or at least on the margins of, the conventional community."

We will not spend time on these philosophical matters in this paper. To a large extent the issues mentioned relate to the general question of innovations and the driving forces behind them. a few words will be spent on the economics of the industries. Both as a driving force behind and as an obstacle for introduction of radically new and safer plants and processes.

A common feature of proposed safe designs for nuclear reactors is that they are small, modular and standardized. The PRISM plant consists of nine pool-type reactors grouped in three power blocks, each producing 415 MWe (net) giving a total of 1,245 MWe. The 1,400 MWe SAFR design consists of four pool-type reactors, each individually controlled and operated in a common control room. Each reactor is coupled to a single 350 MWe turbine generator unit operating with superheated steam. The American design for a modular HTGR plant consists of four reactor modules, each rated at 350 MWt, coupled to two steam turbine generators yielding a net power output of about 550 MWe.

The economic benefits from modular and standardized design of small units can be substantial. The efforts to develop small plants is in conflict with conventional wisdom which says that big plants are cheaper to build and operate than small. By big is meant reactors on the 1000MW range. The rationale behind this traditional opinion is that a much larger proportion of the capital costs of nuclear plants is size-independent compared with the cost of building other types of plants. Other factors have, however, led the industry to reconsider the question of economies of scale. Large plants are increasingly difficult to finance, entail greater liability, and may not match a utility's load growth. Scaling down conventional reactors would, however, not produce a competitive small plant. Instead, some potential advantages inherent in small reactors must also be designed to meet the same criteria for standardization and enhanced safety expected of larger reactors in the future (Douglas 1986).

The economics of safety are changing in the chemical industry too. Traditionally this industry has been allowed to operate in a rather loose framework of environmental regulations. The situation is changing rapidly. Now a substantial proportion of the chemical industry's investments are used for new environmental and pollution control equipment to enable plants to operate under normal operating conditions with stricter environmental protection regulation. According to recent calculations by the Chemical Manufacturers' Association in the U.S.A., the amount spent in 1988 on protective equipment will total $3 billion which is 17% of the industry's planned capital spending (Anonymous 1987).

These investments are spent on protective measures for future operation of the plant. The cost of cleaning up after a long period of polluting activities is not insignificant either. he Environmental Protection Agency has announced that it will impose new controls to reduce the levels in surface waters of 66 toxic chemicals released from 61 plants in New Jersey, Alabama, East Virginia and South Carolina. Together they have been pouring away 10,000 tons too much of toxic chemicals a year. The clean-up will cost them $500m a year.

The cost mentioned above are investments required to ensure legal operation under normal circumstances in the future. The cost of future accidents is an altogether different issue. Nobody knows with certainty what the situation will be. The only assumption which can be made is that future accidents in the chemical industry can be very expensive and lead to plants closing down and companies going bankrupt. The value of investments in inherently safe systems in the chemical industry have to be assessed against the probable costs of other alternative. More information on future hypothetical liabilities resulting from accidents are from a pure cost benefit analysis point of view badly needed. An indication of the amounts involved comes from the fact that Union Carbide has been sued for $3 billion in India. A probable level for a settlement could be around $600m or equivalent to 10% of the company's total assets. The role of the insurance industry will of course change with these new legal environments.

The figures indicated above make it clear that there is a strong economic incentive for more work on inherently safe systems and designs in the chemical industry. The problem is a qualitative issue - how to avoid closing down - and a quantitative issue - how to stay profitable.

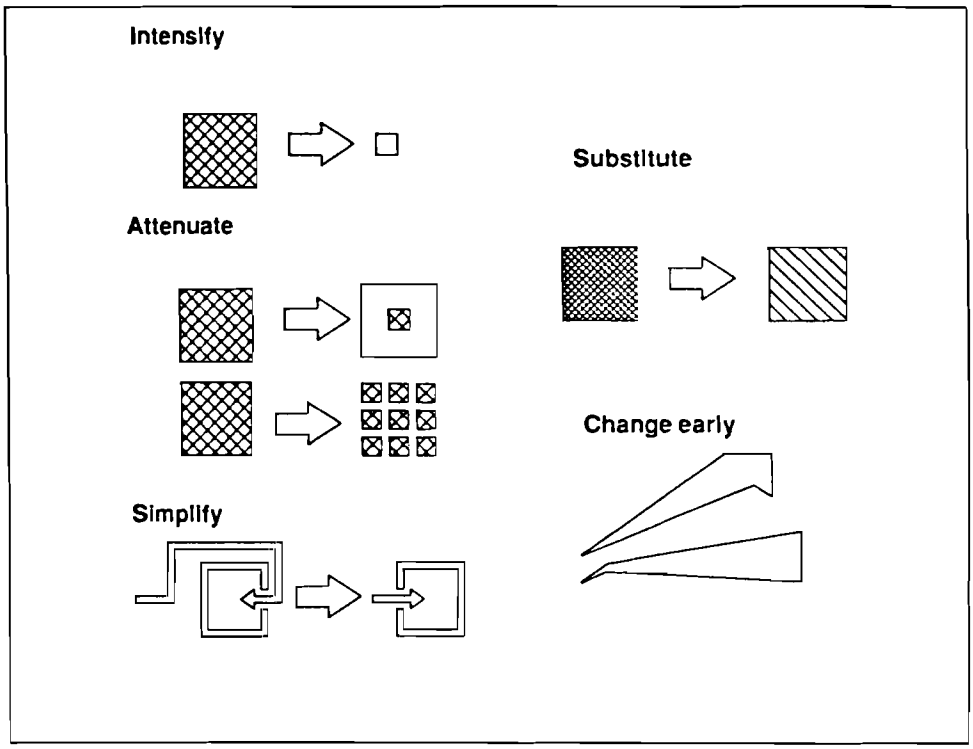


Fig. 2: An Atlas of Safety Thinking according to Kletz (1984, pp118-119)

To find a scientifically valid answer to the question of how to structure and define inherently safe technology will take a long time. This search could be like chasing nonexistent windmills if it is allowed to loose track of the practical constraints of reality, technology and economics which are a prerequisite for all industrial progress in a world structured the way ours is today. And there are no alternative worlds available, as far as I know. Therefore I want to finish this paper with a view given by Kletz in Figure 2. This gives us a practical view of how to live with the reality of research, design and engineering while searching for future perfect solutions to problems which are not even clearly defined yet.

References

Anonymous (1987). American chemical companies: cleaned up or cleaned out. *The Economist*, Dec. 12 1987, pp 73-74.

Clark N (1987). Similarities and Differences Between Scientific and Technological Paradigms. *Futures*, February 1987, pp 26-42.

Constant EW (1984). Communities and hierarchies: structures in the practice of science and technology. In R Laudan (ed), The Nature of Technological Knowledge: Are Models of Scientific Change Relevant? *Reidel*, 1984, p 30.

Douglas J (1986). Toward Simplicity in Nuclear Plant Design. *EPRI Journal*, July/August 1986, pp 4-13.

Kletz TA (1984). Cheaper, Safer Plants or Wealth and Safety at Work. *The Institution of Chemical Engineers*, 1984.

Lester RK (1986). Rethinking Nuclear Power. *Scientific American*, March 1986, Vol. 254 No. 3, pp 23-31.

Lidsky, L. (1987). Nuclear Power: Levels of Safety. Quoted in *The Energy Daily*, November 17 1987, p 4.

4.2. INVESTIGATIONS ON HYPOTHETICAL ACCIDENTS OF THE HTR-500

Prof. Rudolf Schulten
Institute of Reactor Development
Nuclear Research Centre, Jülich, FRG

1. Technical Concept of HTR-500

The HTR-500 is based on the THTR-300 power plant. The dimensions of the power plant are nearly the same but a doubling of a power output can be reached. Fig. 1 shows the overall plant.

In the centre of the HTR-500 power plant complex the reactor containment building is situated housing the prestressed concrete reactor vessel including the primary system, the shutdown facilities, parts of the decay heat removal system and other safety-relevant components. In addition the reactor containment building acts as a protection against external impacts. All the component parts carrying activity are arranged inside the reactor containment building except the fuel element storage, which is, however, also equipped with a protection against external impact. The reactor service building on the one side of the reactor containment building and the turbine building on the other side form a line of buildings facing the electrical equipment building.

Fig. 2 shows a vertical section of the prestressed concrete reactor vessel with its internals. The thermal energy is generated by 1,145,000 spherical elements with a diameter of 6 cm, about 80 % of which are fuel elements and 20 % graphite elements used in the THTR-300 for the initial core only. Each fuel element contains low-enriched uranium fuel in the form of 16,000 coated particles equipped with an additional SiC layer for the retention of metallic fission products. The fuel elements pass through the reactor only once (OTTO-fuelling). The spent fuel elements are discharged from the core through three fuel element discharge pipes without interrupting power operation. The spent fuel elements are directly discharged into casks and transported to the storage. No special conditioning for spent fuel is necessary for long-term interim storage or for final storage.

The waste management concept is adapted to the special characteristics of the HTR line. 10 years' interim storage of the spent fuel elements in fuel

storage casks is intended to be followed by transport to a nuclear waste repository for ultimate disposal. Due to the limited quantitiy of spent fuel elements, closing of the HTR fuel cycle is not a suitable solution, so that - as for other prototype nuclear power stations - direct ultimate disposal is envisaged in the long run.

This concept corresponds to the AVR and THTR-300 waste management concept, as licensed by the authorities.

The reactor pressure vessel is designed as a large cavity prestressed concrete reactor vessel (PCRV) as in the THTR-300. The complete primary system is integrated in the PCRV.

The HTR-500 is equipped with 6 steam generators of heli-coil design operating in countercurrent. Each steam generator is associated with a circulator. The circulator design is the same as that of the THTR circulator, it is, however, equipped with active magnetic bearings and arranged in a vertical position.

The helium coolant flows downwards through the reactor core, then upwards through the steam generators to the circulators from where it is recirculated to the cold gas plenum, cooling on its way the outer surfaces of the primary system.

Because of the availability of the separate two-loop decay heat removal system, the main cooling system consisting of 6 steam generator/circulator units has no safety function. Therefore, the main cooling system is of a purely conventional design outside the reactor containment building, i.e. it is designed to the usual standards applied to modern conventional power plants.

2. Safety Features of the HTR-500

2.1 Safety Characteristics

Due to the design, the core structure and the materials resistant to high temperatures, the HTR pebble-bed reactor is capable of making use of physical laws giving rise to inherent safety characteristics.

On the one hand, these safety characteristics specific to the HTR result in extremely benign and safe operating and accident behaviour which allows

the use of simple and uncomplicated systems for operation and accident control. This is very important to the operator because

- the operating staff has ample time for reaction,
- manual measures are possible to eliminate malfunctions,
- the risk of capital loss is very low.

On the other hand, the special importance of the HTR-specific safety characteristics results from the limitation of damage in the event of accidents. This means that not only the product of damage and frequency is very small but also the damage itself. Therefore, the environment is not exposed to consequences of a serious nature even in the event of hypothetical accidents.

The HTR's principle inherent characteristics are as follows:

- negative temperature coefficient of reactivity effecting self-stabilization and limitation of reactor power,
- ceramic (graphite) core structure and fuel elements ensuring resistance to high temperatures up to about 3500 °C,
- low ratio of power density to heat capacity resulting in a slow rise of the fuel element temperature under accident conditions,
- inert, phase-stable gaseous coolant (helium) ruling out total loss of coolant.

2.2 Shutdown System

The HTR-500 is equipped with two redundant shutdown systems consisting of the reflector rods and the incore rods.

The 48 reflector rods constitute a safety system used exclusively for reactor scram. When their effect is needed, the reflector rods drop into boreholes in the side reflector blocks under the force of gravity.

The 72 incore rods are used for control and long-term shutdown. They are manoeuvred by a pneumatic piston system. Long-term shutdown by the incore rods is effected exclusively by manual release and does not have to be initiated earlier than 10 hours after shutdown of the plant by the reflector rods.

The pyrocarbon and silicon carbide coatings of the fuel particles form a highly effective pressure and gas-tight containment of the fuel and the fission products up to high temperatures safely retaining the radioactivity at the place of generation.

Therefore, the primary coolant has only a very low activity concentration during normal operation and under accident conditions so that the subsequent barriers are much less important than in other reactor types.

The gas-tight fail-safe prestressed concrete reactor vessel having a wall thickness of 5 m and multiple redundant prestressing cables represents another barrier. In the event of hypothetical depressurization accidents the maximum possible leakage cross-section at the metal penetrations and connection lines is limited to 33 cm^2 by structural devices. If rupture occurs in these components, the coolant therefore escapes very slowly. It takes about 1.5 h before pressure equilization is established. During this period the coolant gas is passed directly into the stack through pressure relief valves. When pressure equilization between the reactor containment building and the atmosphere has been established, the helium is discharged through the ventilation air filter system.

The HTR-500 is equipped with a special filter, which under accident conditions is capable of retaining the metal fission products effectively.

3. HTR Basis Accidents

Practical experience gained from the licensing procedure and the operation of the AVR and the THTR-300, as well as risk analyses performed for the HTR plants, have confirmed that the design of the safety system is determined by the following accident categories:

- failure of individual decay heat removal systems or loops resulting in a reduction of the decay heat removal capacity of these systems,
- unintentional power excursion and, as a result, temperature increase in the reactor core,
- depressurization accidents resulting in a reduced cooling capacity of the primary circuit,

- tube rupture in the steam generator, i.e. ingress of water into the primary system.

In the event of design-basis accident, forced cooling of the reactor core remains intact. Design-basis accidents are accidents the control of which has to be verified in the licensing procedure within the permitted limiting dose values according to § 28.3 of the Federal Radiological Protection Ordinance. The fuel element temperatures are reduced below 500 °C within a few hours, so that even the most improbable accident-failure combinations including water or air ingress can be controlled without any problems. Below about 500 °C the reaction rates of steam or oxygen with the graphite of the fuel elements are negligibly low.

4. Recent Studies on Determining Damage during Hypothetical Accidents

The release of radioactive fission products due to excessive temperature can be ruled out, as far as is humanly possible, by the reliable afterheat removal systems /1/. In the case of the THTR-300, for example, a failure probability of 2×10^{-6} has been determined.

Recent experimental results and insights also enable hypothetical accidents and their effects to be described more precisely. Since these accidents are associated in every case with an increase in the temperature of the reactor and the internals of the prestressed concrete vessel, this research work primarily concentrates on the behaviour of the fuel elements, the components and prestressed concrete vessel at high temperatures.

4.1 Behaviour of the Fuel Elements at Elevated Temperatures

The behaviour of fuel elements at accident temperatures has been studied in recent years /2/. For this purpose, spent fuel elements from the AVR reactor were heated under simulated accident conditions. It became apparent that up to a temperature of 1600 - 1800 °C only slight and negligible quantities of fission products were released. If the temperature risis further then the diffusion of metallic fission products through the particle cladding begins /3/. In the case of small reactors in the power range from 200-250 MWth, a dangerous release of radioactivity can thus be ruled out even in severe accidents since the temperature range from 1600 - 1800 °C is not exceeded

due to good heat conduction in the reactor core /4/, /5/. This release is increased with an even greater rise in accident temperatures in larger reactors and failure of the claddings occurs at temperatures above 2500 °C. However, in a core heatup accident only a small section of the reactor is exposed to such temperatures. Processes during the release of fission products can be described by verified computer programs.

4.2 Behaviour of the Prestressed Concrete Vessel at Elevated Temperatures

Experimental studies have also been made of the behaviour of the prestressed concrete vessel at increased temperature load /7/. Representative sections of the inner prestressed concrete surface, including the isolation and the liner structure, were tested at up to 1300 °C. Contrary to previous expectations, the concrete does not crumble into dust but rather forms a vitreous mass. According to the present state of the art, it can be assumed that the bond between the liner and concrete at the inner surface of the prestressed concrete vessel can withstand a temperature of at least 1100 °C without the integrity of the vessel being lost. The temperature inside the concrete walls drops steeply towards the outside. The major fraction of the prestressed concrete vessel thus remains at moderate temperatures. Vessel stability can be expected at all times since in all severe accidents temperatures of 1100 °C are not exceeded at the inner surface of the prestressed concrete vessel /8/. The volumes of carbon dioxide and water vapour arising during heating of the concrete can escape outside due to the porosity of the concrete and thus do not penetrate inside the reactor vessel /7/. Even in the case of the most rapid depressurization, the stability of the concrete vessel restricts the discharge opening of the primary system to 33 cm^2. The maximum escaping gas volume is still so small that it can be purified by a filter system in all accident situations before the gas flows into the environment.

4.3 Absorption and Retention of Fission Products in Graphite

Graphite used in the production of fuel elements and the reflector absorbs fission products, particularly cesium and strontium, even in the high temperature range /6/. According to present knowledge, the major fraction of the released fission products is deposited at colder locations in the reactor core and in the upper graphite reflector. Experimental results have also become recently available on the dynamics of the absorption processes /11/. The most important fission products, namely Cs, Sr and the

rare earths, are practically completely retained. The retention capacity of the upper top reflector can even be improved in comparison to the present status by a suitable choice of materials - namely graphite with an increased binder content. Iodine and silver, on the other hand, display lower absorption.

5. Processes During Hypothetical Accidents

5.1 Leaks of Large Quantities of Water and Steam into the Primary Circuit

The ingress of water into the primary circuit in the case of a leak in the steam generators can also be adequately restricted. Leaks in the steam generators may introduce a maximum of 10 kg/s into the system. Water influences the reactivity and causes corrosion of the fuel elements /9/, but his can be reliably prevented with the aid of the reactor protection system. If a leakage of water is assumed simultaneously with failure of the nuclear shutdown system, in the sense of a hypothetical analysis, then this could lead to an increase in reactor temperature due to the rise in reactivity. As a consequence of this, depending on operation of the circulators, the gas temperature will rise in the upper or lower section of the reactor. A safety fuse is deployed in the upper and lower reflector of the reactor to interrupt the power supply for controlling the motors of the feedwater pumps if the normal temperature is exceeded. The interruption in the power supply for the thyristors of the driving systems for the feedwater pump motors and other units in the primary circuit thus occurs in accordance with physical laws and the maximum water ingress is limited to less than 10 t. Serious corrosion and the formation of explosive gases in the containment can thus also be ruled out even in hypothetical accidents. The power supply to the nuclear shutdown system can additionally be interrupted so that the nuclear reaction is then shut down.

5.2 Leakage of Air into the Primary Circuit

The leakage of air into the primary circuit after a possible despressurization is adequately restricted by the prestressed concrete vessel and the reactor containment. Such a leak is only possible if the helium escapes from the prestressed concrete vessel up a pressure equalization. After depressurization, less than 30 % air and approximately 70 % helium are present in the reactor containment. The residual oxygen, with a fraction of approx. 6 %, in the reactor containment can theoretically penetrate into the prestressed concrete

vessel by slow convection and diffusion processes without causing serious damage. Only apertures of max. 33 cm^2 can arise in the concrete vessel so that even in the case of failure of the vessel no serious damage to the reactor core can occur in the long term due to the low velocity of the natural convection flows. Even in the case of a stack draft with an upper and lower aperture in the prestressed concrete vessel, the corrosion rate will only amount to about 1 t of graphite loss per year.

5.3 Reactivity Accidents in the Hypothetical Range

Reactivity accidents are prevented by two independent diversified shutdown systems. The temperature in the reactor core will rise slowly in the case of a hypothetical, defective failure of the shutdown system and any increasing reactivity is compensated by the negative temperature coefficient /1/.

5.4 Deterministic Establishment of Hypothetical Accidents

The totality of all conceivable accidents over and above design-basis accidents can be discovered by a deterministic assumption of the faulty behaviour of all safety-relevant components. Under the pessimistic assumption that all reactor protection measures fail, particular attention must then be paid to six components the combined faulty behaviour of which covers the entire accident spectrum. These six components are as follows:

- the prestressed concrete vessel,
- the steam generators,
- the nuclear shutdown system,
- the afterheat removal system,
- the circulators and
- the feedwater pumps.

Other components, such as the valves and safety valves as well as the shutoff devices in the primary circuit can be included in this combination scheme if the given major components should fail. For example, a failure of the safety valves is also included in the case of failure of the prestressed concrete vessel.

A total of 124 accident situations in the hypothetical range can be found by a corresponding combination of the failure of these components. This includes accidents with the greatest possible impacts in which failure

of the nuclear shutdown system, afterheat removal and cooling of the prestressed concrete vessel is simultaneously assumed. All other accidents are of minor significance. A total of 16 accident situations thus result which can in part lead to core heatup with various sequences and a temperature rise in the reactor core and prestressed concrete vessel. Their impacts characteristically depend on the rate of depressurization of the prestressed concrete vessel. The water ingress limited by the contact breaker system to 10 t, on the other hand, only plays a minor role. In the case of a core heatup accident, this quantity of water is namely already converted into water gas in the first few hours during a temperature increase in the core before release of the fission products begins. The water gas produced has a high reduction potential and therefore, in comparison to a pure helium atmosphere, has practically no influence on the behaviour of the fission products /10/.

5.5 Depressurization and Release of Fission Products

In the case of a rapid depressurization in a period from 1.5 to 6 hours, a slight quantity of heat is transferred from the reactor core to the internals. In this case, a steep increase in reactor temperature results reaching approx. 2500 °C in the centre of the core after about 40 hours and approx. 1800 °C as an average for the reactor core. The top reflector then has an average temperature of 1200 °C /1/.

On the other hand, with a slow depressurization (in an extreme case up to 100 hours) the heat from the reactor core is largely transported by natural convection to the components and the inner surface of the prestressed concrete vessel. In this case, the reactor temperature amounts to about 1800 °C at the centre while the average temperature is approx. 1200 °C and there is practically no release of fission products. All other accident situations are ranged between these two extremes with the tendency that rapid depressurizations lead to increased temperatures in the reactor core with correspondingly higher releases whereas slow depressurizations result in lower accident temperatures and less release. In all cases, the release starts after about 8 hours and is completed after approx. 40 hours /1/.

According to present experimental experience and conservative calculations, up to 10 % of the particles may fail in the case of rapid depressurization whereas for extremely slow depressurization the failure rate is of the order of magnitude of approx. 1 per 1000. The fractions of the fission products

released vary depending on the individual types. Gaseous fission products and iodine are largely released by particle failure whereas cesium, strontium and other metals diffuse through the particle claddings. A circulation of gas in the reactor core results for all core heatup accidents, as well as a slow flow of gas through the upper reflector (approx. 10 cm/s) into the prestressed concrete vessel caverne by means of natural convection. The fission products are transported from hot to cold locations in the system by this gas movement. Cs, Sr and other metallic fission products are deposited by absorption on the graphite. Strontium and the rare earths are completely retained and this is also expected of Cs /11/, although final statements are not yet possible. Iodine, silver and the noble gases are not deposited.

The prestressed concrete vessel is designed in such a way that the fission products are transported by the escaping helium through defined apertures. Depressurization and consequently transport of the fission products therefore can take place in four possible directions:

- into the space above the prestressed concrete vessel,
- or into the space below the prestressed concrete vessel (fuelling room),
- or into the compartment for the gas purification plant,
- or into the secondary circuit.

The three compartments mentioned above are closed by airlocks during operation and are connected via vent channels to a filter with a cooling bed connected in front so that it is possible to adequately remove all fission products.

If the gas mixture overflows into the secondary circuit, an adequate deposition of iodine and silver is probably to be expected on the still relatively cold components and piping. In particular, the cold condenser with its large heat transfer surfaces will operate in this sense. However, if it should not be possible to obtain this demonstration then an interconnecting tube may be envisaged from the condenser to the filter with a supported rupture disc to transfer the gas mixture into the cooling bed and filter.

6. Summary

On the whole, the following may be said according to present expectations of the behaviour of fission products during hypothetical accidents. The elements strontium, cesium and the rare earths are retained to an adequate content in the cold areas of the reactor core in the upper reflector. In any case, the escape of gas during any depressurization of the prestressed concrete vessel is so slow that a passive filter system can adequately purify the escaping gas of iodine and silver, and thus serious environmental pollution may be ruled out.

Literature

/1/ Sicherheitstechnische Untersuchungen zum Störfallverhalten des HTR-500, Jül-Spez-240.

/2/ W. Schenk, D. Pitzer, H. Nabielek: Spaltproduktfreisetzungsverlauf von Kugelbrennelementen unter Störfallbedingungen, Jül-2091, Oktober 1986.

/3/ K. Verfondern, H. Nabielek: PANAMA: Ein Rechenprogramm zur Vorhersage des Partikelbruchanteils von TRISO-Partikeln unter Störfallbedingungen, Jül-Spez-298, Februar 1985.

/4/ I. Weisbrodt, W. Steinwarz, W. Klein: Status of the HTR-Module Plant Design, IAEA, Technical Committee Meeting on Gas-Cooled Reactors and Their Application.

/5/ S. Brandes, W. Kohl, H. Schmitt: Small Nuclear Power Plants, IAEA, Technical Committee Meeting on Gas-Cooled Reactors and Their Application.

/6/ IAEA Specialists Meeting on Fission Product release and Transport in Gas-cooled reactors, Gloucester (U.K.), October 1985.

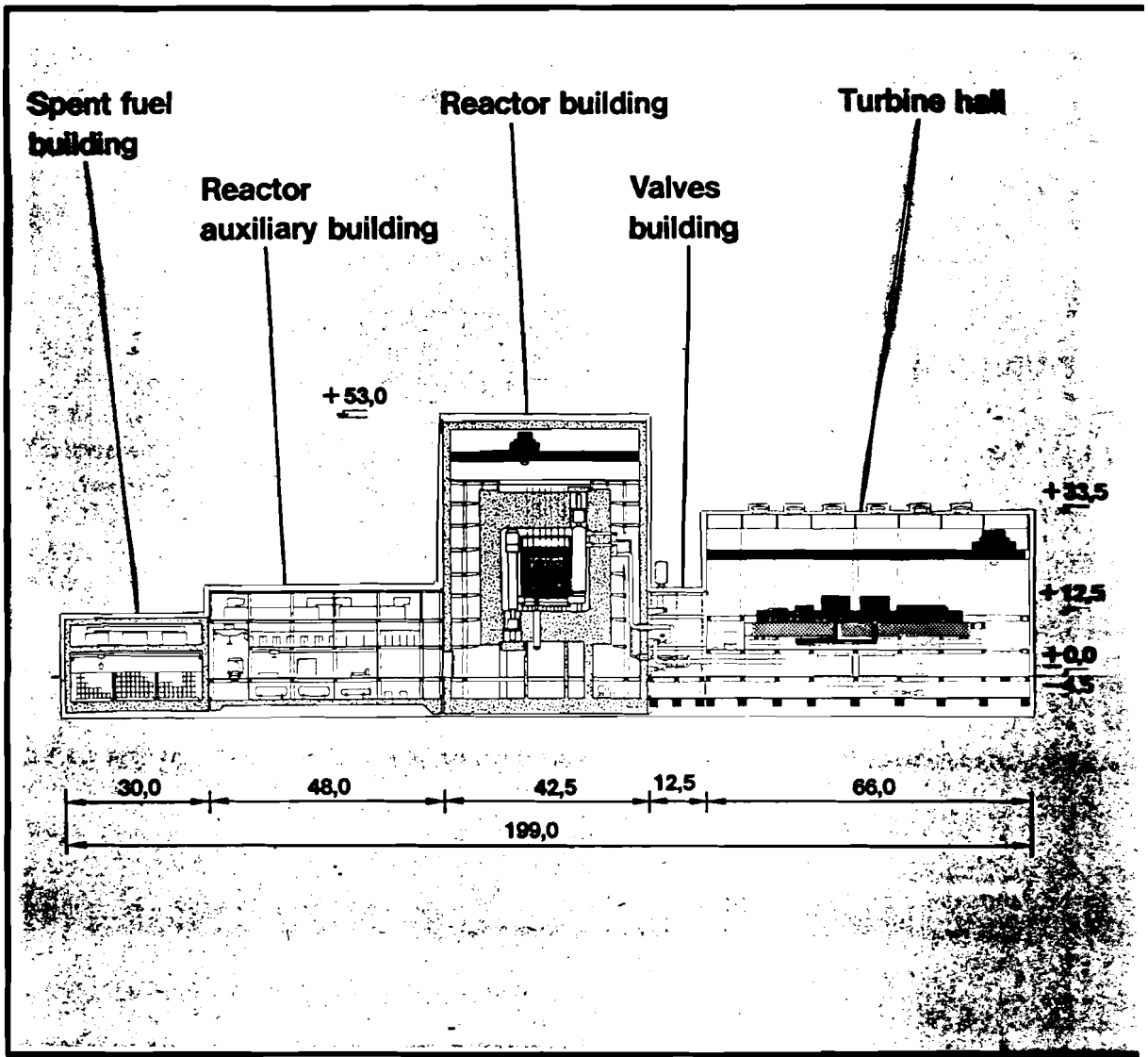
/7/ J. Altes, G. Breitbach, U.H. Escherich, T. Hahn, M. Nickel: Experimental Study of the Behaviour of Prestressed Concrete Pressure Vessel of HTR at Accident Temperatures, Transaction 9. Intern. Conf. on SMiRT, Lausanne, 17,-21.8.1987.

