# Formalized Search Strategies for Human Risk Contributions

## A Framework for Further Development

**Rasmussen, Jens; Pedersen, O. M.**

*Publication date:*
1982

*Document Version*
Publisher's PDF, also known as Version of record

RISØ-M-2351

# FORMALIZED SEARCH STRATEGIES FOR HUMAN RISK CONTRIBUTIONS: A FRAMEWORK FOR FURTHER DEVELOPMENT

J. Rasmussen and O. M. Pedersen

Abstract. For risk management, the results of a probabilistic risk analysis (PRA) as well as the underlying assumptions can be used as references in a closed-loop risk control; and the analyses of operational experiences as a means of feedback. In this context, the need for explicit