/8/ W. Jahn, W. Rehm: Neuere Forschungsarbeiten zum thermodynamischen Sicherheitsverhalten des HTR bei Coreaufheizsstörfällen. BWK-Fachzeitschrift, Düsseldorf, eingereicht März 1987.

/9/ W. Scherer: Untersuchungen zum hypothetischen Wassereinbruchstörfall in Hochtemperaturreaktoren, Interner Bericht, KFA/IRE, Januar 1987, Veröffentlichung in Vorbereitung.

/10/ R. Moormann: Untersuchungen zum chemischen Verhalten der Spaltprodukte bei HTR-Kernaufheizstörfällen. Jahrestagung Kerntechnik 85, München, S. 163-166.

/11/ Iniotakis, C. von der Decken: Interner KFA Bericht, Veröffentlichung in Vorbereitung.



HTR 500 Nuclear Power Station
Fig. 1 Longitudinal Section

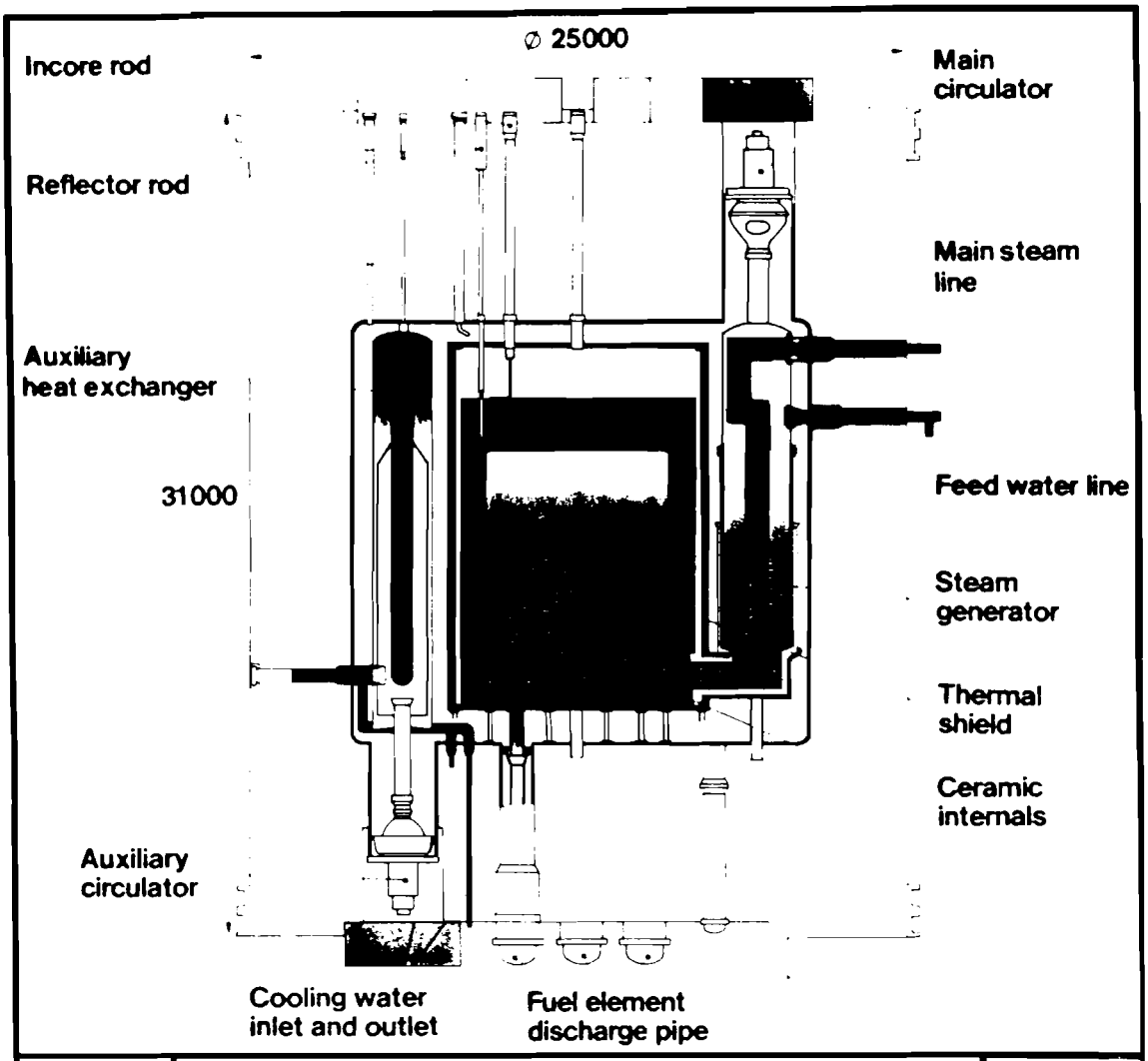


Fig. 2 HTR-500 MW
Reactor Pressure Vessel with Internals

4.3. THE SAFETY CHARACTERISTICS OF THE HTR-500 REACTOR PLANT

Winfried Wacholz
Hochtermperatur-Reaktorbau GmbH
Mannheim, FRG

The safety characteristics of high-temperature reactors, especially those of the HTR 500 reactor plant are illustrated in the following. On the basis of the practical experience the vendor of high-temperature reactors, BBC/HRB gained in more than 20 years AVR operation in Juelich and during the commissioning and experimental power operation of the THTR 300 in Schmehausen.

The primary objective of any reactor protection system is the safe containment of the radioactive fission products generated by nuclear fission. The classical active safety systems for

- shutdown
- decay heat removal and
- activity containment

are used also in the HTR to minimize the impact of the power station on the environment and to protect the plant itself under all operating and accident conditions.

The inherent safety characteristics of the HTR however effectively counteract any hazard arising in case of failure of the active safety measures provided for accident control. The inherent safety characteristics combined with the passive safety systems of the HTR ensure sufficient protection even in the event of extremely improbable accidents. Even under such conditions the release to the environment is low enough so that rapid measures such as evacuation of the population are not required.

The combined effect of the active and passive safety measures and the effect of the inherent safety characteristics in the HTR will be discussed using the HTR 500 pebble bed reactor as example.

Exactly the same safety arguments apply to smaller HTR power stations, such as the HTR 100. Due to their lower power rating and power density, such plants have an even wider safety margin.

The HTR's Inherent Safety Characteristics

Inherent safety characteristics are "innate" characteristics counteracting the effects of malfunctions, incidents and accidents due to physical laws.

Active engineered safety systems, such as pumps and valves always rely on triggering and energy supply for their functioning.

Passive safety systems need neither triggering nor energy supply for their functioning. Their function is therefore more reliable than that of the active engineered safety systems.

Due to the design, the core structure and the materials resistant to high temperatures, the HTR pebble bed reactor is capable of making use of physical laws giving rise to inherent safety characteristics.

On the one hand, these safety characteristics specific to the HTR result in an extremely good-natured and safe operating and accident behaviour which allows the use of simple and uncomplicated systems for operation and accident control. This is very important to the operator because

- the operating staff has ample time for reaction
- manual measures are possible to eliminate malfunctions
- the risk of capital loss is very low.

On the other hand, the special importance of the HTR-specific safety characteristics results from the limitation of damage in the event of accidents. This means that not only the product of

damage and frequency is very small but also the damage itself. Therefore the environment is not exposed to consequences of a serious nature even in the event of hypothetical accidents.

The HTR's principle inherent characteristics are the following:

- low ratio of power density to heat capacity resulting in a slow rise of the fuel element temperature under accident conditions

- ceramic (graphite) core structure and fuel elements ensuring resistance to high temperatures up to about 3500 °C

- negative temperature coefficient of reactivity effecting self-stabilization and limitation of reactor power

- inert, phase-stable gaseous coolant (helium) ruling out total loss of coolant.

In the following the inherent safety characteristics are discussed in detail.

HTR 500 Safety Systems

These safety characteristics are now explained on the example of the HTR 500.
Fig. 1 shows a cross section of the prestressed concrete reactor vessel. You can see the core with the graphite reflector, the steam generator with circulator and in addition an auxiliary heat exchanger for decay heat removal.

In the following only the safety systems are discussed in detail.

Shutdown System

The HTR 500 is equipped with two redundant shutdown systems consisting of the reflector rods and the incore rods.

The 48 reflector rods constitute a safety system used exclusively for reactor scram. When their effect is needed, the reflector rods drop into boreholes in the side reflector blocks under the force of gravity.

The 72 incore rods are used for control and long-term shutdown. They are maneuvred by a pneumatic piston system. Longterm shutdown by the incore rods is effected exclusively by manual release and does not have to be initiated earlier than 10 hours after shutdown of the plant by the reflector rods.

Decay Heat Removal System

The decay heat removal concept is characterized by the following features (cf. Fig. 2):

- use of the main heat removal system (main heat sink)

- separate and redundant decay heat removal system with separate circulators and heat exchangers integrated in the primary system,

- utilization of natural convection should the circulators fail

- restart of the decay heat removal system by manual measures, since prolonged failure of decay heat removal (10 h) is tolerable

- integration of the very simple liner cooling system of the prestressed concrete reactor vessel into the decay heat removal concept in the event of total failure of the decay heat removal systems listed above.

The redundant decay heat removal heat exchangers are arranged separately so as to ensure sufficient natural convection in the primary circuit, should the respective circulators fail.

The two redundant decay heat removal loops are sufficient to control an accident, because their availability is increased by making use of natural convection and manual measures.

In the hypothetical event of failure of both decay heat removal loops and the main heat removal system, sufficient heat can be removed via the liner cooling system, normaly used for cooling the prestressed concrete and its liner during operation.

Activity Containment

The concept of activity containment is based on a multi-barrier principle (Fig. 3).

The fission products are retained by the following barriers:

- the coated particle having a diameter of about 0.5 mm
- the graphite matrix of the fuel element of 6 cm diameter
- the prestressed concrete reactor vessel
- the reactor containment building

The pyrocarbon and silicon carbide coatings on the fuel particles form a highly effective pressure and gas-tight containment of the fuel and the fission products up to high temperatures which safely retains the radioactivity at the place of generation.

Therefore the primary coolant has only a very low activity concentration during normal operation and under accident conditions so that the subsequent barriers are much less important than in other reactor types.

The gas-tight fail-safe prestressed concrete reactor vessel having a wall thickness of 5 m and multiple redundant prestressing cables represents another barrier. In the event of hypothetical depressurization accidents the maximum possible leakage cross section at the metal penetrations and connection lines is limited to 33 cm^2 by structural devices. If rupture occurs in these components, the coolant therefore escapes very slowly. It takes about 1.5 h until pressure equilization is established. During this period the coolant gas is passed directly into the stack through pressure relief valves. When pressure equilization between the reactor containment building and the atmosphere has been established, the helium is discharged through the ventilation air filter system.

The HTR 500 is equipped with a special filter which under accident conditions is capable of retaining the metal fission products effectively.

HTR Accident Behaviour

Practical experience gained from the licensing procedure and the operation of the AVR and the THTR 300 as well as risk analyses performed for the HTR plants have confirmed that the design of the safety system is determined by the following accident categories:

- failure of individual decay heat removal systems or loops resulting in a reduction of the decay heat removal capacity of these systems

- unintentional power excursion and, as a result, temperature increase in the reactor core

- depressurization accidents resulting in a reduced cooling capacity of the primary circuit

- tube rupture in the steam generator, i.e. ingress of water into the primary system.

The analyses performed for the HTR 500, are summarized in Fig. 4. The time-dependent curves of the maximum fuel element temperatures for representative accidents are shown. The load and failure limits of the fuel elements are given for comparison. The various temperature curves show the dependence on the additional failures assumed in decay heat removal than Fig. 4 shows the following accident sequences: rapid cooldown by the main heat removal system (MLC), decay heat removal using two (CACS (2)) or only one decay heat removal loop (CACS) (1)), helium circulator failure and decay heat removal via the decay heat removal heat exchangers by natural convection (LOC), and the depressurization accident with decay heat removal via one decay heat removal loop (CACS (1) (DEPRESS)).

In the event of design basis accidents forced cooling of the reactor core remains intact. Design basis accidents are accidents whose control within the permitted limiting dose values. The fuel element temperatures are reduced below 500 °C within a few hours, so that even most improbable accident-failure combinations including water or air ingress can be controlled without any problems. Below about 500 °C the reaction rates of steam or oxygen with the graphite of the fuel elements are negligibly low.

In addition Fig. 4 shows that even in the event of improbable accident sequences such as total failure of the decay heat removal system and heat removal exclusively via the liner cooling system (LCS), or failure of the scram system (ATWS), the fuel element temperatures remain clearly below the design temperature permitted for continuous operation. Thus it is ensured that there will be no release of activity exceeding that during normal operation.

HTR Accident Sequences

Accident sequences having a very low probability of occurrance (hypothetical events) are not included in the licensing procedure. They are, however, the subject of risk analyses. Comprehensive risk analyses have been performed for HTR plants, permitting an evaluation of the risk incurred by an accident.

Based on the American AIPA-study, a detailed safety analysis was performed for the HTR by the nuclear research center Juelich and the Gesellschaft für Reaktorsicherheit (GRS) on behalf of the Federal Ministry of the Interior. Numerous hypothetical accidents were analyzed for the THTR 300 in addition to the accident analyses performed within the licensing procedure. Detailed data on accident sequences in the THTR 300, which are relevant to the plant risk, were determined as a basis for emergency protection planning by a team at the Juelich Nuclear Research Center. In addition, a risk evaluation was conducted for the HTR 500. It is the consistent and common result of all these analyses that the risk of an HTR is very low. It is of decisive importance that for the HTR not only the product of damage and frequency but also the damage itself is very small.

It has been established in the THTR licensing procedure and by numerous accident and risk analyses that a core heat-up combined with depressurization would result in an accident having the maximum effect.

Core Heat-up with Simultaneous Depressurization

In case of reactor scram the decay heat is primarily removed through the steam generator and the main steam feedwater circuit (Fig. 5). If this system fails, the separate redundant decay heat removal system comes into action (Fig. 6). If this system fails also, the time of decay heat removal interruption will be used to restore decay heat removal by simple manual measures provided in advance. This procedure meets all the requirements of the current regulations and has been confirmed by the German Ministry in charge. The measures described above have been practically tested earlier in the THTR 300 so that decay heat removal is ensured even in extremely rare events.

Independently of these facts, there is, in addition, the liner cooling system which is always operating and capable of ensuring reactor cooling on its own (Fig. 7). Under such conditions the maximum fuel element temperatures will rise to about 1200 °C i.e. absolutely no danger. This redundant liner cooling system operates at a water temperature of about 70 °C. It is of very simple design and, hence, of high availability. Additional redundant possibilities of manual feed are available, which can also be implemented because failure of the liner cooling system is permitted for a period as long as one day. For a further extension of the safety analysis of the HTR system, a simultaneous depressurization of the prestressed concrete reactor vessel was assumed (Fig. 8). Under such conditions the primary gas released into the reactor containment building, is passed through passive-filters and discharged to the to environment. Under such accident conditions only a few percent of the fuel elements will reach temperatures up to 2500 °C, whereas core meltdown is ruled out. Even if the liner cooling system should totally fail, the integrity of the prestressed concrete reactor vessel is maintained. Assuming that any type of cooling in the overall system is interrupted, the temperatures at the inner concrete surface would rise to 1100 °C (Fig. 9). Hereby about 10 % of the wall thickness would be impaired on the inner vessel surface. Nevertheless, integrity of the structure, i.e.

safe containment, is ensured. This statement is based on experiments performed in the Nuclear Research Center Juelich, where parts of the prestressed concrete reactor vessel equipped with a liner on the inner surface were heated to 1200 °C. The core thus remains contained in a fail-safe structure formed by the massive prestressed concrete reactor vessel with 5 m wall thickness (Fig. 10).

The longer-term release of metal fission products from the fuel elements is much retarded and considerably reduced as a result of their deposition on colder surfaces within the primary system and the reactor containment building. A passive metal filter installed at the ventilation stack inlet acts as a further barrier for fission product retention under accident conditions. In total, the radiation exposure of the environment in the event of this hypothetical accident is low enough so that, according to the "general recommendations for emergency protection in the environment of nuclear plants", immediate measures for the population and the environment are not required.

The emergency protection planning for the THTR 300 was based on an analogous event. The competent authorities confirmed that evacuation of the population would not be necessary.

Summary

The HTR is a reactor having a passive safety.

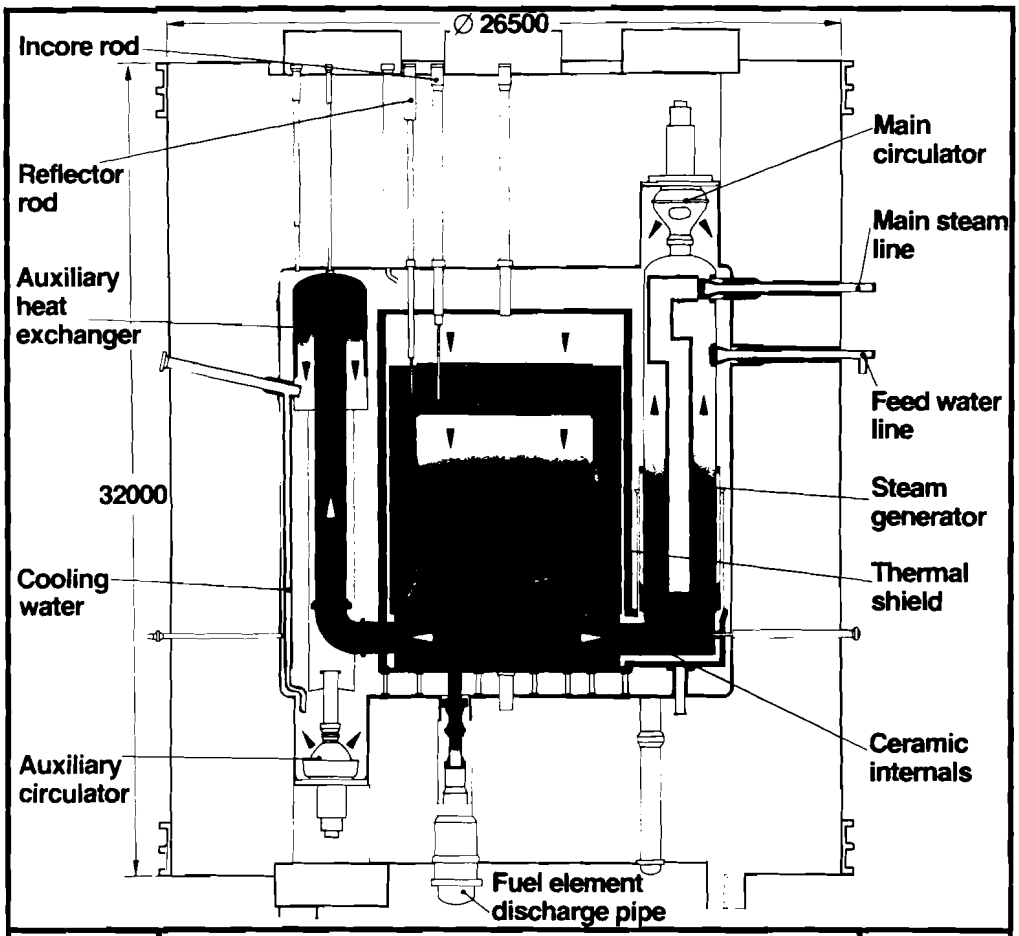
It is equipped with the usual active engineered safety systems in a simplified form.

Due to its inherent safety characteristics and the burst-safe prestressed concrete reactor vessel activity containment is ensured even without the effect of active safety systems.

Even in the event of extremely hypothetical accidents the effect on the environment is low enough so that evacuation or relocaction

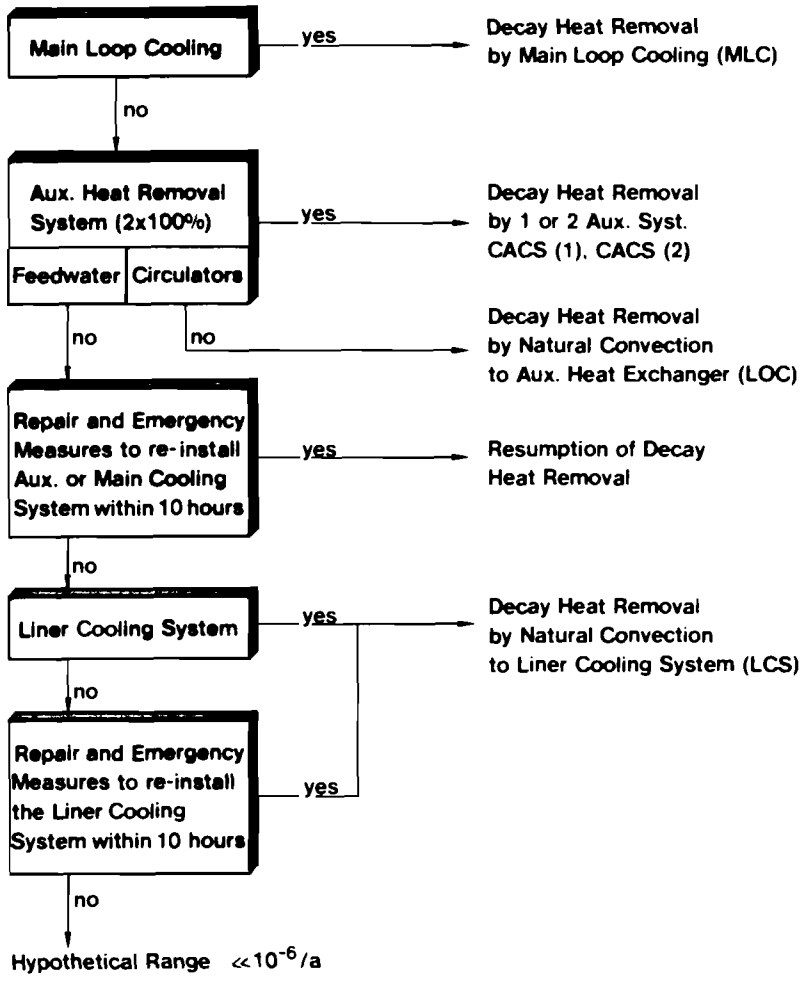
of the population is not required. Therefore large-scale damage of agricultural land and industrially used areas is safely ruled out.

Thus the site selection for this type of reactor is not restricted, i.e. an HTR can be constructed near industrial and urban centers.



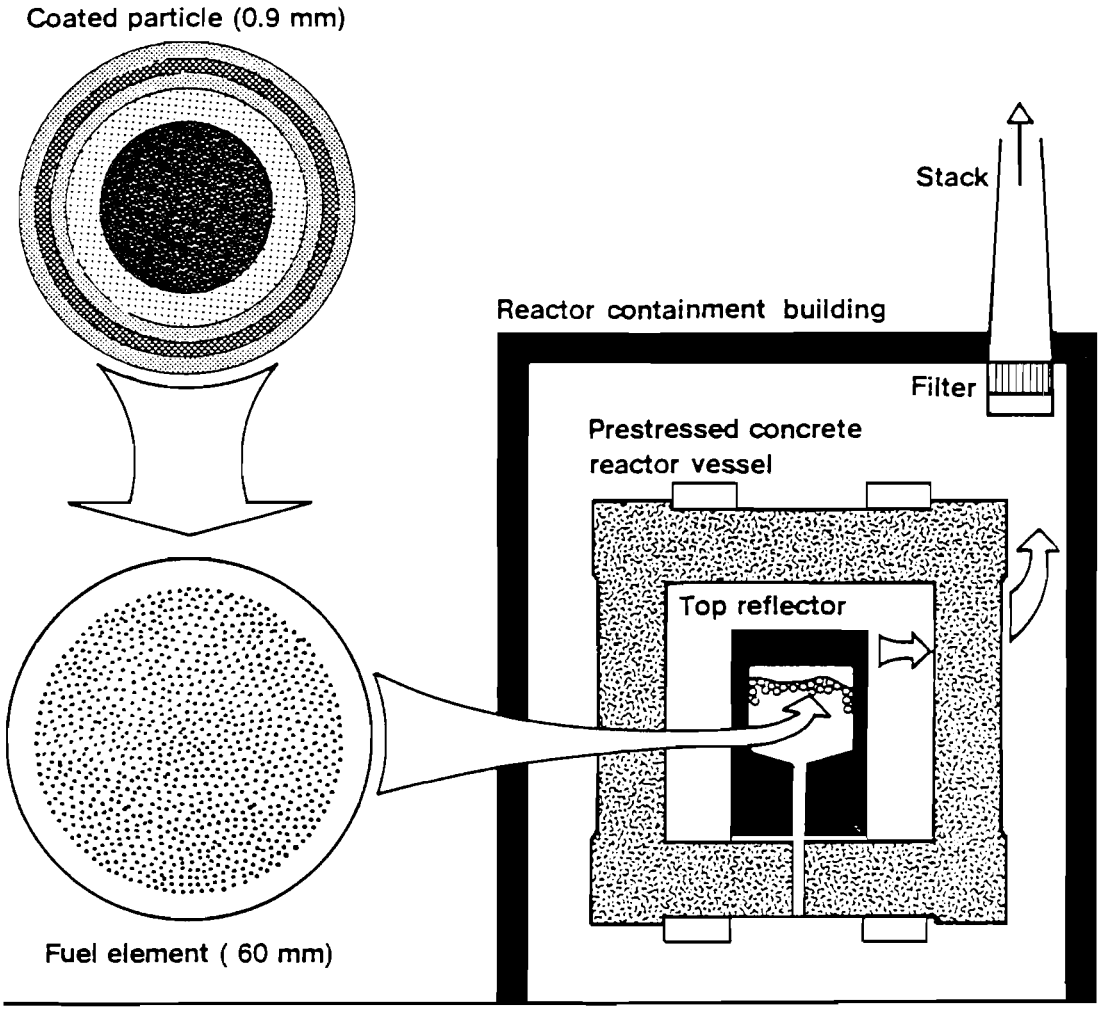
Reactor Pressure Vessel with Internals

Fig. 1



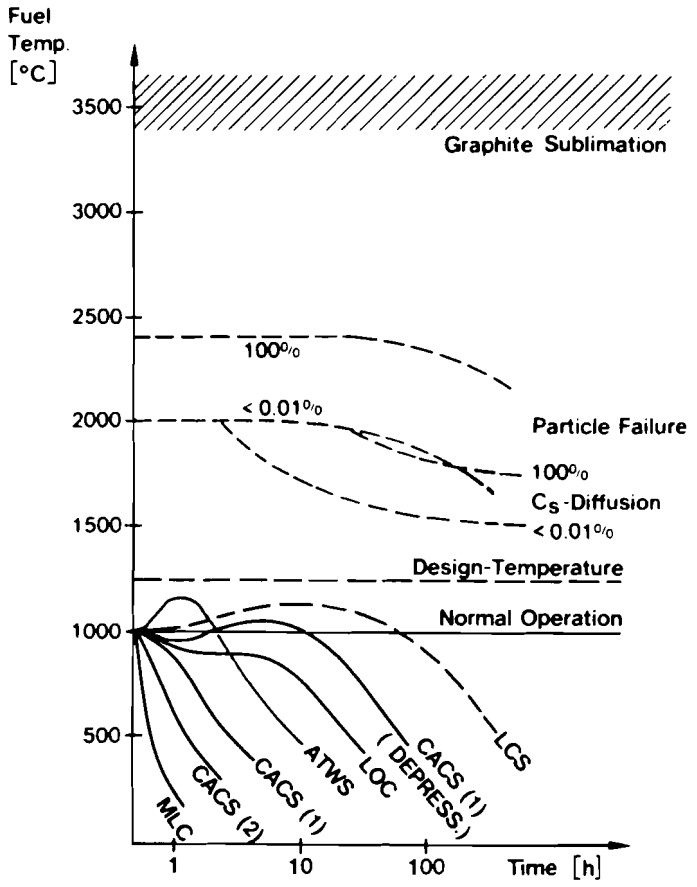
Multiple Measures for Accident Control

Fig. 2



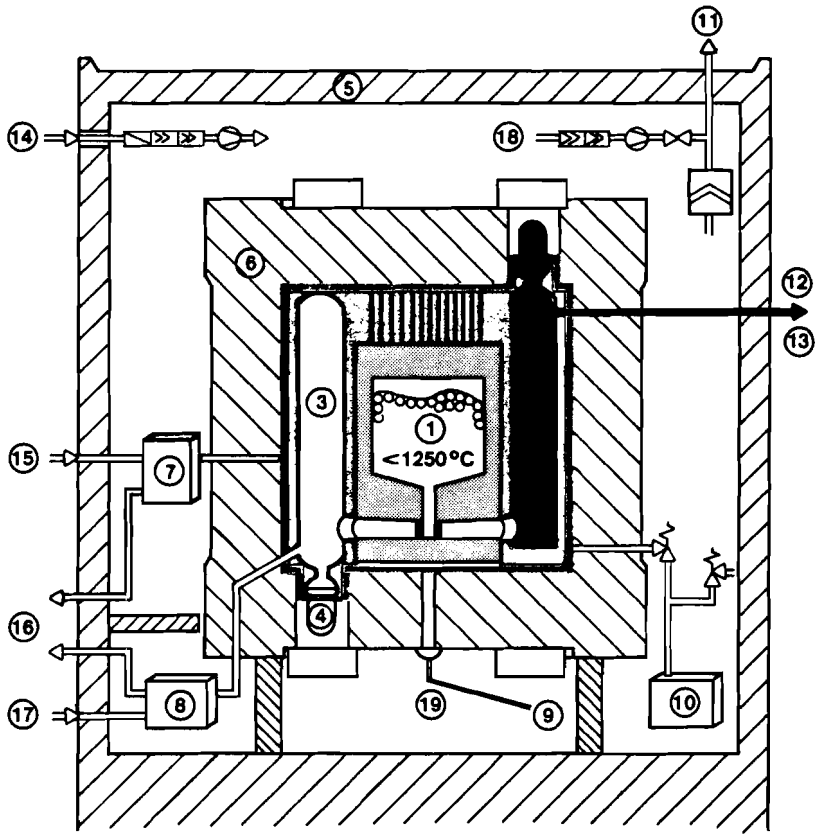
Multiple Barriers for
Fission Product Retension

Fig. 3



High Temperature Resistance of the Fuel Elements

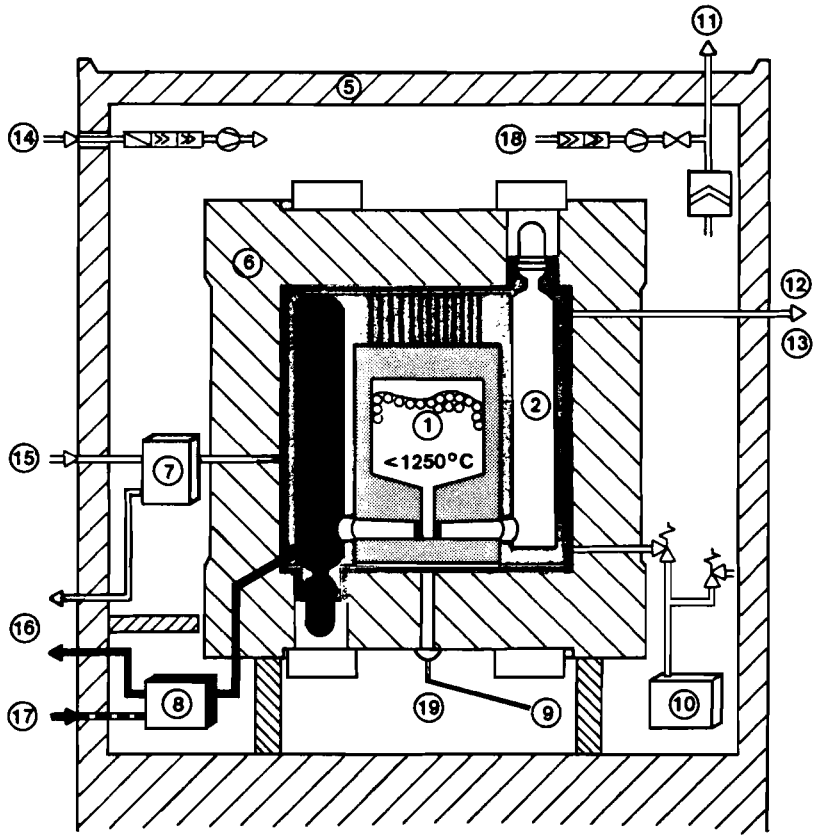
Fig. 4



1 Core
2 Steam generator
3 Heat exchanger
4 Circulator
5 Reactor containment building
6 Prestressed concrete reactor vessel
7 Liner cooling system
8 Decay heat removal
9 Fuel circulating system
10 Helium purification system
11 Stack
12 Steam/feedwater circuit
13 Main heat sink
14 Supply air
15 External make-up
16 Closed-circuit cooling
17 Manual measures
18 Waste air
19 Nominal dia 65

Decay Heat Removal with Main Cooling System

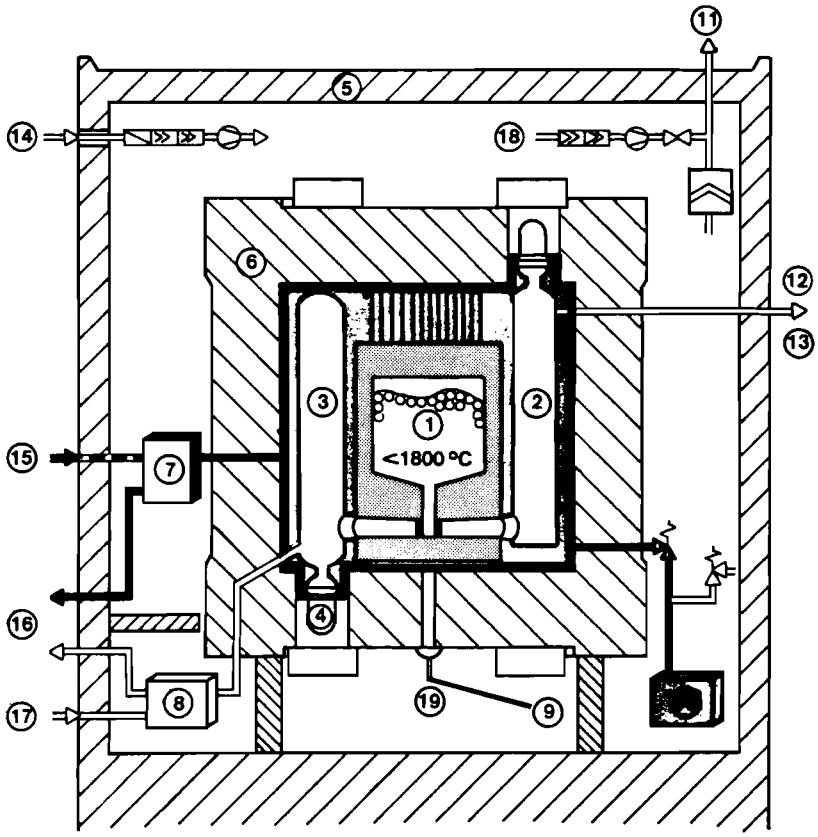
Fig. 5



1 Core
2 Steam generator
3 Heat exchanger
4 Circulator
5 Reactor containment building
6 Prestressed concrete reactor vessel
7 Liner cooling system
8 Decay heat removal
9 Fuel circulating system
10 Helium purification system
11 Stack
12 Steam/feedwater circuit
13 Main heat sink
14 Supply air
15 External make-up
16 Closed-circuit cooling
17 Manual measures
18 Waste air
19 Nominal dia 65

Decay Heat Removal with Decay Heat Removal System

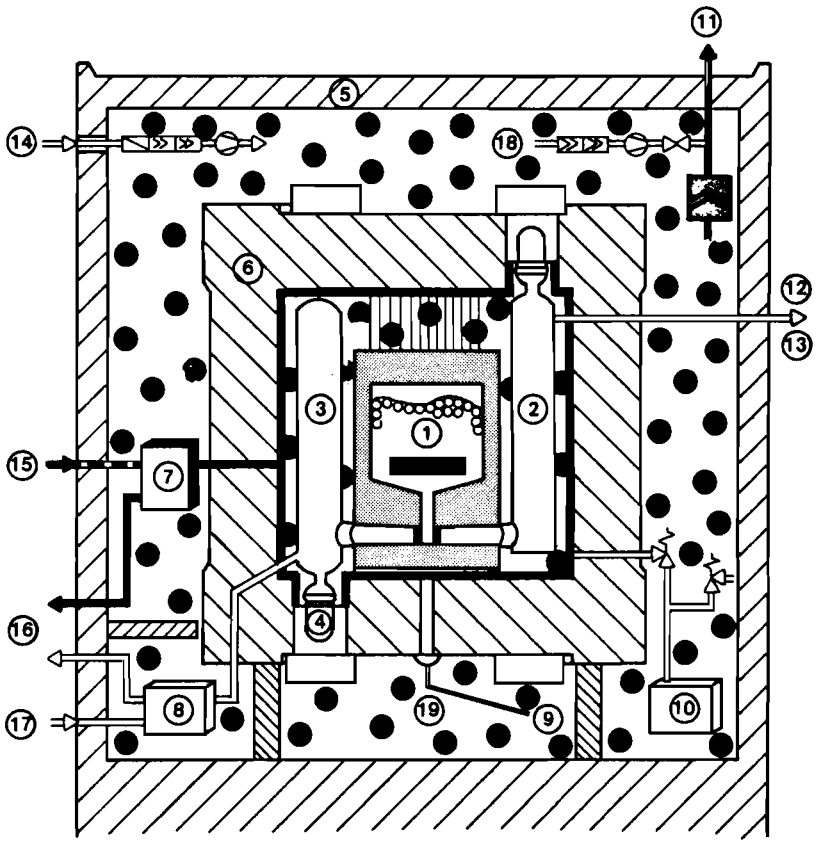
Fig. 6



1 Core
2 Steam generator
3 Heat exchanger
4 Circulator
5 Reactor containment building
6 Prestressed concrete reactor vessel
7 Liner cooling system
8 Decay heat removal
9 Fuel circulating system
10 Helium purification system
11 Stack
12 Steam/feedwater circuit
13 Main heat sink
14 Supply air
15 External make-up
16 Closed-circuit cooling
17 Manual measures
18 Waste air
19 Nominal dia 65

Decay Heat Removal with Liner Cooling System

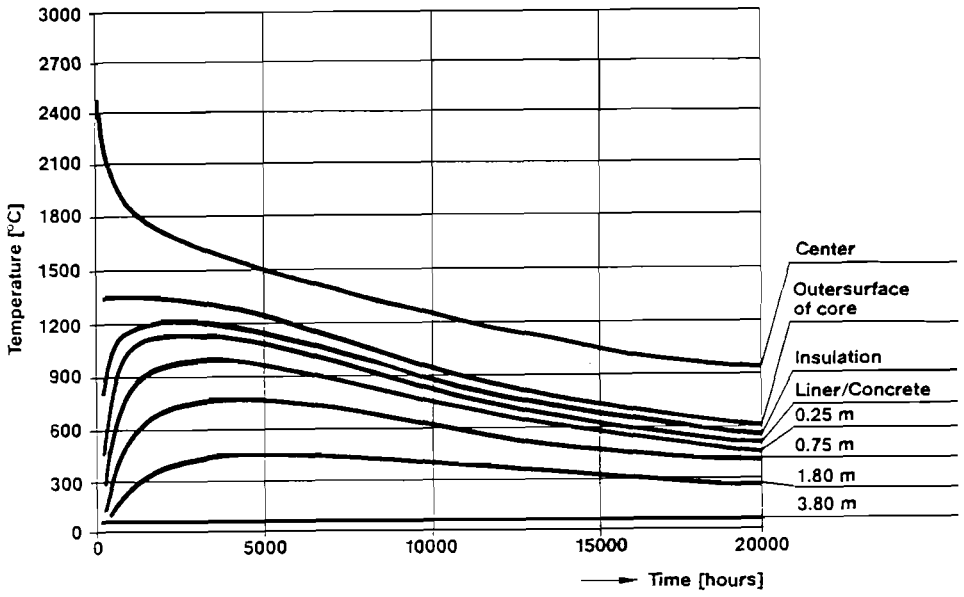
Fig. 7



1 Core
2 Steam generator
3 Heat exchanger
4 Circulator
5 Reactor containment building
6 Prestressed concrete reactor vessel
7 Liner cooling system
8 Decay heat removal
9 Fuel circulating system
10 Helium purification system
11 Stack
12 Steam/feedwater circuit
13 Main heat sink
14 Supply air
15 External make-up
16 Closed-circuit cooling
17 Manual measures
18 Waste air
19 Nominal dia 65

Decay Heat Removal with Liner Cooling System (Drepressurization)

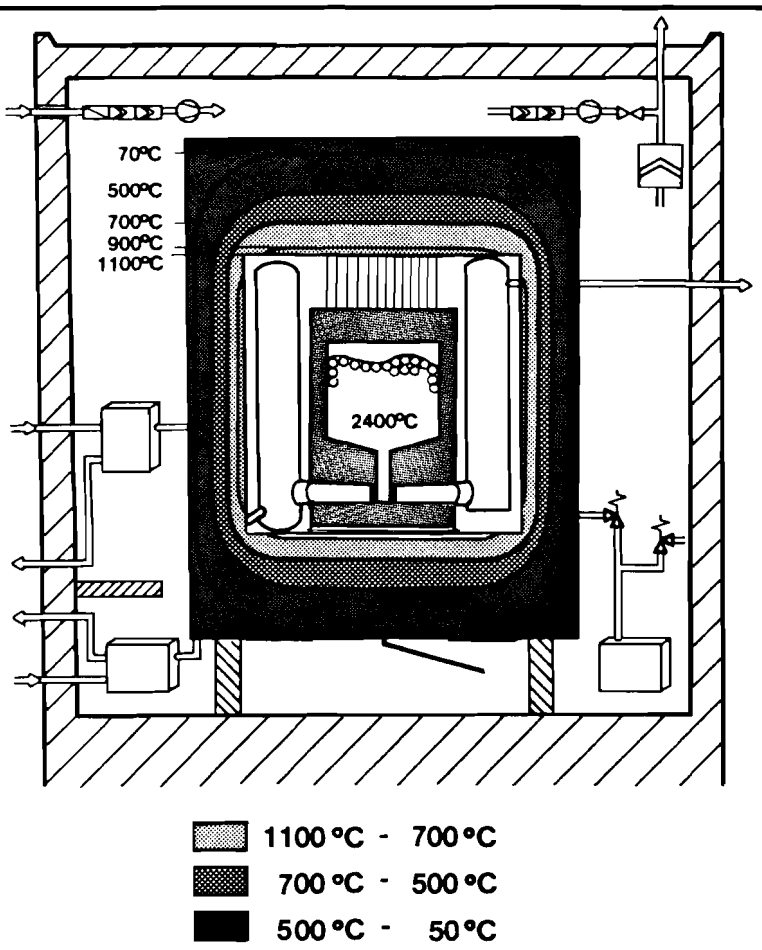
Fig. 8



ref.: KFA, Jülich

Temperatures of
Reactor Regions Versus Time for Loss of Core and Liner Cooling

Fig. 9



Depressurization and Total Loss of Active Cooling Temperatures of PCRV

Fig. 10

4.4. A DYNAMICAL BASIS FOR INHERENTLY SAFER CHEMICAL AND NUCLEAR REACTORS

A. A. Harms
McMaster University, Hamilton, Canada

Abstract

A reaction-kinetics description suggestive of a characterization of safer chemical and nuclear reactors is formulated and examined. At issue is the choice of reactants, the imposition of kinetic conditions which affect reaction channels, and the existence of an intrinsic reaction dynamic which is self-limiting and hence power excursion bounded. Risks associated with the dispersal of hazardous substances due to reaction-driven containment failure may thereby be abated.

Introduction

Our interest here is in the inherent safety of technological devices generically known as reactors. These devices are characterized by reaction domains which sustain matter and energy transformations based on nuclear, atomic, ionic or molecular processes. The process industry, energy industry, transportation industry, and many others are heavily dominated by such devices. As suggested in Fig. 1, these matter-energy transformation devices constitute an essential link between natural resources and human services.

Safety considerations enter because the reactions often yield hazardous substances as reaction products (e.g., poisons, contaminants, radioisotopes, . . .) and because reaction excursion can lead to an excessively rapid accumulation of energy, thereby inducing high temperature and high pressure conditions. Rupture of the con-

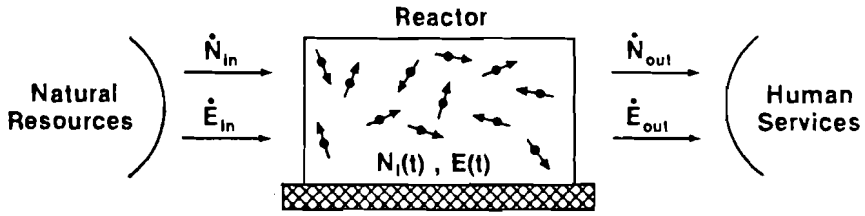


Fig. 1 Generic depiction of a single-stage isolated reactor. An inflow of matter and energy from some primary natural resource occurs, reactions which transform matter and energy under imposed kinetic and density conditions are sustained, and an outflow of transformed matter and energy in support of human services results; this latter outflow may also include polluting and contaminating effects. In practice, numerous reactors may be linked by matter-energy flows forming a complex network and further also include storage components.

tainment structure may result in the dispersement of the hazardous substances.

Conventional approaches to reactor safety have generally focussed upon issues such as

1. licensing/regulatory provisions,
2. operator/equipment reliability,
3. reactor sizing and area distribution, and
4. accident containment and suppression.

These safety considerations[1] generally imply the acceptance of the fundamental physical features of the process in the device and have their origin in the implicit premise of some technological realizability and economic cost/benefit analysis.

As another approach to technological process systems safety, we consider here the underlying reaction process dynamic in the reactor for which we seek to identify

those matter-energy transformations which possess certain safety features as an intrinsic phenomena of the underlying process. We identify the safety features of interest to be the following:

1. the minimization of hazardous substance accumulation and
2. the existence of self-limiting reactions which impose acceptable power-excursion bounds.

Within this context then, we first introduce a generic description of reaction phenomena and their characterization and then examine some underlying reaction-dynamic properties which impose self-limiting processes directly related to energy-driven excursion.

Reaction Process Characterization

The fundamental analysis of all reactors begins at the level of relevant matter-energy transformation processes. Regardless of whether these are nuclear, ionic, atomic, or molecular, there exist but only two broad classifications of reactions: those involving collisional-contact two-body interactions and those involving decay or decomposition of isolated single-body events.

In sufficient generality and including both matter and energy in two-body reactions, we may write

$$Q_1 + a + b \rightarrow c + d + \ldots + Q_2 \,. \tag{1}$$

Here, a, b, c, d, . . . are material species, Q_1 is the average energy supplied to the motion of reactants a and b, and Q_2 is the kinetic energy of the reaction products together with possible electromagnetic energy associated with the process.

In view of the very large number of material species in various categories, Table I, the number of possible two body reactions is indeed very large. Two such examples are the fission process,

Table I

Estimated number of material species in selected categories. The uncertainty may vary from a factor of about 2 for the subnuclear category to perhaps 100 for the number of molecular species.

Category	Number
Photons (mass equivalent)	1
Subnuclear	~50
Elemental	~100
Isotopic	~2000
Ionic	~5000
Molecular	~10,000,000

$$Q_1 + {}^{235}U + n \rightarrow \nu n + P_1 + P_2 + Q_2 , \tag{2}$$

and hydrogen production involving lithium hydride,

$$Q_1 + LiH + H_2O \rightarrow H_2 + LiOH + Q_2 . \tag{3}$$

The rate at which such two-body reactions proceed is given by

$$R_{ab} = \kappa_{ab} N_a N_b , \tag{4}$$

where N_a and N_b are the densities of species and a and b and κ_{ab} is a reaction rate parameter dependent upon the relative kinetic state of the a and b species. The net energy return is $(Q_2 - Q_1)$ and can be positive or negative.

A single-body decay process is represented by

$$e \rightarrow f + ... + Q_2 , \tag{5}$$

and proceeds at the rate

$$R_e = \lambda_e N_e , \tag{6}$$

where λ_e is also a reaction rate parameter.

The decay of radioactive ^{137}Cs into a stable isotope

$$^{137}Cs \rightarrow {}^{137}Ba + \beta^- + Q_2, \tag{7}$$

and the decomposition of dimethyl ether

$$(CH_3)_2O \rightarrow CH_4 + CO + H_2 + Q_2, \tag{8}$$

are examples of single-body reactions.

The evolution with time of matter associated with various types of reactions together with the evolution of energy in the reaction chamber is described by a set of reaction rate equations. For a typical i-type reaction species and net energy release in the reaction chamber, we write

$$\frac{dN_i}{dt} = \sum_i R_{+i} - \sum_i R_{-i}, \tag{9a}$$

and

$$\frac{dE}{dt} = \sum_i R_{\pm i} (Q_2 - Q_1)_i, \tag{9b}$$

where R_{+i} and R_{-i} are the reaction rates which add to or subtract from the population of i-type species in the reaction chamber.

In general the existence of i-type particles is determined by the competition of various reaction channels involving not only i itself but also other progeny species. Thus, the i-type species may appear as a result of two-body reaction and, similarly, it may appear as a daughter product by the decay of its parent. Further, the i-species may be transformed in the reaction chamber by their own decay tendency or become absorbed by reacting with other species. These processes are suggested in Fig. 2 and may be used, together with the various forms of the two-body and one-body reaction rate expression, Eqs. (4) and (6), to write explicitly for Eqs. (9):

$$\frac{dN_i}{dt} = \sum_m \sum_n p_{mn \rightarrow i} \kappa_{imn} N_m(t) N_n(t) + \sum_\ell p_{\ell \rightarrow i} \lambda_\ell N_\ell(t) \tag{10a}$$

$$- \lambda_i N_i(t) - N_i(t) \sum_p \kappa_{ip} N_i(\lambda),$$

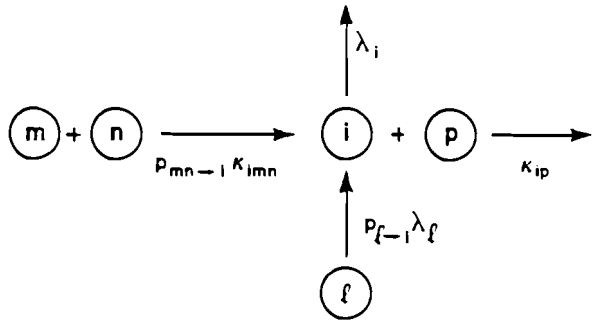


Fig. 2 Graphical representation of two collisional and two decay processes which may affect the existence of a general i-type species. Here $\kappa_{(\,)}$ and $\lambda_{(\,)}$ are reaction rate parameters and $p_{(\,)}$ represents the probability of the i-species resulting from the suggested reaction.

and

$$\frac{dE}{dt} = \sum_{q} \sum_{r} \kappa_{qr} N_q(t) N_r(t) [Q_2 - Q_1]_{qr} + \sum_{s} \lambda_s N_s(t) Q_{2,s} \,. \tag{10b}$$

If there exist I material species, then this system represents I+1 first order, nonlinear, coupled differential equations; the nonlinearity may be further increased if some of the reaction rate parameters, $\kappa_{(\,)}$ and $\lambda_{(\,)}$, possess a specific density dependence.

Hazardous Species Accounting

For reasons of expository clarity and algebraic convenience, we suppose that the number of relevant species in an operating reactor, may – on the basis of some numerical toxicity assignment – be classified as either benign (i.e. non- hazardous) or hazardous. Hence, we consider a set of species represented by $b_1, b_2, b_3, \ldots$ as benign and the remaining species $h_1, h_2, h_3, \ldots$ as hazardous.[2]

The dominant source of hazardous species are reactions yielding an increasing accumulation of these species, e.g.

$$b_1 + b_2 \rightarrow h_1 + \ldots , \tag{11a}$$

$$b_3 + h_2 \rightarrow h_3 + h_4 + \ldots . \tag{11b}$$

While hazardous species may appear as a result of two-body reaction, they may similarly be so destroyed, e.g.

$$b_4 + h_1 \rightarrow b_5 + \ldots , \tag{12}$$

$$h_1 + h_2 \rightarrow b_6 + \ldots .$$

Additionally, they may transform into benign species by decay according to

$$h_1 \rightarrow b_2 + \ldots . \tag{13}$$

The frequency with which all of the above processes occur depends upon the magnitude of the reaction rate parameters and these in turn may depend upon the kinetic conditions of the interacting particles. Thus, the choice of primary reactants and the kinetic state determines the extent of hazardous species accumulation. A reactor design and operational goal to be sought is, therefore,

(1) a minimization of hazardous species accumulation and

(2) an internal recirculation/destruction of hazardous species.

This is suggested by the following example of a reaction network desirable for reason of inherent minimization of hazardous substances:

$$\begin{aligned} b_1 + b_2 &\rightarrow h_1 + \ldots \\ b_3 + h_1 &\rightarrow h_2 + b_4 + \ldots \\ h_2 &\rightarrow b_3 + \ldots . \end{aligned} \tag{14}$$

The net effect is $b_{(\,)} \rightarrow b_{(\,)}' + O(h)$ in which O(h) represents an acceptably small hazardous specie accumulation.

Power Excursion Bounds

The issue of hazardous species accounting involves principally reaction processes upon which the species dynamic Eq. (10a) is based. Then, while the power excursion-bound is governed by the companion energy rate equation, Eq. (10b), it is nevertheless dependent upon the matter rate equation, Eq. (10a).

Equations (10) describe, in general, a very large set of materials species $N_i(t)$. It may frequently be possible to identify a very small number of species as the dominant contributions to energy production. For present purposes and without restricting the notions resulting therefrom, we take the dominant species to be represented by $N_x(t)$. Hence,

$$\frac{dE}{dt} \sim \kappa_{jx} N_j(t) N_x(t) (Q_x - Q_j) \qquad (15)$$

$$= \kappa' N_x(t),$$

with the $\kappa'(t)$ time variations to be much less in comparison with $N_x(t)$.

Evidently, dE/dt will be bounded if $N_x(t)$ is bounded. The question now is the following: "What imposition on $N_x(t)$ and relevant reaction rate parameter will yield a bounded $N_x(t)$?"

Consider rewriting Eq. (10a) for i = x with the probabilities folded into the rate parameters:

$$\frac{dN_x}{dt} = \sum_m \sum_n \kappa_{imn} N_m(t) N_n(t) + \sum_\ell \lambda_{i\ell} N_\ell(t) \qquad (16)$$

$$- \lambda_x N_x(t) - N_x(t) \sum_p \kappa_{xp} N_p(t) .$$

The complexity of reactions involving the numerous $N_m(t)$, $N_n(t)$ and $N_\ell(t)$ may be such as to possess a coupled time variation component -- relative to $N_x(t)$ -- so that we may well approximate

$$\sum_m \sum_n \kappa_{imn} N_m(t) N_n(t) + \sum_\ell \lambda_{i\ell} N_\ell(t) = a + b N_x(t) . \qquad (17)$$

because the summations do include x. Further, we suppose that $N_x(t)$ possesses a significant self-destruction process[3] so that for the last term of Eqs. (10a) and (16) we may write

$$N_x(t) \sum_p \kappa_{xp} N_p(t) \simeq \kappa_{xx} N_x^2(t) \quad . \tag{18}$$

since p does include x.

Substitution of Eqs. (17) and (18) into Eq. (16) then gives a dynamic for the species of interest $N_x(t)$ as

$$\frac{dN_x}{dt} \simeq \theta_0 + \theta_1 N_x(t) + \theta_2 N_x^2(t) \quad . \tag{19}$$

As formulated, θ_2 is negative, θ_1 can be positive or negative, and θ_0 positive; however, if some constant leakage of $N_x(t)$ from the reaction domain is admitted, then θ_0 might also be negative.

An assessment of the time variation of $N_x(t)$ defined by Eq. (19), subject to the admissible range of the rate parameter coefficients $\{\theta_0,\theta_1,\theta_2\}$, may well be undertaken by drawing upon selected aspects of the geometrical theory of nonlinear dynamical equations[4]. The relevant conceptual-analytical points of interest are the following:

1) determination of equilibrium points N_x^* of Eq. (19) defined by

$$\theta_0 + \theta_1 N_x(t) + \theta_2 N_x^2(t) \Big|_{N_x(t)=N^*} = 0, \text{ (t arbitrary)} , \tag{20}$$

2) vector-flow properties of dN_x/dt for range of N(t) and t.

Further, of interest here are evidently only those particle densities $N_x(t)$ which are real and positive.

We have examined the entire range of conceivable dynamics resulting for this range of parameters and display the result in Figs. 3 and 4. Evidently, an asymptotically stable upper bound attract for the particle density – and hence for the power excursion – exist for a set of reaction parameter $\{\theta_0, \theta_1, \theta_2\}$.

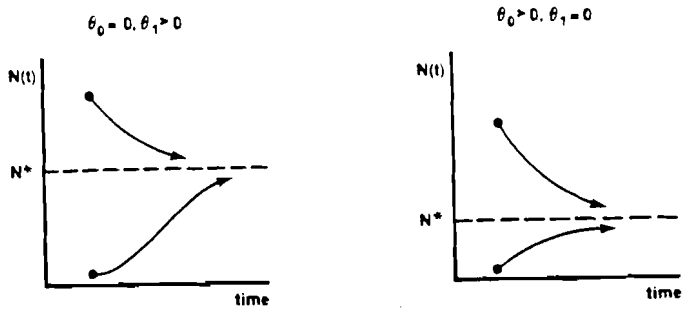


Fig. 3 Conceivable time variation of $N_x(t)$ for the two cases of $\{\theta_0 = 0, \theta_1 > 0, \theta_2 < 0\}$ and $\{\theta_0 > 0, \theta_1 = 0, \theta_2 < 0\}$. Regardless of the initial condition, the dynamic which governs $N_x(t)$ causes it to approach a stable equilibrium attractor N^*. An unbounded excursion is thus not possible.

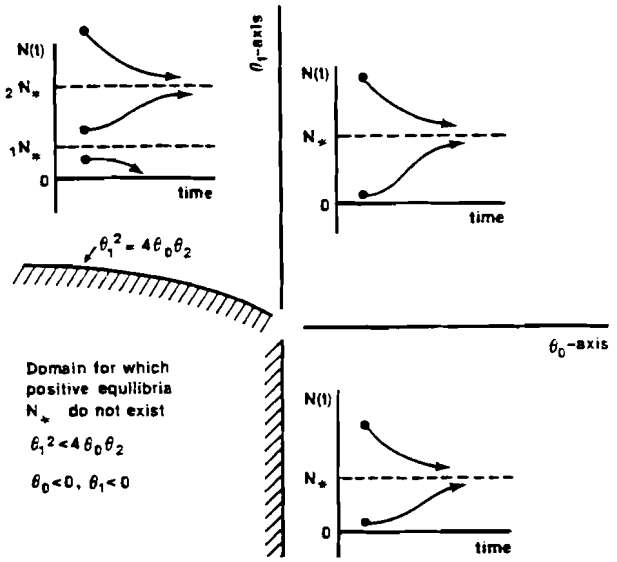


Fig. 4: Conceivable time variations of $N_x(t)$ in the phase-plane $\theta_0 - \theta_1$. All dyanamics subject to $\theta_0 \neq 0$, $\theta_1 \neq 0$, $\theta_2 < 0$ and for all initial conditions, lead to a stable attractor N^*; no unbounded excursion is possible. (The domain on the $\theta_0 - \theta_1$ plane bounded by $\theta_1^2 \leq 4\theta_0\theta_2$ and $\theta_1 \leq 0$ does not admit steady-state reaction operation.)

Concluding Comment

The analysis undertaken here suggests a basic matter-energy transformation characterization for reactors which provides an "intrinsic" measure of safety against hazardous substance accumulation and an "inherent" protection against unbounded power excursions. The practical realizability of such systems depends upon the choice of interacting species and the provision of kinetic conditions both of which need to be specified for selective "internal-recycling", Eq. (14), and for the specification of a dominant "negative-squared" term in the reactive dynamic. It is evident that an extensive combinatorics examination of the available species, Table I, needs to be undertaken as well as an expanded perspective on the range of particle kinetic phenomena.

Acknowledgement

The research reported upon here has been supported by the Natural Sciences and Research Council of Canada.

References

1. The literature on industrial and product safety is very extensive with the following a representative sampling:

1.1) W.W. Lawrence, Of Acceptable Risk, W. Kaufmann, Inc., Los Altos, CA, USA (1976); 1.2) E.W. Lawless, Technology and Social Shock, Rutgers University Press, New Brunswick, N.J. U.S.A. (1977); 1.3) B. Persson, Ed., Surviving Failures, Aliquist and Wiksell, Stockholm, Sweden (1979); 1.4) S.C. Flormnan, Blaming Technology, St. Martin's Press, New York, NY, USA (1981); 1.5) T.A. Kletz, What Went Wrong?, Gulf Publ. Co., Houston, TX, USA (1985).

2. There exists an ambiguity here in the sense that the purpose of a reactor may very well be the production of hazardous substances, e.g. fungicides for agriculture, radioactive cobalt-60 for medicine, etc. Hence, we need to take this assumption in the context of the production of those needless hazardous substances discharged into the environment.

3. We add that there exist numerous material species which will interact with species of their own type to form new species particularly so if their relative speeds or temperatures are sufficiently high. Further, special purpose devices may need to be introduced designed specifically for purposes such as the transmutation or total disassembly of hazardous substances into their elemented form; concepts such as the fusion torch and devices such as spallation accelerators may need to be incorporated into an integrative systems concept.

4. The following two references seem to span the mathematical range of the subject:

4.1 M. Braun, Differential Equations and Their Application, Springer-Verlag, New York, NY, USA (1981).

4.2 J. Guckenheimer and P. Holmes, Nonlinear Oscillations, Dynamical Systems, and Bifurcation of Vector Fields, Springer-Verlag, New York, NY, USA (1983).

4.5. SAFETY PRINCIPLES FOR ADVANCED PLANT

M. R. Hayns and D. W. Phillips
UKAEA, Safety and Reliability Directorate
Culcheth, Cheshire, United Kingdom

Abstract

One of the criticisms of the nuclear industry is that existing designs of reactors have evolved from systems designed originally for other, usually military, applications. The logic of this line of thinking then continues - if designers had stopped to consider the need of large scale electricity generating plant specifically, then other design solutions may have been preferred. We do not subscribe to this argument as a reason for abandoning existing plant, but it is useful to consider the essential safety principles which should be applied when considering new designs or developments of existing designs for the 'advanced plant' which ought to be considered for the next generation. These safety principles are discussed under the following generic headings:

1. Reactivity control

2. Heat removal from the core
   a. At power
   b. Decay heat removal

3. Containment

4. Materials properties

How these principles apply in practice is considered by reference to both revolutionary and evolutionary advanced designs. Revolutionary designs claim that they utilize 'inherent' or 'passive' safety features which make them benign and incapable of causing harm to people. Evolutionary designs follow a route of improvements from existing, well developed designs which incorporate many elements of 'inherent' or passive safety but rely upon the basis of experience gathered in operating existing designs over several decades. We argue that no reactor design to date is truly inherently safe and that all must rely to a greater or lesser extent on engineered features. Application of the safety principles provides criteria against which to judge such designs. This leads to the conclusion that our current best judgement is that the evolutionary route provides the best way forward on both safety and economic grounds.

1. INTRODUCTION

In releasing the energy of nuclear fission a reactor must be provided with a means of controlling the nuclear chain reaction, removing the heat generated and ensuring that potentially harmful radionuclides are kept safely within the fuel. Current trends have led to large reactors, with relatively high power densities whose safe operation is ensured by means of a range of 'engineered safety features' which act to control the system. These ESFs have to be very reliable; the basic hazard posed by such plant is the combination of a great deal of energy and a large amount of hazardous material in the same location. In addition to ESFs all large nuclear plant, in common with other industrial plant, relies to a greater or lesser extent on the correct operation of the plant by human beings. Last year has seen the catastrophic effects of a combination of poor design, inadequate ESFs and operator error and mal-practice in the accident at Chernobyl. One of the many consequences of this event has been to refocus attention on a range of alternative nuclear reactor designs which are claimed by their protagonists to exhibit "inherent safety features". These are important issues. The public will require reassurance that reactors currently being operated are adequately safe. Pressure to change course and adopt alternative, perhaps radical designs, has already been seen in various media articles and a strong justification as to why we are not planning to adopt them is needed. Below, some of the features of nuclear reactors central to both safety and operability are explored in order to examine the possibility for increasing safety levels in advanced plant.

2. REACTIVITY CONTROL

Power reactors operate with an excess of reactivity to provide margins which allow a degree of load-following and to extend the core lifetime when refuelling is off-load. The reactivity excess is balanced by neutron absorbers which control the reactivity level and hence the power production.

Control is made possible by the small contribution (typically < 0.6%) made to overall reactivity by delayed neutrons. The majority of the reactivity thus comes from prompt neutrons whose lifetimes are the order of 1 ms or less and this makes their control through the use of absorber movement difficult to engineer. It is important, therefore, to ensure that the available reactivity margins are sufficient to ensure that the reactor does not become 'prompt critical' and hence uncontrollable by engineered systems. Inherent natural processes such as Doppler broadening can limit the fuel temperature rise resulting from a prompt criticality transient and hence reduce the potential for prompt criticality transients to degrade the core and inhibit core cooling. A further consideration for breeder reactors is that their cores are designed to be in a configuration which does not maximise reactivity

so that disruption of the core could increase reactivity.

These points are discussed further below but the need for an element of inherent control of reactivity in any reactor design is an important and generally an overriding consideration. A reactor requires reactivity control which ensures stability under normal operation to reduce thermal fatigue effects on structures and natural passive processes which lead to a safe and controlled shutdown in response to any disruptive transient. These two requirements can be in competition since stability in reactivity for small transients can slow the reactivity response in the case of large and rapid transients. Indeed, a very stable behaviour may not be compatible with ease of start-up or shut-down, or with "load-following".

The central feature of reactivity control by inherent means is that changes in core conditions produce differing effects on core components in terms of reactivity (and for thermal reactors, moderation). Such changes include temperature and pressure, core ageing and refuelling, and mechanical disruption of the core geometry. The diversity of possible effects means that reactivity control is most readily considered in terms of specific transients and this approach is taken here.

2.1 Local core changes

Accidents initiated locally within a core may not be terminated quickly because of an insensitivity of the global reactivity control to local reactivity transients. This insensitivity is less likely in small cores, but the individual discrete components in small cores may then have high reactivity worth. In this case single failure can affect global control. The implication is that small homogeneous cores may exhibit superior reactivity control characteristics for both "local" and global reactivity transients.

2.2 Temperature changes

The various core components have different reactivity significance and temperature coefficients and both these may change when the core is refuelled or as it proceeds to high burn-up. Similarly, the overall moderation characteristics depend upon the properties of the various core components. Safety and stability requirements for a safe reactor are that the reactivity should decrease in response to an increase in fuel temperature at both full power and in other states. Also, over-cooling of the core should not lead to reactivity rises which are not readily controllable and reactor start up and high burn-up power operation should be safe and readily controlled. These requirements have contradictory elements and almost certainly cannot be met by inherent features alone. Reactivity control over the full range of operational and fault conditions requires active engineered systems to compensate for, and where necessary to overcome, the

natural inherent features which change reactivity. In a safe reactor the natural inherent features should be used to mitigate the risk important effects of transients without worsening either the effects of other transients or the overall operability.

2.3 Core geometry changes

The core of a safe reactor should be in the most reactive configuration when in normal operation. This would ensure that any configuration change would decrease reactivity both locally and globally. Such changes include slow and predictable effects due to refuelling or mechanical distortions and rapid effects due to sudden structural failure. This goal is achievable in thermal fission reactors provided that the negative reactivity influence of absorber/moderator/structural components is not lost as a result of geometry change. In the LMFBR designs currently being developed this goal is in general not possible to achieve; additional considerations, such as the core structural design and appropriate consideration of possible core disruption events, must be brought into play.

3. HEAT REMOVAL FROM THE CORE

A reactor core remains safe and stable if it remains in thermal equilibrium. The control of the heat removal rate is straightforward provided that the rate is relatively stable. For example, full load power production may typically be one thousand times greater than the long term decay heat power production but the change from one state to the other may be accomplished under controlled conditions which make feasible the use of diverse heat removal systems matched to the two states.

Control may be less straightforward under certain operational and transient full power conditions and a range of feedback mechanisms influencing the core power exist. Negative feedback is provided by the Doppler temperature coefficient which decreases the neutron flux available for fission with increasing temperature, and thermal expansion which operates similarly by decreasing the density of fissionable atoms in the core. Also, for under moderated, thermal reactors, loss of moderator (which is also the coolant in LWRs) serves to reduce power too. These negative feedback mechanisms have to be seen to dominate over potential positive feedback mechanisms such as loss of coolant in over-moderated reactors (which we now know was the basic mechanism for the power excursion at Chernobyl) or mechanical means of increasing the core density, eg. displacement of fuel rods by mechanical means, in fast neutron reactors. As long as the overall power coefficient is negative, under all circumstances, then the fission reaction will be self limiting. This serves to show how reactivity and heat removal are closely related and should in general be considered together.

For any level of reactivity, heat removal processes have a greater margin of safety, and natural convection is able to give a greater contribution to cooling, for cores with low power densities. In fact for many "inherently safe" design concepts the requirement that decay heat removal should be achieved without forced convection is a major design constraint which leads to smaller reactors and de-rated cores with low power densities. Low core power densities are a valuable safety feature in two quite distinct ways as explained below.

3.1 Extended accident timescales

After tripping, either by engineered or inherent means, the heat output of a fission reactor falls initially to about 5% and eventually to below 0.1% of the full power output. During the early part of the transient natural heat transfer is usually insufficient for any practical power reactor geometry to cool the core and unacceptable core temperatures can only be avoided if the core is itself a sufficiently large heat sink. Whilst this is generally true, the detailed position may vary with reactor type. Thus, for the LMFBR, the actual core itself is small, with low thermal capacity (although the pool design provides a very high coolant thermal capacity) and after a trip, the core may temporarily be over-cooled by the main pump coast down. After this, many current LMFBR designs indicate adequate cooling from natural circulation, with the high thermal capacity coolant providing the means for extending the time during which mitigating action could be taken. Lower core power densities also favour this characteristic which may be enough to maintain the core in a safe condition until the decay heat output falls within the capability of the natural cooling available. A secondary benefit of extended accident timescales is that it provides an opportunity for operator action to intervene to aid recovery. Such action may be of limited relevance to an inherently safe reactor since there will be little scope for the repair or realignment of safety features which are governed by the basic structural design rather than engineered active systems consisting of many individual components.

3.2 Natural cooling

A safe reactor should have a capability to remove decay heat by natural rather than forced cooling. This is practical in many cases as core power densities are not too high relative to the coolant heat removal capability. The major design options are whether the passive decay heat removal is always operating as opposed to being positively "switched on", and whether elements of diverse decay heat removal paths should be provided using, for example, steam generators and air heat exchangers.

The reliance upon natural circulation flows as a major

natural heat transfer mechanism is not necessarily without some difficulties. In complicated geometries multiple flow paths may be possible and some of these may have insufficient cooling capability. Also, cavitation boiling and stagnation may occur and adversely affect core cooling both locally and overall. Finally, a passive convective flow may be difficult or impossible to enhance or divert without engineered systems. All these considerations suggest that given the difficulty in predicting circulatory flows in complicated geometries with a wide range of possible core conditions, the safety demonstration for decay heat removal must be based on a wide range of tests and a good knowledge of possible fault conditions (including structural failures) and scaling effects.

Natural circulation flows are more stable and effective if large height differences exist between hot and cold zones. This may suggest that decay heat removal through steam generators is less attractive than through external heat exchangers mounted high on or in the reactor building. However, decay heat removal without natural circulation may also be possible if heat removal paths are short and thermal conductivities are high. Convective transfer must ultimately play some part, either in core cooling or further down the heat transfer chain in the interface with the ultimate heat sink. It cannot be ignored as it provides a means for overheating structures which the heat is transferred to. This is an additional safety consideration.

4. CONTAINMENT

The containment system can rely principally on engineered features as is the case with most contained power reactors operating today. Natural features are used to complement the engineered features of the containment system, and to a greater extent as in the case of floating or underground design concepts. In this sense containment is directly related to siting although the origin of the need for containment also lies in the appreciation of the risk potential of an uncontained LWR in a non-remote site.

An outer containment building enclosing the whole primary circuit serves two safety functions. Firstly, it provides a final barrier to the release of fission products if the inner barriers fail and can be designed to remain effective even under energetic accidents. The second function is to provide protection to the primary circuit against the effects of some external hazards. However, even in an advanced design concept, containment is seldom a purely passive system since it must be able to transfer the heat from the primary circuit to some external heat sink and may additionally feature other safety items such as mechanical pressure relief, pressure suppression, isolation and electrical combustible gas igniter systems. Thus, the containment system tends to be an active engineered system which includes a passive

structure as an obvious component.

A containment system is passive only for the limited case where natural heat transfer processes are sufficient to cool the interior without significant degradation of the containment function. In practice this requires large containment buildings with the wall and surface areas maximised and perhaps with external and internal convection processes enhanced by the provision of specific structures. The ability of such a structure and the allied convective heat transfer mechanisms to cool liquid pools with low vapour pressures, such as might arise from a molten core, may not be adequate and in these conditions radiative heat transfer may be important.

The assessed risk of a nuclear reactor depends upon the distribution of population around the site and remote siting is a well-established way of minimising risk. Remote siting is also an inherent feature in that population growth around the site can be inhibited and in emergencies the population can be temporarily relocated by accident management interdiction. The main benefit of remote siting is in reducing the assessed probability of severe reactor accidents causing early deaths in the off-site population. Remote siting cannot effect the risk to the operators and may have little benefit for off-site delayed health effects or economic consequences of severe accidents.

5. MATERIALS PROPERTIES

Safe reactors should not be vulnerable to chemical degradation in structures and components important to safety such as in the primary circuit. Therefore, the choice of materials is restricted to avoid the chemical/metallurgical incompatibilities which could lead, at one extreme, to corrosive weakening of structures and, at the other extreme, energetic runaway chemical reactions. Some examples of incompatibilities are well known (eg. embrittlement of stainless steel by trace quantities of chlorine, voidage swelling of stainless steel in fast neutron fluxes, bearing seizure in pure helium or sodium environments and zirconium-steam exothermic oxidation) but materials incompatibility is a complicated phenomenon requiring detailed examination of specific designs and such incompatibilities may not express themselves early in the plant lifetime and could be dependent on the method of fabrication as well as the operational or faulted environment. The actual safety implications for specific materials problems will depend upon the timescale involved. Thus, a gradual degradation may render a design economically non-viable but may not pose a severe safety problem. Rapid interactions pose immediate safety problems requiring different safety considerations.

In these respects materials compatibilities cannot be established without long term experiments in prototypical

environments which model both the gross physio-chemical conditions and the trace elements which may be present in low or time dependent concentrations. It is perhaps in this way that the questions of safety and operability or cost are most closely coupled since the desire to avoid some of the more obvious chemical incompatibilities and hence potential for fires or explosions may lead to long term degradation of structural competence and hence to an increased potential for ageing related mechanisms to cause structural failures. Operability or cost may be influenced directly through increased capital cost, shortened plant lifetime and restrictions on the manner of operation to avoid corrosion or fatigue effects.

6. RAMIFICATIONS FOR REACTOR DESIGN

Even with the very brief description above of the requirements of all reactors for adequate reactivity control and shutdown provision and heat removal under operation and post shutdown conditions it would appear obvious that current designs have evolved through reliance upon engineered systems. Because of the basic heat transfer requirements to get rid of heat from the core, usually a large core can only be contemplated if existing natural processes are helped by engineered systems. Similarly, control and feedback require sophisticated instrumentation and detection systems to guarantee stable operation. The only means by which such reliance can be reduced is by making the reactor <u>smaller</u>. This means physically smaller, although a combination of small size <u>and</u> lower power density are sometimes proposed. It is for this reason that economics becomes such an important issue for these designs as 'economies of scale' are possibly lost and the cost per kW-hr could be much higher than with existing plant. Consequently much of the debate concerning such designs centres upon economic considerations. Since a lot of the basic data for the necessary calculations cannot be available until after prototype development, this ensures that unquantifiable, subjective interpretations can fuel these debates for some considerable time. Additionally, smaller reactors (and/or reduced rating) means more individual units for a given output with the possibility of an adverse effect on the overall risk.

A further ramification of the implementation of the concept of inherent safety on design is that it must be <u>simple</u>. Simplicity is fundamental to the 'passive' or natural processes called upon to provide the essential functions in such reactors. If no reliance needs to be placed on ESFs then, of course, certain advantages are immediately apparent viz:-

i If there is no equipment for operators to use, the chance of them doing it incorrectly is removed.

ii If there is no equipment to maintain, the chance of common mode failure due to maintenance error is removed.

iii If there is no equipment exposed, it cannot be sabotaged.

iv If staff do not need to access plant, occupational dose levels can be reduced.

v If there is no equipment which depends upon high reliability on site electricity - problems with eg. diesel generators are eliminated.

vi If safety systems are really simple, there is the possibility of de-institutionalising regulation.

These are some of the benefits which could be claimed if reliance upon ESFs could be totally removed. No such situation has been achieved to date - although simplification in many areas of reactor operation may be achieved in the future. A compromise of having some engineered features may negate the philosophical argument but represents perhaps a more balanced approach, ie. if ESFs can be provided, why not do it?

7. EVOLUTION TO THE NEXT GENERATION

The need to control reactor neutronics and temperatures in a safe, reliable and economic manner constrains design options in many ways. Existing mainstream designs of commercial reactors offer examples of how a successful design solution can be achieved. They also indicate how different degrees of implementation of the two basic safety elements - engineered safety and inherent safety - have been achieved. Other, perhaps more radical, designs have been proposed and occasionally developed to a small scale prototype stage and these also offer some insight into how the balance between safety, reliability and cost is difficult to maintain and even more difficult to demonstrate.

Any examination of existing or proposed reactor designs soon reveals that comparisons must be done on a whole plant basis and that every aspect of plant design is ultimately related to every other aspect. It is therefore misleading to base a comparison on only one or a few conditions. Moreover, whilst safety aspects can be compared at one stage of design development, reliability and economic aspects can only emerge properly with operating experience.

Continual improvements in plant design, for both safety and efficiency, have been effected since the earliest commercially usable electricity generating plant went into service in the 1950s. There have, however, been several milestones which precipitated particular effects in adapting and evolving existing plant. Most obvious, in the West, was the accident at Three Mile Island which had, and is still having, a profound effect upon the provision of safety equipment, personnel training and operational

procedures, particularly in the USA. A similar, though perhaps less intense response occurred in the UK following the Windscale fire in 1957. Presently, however, we do not expect such dramatic 'quantum leaps' in safety thinking partly because of the confidence we have that a really serious accident has been made much less likely by the lessons learned from these earlier events but also, and perhaps more importantly, because of the much more detailed monitoring of potential initiating events which allows a continuous appraisal of a range of safety systems. Thus, for example, the failure of the under voltage relays in the Reactor Protection Systems at the Salem plant in the USA was communicated to operating utilities worldwide to affect any necessary procedural changes.

It is now approaching a decade since TMI and enormous amounts of effort have been expended in re-appraising the safety of existing reactors. This applies particularly to LWRs but a proportion is of relevance to gas cooled reactors and to the developing LMFBR systems. Consequently a great number of improvements or changes to enhance operability have been identified and indeed for many reactors in the USA, engineered systems have been retro-fitted to them. However, there are good prospects for continued evolutionary development, some of which are presented for illustration below.

In the UK the PWR design has been re-vamped for the UK licensing requirements and many aspects of its design would merit an 'inherent safety label'. Others seem to be just good common sense (or engineering judgement) which should be expected in any new design. In the USA Westinghouse Corporation have collaborated with Japan to produce an advanced PWR and the Electric Power Research Institute (EPRI) have come up with a similar approach but in this case, for a boiling water reactor. Some of the improvements which can be considerd now are, for example:

i Elimination of low points in pipework (no sumps present to inhibit refluxing (natural circulation)).

ii An increase in water inventories to ensure that the core is always covered.

iii Re-design of main circulation pumps to remove active seals (hermetically sealed pumps). This to remove the dependence upon essential service water supplies for pump seals - a cause of small loss of coolant accidents in PWRs.

iv Replacement of borated water by 'grey' control rods.

v Diversity in pumping power - steam driven pumps (this feature is included in the Sizewell B design and has been implemented by the French on their PWRs).

Many such changes can be envisaged, each of which offers a distinct improvement for a specific system. More

general trends can be discerned too. "Containment" has been identified as being crucial to arguments for insulating the environment from potential severe accidents. In this case this is not accident prevention in the sense that containment per se cannot influence whether a serious core melt accident may happen or not, but its function as a barrier between whatever may ensue from such an accident and the environment is becoming much more appreciated. One of the principal outcomes of the research on fission product source terms is the realisation of the potential effectiveness of containment, even in conditions well beyond its design basis. In this context, 'containment' is used in the LWR sense, ie. as a large concrete (or steel) vessel which surrounds the NSSS. Nevertheless the general principles also apply to reactors with different realisations of the containment concept.

The first improvement which may be envisaged along the evolutionary route is simply to understand better the capabilities of containments which have been provided for existing plant, especially in their response to beyond design basis accidents and the potential for inadvertent leakages (through left open valves, etc.). Once this has been done, and there is little doubt that 'containment' has been the poor relation so far as severe accident research has been concerned, the potential for accident management and the possibilities for release mitigation can be investigated. In the future lie several 'advanced' containment concepts which offer greater reliability in severe accident conditions. (Note that this implies a divergence of accepted practice in the definition of the design basis). Several of the more developed ideas are:

i Provision of enhanced passive heat sinks (eg. Ice condenser - implemented on some PWRs - or the pressure suppression pool - implemented on BWRs and the RBMK at Chernobyl.

ii Severe accident management - controlled containment venting - with or without filters, chill venting etc.

iii Underground siting - several feasibility studies have been made, particularly in Europe.

Other possibilities include the adoption of lower power densities, lower fuel ratings and more sophisticated fuel management procedures.

For fast neutron reactors various other options are available. These include advanced fuels such as carbide or nitride which offer some of the advantages (without the particular problem of low melting point eutectic formation of the metal fuel being supported in the US for various Integral Fast Reactor (IFR) concepts). Also, more use of natural circulation as a bonus for using sodium as a coolant and 'fail safe' shutdown systems may offer benefits which could be exploited even further.

More generally, the dramatic advances in micro-processors, information technology and control systems offer good prospects for very much improved instrumentation, control and man-machine interactions although this may lead mainly to the transfer of "human factors" efforts from hardware to software. Successful development of this field, when coupled with our heightened awareness to and improvements in operability, training, operator psychology etc., offer real advances in efficiency and safety. Developments in other fields of technical endeavour will also assist - particularly in materials, component reliability, inspection and maintainability of plant. These are, however, still evolving at present and could, as many of the other possibilities mentioned above, apply equally to the radical designs too.

8. CONCLUSIONS

In summary, there are excellent prospects for improvements in certain areas which could be incorporated in an evolutionary approach to future reactor design. One of the principle problems appears to be that current designs are safe enough now and that these improvements will provide at least as good a level of safety as the alternatives, at the time when the latter might be brought into service. The evolutionary approach offers a contrast in concept to revolutionary changes in reactor design. The basis of such revolutionary designs include the following factors:

i Lower power density and fuel rating
ii Reliance upon natural processes
iii Simplicity
iv Passive systems
v Less reliance on operator actions

There is, of course, room for debate as to how 'revolutionary' several of the currently supported design concepts are. Indeed, the principal selling points of some, the High Temperature (gas cooled) Reactors (HTRs) in particular, are that they are not revolutionary at all and only call upon well proven materials, components and other design solutions. The HTRs in particular can claim a lineage back through to the early UK Magnox gas cooled reactors. Similarly, the IFR utilizes well developed engineering in the use of sodium as a coolant; even the use of metal fuel in the current realization of that design is hardly revolutionary as it covers the first type of fuel to be used in early breeder programmes in the UK, US and France. In contrast to HTR and IFR, only the PIUS system from Sweden meets a stringent definition of 'revolutionary' in that the means for providing shutdown, the use of natural circulation in a large volume of water and the overall design are quite different from any other reactor. Even here, however, it is envisaged that the fuel would be in the same form as that used in current LWRs.

It is important to distinguish between some "inherently safe" systems on offer which call upon a strong development history from related, currently utilised reactors, and those which represent significant departures. In many ways both the IFR and HTR (in its several forms) should properly be seen as evolutionary divergences from current design materials practices. Therefore, it is only a matter of degree as to how much improvement in safety is really on offer and this must be balanced against the need for further engineering development, even for systems claiming such a long inheritance, before they could be deployed in commercial electricity generation.

The PIUS system is different again. Notwithstanding the claims of its protagonists, the design cannot be underwritten until the prototype has been built and shown to live up to all its expectations and a full and extensive safety analysis performed to show that the benefits claimed extend to all possible accident initiators.

There is no black and white division between current reactors and how they may be developed and possible alternatives which purport to offer advantages in terms of safety. For current plant designs work is being done to increase the safety margins available. Whilst some 'new' systems may offer some advantages over existing systems and be rooted in the knowledge base already accumulated, it is difficult to justify the radical changes in direction required in order to implement them for a return which may be an increased safety margin over one which is already adequate and can be improved. Further, if these radical designs are more expensive to construct and operate than current plant, further inhibition to the development of nuclear power may be introduced, perhaps inadvertently by attempting to follow unattainable goals in absolute safety.

All the above represents a logical appraisal of these new systems, of course from a point of view within the nuclear industry. The political appreciation of the same issue may be rather different. For example, the prospect of benign or passive reactors is very appealing. When this is coupled with the real, or imagined difficulties with existing reactor and their potential for harm, it is easy to see why such arguments become very appealing. Anti-nuclear groups are even beginning to take up a stance that if we have to have nuclear power then why not utilise these alternatives which are available now and are so much better than what we have? This, of course is a "the grass is always greener" interpretation of reality or perhaps less kindly, a deliberate attempt to divert resources and attention to what is known to be unattainable - absolute safety.

Overall, it would seem that there is no technical

basis for a complete diversion of effort into any of the new designs on offer. Attention to detail and the implementation of hard won knowledge for existing reactors appears the most secure route for the next few decades for electricity generation. However, the industry should not turn its back on new ideas and concepts as they come along because there is always the need to learn from whatever source. In many countries we concentrate upon the need to supply a single grid with essentially base load nuclear power stations and low efficiency, small units are of little interest. However, in many parts of the world such units could be exceptionally valuable in remote regions, in cold (or hot) regions, for desalination and for a range of industrial uses. If designs like PIUS can be shown to be so benign that true urban siting is possible then the demand for such a system would be very strong. Several countries have already developed designs for such applications. The Canadians have 'SLOPOKE', a small (10-100 MW) unit designed for unattended operation in the Canadian Arctic. The Russians claim to have a unit for space heating ready for test during 1987. The Argentinians claim such a unit for remote siting. Such radical reactor designs may not fit the bill for every country's needs at present but it is possible that the rest of the world will find uses for them.

4.6. APPLICATION OF FAULT TREE ANALYSIS TO THE BUBBLING DEPRESSURIZATION SYSTEM OF A NUCLEAR POWER PLANT WITH THE VVER-440 REACTOR

V. Krett, K. Dach, and J. Dusek
Nuclear Research Institute, Rez, Czechoslovakia

Abstract

Safety systems, having the task to limit and localize the consequences of design accidents, contribute significantly to the enhancement of operational safety of nuclear power facilities. By means of such systems, the soviet pressurized 213-type VVER-440 reactors, installed in the Czechoslovak nuclear power plants, are secured against the design basis accident, which is the loss of coolant accident with the disruption of the cold leg of the primary circuit main circulation pipe with the two-sided outflow of coolant. The bubbling depressurization system, performing the function of containment, is one of the most important safety systems which take part in dealing with this accident.

The bubbling depressurization system is designed to suppress the pressure in the hermetically sealed areas of the primary circuit after the accident under the ambient pressure and, by this way, to prohibit the escape of radioactive substances from the nuclear power plant. The under-pressure is obtained through condensation of steam component of the steam/air mixture escaping from the primary circuit and by subsequent holding of the mixture in the holding tanks. Condensation occurs during the bubbling of the mixture through water layers in the bubbling tower and the pressure is further decreased by spraying by means of the separated spray system and, after the bubbling process, by spraying with the water from the bubbling depressurization unit.

The fault tree method, which has been successfully applied to the analyses of several other safety systems (LPIS, HPIS, a passive system of hydraulic tanks, a spray

system, a steam generator emergency feedwater system), has been employed in the analysis of possible failures of the system and its probabilistic analysis. The main task of this analysis was to perform qualitative analysis and to find possible causes of the following events : (i) the under--pressure is not obtained and, (ii) formation of the under--pressure is delayed. On the basis of such analysis and the assembled fault tree, weak points of the system can be found and economical measures increasing the overwhole reliability of the system can be proposed.

In the analysis itself, the importance to confront the design documentation with the real facilities and also to evaluate properly the effectiveness and redundancy of the system on the basis of the thermal-hydraulic analyses was revealed. Human errors during outage of the nuclear power plant have turned out to be the most important possible causes of failures. The results of analysis during elimination of human errors by means of engineering and organizational measures confirmed high reliability of functional components of the system in contrast to the relatively low reliability of the auxiliary systems (ventilation of the holding tanks).

The analysis has suggested, among other things, the possibility to employ the fault tree method also in the case of a non-traditional system. The results have proved to be useful and became a stimulus for a proposal of possible modifications leading to an increase of the system reliability.

1. INTRODUCTION

Design, manufacture, implementation and operation of nuclear facilities in Czechoslovakia are carried out in accordance with the decrees and regulations of the Czechoslovak Atomic Energy Commission (ČSKAE), which by law performs the role of regulatory body in the field of nuclear safety of Czechoslovak nuclear facilities. Safety documentation is prepared in principle in the following three stages:

a) An ordering safety report containing mainly a preliminary analysis of environmental effects of the nuclear facility, requirements on the facility from the point of view of nuclear safety, and specification of programmes of quality assurance of the facility is a part of the design task and a necessary condition of the territorial decision regarding the siting of the facility.

b) Before the construction is commenced and during release of construction approval, a preliminary safety report, containing analytical and experimental proofs of meeting the demands of nuclear safety, programmes of quality assurance during manufacture and construction of the nuclear facility, and programmes of inspections is being presented together with the design documentation.

c) After the construction is finished, a pre-operational safety report /4/, containing concrete date regarding meeting the provisions of nuclear safety of the facility and conditions and requirements of its further safe operation is being presented in the licensing procedure before reactor loading. The pre-operational safety report is the highest stage of the safety documentation. One of the important chapters of this report is the chapter "Safety Analyses". Elaboration of the safety analyses is based on the "Act on Government Supervision of Nuclear Safety of Nuclear Facilities" /1/, decrees, regulations and directions of the ČSKAE. Those, who elaborate the safety documentation, propose, according to the approved

safety philosophy, the scope of the event analysed, define the safety criteria, computing assumptions, input data, carry out the analyses and evaluate the events. Standardization of computer programmes is gradually carried out. In the Nuclear Research Institute (NRI) evaluation of quality and completness of the safety analyses is carried out before their approval by the ČSKAE, which then releases the operating license.

2. THE MOST IMPORTANT ANALYSES OF ACCIDENTS

From the point of view of possible failures in the nuclear power plant (NPP), the following accidents are analysed in the safety reports:

1) Reactivity initiated accidents (RIA)

Analyses of possibilities of these accidents both during the startup of the reactor and during normal operation are carried out. Choice of the situation able to initiate the changes of reactivity of the reactor core is limited to the following five possible events:

- Uncotrolled withdrawal of groups of control element assemblies
- Ejection of the control element assembly
- Inflow of cold water into the reactor
- Spontaneous decrease of H_3BO_3 concentration
- Release of boron depositions from the structural parts of the core.

2) Accidents with loss of tightness of the primary circuit

Conditions in the core, fuel element assemblies, hermetically sealed areas, the primary circuit and also the outside of the NPP are analysed with the aim to determine the thermal hydraulic conditions and effects on the structural parts, and also propagation of radioactivity. The analysis is limited to the following four possible events:

- Large loss of coolant during the design basis accident (DBA)
- Non-compensatible loss of coolant
- Compensatible loss of coolant
- Loss of coolant after a rupture of the steam generator tube.

At present, the philosophy of safety in the case of the accidents beyond design basis is being developed.

3) Accidents following a loss of tightness of the secondary circuit

The analyses are carried out on the assumption of correct or incorrect function of the control and safety systems and are limited to the following three possible events :

- Rupture of the main steam collector
- Rupture of the main steam piping
- Rupture of the feedwater collector.

4) Accidents following an incorrect function of components

Heat transfer between the primary and secondary circuits can be inadequate owing to the incorrect function of components. Several possible events are being considered , as, for example:

- Fuel element assembly blockage
- Seizure of the rotor of the main circulation pump
- Loss of electric power supply of some or all main circulation pumps
- Failure of turbo-generators, feedwater regenerators and loss of feedwater supply.

5) Accidents in the systems of radioactive materials

In the systems of radioactive materials, accidents during fuel handling, reactivity change caused by an incorrect fuel loading, deterioration of cooling of fuel element assemblies

and their mechanical damage can occur. In the systems of radioactive waste, accidents during management of gaseous, liquid and solid waste are possible.

6) Accidents initiated by external events

Implications of an impact of external and internal flying objects, effect of fires, external pressure wave, floods and earthquakes are analysed.

These analyses are to confirm that the equipment of the NPP and its control and safety systems meet the design specifications and standards and that their function and characteristics ensure the integrity of at least one of the protective barriers (fuel element cladding, primary circuit, containment) is maintained in a case of failure. The analyses also verify correctness of "Limits & Conditions" (technical specifications) during operation of the NPP equipment and of activities of the operational personnel.

From the point of view of safety analyses, the design basis accident following a rupture of the primary circuit main circulation piping represents the largest (as to the phenomena involved) and, at the same time, the most heterogeneous event. Here, keeping the limits of admissible radiation dose of public near the site of the NPP is the main safety criterion.

3. SAFETY SYSTEMS OF A NPP WITH VVER-440 REACTOR OF TYPE V-213

The loss of coolant accident following the rupture of the main circulation piping (diameter of 500 mm) with a double-sided outflow of coolant is considered to be the most severe possible accident for the 213-type VVER-440 reactor /2,3/. In order to localize such an accident, which is considered to be the design basis accident, the NPP is equipped with a number of safety systems. The emergency core cooling system (ECCS), destined to flood immediately the core and to remove the heat from the core in order to prevent its melting is the most important safety system. To this system, a next safety

system, the spray system (SS), ensuring pressure suppression after accident and washing out the released fission products from the environment of hermetically sealed areas of the power plant, is partially connected. The spray system co-operates during its function with a special Soviet-designed bubbling depressurization containment (bubbling system,BS), which ensures pressure suppression and reduction of temperature in the hermetically sealed area. This large-volume system is an absolutely passive system with no need of power supply and serves as a containment of the NPP. A diagram of these systems is in Fig. 1.

3.1. Emergency core cooling system

According to the function determination and the principle of action, the emergency core cooling system (ECCS) is divided into:

- passive system (PS)
- active low-pressure injection system (LPIS)
- active high-pressure injection system (HPIS).

3.1.1. Passive system

The passive system (100 per cent redundancy) consists of two accumulators (volume of 70 m^3) with 40-50 m^3 of H_3BO_3 solution with concentration of 12 g/l and temperature higher than 55 ^oC. Above the solution level, there are 20-30 m^3 of nitrogen with pressure of 6 MPa.

The accumulators are interconnected with the reactor by means of conduits with the rated I.D. of 250 mm; one conduit (from one of the accumulators) leads above the core, the other leads under the core. The system operates for some time without any power supply till it is emptied. Then the passive system must be changed for the active low-pressure injection system, which is capable of prolonged operation. The passive system is situated inside the hermetically sealed zone.

3.1.2. Active low-pressure injection system

The system consists of a low-pressure pump of the primary circuit emergency cooling (flow rate of approximately 380 m^3/h), storage tank with boric acid H_3BO_3 solution (concentration of 12 g/l, temperature of 40 ^{8}C and volume of about 350 m^3) and coupling piping. The system is activated in the event of large leakage from the primary circuit and follows the function of the PS.

The system is composed of three functionally and technologically identical subsystems, which are mutually independent and each of them is able to ensure cooling of the core in the event of the DBA. Two subsystems are connected to the piping leading from the accumulators to the reactor, the third subsystem is connected directly to the cold and hot legs of one loop of the primary circuit. If the tanks are already empty, the pump suction is automatically switched over to the coolant collection line from the well in the floors of the hermetically sealed boxes via the heat exchanger.

3.1.3. Active high-pressure injection system

The HPIS has the same redundancy as the LPIS, that is, it consists of three independent loops equipped with high-pressure pumps (flow rates of approximately 60 m^3/h) and with storage tanks (about 100 m^3). The system is activated in the event of smaller leakages from the primary circuit and also in the case of rupture of the main steam collector or the main steam piping. Concentration of the H_3BO_3 solution in the tanks is 40 g/l. Pressure tubes of high-pressure loops lead directly to the cold legs of three out of the six main circulation loops.

The emergency cooling system is activated in the event of signalling a decreasing level in the pressurizer and decreasing primary circuit pressure. The first of these signals activates the HPIS. If the decrease of the pressurizer level continues and the primary circuit pressure falls below 4 MPa, the passive system with accumulators intervenes auto-

matically. At this moment, the LPIS already received an impulse to start its operation (at the second signal - pressure lower than 12 MPa). This system delivers coolant into the core for 60 seconds after the loss of coolant accident (LOCA) at a pressure of 0.7 MPa, that is during the period when the accumulators are already empty and are being closed.

3.2. Systems of accident localization

These systems must decrease pressure and temperature in the hermetically sealed area and to wash out the fission products from the environment of this area.

In the hermetically sealed area, the following principal technological equipment is situated : a reactor, main circulation piping, steam generators, main circulation pumps and drives, a main closing valve and drives, a pressurizer with its bubbling tank, process equipment, filters of the system of continuous purification of the primary circuit coolant, a recirculation air-conditioning system of the hermetically sealed area, and pressure suppression containment with holding tanks.

This equipment is situated in separated rooms, which are interconnected in such a way that they form one common hermetically sealed area, designed for a pressure range from 0.08 MPa to 0.25 MPa (underpressure and overpressure relating the ambient pressure). In this area, slight underpressure (100-200 Pa) is maintained during normal operation.

All rooms of the hermetically sealed area are according to their functions classified as non-attended (rooms of steam generators and main circulation pumps, room of filters of continuous purification) and partially attended (room of drives of the main circulation pumps and main closing valves). The boxes of the steam generators and main circulation pumps are connected with the bubbling tower via a coupling corridor, through which the steam/air mixture flows after an accident.

The coupling corridor has flow section for the steam/air mixture of 11 x 6.3 m.

3.2.1. Spray system

Similarly to the active ECCS, the spray system(SS) consists of three functionally independent subsystems (200 per cent redundancy). Each subsystem includes a large--capacity pump (approximately 600 m^3/h) and, in contrast with the LPIS, also a tank with N_2H_4 and KOH solution, a water-jet pump and spray nozzles. The spray system starts its operation when the pressure in the hermetically sealed zone rises to 0.108 MPa. The pump delivers the solution from the tank of the LPIS into the spray nozzles located in the hermetically sealed area. The solution is sprayed, the steam component condenses and the pressure in the hermetically sealed area decreases.

The switching over to suction from the well in the floor of the hermetically sealed area via the heat exchanger is identical to that of the LPIS.

All three subsystems are put into operation simultaneously and automatically and the operator cannot affect their operation for some time. This principle holds also for the LPIS and HPIS.

Electric power supply of all three groups of low-pressure, high-pressure and spray pumps is realized independently from three independent voltage sources. The motors of all pumps are connected to the home consumption system of the NPP and receive voltage from the working or reserve transformers. The third source in the event of complete loss of home consumption (which is assumed during the DBA) is the power supply from diesel generators (DG). Each group is supplied from its own DG station. The DGs start up within 10 seconds and, for example, the low-pressure pumps are, according to the schedule of gradual DG loading, connected after another 15 seconds.

System reliability is ensured by various kinds of verifications, inspections and checks of the state of the

system and components. The comprehensive inspections and testing are carried out with the reactor shut down and cooled. With the reactor at power, the operator can perform a check of accumulator level, pressure and boron concentration and a check of tightness and proper function of check valves without adversely affecting the operability and effectivity of the passive system. During reactor operation, the active system pump wear, delivery and capacity can be verified, for which a special collector for the testing of recirculation régime in the circuit storage tank-pump-collector-storage tank is provided. At the same time, the diesel generators are also checked. This periodic inspection is carried out each month and lasts approximately 30 minutes.

3.2.2. Bubbling depressurization containment

This system has the task to decrease temperature in the primary circuit hermetically sealed area after the accident and to establish there an underpressure relating the NPP ambient pressure. In this way, any escape of radioactivity from the hermetically sealed area is prevented. During an accident, a fast evaporation of the escaped coolant flowing through the coupling corridor into the BS (Fig. 2,4) takes place. The underpressure in the hermetically sealed area is maintained by means of condensation of the steam component of this steam/air mixture during the bubbling through the boric acid (concentration of 12 g/l, temperature of 40-60 ^{o}C) layer in the bubbling depressurization unit. Cooling and condensation is promoted also by spraying of the hermetically sealed area of the primary circuit by the spray system. The non-condensed residual of the mixture, which travelled through the hydraulic closure of the bubbling depressurization unit, goes immediately to the hermetically sealed holding tanks for a long-term storage.

The bubbling depressurization containment itself consists of a large number of bubbling depressurization units (Fig. 3). These units are composed of parallel trougs filled with boric

acid and covered by caps, forming a hydraulic closure between the walls of the troughs and the caps. The steam/air mixture enters the unit through the inlet channel from below among the troughs, during an impact on the cap reverses its flow direction, pushes the hydraulic closure and bubbles through the water layer (height of approximately 0.5 m) behind the closure. Such design of the hydraulic closure has large flow section and low hydraulic drag (approximately 5 kPa). The whole system is located in a tower with twelve independent floors, each floor containing 153 bubbling depressurization units. The areas behind the hydraulic closures of the individual floors are mutually separated and connected with the holding tanks via a duplicated check valve. Each triad of the floors has its common holding tank, that is, there are altogether four holding tanks.

During an accident (within 10 to 15 minutes), the pressure in front of the hydraulic closure (that is, in the hermetically sealed area of the primary circuit) decreases after the passage of the steam/air mixture through the bubbling depressurization unit under the NPP ambient pressure by the effect of the spray system(Fig. 5). This effect is contributed also by spraying with the water from the floors of the bubbling depressurization containment. This water is pushed into the area of the bubbling tower by overpressure, arising behind the hydraulic closure. The water flows from the bubbling depressurization unit floors only until the pressure in the hermetically sealed area decreases under the NPP ambient pressure. At this moment, two identical and mutually independent check valves (which directly connect the areas in front of and behind the hydraulic closure) turn open into the area in front of the hydraulic closure and, in this way, enable pressure equalizing (this is effective during a "small LOCA" accident). These valves are equipped with a special duplicated lock blocking their opening if the pressure in the hermetically sealed boxes is higher than the NPP ambient pressure.

After the bubbling depressurization phase is finished, the overpressure regarding the NPP ambient pressure remains only in the holding tanks, which are hermetically sealed and where the pressure can be decreased a long time after the accident by means of the by-pass piping. This piping connects the holding tanks with a special air-conditioning system used during repair work and is closed by a valve, operated manually from a place outside the hermetically sealed area. Besides this piping, also the ventilation piping, serving only during outage of the unit and closed during operation of the NPP by an electrically operated valve, leads to the holding tanks. At least six floors of the bubbling tower must operate properly in order that the whole system may fulfill its task during LOCA.

4. RELIABILITY ANALYSIS OF THE BUBBLING DEPRESSURIZATION CONTAINMENT (BS)

The BS reliability analysis has been carried out with the aim to find weak points of the system and, eventually, to propose measures increasing its reliability /5 ÷ 11/. The work was focused on the qualitative issues of the analysis. The fault tree method, which was successfully employed in the analysis of safety systems presented in Chapter 3, was selected.

4.1. Analysis of BS failures

The complete non-execution of the BS basic function, that is, a failure to establish underpressure in the hermetically sealed areas of the primary circuit regarding the NPP ambient pressure, must be considered as the principal failure of the BS. In the analysis, the delayed execution of this function, that is after the time period specified in the design (approximately 15 minutes) is, however, also inadmissible. This assumption is, of course, already to a great extent conservative. Further function of the BS rests in a long-term storage of the steam/air residuals after condensation in the holding tanks. Probability of its non-execution will be

neglected here with regard to the design of the holding tanks, the probability of the two preceding failures and a possible extent of exposure to danger of population near the NPP.

4.2. Causes of non-execution of the BS function

The underpressure in the hermetically sealed area of the primary circuit is not established if the area has a large leakage. This leakage can arise when some of the six hermetic doors into this area are open. Their locking is signalled into the unit control room and their opening during operation of the NPP is possible only after unblocking of their locks by the operator. Probability of this failure is very low and depends mainly on the operator's error (error of signalling equipment can be, in this case, neglected).

The second possible cause why the underpressure is not established can be a failure of two holding tanks (a failure of each of them is equivalent to elimination of three floors of the bubbling tower from operation) or six floors of the bubbling tower (more conservative assumption with regard to the approval to operate the system with one floor without water on the basis of the operational regulations).

The most serious failure of the holding tank is its interconnection with the area in front of the hydraulic closure, which can occur after the opening of one of the two hermetic doors of the holding tank (analogous conclusion as for the door of the hermetically sealed area) or opening the ventilation piping (rated I.D. 200 mm) against the operational regulations (again, the main cause is the operator's error). The same reasoning holds even in the case of failure of the BS floor, which is again designed with two hermetic doors interconnecting the areas in front of and behind the hydraulic closure. In all three events, a very fast pressure equlization in all areas occurs and the bubbling depressurization is suppressed. Further possible causes leading to a failure to establish underpressure can be neglected with regard

to their probabilities (for example, loss of wall tightness, check valves into the holding tanks stuck closed).

Formation of underpressure can be delayed during both the bubbling stage and the subsequent spraying.

The first event can be caused by a small leakage of the holding tanks as a result of either a leakage of the by-pass conduit with rated I.D. of 57 mm (the valve is not closed or is mechanically damaged in the area of the coupling corridor) or a leakage of the check valves with rated I.D. of 500 mm between the holding tanks and the area above the hydraulic closure.

Spraying is considered to be insufficient when less than six floors of the bubbling depressurization unit are in operation. A floor is eliminated from operation when there are equal pressures in front of and behind the hydraulic closure. This pressure equilization can occur when the hermetic door of the floor is not drawn close (in the bubbling depressurization phase, this door draws close and opens only when the overpressure in the area behind the hydraulic closure is established) or in the event of the opening of one of the check valves of the floor (both locks of this valve are not locked up) with the rated I.D. of 250 mm. Other causes are considered to be less probable. The slowing down of spraying caused by an insufficient operation of the spray system (slow formation of underpressure in the hermetically sealed area) is not considered, either.

4.3. Assessment of BS reliability

On the basis of preceding considerations, a fault tree, which is in a simplified form presented in Fig. 6, has been assembled. The fault tree with 147 initiating events employed for the mathematical treatment (Fig.7) was evaluated qualitatively and quantitatively by means of the computer programme KADO. The input data used were estimated.

As the most consequential causes leading to the top event of the fault tree, the opening of valves in the ventilation piping from the holding tanks (oparator´s error) and mechanical loss of tightness of the by-pass piping from the holding tanks (or even not closing of their valves owing to human error)were identified. Both presented failures manifested themselves pronouncedly even in the subsequent analysis focused on a search of common cause failures. When these causes were limited, the failures connected with not closing of some of the hermetic doors in the hermetically sealed areas turned out to be significant.

4.4. Proposals of BS modifications leading to higher reliability

In connection with the results of the analyses, organizational and technical measures limiting significantly the effect of the operator and the possibility of the effect of a ventilation system on the BS were proposed. Further, technical modifications leading to assurance of integrity and compactness of the by-pass piping from the holding tanks (protective shields in the area of coupling corridor,fixed guying of piping or additional mounting of a valve in the vicinity of the holding tanks) were proposed. The check of the closing up of the hermetic doors before the repeated start of the NPP operation after planned or unplanned outages was made more stringent.

5. CONCLUSION

One of the most important safety systems of the Czechoslovak NPPs with pressurized water reactors VVER-440 type 213, the bubbling depressurization containment having the task to localize (pressure suppression) the design basis accident (loss of coolant accident after a rupture of the main circulation pipe with double-sided outflow of coolant and simultaneous loss of home consumption electric power supply) has been analysed. The reliability analysis was carried out in the

Nuclear Research Institute, Řež, using the fault tree method, which proved to be successful already in the preceding analyses of several safety systems /12/. The passive and active systems of emergency cooling (HPIS. LPIS), the spray system and the system of emergency supply of steam generators were analysed.

The aim of the analysis of this passive and 100 per cent redundant BS has been a qualitative analysis and identification of possible causes of failure to establish underpressure and possible causes of delayed formation of this underpressure. On the basis of such analysis and of the assembled fault tree, it was possible to identify "weak" points of the system and to propose economical measures increasing the system overall reliability .

During the analysis itself, the importance of confrontation of design documentation with the real construction work was demonstrated. On the basis of this confrontation, the analysis was successively made more accurate, supplemented and modified. Also the need of proper evaluation of the effectiveness and redundancy of the system on the basis of thermal hydraulic analyses has turned up to be significant.

The human errors during the NPP outage (the possibility of non-execution of the closing of some hermetic doors of the hermetically sealed areas after a check of BS, non--execution of the closing of manually operated valves on the by-pass piping, the opening of valves on the piping connecting the holding tanks with the ventilation system for the repair régime) were identified as the most frequent causes of failures. The results of analysis with human errors eliminated by means of technical and organizational measures manifested the high reliability of functional parts of the system, which contrasted with a relatively low reliability of the auxiliary systems (ventilation of the holding tanks).

The analysis showed, among other things, also the possibility to use the fault tree method for a non-traditional

system even in the case of serious absence of credible reliability data. The analysis carried out and the results turned out to be useful and formed a stimulus for a proposal of possible modifications increasing the system reliability.

REFERENCES

/1/ "Act on Government Supervision on Nuclear Safety of Nuclear Facilities", Digest of Czechoslovak Acts, Part 5, Act No. 28, issued on 4th April,1984 (in Czech).

/2/ KRETT,V. ; The Study of the Maximum Accident of LWRs, Škoda Review, 4/74.

/3/ MLADÝ,Z. , KRETT,V. , Questions of the Design Basis Accident of LWRs. Proc. ČSVTS conf., p.94, Zbraslav 1978 (in Czech).

/4/ Pre-operational safety report of the NPP Dukovany, March 1984 (in Czech).

/5/ HOJNÝ,V., DUŠEK,J., Reliability analysis of bubbling depressurization containment of the nuclear power plant with the reactor VVER 440, Jaderná energie 32, No.8-9 /1986) 329 (in Czech).

/6/ DUŠEK,J., DACH,J., "Probabilistic safety evaluation in Czechoslovakia", IAEA Safety Codes and Guides (NUSS) in the Light of Current Safety Issues (Proc. Symp. Vienna, 1984), IAEA, Vienna (1985) 217 .

/7/ DUŠEK,J., HOJNÝ,V., BRIŠ,R., "Possibilities of enhancement of the reliability of the pressure suppression safety systems in the hermetically sealed region of the NPP with a VVER-440 reactor", Operating Experience and Methods of Improvement of Performance of the NPP with VVER Reactors (Int. Conf. Pleven, 1984) (in Russian).

/8/ HOJNÝ,V., Reliability Analysis of the Bubbling Depressurization Containment of the V-2 Jaslovské Bohunice Nuclear Power Plant, Nuclear Research Institute Rep. 7075 T, Řež (1984) (in Czech).

/9/ DUŠEK,J., HOJNÝ,V., Reliability Analysis of the Bubbling Depressurization Containment of the VVER-440 type 213 Power Plant, Nuclear Research Institute Rep. 6280 T, Řež (1982) (in Czech).

/10/ DUŠEK,J., HOJNÝ,V., Reliability Analysis of the VVER-440 type 213 Power Plant Safety Pressure Suppression Systems after LOCA, Nuclear Research Institute Rep. 6049 T, Řež (1981) (in Czech) .

/11/ SUCHOMEL,J. et al., Analytical and experimental verification of the bubbling depressurization containment of NPP with VVER-440 reactors. Report EGÚ Bratislava, Jaslovské Bohunice (1980) (in Slovak).

/12/ DUŠEK,J., Reliability Analysis of Complex Systems with a View to the VVER Nuclear Power Station Emergency Core Cooling System, PhD Thesis (1984) (in Czech).

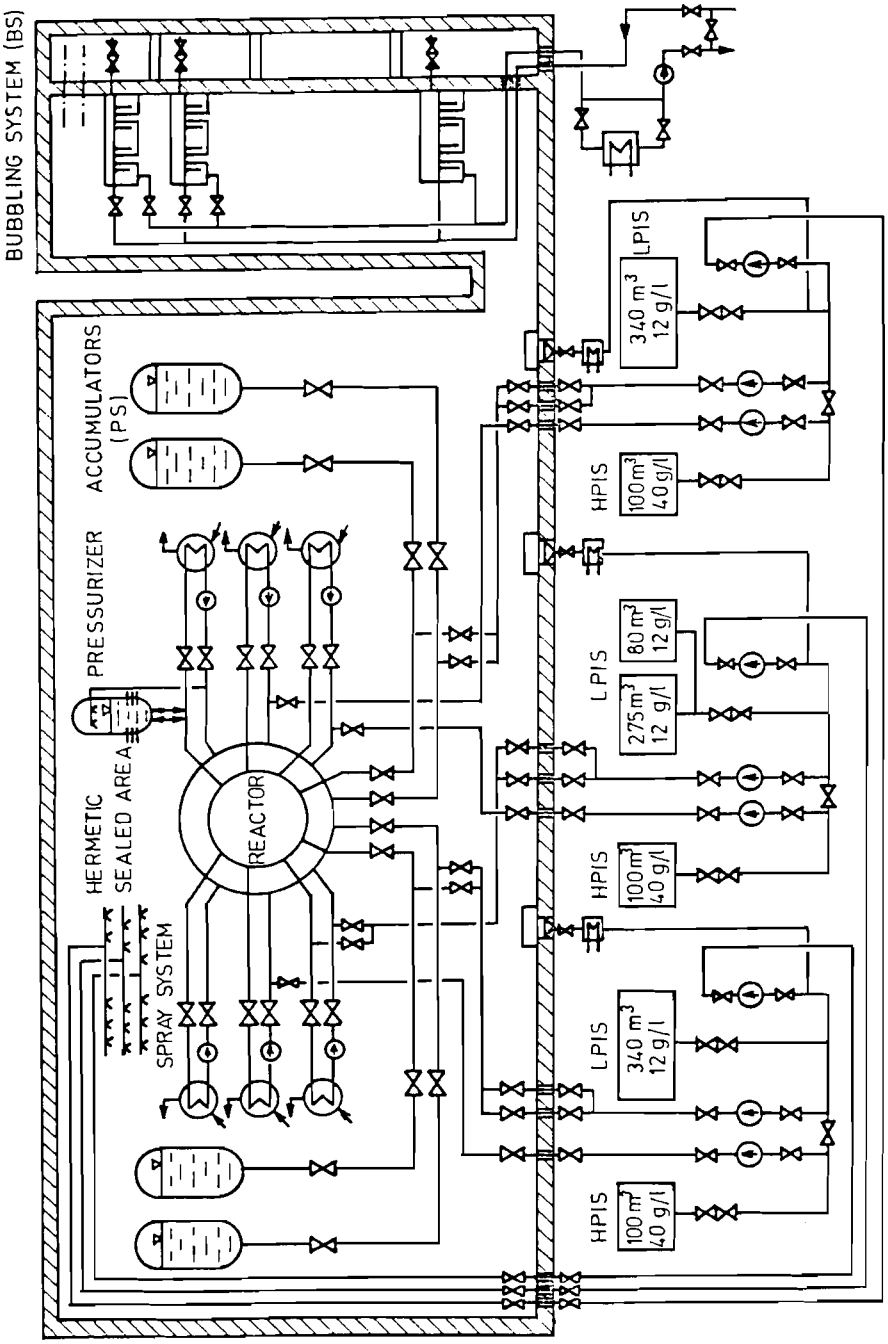


Fig.1. VVER-440 SAFETY SYSTEM

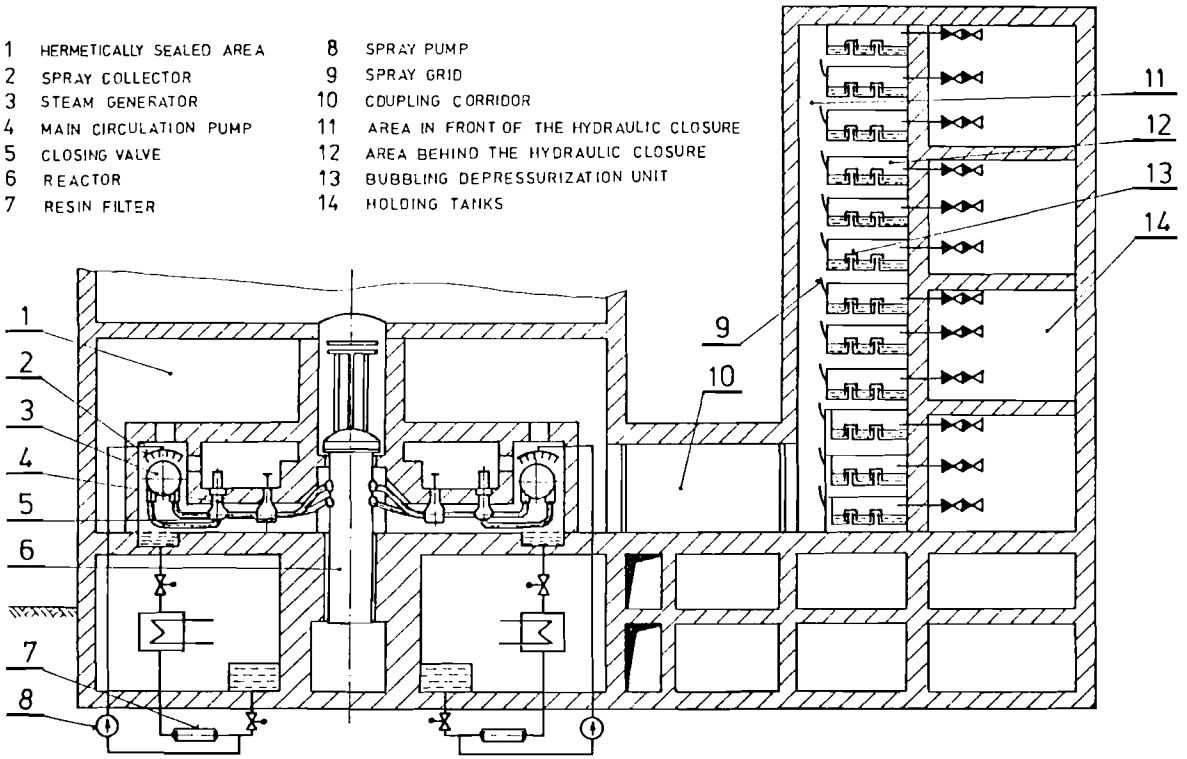


Fig. 2. DIAGRAM OF THE BUBBLING DEPRESSURIZATION CONTAINMENT

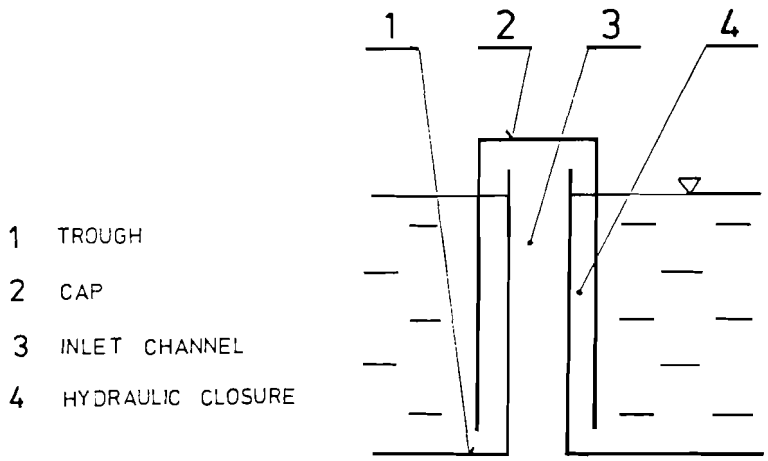


Fig. 3. BUBBLING DEPRESSURIZATION UNIT

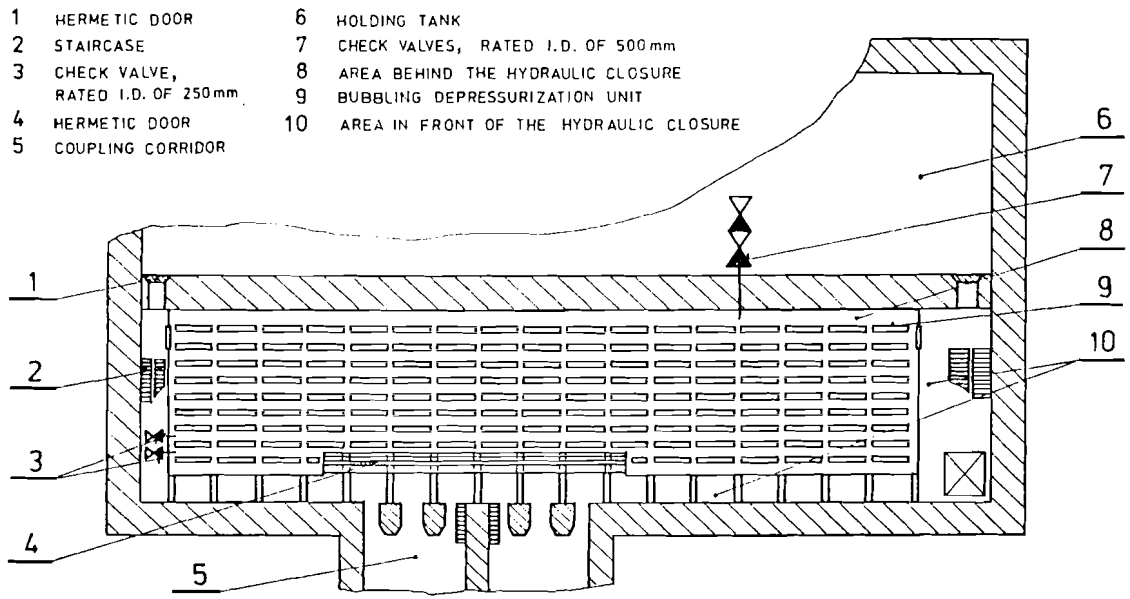


Fig.4. GROUND PLAN OF THE BUBBLING SYSTEM

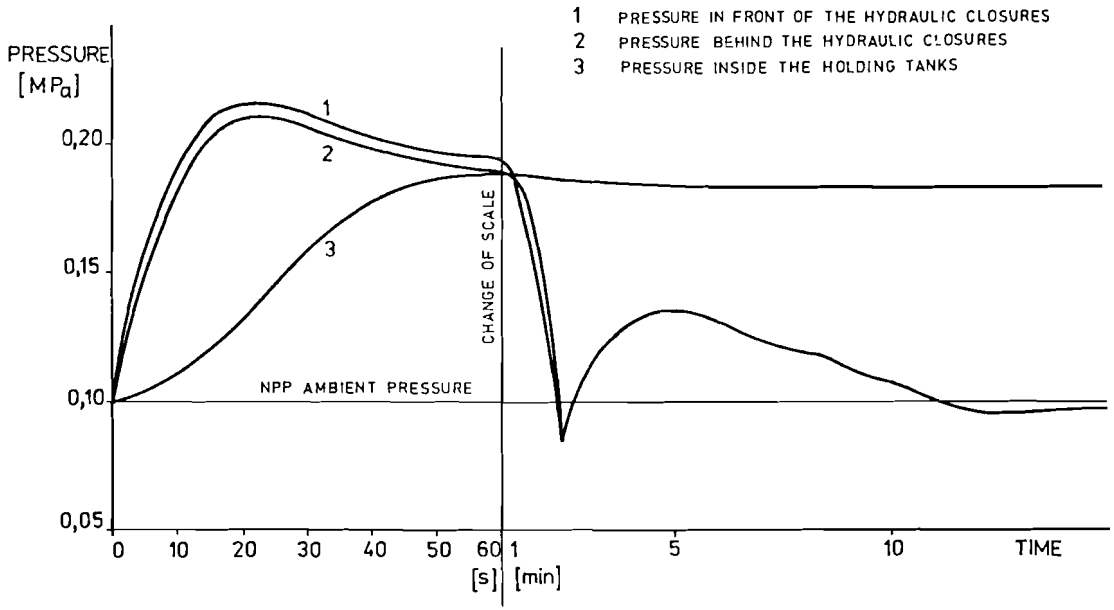


Fig.5. APPROXIMATE ESTIMATION OF PRESSURE DISTRIBUTION IN THE HERMETICALLY SEALED AREAS OF PRIMARY CIRCUIT AFTER LARGE LOCA

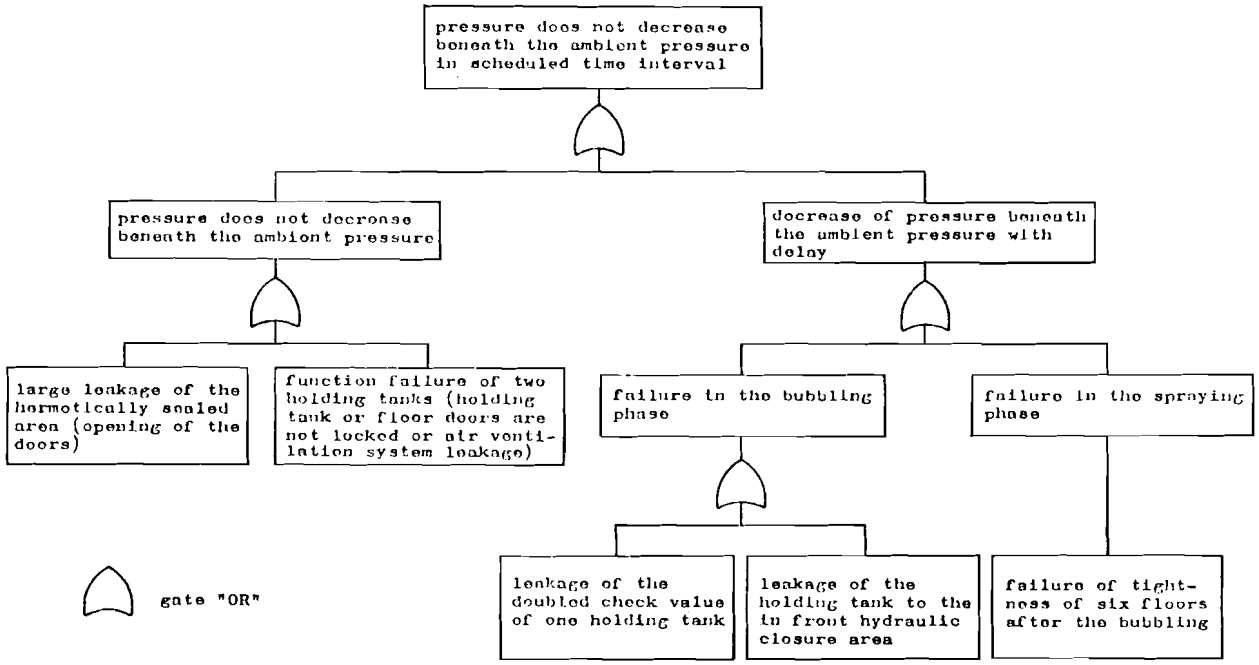


Fig. 6. Simplified fault tree of a bubbling depressurization containment

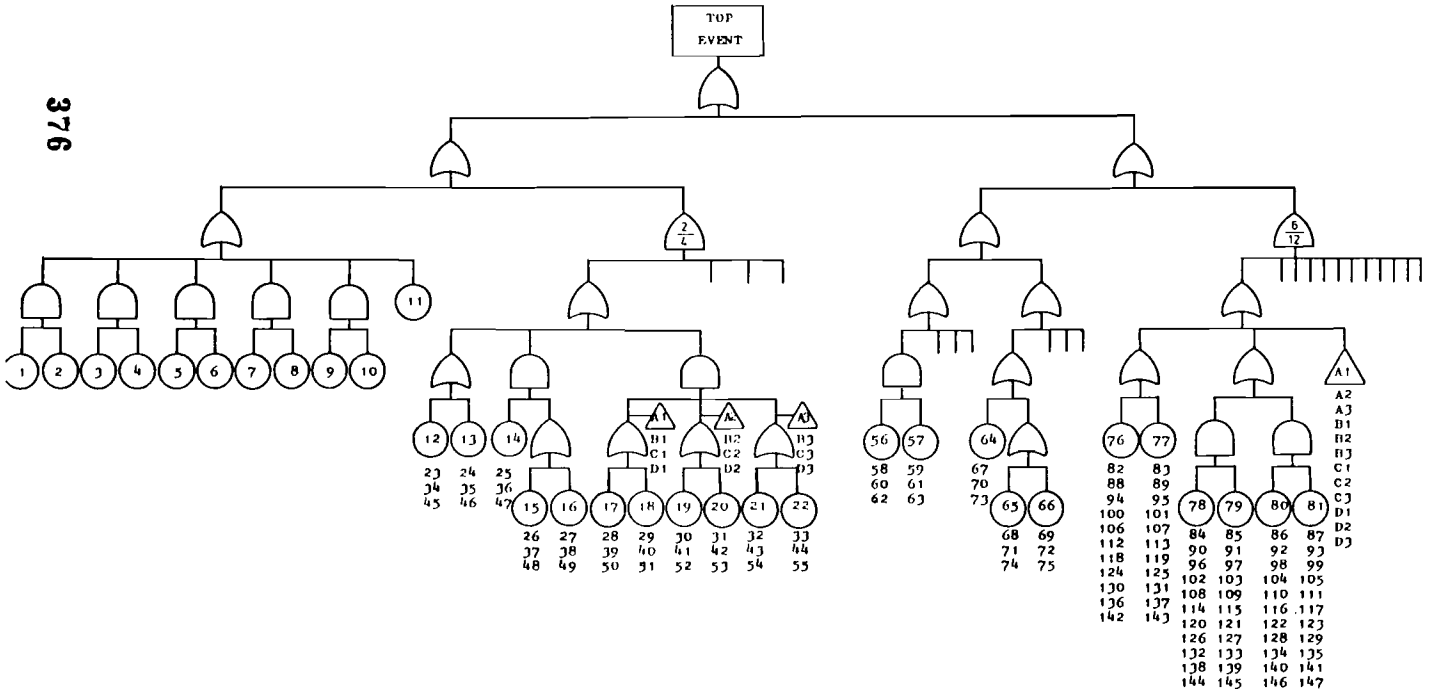


Fig. 7. Modified fault tree of a bubbling depressurization containment for reliability evaluation

5. CRITERIA, POLICIES AND CONSTRAINTS

5.1. DESIGNING FOR SAFETY

Martin Ollus and Björn Wahlström
Technical Research Centre of Finland
Espoo, Finland

ABSTRACT

The development of technical processes has resulted in large and complex installations with a potential for large consequences of unwanted events. The systems have become less transparent for all parts dealing with the systems and the identification of causes and consequences may be difficult. The design for safety could use a control system approach where feedback of operational information is used to improve the safety of the system. Feed forward approaches are used to predict the safety level of the system. The design of safety also includes the design for humans in the system e.g. the design of the working environment. Different methods such as alarm handling, feedback of actions , simulation and other operator support systems can provide means to improve the working environment.

The control system connects different parts of the process to each other and is also a link to the humans. The safety of the control system requires methods for safety analysis of both equipment and application planning. For the later part a review method similar to the HAZOP method for process components is presented. The method has been tested on the sequence control of a chemical plant with good results.

INTRODUCTION

After the recent accidents in large technical systems (nuclear and chemical plants, space shuttle) there has been a large debate on the safety of complex technical system. In many countries the public confidence in technological development has been seriously challenged. Some of the problems are undoubtedly connected with the rapid technical development where organizational and managerical practise has not been able to develop with the same speed.

The need for high efficiency has influenced on both technical design and operational practise. By designing larger installations a more efficient production is possible due to the scale. This development also means that there is a potential for large consequences of accidents and unwanted events. Correlated to the increase of scale the complexity of the plants has also increased. Several separate processes may be connected into production lines without or with very small intermediate storages which could serve to decouple the system. Also energy savings systems and thight overall control systems introduce interactions making the system less transparent both to designers and operational staff.

In the use of plants the need for efficiency has led to an operation with smaller margins, which is possible due to the technological development and more accurate control.

Operation may in some cases be difficult because of new less known raw materials and products, which also may be dangerous if they are not treated in a proper way. The same production facilities may also be used for the production of a variety of products. A need for flexibility against the markets and the costumers together with the need of efficiency require a fast switch over from one product to an other in order to keep storages small. In these circumstances the operation becomes quite complex with a variety of operation strategies available where the consequences of a wrong choice may be large.

As a result of the described development the technological systems have become less transparent for all the parts dealing with them. There may be difficulties to identify causes and consequences due to both process connections and control interactions. In the following some ideas of how to deal with the problems are discussed.

CONTROL OF SAFETY

Designing for safety can be considered as a control problem, where the feedback of operational experience can be used as input for improvements of the system safety. Because the planning for safety includes large and complex industrial installations also very unlike accident scenarious with large consequences have to be considered. In these cases a feedback approach is not possible because of the lack of operational experience. Hence, a feedforward concept has to be adapted, where the safety level is predicted by using different kinds of models. The prediction is then used to optimize the design in order to reach an acceptable level of safety. Feedback in this concept is used to ensure the validity of the models used in the prediction of the safety level.

The validation of the feedforward safety control using operational feedback is possible because of the fact that events with low probability usually are a combination of events with higher probability. By arranging a systematic gathering of information in parallell from these events operational experience can be used to improve the models used for the estimation of also low probability events.

Although many situations can be covered by the described approach all events will not appear under normal operations. Consequentially all information can not be gathered. Also the validity of the models used could cause some problems. In many calculations independency is assumed between small events causing a large event. However, the calculations will fail if they are not independent or there is some common cause which

has not been considered. A common cause failure may e.g. imply that several failure precautions are inoperable at the same time. Common cause failure are usually introduced by humans in the system. E.g. a design or a maintenance error can make the components inoperable.

HUMANS IN THE SYSTEM

Humans have an important role in all complex industrial plants. People are responsible for decisions, design, operation and maintenance. Also the risk analyses are done by people as a part of the design procedure. Due to these facts the humans and the plants are interconnected in a very complex system of causal relationships which implies that the humans have a large influence on the system either by making errors which may initiate a chain of unwanted events or by performing correct actions which inhibit an ongoing chain of events. The important role of humans is a reason for considering him also in the risk analysis. The reason for human errors can usually be seen as a mismatch between the actual situation and the resources available for the human. Typical examples of the mismatch are inrrelevant information presented e.g. in the control room, unsatisfactory operation guides, lack of training, etc. The detection and correction of these mismatches in advance are important parts of the work for improved system safety.

The safe design of the working environment could start from task analysis of the different states of the plant. The aim of the design should be an error tolerant system, where the errors could be observed and reversed before they have developed unacceptable consequences. This could be achieved by feedback from actions made in the system.

The task analysis will also be a base for control room design where different operator support systems will play an important role in the future. Such systems may be used to give the operator guides how to work in new situations. Also alarm handling can be used to provide the operator with relevant information about

the state of the process. On-line simulations available in the control room gives the operator a possibility to compare the consequences of different actions and can be a support for the choice of operations.

SAFETY OF CONTROL SYSTEMS

Two important parts of the control systems are the man-machine interface (MMI) and the control functions. MMI is one of the most important parts to support the humans in the system. Many guidelines and checklists have also been developed for MMI design. Due to their general nature their use in practical design may be difficult.

The control functions in a modern automation system are realized by handware and software and the software portion is growing. The software can be divided into system software and application software. The system software and its reliability analysis can be considered as a part of the equipment. For the reliability analysis of the equipment many tools are available. Generally, the equipment are reliable. The synthesis of a reliable configuration for a specific application is, however, still a difficult task. This synthesis is based on the application software and the reliability will much depend on the quality of this design. Despite of the common opinion that many serious errors are made in early design stages little attention has been given to this functional specification of control applications.

The application software is usually system specific and some application oriented languages are used. The programming for a specific application is usually called configuration. The configuration task is very similar to normal programming and many of the methods of software engineering could be applied. Some modifications may, however, be necessary.

Te ensure the functional performance of a control system some design review methods are needed. this could be used to ensure that safety related functions are specified correctly.

A DESIGN REVIEW EXAMPLE /1/

A method to review the safety of the design of the sequential control functions has been used in connection with a large batch process. Sequential control was chosen because of its great importance in this type of processes, where up to 40 % of the programming effort in the control implementation is devoted to abnormal situations and interlocks.

The review method is developed to evaluate the specifications of the sequential functions by a systematic talk-through in a review team, where special attention is given to safety considerations. The review is permormed in a team in sessions conducted by a chairman. The team includes the author of the specifications, a process engineer, a system user and an experienced control engineer.

The procedure is done in two phases. In the first phase the structure of the sequence control system is evaluated and in the second phase a step by step evaluation is performed.

In the evaluation of the structure the following topics are discussed:

- acceptable rules and design principles
- allocation of control tasks to different sequences
- hierarchy of the sequences
- communication and syncronization of the sequence
- interactions with other parts of the control system.

Although some of these aspects are related to the software implementation the functional specification should not be constrained by the charasteristics of some specific control system.

In the step by step evaluation three questions are of general interest:

- is the operator allowed to ask for this control action
- is the process in a state where this action is permitted
- will the intended action be successful

These checks are intended to prevent abnormal situations by ensuring the availability of necessary equipment and raw-materials and by checking relevant measurements and process components.

At each step the following topics are discussed:

- what are the most critical process parameters in this process state
- what are the critical process components at this step
- what are the prerequisites for successful operation, e.g. the following checks are done
  - availability of raw-materials and utilities
  - availability of process components
  - validity of critical measurements and controls
  - validity of checks performed earlier in the control sequence
- possible exceptions are checked by key-words analogous to the HAZOP-method (cf. table 1)
- the behaviour of the control system in abnormal situations, e.g. alarm generation, active shut down, etc.
- consequences of aborted execution of control actions, e.g. due to errors
- Comparison of the sequence control to earlier design decisions e.g. interlock and functional requirements given in the HAZOP notes.

Table 1 Example of keywords

parameter	keyword
setpoint	missing (not updated)
	too low
	too high
measurement	not available
	too low
	too high
	not valid
status signal	not available
	not stable
calculated variable	missing
	not valid
operation action	missing
	extra actions
	error
timing	too early
	too late
	in wrong order
	simultaneously
	delayed

The described review method was uses for analysis of a reactor control program containing 60 steps. The analysis was done during three sessions and the time used was about ten hours. The review was regarded as useful and a lot of improvements were suggested. Moreover the sessions provided a good communication channel between process engineers and control system designers.

CONCLUSIONS

In the designing for safety a control system approach was suggested where both feedback and feedforward techniques are used. The safety design also includes the planning of the working environment for the humans in the system and the task analysis will then have an important role e.g. in the MMI design.

With the increasing role of software in the control systems the importance of the application programming has grown. A method for review of this programming in connection with sequence control was presented. The experience of the method has been promising and the method will be developed in the future, when there also will be efforts to develop it from a pure manual method towards more automatic reviews.

For the analysis of the handware reliability of modern control systems computerized tools are necessary and there is still a need for development works in this field. However, the control system is an integrated functional part of the process and the safety of the control system has to be considered together with the safety analysis of the plant. Moreover, the safety design should be embedded in the normal design practise, when no separate safety and quality control groups should be needed for the control systems.

REFERENCES

1. Tommila T.: Considering Safety in Control System Design. Cost A1-project, working report, Technical Research Centre of Finland, April 1987.

2. Heimbürger H., Tommila T. : A Review Method for Graphic Displays, Cost A1-project, working report. Technical Research Centre of Finland, April 1987.

3. Fieandt J.: Application of Safety Analysis for Design of a Large Organic Fine Chemicals Plant. Proc. of SRE-symposium 86, Otaniemi, Finland, 14-16-October 1986. Society of Reliability Engineers, Scandinavian Chapter.

4. Roodhuyzen M.: Experience with Integrated Control Systems. Proc. of IFAC Workshop on Reliability of Instrumentation Systems for Safeguarding Control. The Hague 12-14 May, 1986.

5. Shaw W.T.: Structured Design Produces Good Batch Control Programs. Control Engineering, November 1983., pp 72-76.

6. Wahlström B.: High Costs and Low Probabilities - Problems of Risk Management. Technical Research Centre of Finland, March 1987. Internal paper.

5.2. ADVANCED SAFETY CRITERIA FOR NUCLEAR POWER PLANTS: PROPOSAL TO LIMIT CATASTROPHIC RELEASES

W. Kröger
Institute for Nuclear Safety Research
Nuclear Research Centre, Jülich, FRG

Extended summary

Taking West Germany as a representative example, statutory regulations guarantee a high safety standard for nuclear power plants. Primary aims are to prevent the public from radiological damage and to minimize risk. For this purpose dose limits are established for an unsheltered reference person at worst location for design-relevant accidents (5 rem, WBγ). Conservative calculation principles (all exposure pathways including 24 h-ingestion, 50 years exposure time, worst weather conditions including rain, etc.) have been fixed. For large light water reactors (LWR's) safety criteria are formulated which require a complex, highly active safety system, often with four redundant trains and with no need for operator action within the first 30 minutes. The high safety standard is confirmed by comprehensive risk assessment, e.g. the German Risk Study for the Biblis B-PWR (DRS), showing low figures for individual and societal risk.

Nevertheless, the risk defined by compounding factors is not acceptable to a large part of the public, mainly because severe (beyond design) accidents with catastrophic activity releases and consequences for this relatively small country with a high population density cannot be excluded. Taking the more favourable results from Phase B of the DRS, which is near completion, in comparison with Phase A from 1978, it can be seen that almost 100% of the inventory of noble gases, a few percent of the iodine and cesium as well as significantly less strontium (0,02%)

are expected to be released in the case of the accident category with the greatest release. The overall frequency of this category is in the range of 10^{-7} to 10^{-6} per reactor-year, which is extremely low; it includes event sequences with core meltdown and early containment failure.

The calculation of radiological consequences[+] results in

- no or only a few acute fatalities,
- several thousand additional cancer deaths (7000/14000),
- evacuation and relocation of several thousand people (3800/240000),
- contamination of large areas and subsequent decontamination of hundreds of square km, as well as
- financial damage to the public in the range of milliards (US billions) of DM.

The results are sensitive to the modelling of counter-measures, e.g. a delay or collapse of evacuation procedures may increase acute health effects significantly.

The aversion of the public to accidents with high and longterm possibly trans-generation consequences cannot be eliminated by their extremely low frequency. Added to this is the fact that the Chernobyl disaster has removed the hypothetical character from this type of event. Therefore, effort has been made by the Institute to evaluate more restrictive safety requirements which may help to overcome public resistance to nuclear power and to realize urban siting. In any case, they should be used as a starting point for a discussion on an international level aimed at developing common or comparable safety criteria for super-safe advanced reactors.

The basic idea for the proposed Advanced Safety Criteria (ASC) (Table 1) is to limit the activity release resulting from severe accidents in such a way that emergency measures no longer need to be considered for the protection of the public and financial

---

[+] By use of B04-version of UFOMOD-Code, which has been developed within DRS Phase A and which is under revision now; average ($\overline{KS}$) maximum values in brackets.

damage can be coped with by the society. Emergency measures include

- acute measures such as evacuation, distribution of stable iodine tablets and early relocation, as well as
- late measures such as late relocation and area decontamination.

For this purpose dose limits for short-term (7 days) and long-term (30 years) exposure after severe accidents are proposed for individuals at worst location. They must assure sufficient protection of the public. Quantitative safety goals in terms of tolerable risk figures are not proposed, mainly because of substantial uncertainties in radiological consequence calculations and questionable comparability of different risks. Reasonable values for dose limits derived from intervention levels for protective actions show whole-body doses ranging from

1 to 25 rem for short-term exposure and
10 to 250 rem for long-term exposure.

Based on these dose limits maximum releases for severe accidents can be back-calculated. For these calculations principles are suggested which have originally only been valid for design-relevant accidents and which are conservative. They can be slightly reduced in their degree of conservatism for this purpose, e.g. by shortening the exposure time, and by considering natural sheltering and the normal behaviour of the reference person at worst location.

"Severe accidents" include all events and event sequences of such a low probability that the plants do not need to be designed against them. They normally dominate the risk and need to be identified by comprehensive probabilistic safety analysis (PSA), which is regarded as being sufficiently developed for this purpose. This assures consideration of events of frequencies down to 10^{-8} per reactor-year, which is proposed as a quantitative cut-off criteria. Vulnerability in relation to acts of sabotage and catastrophic rare events should be as small as possible.

The application of these advanced safety criteria is demonstrated by the following example:

Assuming 1 rem as the reference dose limit for 7 days and 10 rem as an even more stringent limit for 30 years exposure time, as well as the proposed conservative principles for back-calculation, the tolerable release of the representative nuclide Cs-137 is in the range of 35 rem (Fig. 1) for an unpopulated zone with a radius of 400 m, 100 m emission height and unfiltered short-term release. More favourable technical parameters may lead to greater, less favourable to slightly smaller, tolerable releases.

We do not intend to dictate the technical measures by which these criteria can be fulfilled. But we know from PSA experience and risk reduction studies for mitigation features that designing reactors with passive inherent safety characteristics is the only promising approach:

> The reactor may not loose its retention capability even under total loss of cooling conditions due to physical reasons; the attempt to exclude loss of cooling conditions by providing an additional active safety system is misleading.
>
> The course of severe accidents must be slow to allow for mitigating counter-measures and for the reversal of wrong human actions.

Attempting to make high consequence accidents tolerable by adding additional active equipment and forcing frequencies below cut-off values is less promising because of unavoidable intercomponent/system dependent failures which limit the attainable realistic figures for the reliability of active systems.

The question of whether these stringent requirements can be fulfilled by a competitive technical reactor system has been evaluated for current German HTGR concepts. In conclusion, it seems to be clearly possible for small HTR's (200 MWt HTR-Modul of KWU and 250 MWt HTR-100 of BBC) and potentially even for medium HTR's (1200 MWt HTR-500 of BBC) to meet them. The physical characteristics of small HTGR's are such that under core heatup conditions following total loss of cooling maximum temperatures of the fuel elements do not exceed values where the elements would be subjected to temperature induced failure (Fig. 2). For medium HTGR's,

the maximum temperatures are in the range of total particle failure, but due to a strong profile, only a few percent of the fuel elements reach these temperatures and the average temperatures are below 1600 ^{o}C. This phenomenon and the strong retention capability of 'cold' graphite for fission products released from the core result in relatively small releases into the environment under hypothetical total loss of cooling conditions.

TABLE I

Advanced Safety Criteria (ASC)
proposed by the Institute

The aim is to limit activity release of severe accident in such a way that emergency measures do not need to be considered (no evacuation, relocation, decontamination) and the financial damage can be coped with

The way is to establish short-term and long-term dose limits for individuals at worst location, ranges of

1 to 25 rem for 7 days exposure
10 to 250 rem for 30 years exposure

Reactor with passive inherent safety characteristics is most promising for fulfilment

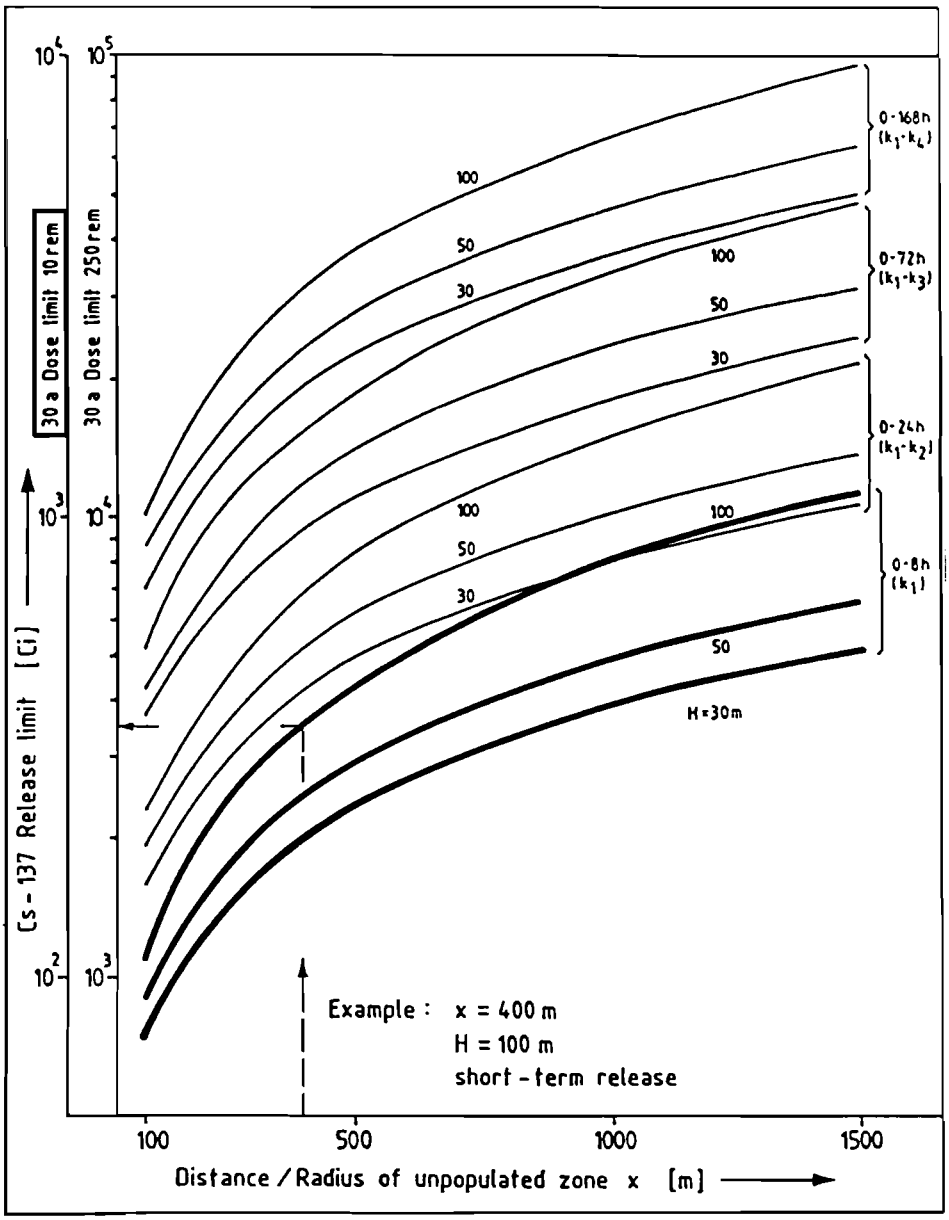


Fig. 1: Limit values for unfiltered Cs-137 release under beyond-design accident conditions, assuming 250 or 10 rem, as long-term dose limits

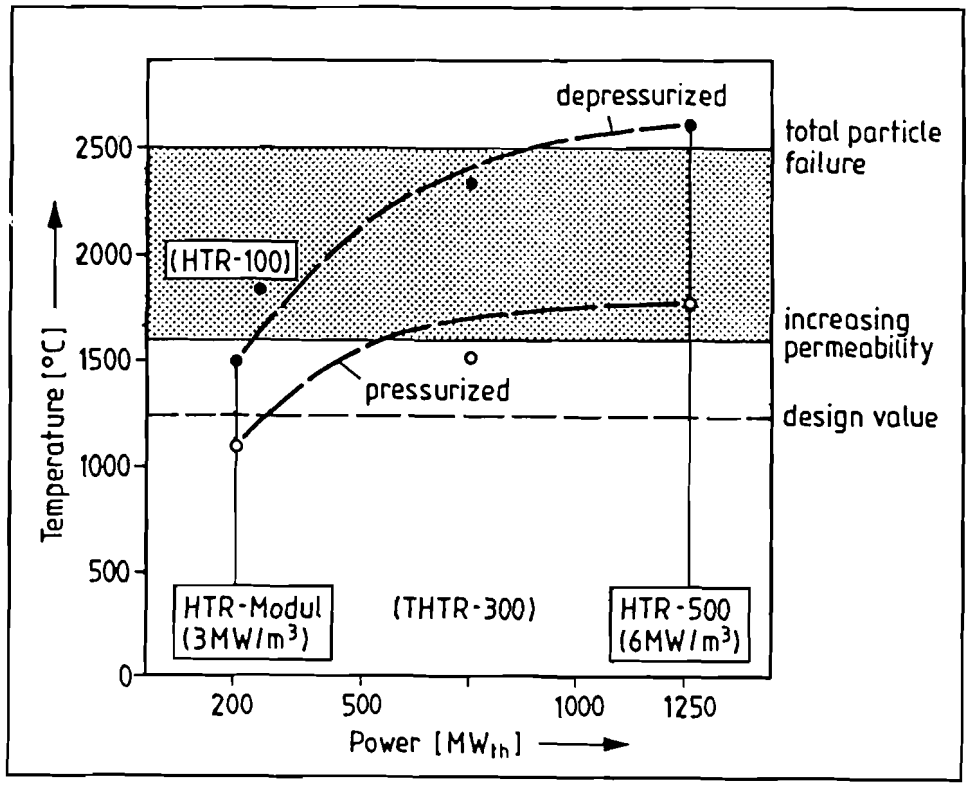


Fig. 2: Maximum temperatures of fuel elements for core heatup accidents in pebble-bed HTGR's (according to Rehm, KFA)

5.3. REFLECTIONS ON THE SAFE TECHNOLOGY MOVEMENT

Alvin M. Weinberg
Institute for Energy Analysis
Oak Ridge Associated Universities, Tennessee, USA

Four dramatic technological failures--Three Mile Island, Bhopal, Challenger, and Chernobyl--have shaken the public's confidence in technology. The reaction to these failures has followed three divergent paths. (1) In many countries strong voices urge abandonment of some of these technologies, particularly nuclear power. (2) A middle ground is the proposal to improve, incrementally, the existing technologies. These improvements are both technical and organizational. This is the response of most of the established nuclear and chemical industries. (3) An extreme view, which in the past few years has acquired a considerable constituency, has been to replace the existing technologies, whose safety is largely probabilistic, with technologies whose safety is deterministic, that is, inherent. I call this trend the Safe Technology Movement (STM). My paper will attempt to trace the growth of the Safe Technology Movement, particularly in chemical and nuclear industry, and to assess its prospects.

The Inherently Safe Chemical Plants

The main proponent of inherently safe chemical plants has been Prof. Trevor Kletz of Loughborough Technological University. After the disaster at Flixborough in 1976 where an explosion in a plant producing cyclohexane caused 28 deaths, Kletz proposed designing chemical plants so as to be "inherently safe." Kletz's main idea was to keep the inventories of highly toxic or highly explosive materials so small that even in the event of a catastrophic failure, not very much damage would be done. Kletz has propounded these views widely, and he published a book under the auspices of the Institution of Chemical Engineers, in which these ideas were presented systematically.

Three years ago I participated in a National Academy study on Risk and Fairness which gave me an opportunity to discuss inherent safety of chemical plants with managers of one of America's largest chemical companies. Bhopal had stunned these managers, yet it would be an exaggeration to say that they have incorporated Kletz's somewhat unorthodox views into the design, or even the redesign of their chemical plants.

One suggestion, which IIASA may be able to help implement, would be the stronger injection of principles of safety, even inherent safety, into the curricula of chemical engineering schools. Chemical engineering in the United States is taught by unit process--that is, by identifying processes such as distillation, heat transfer, control, etc.--that are common to essentially all chemical plants. I should think inherent safety could be identified as a unit process also, and possibly could be incorporated in the instruction of chemical engineers.

IIASA might play the role of convening chemical engineering professors from various countries to discuss their reaction to Bhopal. In final analysis, Bhopal was a design failure, probably more than an operations failure. Had the engineers who designed Bhopal been made aware of Kletz's inherently safe design precepts, and had these been incorporated in Bhopal, the accident would not have happened. A transnational dialogue on Bhopal, with the aim of greatly increasing the emphasis on safety in engineering curricula, seems like a worthwhile enterprise which could be undertaken by IIASA.

Inherently Safe Nuclear Reactors

Though the idea of inherently safe nuclear reactors was first publicly articulated by David Lilienthal in 1980, the idea itself is much older. One finds in the old literature various ideas for reactors that were inherently safe, or at least much safer than today's light water reactors. Thus Edward Teller had long advocated putting reactors underground--an idea recently resurrected by Andrei Sakharov; S. Untermeyer had proposed an essentially inherently safe BWR some 30 years ago; W. Ergen had suggested reducing the power output of a reactor so that the reactor would be self-cooling, even if all external heat transfer systems were lost.

Three Mile Island gave impetus to the technical development of inherently safe reactors. Most prominent were K. Hannerz's Process Inherent Ultimately Safe reactors; Lohnert's modular HTGR; and P. Fortescue's "forgiving" reactors--particularly large gas-cooled, graphite moderated systems. These technical proposals were accompanied by three major studies of the technical and institutional problems involved in moving to inherently safe reactors; the Institute for Energy Analysis' A Second Nuclear Era; Massachusetts Institute of Technology's National Strategies for Nuclear Power Reactor Development; and the Office of Technology Assessment's Nuclear Power in An Age of Uncertainty.

Most of these studies and proposals originated outside the mainstream of nuclear industry. Many in the industry feared that introduction of a new generation of reactors that was inherently safe would lead to pressure to shut down existing reactors. Thus industry chose to respond to the challenge by incremental improvements both in the design of new reactors, and in the operation of existing reactors.

Nevertheless the words "inherently safe" seemed to have so powerful an appeal that, by around 1982, one found the words being used frequently in Department of Energy budgets. The Department, however, was somewhat equivocal: modular reactors had caught its fancy (as being better suited to the financing practices of the utilities). That these reactors also were "inherently safe" or at least possessed inherently safe features was conceded but was not emphasized at the time. Nevertheless, both of the main lines of advanced civilian reactor development within the Department of Energy, the modular HTGR and the Liquid Metal Reactor, were inherently safe as well as being modular.

Chernobyl has pushed inherent safety to the fore (where I believe it belongs). With nuclear energy's future now hanging in the balance in many countries, inherent safety has now become an important, possibly predominant as a design criterion. What was believed originally to have been an impossible goal, now seems to be taken more or less for granted. As a result, no fewer than a dozen or so ideas for inherently safe reactors now are under discussion in many parts of the world.

A Catalog of Inherently Safe Reactors (after Lu Yingzhong)

Professor Lu Yingzhong of the Institute of Nuclear Energy at Tsinghua University in Beijing, China, has recently catalogued and classified some thirteen different "inherently safe" reactors.[1] Here I shall only summarize briefly the principles underlying inherent safety as identified by Professor Lu. These principles are two in number.

a.) Passive shut-down capability without core damage under any transient condition. The Chernobyl accident was touched off by a large reactivity transient; an inherently safe reactor would have to (1) eliminate all dangerous reactivity transients; or (2) withstand without damage any possible reactivity transient.

b.) Passive decay heat removal under any condition. The Three Mile Island accident occurred after the reactor was shut down. Had TMI-2 been equipped with means for decay heat removal under any circumstances, the accident would not have occurred.

Lu catalogues the thirteen inherently safe reactors under five main categories:

I. PIUS family: These reactors derive from the original SECURE design of ASEA-ATOM. The reactor, which is a PWR, lies at the bottom of a very large pool of borated water; the primary cooling system is separated from the borated water by two hydraulic density locks. Any upset in the coolant flow breaks the locks, and allows the borated water to quench the chain reaction and to remove the afterheat. Six distinct reactors based on this principle have been identified by Prof. Lu and are summarized in Table 1, taken from Lu's paper.

II. HTGR family: These semi-homogeneous reactors are graphite moderated and helium cooled. In all cases the reactors are so small--less than 300 MWe--that afterheat can be removed by completely passive natural convection. Lu identifies four reactor designs in this family. Table 2.

III. LMFBR family: Liquid metal breeders, ordinarily considered the least forgiving of all reactors, turn out to possess certain inherent safety features that are being exploited in several proposed inherently safe FBRs. These reactors are all pool-type rather than loop-type; several of them use metallic rather than oxide fuel; and all incorporate passively actuated shutdown systems. Three inherently safe FBRs are listed in Prof. Lu's Table 3.

[1]"Ordeals of Chernobyl and the Re-Justification of Inherently Safer Reactors," Working Paper, Institute for Energy Analysis, Oak Ridge Associated Universities, January 26, 1987.

Tab.1. The Characteristics of PIUS Family

Concept	El.Power	Main Features	Designer
PIUS	500 MW	1.PCRV,9.4MPa,13DX34.5MH,135000t 2.Static fluid valves	ASEA-ATOM
PIUS-II	500 MW	1.Three modules 2.PCRV, fluid valves as above	ASEA-ATOM
ISER-1 (Cold Vessel)	500 MW	1.Steel V,9.4MPa,9DX32MH,2100t 2.St.fl. valve/Float. ball valve	IHHI*
ISER-2 (Cold Vessel)	200 MW	1.Steel V,12.5MPa,6.6DX24MH,1000t 2.St.fl. valve/Float. ball valve	IHHI*
ISER-HV (Hot Vessel),	350 MW	1.Steel V,12 MPa,6.6DX28MH 2.St.fl. valve/Float. ball valve	JAERI
PIUS-BWR	750 MW	1.PCRV,6.8MPa,13DX35MH 2.Dynamic (Vortex) fluid valve	ORNL

*Ishikawajima-Harima Heavy Industries Co. Ltd.

Tab.2. The Major Characteristics of IS HTGR Family

Concept	El.Power	Main Features	Designer
MHTGR	139.5MW	1.Prismatic fuel element	GA Tech.
		2.Steel V,8.93MPa,6.8DX13.34MH,750t	
		3.Side-by-side arrangement	
HTR-M	80MW	1.Spherical fuel element	KWU
		2.Steel V, 6MPa, 6.6DX7.5MH, 775t	
		3.Side-by-side arrangement	
HTR-100	100MW	1.Spherical fuel element	HRB
		2.Steel V, 7MPa, 6.1DX11.7MH, 750t	
		Also PCRV under consideration	
		3.Integrated, SG above core	
SPGR-750	285MW	1.Spherical fuel in central holes	JAERI
		of prismatic graphite blocks	
		2.Steel V, 7MPa, 6.6DX27.2MH	
		3.Integrated, SG under core	

Tab.3. The Main Characteristics of IS FBRs

Concept	El.Power	Main Features	Designer
LSPB	1319MWe	1.Loop or pool configuration 2.Passive rod release from Curie-point or other temperature effect 3.Natural circulation system decay heat removal from reactor to atmosphere	EPRI
SAFR	350MWe	1.Pool configuration 2.same as LSPB for shut down 3.Same as LSPB for decay heat removal 4.Module "Power Pack" design	Rockwell Intl.
PRISM	133MWe	1.Pool configuration 2.Self-actuated release of shutdown rods from over-temperature 3.Radiant Vessel Auxiliary Cooling System (RVACS) for decay heat removal 4.Three modules couple with one turbine	GE

IV. Low pressure ISRs using novel coolants: Three schemes based on the use of low pressure, high boiling coolants have been suggested. These include the lead cooled DIONYSIUS (from EIR, Switzerland); the organic cooled CANDU; and the molten salt, graphite moderated system.

V. The Heat Only BWR: The Institute for Nuclear Energy Technology in Beijing is now building a 5-megawatt thermal, heat-only inherently safe boiling light water reactor for district heating. The reactor is a variant of the Soviet reactors for district heating being built in Gorky; the INET design uses an ingenious hydraulic control rod drive that is coupled to the primary circulating pump. Any loss in pressure automatically and passively actuates the control rods. This 5 MWt reactor is the first that actually will demonstrate a passively safe system.

The Impact of Inherent Safety

Those of us who are intrigued by the idea of inherent safety somehow see this as a way out of the nuclear impasse. We argue that if nuclear reactors were inherently safe, then nuclear energy would no longer be opposed by the environmental movement (this assumes that the waste disposal system could also be made inherently safe). This position is supported by suggestions, such as those of environmentalist, J. Beyea, that inherently safe reactors might be accepted by environmental activists provided their development were accompanied by serious attempts to develop solar energy. And often in the writings of environmental activists one sees allusions to the desirability of inherently safe reactors.

The problem, of course, is, How does one prove that an inherently safe reactor is inherently safe; or, having proven this to the satisfaction of the technical community, how does one persuade the skeptical public? One certainly can prove that an inherently safe reactor can withstand mishaps that would destroy existing reactors; for example, an incident like TMI-2 or Chernobyl simply could not happen in PIUS or in mod-HTGR. The difficult point is to prove that some other mishap, particularly one that no one has thought of, cannot cause serious damage.

I don't see any total resolution of this dilemma except through consultation with serious informed skeptics. Perhaps what is needed is a "Peace Treaty" between nuclear supporters and nuclear opponents, the purpose being to establish what degree of safety, if incorporated into

nuclear systems, would make them acceptable to the skeptics. IIASA might be the focus for drawing up such a treaty, and for promoting its ratification by pro- and anti-nuclear groups.

I should think that a most important step in restoring the public's confidence in nuclear energy would be to restore the confidence of the environmental movement in nuclear energy. After all, 25 years ago environmentalists by and large were supporters of nuclear energy--because if the nuclear system is operating properly, it is environmentally benign. A renewed coalition of environmentalists and nuclear enthusiasts seems like a fantasy today; perhaps inherently safe reactors could be made the basis for such a coalition.

The Future of the Safe Technology Movement

Safe technologies, particularly in chemical industry and in nuclear power, would constitute a technical fix for the debilitating attacks on advanced technologies that are now so prevalent in much of the Western world. Unfortunately, the safe technology movement encounters opposition both from existing industry, which sees it as threatening technologies that are already in place; and from the Greens, who are opposed to technology for political reasons.

The opposition of existing industry could be overcome, in principle, through operation of the market. If the new technologies were economical as well as inherently safe, they would ultimately prevail. A more difficult question is whether the new technologies will develop through a succession of incremental improvements of the old technologies ("quantity giving rise to quality") or whether completely new approaches are required. For example, there are some in the nuclear community who insist that Artificial Intelligence is a key to great improvement in safety. The general idea is to build into the safety systems elaborate pre-analyzed scenarios; any incipient malfunction is immediately categorized as being an instance of a scenario, is analyzed, and appropriate corrective action is taken. Whether such improvements will be perceived as constituting adequate safety is hard to say. Over 2000 reactor years of safe operation in light water reactors has now been observed since TMI-2. This already

means that we can say with about 87 percent confidence that the a priori core melt probability is no higher than 10^{-3}/reactor-year. By 2000, there will be about 8,000 light water reactor years; if there are no core melts by then, we can say with 99.97 percent confidence that the a priori core melt probability is no higher than 1 in 1000; but only with 55 percent probability that it is no higher than 1 in 10,000. This is not very reassuring. Thus the incremental approach would have to be supplemented by demonstration experiments in which accidents that would damage an unimproved LWR are shown to be aborted in an improved LWR. Largely for this reason, I favor the inherently safe design approach.

As for the opposition from the Greens, all one can say is that there are technologies--the so-called soft technologies--which are accepted by this group. Is it possible that the Appropriate Technology Movement, which has been embraced by anti-technology groups, could be transformed into a Safe Technology Movement? I would think that a new coalition involving centrist elements drawn from both the Greens and the technologists might rally around a Safe Technology Movement. The challenge would then rest with the technologists to produce economical, safe technologies; I would hope the technologists have more success in responding to this challenge than they have had in responding to the challenge of the Appropriate Technology Movement.

5.4. SAFE TECHNOLOGICAL SYSTEMS: REFLECTIONS ON THE CONDITIONS FOR THEIR SOCIAL ACCEPTABILITY

Harry Otway
Joint Research Centre, Commission of the European Communities, Ispra, Italy

Abstract

Engineers have always proposed only those technologies they believed to be "safe". Nevertheless, some technologies have encountered public opposition which has delayed implementation or even blocked it completely; other, emerging, technologies face similar prospects. Since earlier claims of safety on the part of experts were either not believed, or safety was not even the main cause of concern, it seems unlikely that public groups will be convinced by assertions that, this time, the technologies in question are "inherently safe". This paper uses insights gained from earlier social science research on public perceptions of risky technologies as background for a discussion of how technical, institutional and procedural aspects of technologies might be designed to improve their social acceptability.

Background

There is a general consensus that "risk" expresses some combination of the probability of an adverse event and the magnitude of the consequences of that event. Although this definition is useful for engineering calculations, it is insufficient for the broader and more complex questions of societal risk management. Common sense, lay definitions of risk seem to be related more to the magnitude of loss than its probability. This is not unreasonable; risk is an abstraction which, despite the titles of research papers suggesting the contrary, cannot be "perceived".

Rayner and Cantor (1) view risk as a polythetic concept, that is, one composed of a chain of items, each of which shares some features with its neighbours on either side, but without any single essential feature common to all of them. In practical terms, we can liken this to a queue of people, each of which has his or her own definition of risk. Each person's definition overlaps that of the people standing immediately next to him, but the definitions of the people at the two ends of the queue might have nothing in common with each other. (This is reminiscent of the children's game in which a whispered message is passed from one person to the next until, with great amusement, what the last person understood is compared to what the first person really said.) Confusion of this sort seems typical of

many public debates, ostensibly about risks to health and safety, where engineering assurances about probability and magnitude of loss do not correspond to the concerns of public groups opposed to the technology; as we pass along the queue, not only does the emphasis on placed on probability of loss change, but we also encounter differing opinions about which qualitative attributes of loss should be considered legitimate.

The difference between technical and social definitions may be reflected in a survey of public attitudes toward nuclear power in Italy (2), in which 24% were found to be in favour and 60% opposed. When the question was re-worded for the case of reactors with "demonstrated safety", there was a shift to 35% in favour with 43% opposed. This suggests that, although enhanced safety might help to make nuclear power generation more attractive, it may not be enough to ensure social acceptability.

However this is completely consistent with insights gained from social science research on public perceptions of hazardous technologies. Although this research has used a variety of methods based on different theoretical perspectives, a broad set of general principles has emerged to describe (not prescribe) how normal people integrate information and experience to form attitudes. It is generally agreed that beliefs about environmental damage, health and safety (hereinafter called measurable losses) are just some of the many beliefs that underlie attitudes towards risky technologies.

Results of Empirical Studies

There is now a large body of empirical research on public attitudes and beliefs related to risky technologies (3). In addition to perceptions of measurable losses and economic benefits, a number of qualitative attributes of losses (and the technologies that cause them) have been found to cause technologies to be perceived as being more dangerous than might be indicated by engineering risk estimates. If these factors, mostly related to individual psychology, are included in a person's definition of the risk concept, they will likely increase his awareness of danger:

- the risk exposure is involuntary, as opposed to risk-taking with consent, eg, a skier's exposure is voluntary while most environmental hazards are involuntary;

- there is no personal control over the hazard eg, a skier has skill-based control, an airline passenger none;

- there is uncertainty about the outcome of the exposure, eg, the effects of exposure to many chemicals is not well known, even to experts;

- there has been no personal experience of the situation in the past--fear of the unknown increases anxiety;

- the risk-causing agent cannot be detected by the human senses, eg, is odourless, invisible, silent, making it impossible for people to know if they have been exposed or not;

- the loss is the result of technical failure, which people expect should not be allowed to happen, as opposed to natural hazards which we do not expect to control (this has been empirically found to be a source of stress, see ref 4);

- there can be delayed effects of the risk exposure even after direct exposure has ceased, eg, the risk of crossing the street is over once the street has been successfully negotiated, the risks of radiation continue for years after the actual exposure is over (this has been observed as a source of stress in those who believed they were exposed to radiation in the Three Mile Island Accident, ref 5);

- future generations can be affected by present exposure--a threat to a basic human need to assure the continuation of species;

- the benefits of the technology are not highly visible, or are received by a group other than the one at risk--a question of the fairness of the principles and procedures used to allocate risk;

- there is a possibility of large, catastrophic accidents which could affect the entire community--this fear is not just a psychological quirk, the Chernobyl and Bhopal accidents graphically demonstrated both the potential magnitude of accidents and the problems of crisis management.

A technology may also be perceived as having social and political outcomes associated with its use. The following beliefs been found to either enhance or diminish acceptability, depending on the values of those doing the perceiving; some of them have contributed negatively to the attitudes of those opposing technologies, but positively to those of supporters:

- the technology will lead to the increased centralisation of political and economic systems;

- it will cause increased dependence on small groups of technical elites;

- it will increase GNP;

- it will create new jobs;

- it will require strict physical security measures or special police powers;

- it will enhance national prestige;

- it will allow independence of foreign suppliers;

- the benefits provided are thought to be frivolous rather than socially necessary;

- the technology also has potential military applications.

Some Generalisations

Taking a step back from these lists of specific attributes that can influence perception and acceptance of technologies, we can list a few broad, general findings that come from this research that are also supported by psychological theory.

- In principle, lists such as these cannot be exhaustive. The attributes that people use to characterise a technology can be anything that they have come to associate with it.

- It follows from this that public attitudes toward different technologies can be determined by different attributes.

- Not only might the salient attributes vary from one technology to the next, but their relative importance also depends on the particular technology in question, which group is interviewed and when.

- Finally, risk, whether estimated or even taken from statistical tables, is usually only one determinant of technology acceptability. Technologies are judged, and accepted or rejected, on the basis of a complete package of beliefs about them, not just on risks alone. (Think of debates on the social acceptability of large computer systems where discussion tends to focus on aspects such as privacy, social change, working conditions; mortality risk is hardly an issue here, although many applications of the technology are controversial.)

Some Observations

Despite our assertions that risk, per se, may not be as important to public attitudes as is sometimes thought, public debates do often seem to centre on discussions of risks. Looking at these debates more closely in the light of the research results summarised earlier leads to the following observations:

- Technical people, consistent with their training, tend to define "the system" in technical terms (eg, ref 6) and risk in terms of those losses that are measurable and insurable.

- Lay people seem to define "the system" globally, including its interactions with social and cultural systems, and thus define risk as including how they expect the system to impact on their lives.

- Both definitions are "rational" within their own frames of reference--that is, they are consistent with the goals, interests and responsibilities of the people holding them.

- Many public hearings, etc, are structured by those sympathetic to the technical definition of system and risk, thus lay participants may be forced to frame their arguments in those terms.

- Therefore debates about risk are often carried out with the parties implicitly using different definitions of terms.

- Once attitudes are established they are relatively stable because existing beliefs serve to mediate and filter new information. What appear to be rapid swings in public attitudes are often cases of image formation, where a new product or political candidate appears on the scene and attitudes respond rapidly as new information is assimilated.

- Attitudes are most sensitive to new information that can be verified by first-hand experience, and can also be influenced by events external to the technology in question (eg, an oil crisis, international tensions).

- Improved safety cannot be verified by lay people, thus is not likely, by itself, to ensure social acceptability.

Implications for Inherently Safe Systems

The main point of the argument so far is that physical risk alone is clearly not the only determinant of how technologies are perceived and that, since improvements in safety cannot be independently verified by lay people, they may not even cause large changes in how risk itself is perceived. Thus I think it reasonable to assume that reducing physical risks by changes in design philosophies and physical plant are unlikely to have a large enough effect on public attitudes to create a climate for the acceptance of technologies previously rejected. This is especially true when we reflect on the fact that acceptance problems of the past were partly caused precisely because the public did not find expert assurances credible.

In the following paragraphs I will speculate on how a system might look if we took into consideration other, non-safety factors which influence public concerns about a technology. I will not pay attention to questions of technical and economic feasibility, and will consider the institutions and procedures associated with the technology as well.

To begin with, we might imagine that systems could be made smaller, and thus more likely to be perceived as providing benefits for the same community that must bear the risks. Smaller, decentralised systems would also be responsive to the concerns of those worried about increasing centralisation and

depersonalisation caused by larger technologies. Although smaller systems could result in the loss of economies of scale, this might be offset if siting were less controversial. A smaller plant, sited quickly and with little uncertainty about the outcome of the site application might, in the long run, be cheaper than a large plant of an economical scale affected by interminable delays and high uncertainty.

We can also speculate on how institutions and procedures could be changed to respond to public concerns. The debates that surround decision making for the siting of hazardous technologies essentially reflect the political rejection of technically dominated perceptions and policies. One suggestion for improving the credibility of experts and of technical information is to provide increased social access to them. This could take the form of power sharing where the technical system, now of a scale to supply local needs, is designed, sited and managed by a group composed of technical experts and managers from the corporate sponsor and representatives of the community. This sort of approach could help to ensure citizen familiarity with both technical process and people and could help to modify perceptions of the voluntariness of exposure and the control over the outcome of accidents, assuming that participation in crises management teams is also foreseen.

Recent research has begun to explore approaches in which professionals do not alone make the critical judgements about what are the significant attributes of decisions and how risks should be managed. These approaches (eg, 7), based on models of mediated dispute resolution, focus analysis and discussion on a wider range of concerns than are usually accepted by technical experts and allow the perceptions of both lay and technical publics to become a legitimate part of decision making. They seek to legitimate lay involvement and to convert conflicts into relationships where public officials and local residents seek to produce together mutually acceptable outcomes (see also Kunreuther, this volume).

These are new ideas, and experience is needed to determine their feasibility; obviously they cannot be effective if they are never tried. Lay people do appear to act rationally in siting disputes in the sense of working effectively to promote their own interests (8), and experience of user participation in the design of informatics systems has also been encouraging. In the final analysis, the level of actual citizen control may be far less important than the trust that can be developed through working together. Still, even if power sharing schemes did succeed in creating a more receptive climate, it is not obvious that they would actually result in lower risks or better management.

Communications is a relatively new theme in risk research. This is partly in response to recent legislation, in both Europe and the USA, which requires that people exposed to industrial hazards be informed of the risks and how they should behave

should an emergency occur. It is also due in part to the awareness that the confidence and sense of consensus needed to resolve acceptance problems can only be helped by effective communications between technical and lay groups.

There is a great deal of research being undertaken now to better understand what makes for effective communications (9). However, as a beginning, one can make some general recommendations for improving communications about technical matters:

- Start communications efforts early, before designs have been completed and sites selected.

- Listen to lay people--communication is a two-way street.

- Try to understand what people are telling you and acknowledge the validity of their perceptions for them. (The US EPA experience of communications about the risks from arsenic emissions from the Tacoma smelter suggested that formal educational activities had no effect on public risk judgements, but that informal aspects of communication did, eg, the demonstration that public concerns were being taken seriously and that the public were considered capable of contributing to risk management activities (10).)

- Always be honest, balanced and complete. People are exposed to a wide variety of communications every day in the form of advertising and have become rather skilled at detecting and rejecting one-sided and self-serving messages.

- Don't claim too much for improved safety--something unforeseen will inevitably happen and the damage to public confidence will be proportional to the claims made. Knowledge is always limited and every new discovery also reveals new areas of ignorance.

Summary and Conclusions

The idea of improving industrial safety through inherently safe design features, such as passive safety devices or self-limiting processes is a good one. Unfortunately, it is only loosely coupled to the problem of the social acceptability of these systems. To begin with, most systems proposed have always been claimed to be safe and, sometimes, experience has cast doubt on these claims. Further, risk perception research has rather clearly shown that risk, as such, is only one of many determinants of how people perceive technologies and judge their acceptability. Indeed, the relative position of safety in the social judgement of acceptability is illustrated by the fact that society has chosen to accept a great number of inherently unsafe technologies, eg, the automobile.

Some thought should be given to supplementing enhanced safety with innovative ways of increasing public involvement in deci-

sion making and risk management. This is something which could be the subject of experiments, perhaps first at the community level. Improved communications is an integral part of this. These efforts, however, are likely to be more successful for "new" technologies which are just emerging as public policy issues, such as bio-technology, than for older technologies were battle lines are established and positions entrenched, such as nuclear power. For the latter case, the main problem is one of establishing credibility--where credibility has been damaged through past behaviour and confidence undermined by accidents that experts had said couldn't happen, this is a difficult, long-term task.

References

1. Rayner, Steve and Robin Cantor, How fair is safe enough? The cultural approach to societal technology choice, Risk Analysis 7, 3-9, 1987. In attitude theory, the idea of a polythetic concept could be understood as different beliefs (subjective probabilities linking the attitude object to attributes used to describe it) being salient (relevant) for different people. They might overlap from one person to the next, but not necessarily so. See M Fishbein and I Ajzen, Belief, attitude, intention and behavior: An introduction to theory and research, Reading, Addison-Wesley, 1975.

2. Umberto Columbo, Private Communication, Salzburg Seminar 257, March 1987. This study also explored other determinants of acceptability, such as the difference between national policy and local siting, economic aspects, etc.

3. Technological risk perception research began more than 10 years ago and, by now, there are literally hundreds of publications on this topic. There have been two main approaches taken. One was to have respondents rate a large number of different technologies on the same set of attributes to see how perceptions of the technologies differed in the resulting two-dimensional factor space, eg, B Fischhoff, P Slovic, S Lichtenstein S Read and S Combs, How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits, Policy Sciences 9, 127-152, 1978. The other approach was to study attitudes towards specific technologies in depth (eg, nuclear power or alternative energy systems) as a function of the underlying beliefs and values, eg, H Otway and M Fishbein, The determinants of attitude formation: An application to nuclear power, IIASA-RM-76-80, 1976; H Otway and M Fishbein, Public attitudes and decision making, IIASA-RM-77-54, 1977.

4. A Baum, R Fleming and L Davidson, Natural disaster and technological catastrophe, Environment and Behaviour 15, 333-54, 1983.

5. India Fleming, A Baum and Ann Israel, Chronic stress in natural and human-made disasters, Journal of Clinical and Community Psychology, in press, 1987.

6. K Thomas, E Swaton, M Fishbein and H Otway, Nuclear energy: The accuracy of policy maker's perceptions of public beliefs, IIASA-RR-80-18, 1980.

7. L Susskind and A Weinstein, Towards a theory of environmental dispute resolution, Boston College Environmental Affairs Law Review, 9, 311-357, 1980.

8. M O'Hare, L Bacow and D Sanderson, Facility Siting, New York, Van Nostrand, 1983.

9. V Covello, D von Winterfeldt and P Slovic, Risk communication: A review of the literature, Risk Abstracts 4, 171-182, 1986.

10. T Earle and G Cvetkovich, Failure and success in public risk communication, presented at the Air Pollution Control Association Conference, Vancouver, November, 1985.

APPENDICES

International Institute for Applied Systems Analysis (IIASA)
in collaboration with the
International Atomic Energy Agency (IAEA)

Task Force Meeting

TECHNOLOGICAL RISK IN MODERN SOCIETY

Laxenburg, March 18-20, 1987

Final List of Participants

Amendola, Dr. Aniello
Systems Engineering & Reliability Division
CEC Joint Research Center
I-21020 Ispra, Varese
ITALY
Phone: 0039 332 789208
Fax: 0039 332 789001
Telex: 380042/380058

Bainbridge, Dr. Lisanne
Department of Psychology
University College London
26 Bedford Way
London
UNITED KINGDOM
Phone: (01) 387 7050 x5399
Telex: 28722

Birkhofer, Prof. Dr.-Ing. E. H. Adolf
Geschäftsführer
Gesellschaft für Reaktorsicherheit (GRS) mbH
Forschungsgelände
D-8046 Garching
FRG
Phone: 089 32004100
Telex: 5215110

Costa-Ribeiro, Mr. Carlos
Executive Director
Centro de Tecnologia Promon
Caixa Postal 1798
Praia do Flamengo, 154
Rio de Janeiro, RJ 22210
BRAZIL
Phone: (021) 205-0112
Telex: 2123338 prom br

Demin, Prof. V.
Senior Researcher
Institute of Atomic Energy
Ulitsa Kurchatova 46
Moscow
USSR

Dickerson, Dr. Marvin Hubert
Atmospheric & Geophysical Sciences Division (L-262)
Lawrence Livermore Lab
University of California
P.O. Box 808
Livermore, CA 94550
USA
Phone: (415) 422-1806
Telex: 910-386-8339 uclll lvmr

Dynes, Prof. Russell
Department of Sociology
University of Delaware
Newark, Delaware 19716
USA
Phone: (302) 451-8233
Telex: 709985 univdel

Faure, Mr. Jacques
Contrôleur Général
Direction de l'Équipement
Électricité de France
22 et 30 Avenue de Wagram
75382 Paris Cedex 8
FRANCE
Phone: 47.64.70.00 or
47.64.88.58
Fax: 47.64.71.10
Telex: 640515 edf equip F

Hayns, Dr. Michael
Head, Nuclear Safety Technology Branch
UKAEA/SRD
Wigshaw Lane, Culcheth
Warrington, Cheshire WA3 4NE
UNITED KINGDOM
Phone: 0925 31244 x4241
Telex: 629301

Hohenemser, Dr. Christoph
Professor of Physics
Clark University
Worcester, MA 01610
USA
Phone: (617) 793-7175

Ikeda, Prof. Saburo
Center for Technology, Environment and Development (CENTED)
Clark University
950 Main Street
Worcester, MA 01610
USA
Phone: (617) 793-7375
Telex: 951829 CENTED Wor

OR Home Institute:
University of Tsukuba,
Institute of Socio-Economic Planning
Sakura, Ibaraki 305
JAPAN
Phone: 0298 53 5182
Telex: 3652580 untuku j

Keeney, Dr. Ralph
(Professor of Systems Science
University of Southern California)
Mailing address:
101 Lombard Street, Suite 704W
San Francisco, CA 94111
USA
Phone: (415) 433-8338

Krett, Dr. Vasil
Director
Nuclear Research Institute
Rez
CZECHOSLOVAKIA
Phone: (Prague) 844772
Telex: UJV 122626

Kröger, Dr. W.
Institute for Nuclear Safety Research (ISF)
Kernforschungsanlage Jülich
P.O. Box 1913
D-5170 Jülich
FRG
Phone: 02461 615336

Kuzmin, Prof. I.
Senior Researcher
Institute of Atomic Energy
Ulitsa Kurchatova 46
Moscow
USSR

Lagadec, Dr. Patrick
l'Ecole Polytechnique
1, rue Descartes
75230 Paris
FRANCE
Phone: 46.34.32.42

Larichev, Prof. O.
Institute of Systems Studies
Academy of Sciences
Moscow
USSR

Midden, Dr. Cees
Energy Research Foundation
P.O. Box 1
1755 ZG Petten
NETHERLANDS
Phone: 02246 4347
Telex: 57211

Moray, Prof. Neville
Department of Industrial Engineering
University of Toronto
Toronto, M5S 1A4
CANADA
Phone: (416) 978-6420
Telex: 06-21819 ut eng tor

Neumann, Dr. Jan
Scientific Secretary
Energy Commission
Czechoslovak Academy of Sciences
Seidlova 471
14018 Praha 4 - Lhotka
CSSR
Phone: 434722

Niehaus, Dr. Friedrich
Head, Reliability and Risk A.
IAEA, Division of Nuclear Safety
P.O. Box 100, B 07 Room 39
A-1400 Wien
AUSTRIA
Phone: 2360-2036
Fax: 2301-84
Telex: 1-12645

Nishiwaki, Dr. Yasushi
Atomic Energy Research Institute of Kinki University
Higashi-Osaka City,
Osaka
JAPAN

Peters, Dr. Hans Peter
Kernforschungsanlage Jülich
P.O. Box 1913
D-5170 Jülich
FRG
Phone: 02461 615336

Purini, Dr. Roberto
I.F.A.-C.N.R.
Ple L. Struzo 31
00133 Rome
ITALY

Rasmussen, Prof. Jens
Risk Research Establishment
P.O. Box 49
DK-4000 Roskilde
DENMARK
Phone: 45 02.371212
Fax: 45 02.360609
Telex: 43116 D

Schönhofer, Dr. Franz
Abteilung Strahlenschutz
Umweltbundesamt
Berggasse 11
A-1090 Wien
AUSTRIA
Phone: 34.54.18 or 31.91.69
Fax: 34.03.99

Slater, Dr. D.
Director
Technica
355 East Campus View Blvd.
Columbus, OH 43085
USA
Phone: (614) 848-4000

Sztanyik, Mr. Laszlo
Director-General
Frederic Joliot Curie
National Research Institute for Radiobiology
P.O. Box 101
H-1775 Budapest
HUNGARY
Phone: 0036 1 385954
Telex: 225103 osski h

van Kuijen, Mr. C. J.
Deputy Director of Administrative Affairs
Dept. Head for Risk Evaluation
Ministry of Housing, Physical Planning & Environment
Dokter v.d. Stamstraat 2
Box 450
2260 MB Leidschendam
NETHERLANDS
Phone: 070 209367 3136
Telex: 32362 vromi nl

Wahlström, Prof. Björn
Technical Research Centre of Finland
Vuorimiehentie 5
SF-02150 Espoo
FINLAND
Phone: 358 0 456 6400
Fax: 358 0 455 0115
Telex: 123704 vttte sf

Weidlich, Dr. Helmut
Gesellschaft für Reaktor-
sicherheit
Forschungsgelände
D-8046 Garching
FRG
Phone: 089 32004 100
Telex: 521 5110

Wölk, Dr.
KWU Erlangen, Abtlg. VPE11
Postfach 3220
D-8520 Erlangen
FRG
Phone: 09131 184460

Woodard, Dr. Keith
Pickard, Lowe & Garrick, Inc.
1615 M Street, N.W., Suite 730
Washington, D. C. 20036
USA
Phone: (202) 659-1122
Fax: (202) 296-0774

Woods, Dr. David
Westinghouse R & D Center
1310 Beulah Road
Pittsburgh, PA 15235
USA
Phone: (412) 257-2745
Telex: 703669 westrd pgh

****

From:
International Atomic Energy
Agency (IAEA)
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna
AUSTRIA
Phone: 43 222 2360
Fax: 43 222 230184
Telex: 1-12645

Prof. L. Konstantinov, Deputy
Director General
Dr. J. Ahmed
Mr. E. Asculai
Prof. Y. Nishiwaki
Mr. A. Novegno
Dr. Anneli Salo
Dr. E. Swaton

From:
International Institute for
Applied Systems Analysis
A-2361 Laxenburg
AUSTRIA
Phone: 43 (02236) 71521.0
Fax: 43 (02236) 71313
Telex: 079137 iiasa a

T. H. Lee, Director
B. Segerståhl, Deputy Director
V. Kaftanov, Deputy Director
M. Antonovsky
G. Krömer
F. Mautner-Markhof
J. Bayer-Linneroth

International Institute for Applied Systems Analysis

Task Force Meeting

SAFE TECHNOLOGICAL SYSTEMS

Laxenburg, May 11-12, 1987

Final List of Participants

Ale, Dr. B. J. M.
Environmental Protection
Ministry of Housing, Physical Planning & Environment
Dokter v.d. Stamstraat 2
Box 450
2260 MB Leidschendam
NETHERLANDS
Phone: 070 209367 3128
Telex: 32362 vromi nl

Cachera, M. Pierre
Chargé de Mission
Direction de l'Équipement
Électricité de France
22 et 30 Avenue de Wagram
F-75008 Paris
FRANCE
Phone: 47.64.88.52
Fax: 47.64.72.66
Telex: 640515 F

Finzi, Dr. Sergio
Director, Nuclear Safety Research, Commission of the European Communities
200, rue de la Loi
B-1049 Brussels
BELGIUM
Phone: 0032 2 2359177
Telex: 21877 COMEU B

Gränicher, Prof. Dr. H.
Director, Eidgen. Inst. f. Reaktorforschung
CH-5303 Wuerenlingen
SWITZERLAND

Hadas, Mr. Janos
Chief Engineer
Informatics Center of the Hungarian Industry
Budapest
HUNGARY

Harms, Prof. A. A.
Dept. of Engineering Physics
Faculty of Engineering
McMaster University
Hamilton, Ontario L8S 4M1
CANADA
Phone: (416) 525-9140, x4545
Telex: 061-8347

Innerhofer, Dipl.-Ing. Hans
Abteilung für Reaktorsicherheit
Österreichisches Forschungszentrum
Seibersdorf GmbH
A-2444 Seibersdorf
AUSTRIA
Phone: (02254) 80, ext. 2700

Jihui, Qian
Senior Engineer
Adviser & First Secretary
Permanent Mission of the People's Republic of China to the Int'l Atomic Energy Agency
Steinfeldgasse 1 & 3
A-1190 Vienna
AUSTRIA
Phone: 37.48.39

Kröger, Dr. W.
Institute for Nuclear Safety Research (ISF)
Kernforschungsanlage Jülich
P.O. Box 1913
D-5170 Jülich
FRG
Phone: 02461 615336

Kunreuther, Prof. Howard
The Wharton School
Risk & Decision Processes Ctr.
University of Pennsylvania
Philadelphia, PA 19104-6366
USA

Kupitz, Dr. Jürgen
Int'l Atomic Energy Agency
Wagramer Strasse 5
A-1220 Vienna
AUSTRIA
Phone: 2360.2814
Fax: 2301.84
Telex: 1-12645

Ollus, Prof. Martin
Technical Research Centre of Finland
Vuorimiehentie 5
SF-02150 ESPOO
FINLAND
Phone: 358 0 456 6400
Fax: 358 0 455 0115
Telex: 123704 vttte sf

Ostberg, Prof. Gustaf
Engineering Materials
University of Lund
Box 118
S-221 00 Lund
SWEDEN
Phone: (46-46) 10 79 97

Otway, Dr. Harry
CEC Joint Research Center
I-21020 Ispra, Varese
ITALY
Phone: (0332) 789111 (switch)
(0332) 789951 (direct)
Fax: (0332) 789001
Telex: 380042/380058 eur i

Phillips, Dr. D. W.
Nuclear Safety Technology Branch
UKAEA/SRD
Wigshaw Lane, Culcheth
Warrington, Cheshire WA3 4NE
UNITED KINGDOM
Phone: 0925 31244 x4241
Fax: 0925 76 6681
Telex: 629301

Pinchera, Prof. Giovanni Carlo
Direzione Centrale Studi
ENEA
Viale Regina Margherita 125
I-00198 Rome
ITALY
Phone: 06 8528.2426

Schulten, Prof. Dr. R.
Kernforschungsanlage Jülich
Postfach 1913
D-5170 Jülich
FRG
Phone: 02461 615911

Sheng, Mrs. Weilan
Int'l Atomic Energy Agency
Wagramer Strasse 5
A-1220 Vienna
AUSTRIA
Phone: 2360.2811
Fax: 2301.84
Telex: 1-12645

Wacholz, Dipl.Ing. W.
HRB
Postfach 5360
D-6800 Mannheim
FRG
Phone: 0621 451424

Weinberg, Prof. Alvin
Director
Institute for Energy Analysis
Oak Ridge Associated Universities
PO Box 117
111 Moylan Lane
Oak Ridge, TN 37830-0117
USA

Yadigaroglu, Prof. George
Institut für Energietechnik
ETH-Zentrum
CH-8092 Zürich
SWITZERLAND
Phone: 01/2564615 or
01/2564603

From IIASA:
Lee, T. H.
Kaftanov, Vitali
Segerståhl, Boris
Krömer, Gerhard
Linneroth-Bayer, Joanne
Mautner-Markof, Frances
Munn, Ted

International Institute for Applied SystemsAnalysis (IIASA)
in collaboration with the
International Atomic Energy Agency (IAEA)

Task Force Meeting

TECHNOLOGICAL RISK IN MODERN SOCIETY

Laxenburg, March 18-20, 1987
Final Agenda

First Day (March 18)

8:30- 9:00	Registration
9:00- 9:15	Welcome address (T. Lee, IIASA)
9:15- 9:30	Welcome address (L. Konstantinov, IAEA)
9:30-10:00	IIASA's risk activities (B. Segerståhl, IIASA)
10:00-10:15	Organizational remarks (G. Krömer, IIASA)
	Break

1. **REGIONAL RISK MANAGEMENT (ECONOMY)**
Chairman: Dr. F. Niehaus (IAEA)

10:45-11:00	Introduction (F. Niehaus)
11:00-11:20	Risk Management of Potentially Hazardous Industrial Installations (D. Slater)
11:30-11:50	The European Approach to Risk Management (A. Amendola)
12:00-12:20	Decision Criteria for Siting of Complex Industrial Facilities (R. Keeney)
	Lunch
14:00-14:20	Emergency Planning and Preparedness (M. Hayns)
14:30-14:50	Risk Management in the Netherlands (C. van Kuijen)
	Break
15:30-15:50	Advanced Safety Criteria for Nuclear Power Plants: Proposal to Limit Catastrophic Releases (W. Kröger)
15:50-	Discussion

Second Day (March 19)

2. SPECIAL SESSION
Chairman: Prof. V. Kaftanov (IIASA)

9:00- 9:30	Chernobil Accident: Measures and Lessons (Video, I. Kuzmin)
9:30-10:10	Crisis Management (Video, P. Lagadec)
	Break
11:00-11:20	Industrialization, Infrastructure, Risk Management: The Case of the Cubatao Area in Brazil (C. Costa-Ribeiro)

3. MAN-MACHINE INTERACTION (TECHNOLOGY)
Chairman: Prof. B. Wahlström (Technical Research Centre of Finland)

11:30-11:50	Introduction (B. Wahlström)
12:00-12:20	Social and Economic Aspects of System Safety (R. Dynes)
	Lunch
14:00-14:20	Human Error Analysis (J. Rasmussen)
14:30-14:50	New Interface and Control Technologies as Sources of Difficulty for the Human Operator (L. Bainbridge)
15:00-15:20	Problem Solving in Complex Worlds (D. Woods)
	Break
16:00-16:20	The Design of Operating Procedures (N. Moray)
16:30-16:50	Application of Fault Tree Analysis to the Bubbling Depressurization System of a Nuclear Power Plant with the VVER-440 Reactor (V. Krett)
16:50-	Discussion

Third day (March 20)

4. MANAGEMENT OF ENVIRONMENTAL CONSEQUENCES
Chairman: Prof. M. Antonovsky (IIASA)

9:00- 9:20	Introduction (M. Antonovsky)
9:30- 9:50	Atmospheric Dispersion Models (M. Dickerson)
10:00-10:20	Management of the Consequences Following the Chernobil Accident in Austria (F. Schönhofer)
	Break
11:00-11:20	Marginal Effectiveness of Safety Costs (I. Kuzmin)
11:30-11:50	Methodological Problems of Decision Alternatives Comparison and Risk Factors (O. Larichev)
12:00-12:20	The General Indicator of Risk Analysis (V. Demin)
	Lunch
14:00-14:20	Environmental Aspects of Nuclear Power (L. Sztanyik)

5. CONCLUDING SESSION
Chairman: Prof. B. Segerståhl (IIASA)

14:30-14:50	Technological Risk and the Policymaker (J. Neumann)
15:00-15:20	Summary and discussion, session 1
15:20-15:40	Summary and discussion, session 2
15:40-16:00	Summary and discussion, session 3
16:00-16:30	Closing remarks

International Institute for Applied Systems Analysis

Task Force Meeting

SAFE TECHNOLOGICAL SYSTEMS

Laxenburg, May 11-12, 1987
Final Agenda

First Day (May 11)

8:30- 9:00	Registration
9:00- 9:15	Welcome address (T. Lee, IIASA)
9:15- 9:30	IIASA's risk activities (B. Segerståhl, IIASA)
9:30- 9:45	Organizational remarks (G. Krömer, IIASA)
	Break

SESSION I: TECHNICAL CONCEPTS
Chairman: Dr. W. Kröger (Kernforschungsanlage Jülich)

10:20-10:30	Introduction (W. Kröger)
10:30-10:50	Hypothetical Accidents of High-Temperature Reactors and their Implications (R. Schulten)
11:10-11:30	The Inherent Safety Characteristics of the HTR-500 Reactor Plant (W. Wacholz)
11:50-12:10	Safe Technological Systems by the Intermediate State Approach (H. Gränicher)
	Lunch
14:00-14:20	A Dynamic Basis for Inherently Safer Chemical and Nuclear Reactors (M. Harms)
14:40-15:00	Safety Principles for Advanced Plant (D. Phillips)
15:00-15:30	Summary and Discussion, Session I
	Break

SESSION II: GENERAL SAFETY CRITERIA
Chairman: Prof. H. Kunreuther (University of Pennsylvania)

16:00-16:20	Large Scale Accidents and Public Acceptance of Risk (G. Yadigaroglu)
16:40-17:00	Designing for Safety (M. Ollus)

Second Day (May 12)

9:00- 9:20	Outlines of a Managerial Approach to Risk (G. Ostberg)
9:40-10:00	Probabilistic Risk Analysis in the Netherlands (B. Ale)
10:00-10:30	Summary and Discussion, Session II
	Break

SESSION III: POLICIES AND CONSTRAINTS
Chairman: A. Weinberg (Oak Ridge Associated Universities)

11:00-11:20	Reflections on the Safe Technology Movement (A. Weinberg)
11:40-12:00	Safe Technological Systems: Reflections on the Conditions for their Social Acceptability (H. Otway)
	Lunch
14:00-14:20	Role of Compensation and Insurance in Siting Hazardous Facilities. (H. Kunreuther)
14:40-15:00	System Approach to Risk Prevention (J. Hadas)
15:00-15:30	Summary and Discussion, Session III
	Break

CONCLUDING SESSION
Chairman: B. Segerståhl (IIASA)

16:00-17:00	Concluding Remarks of the Session Chairmen and Final Discussion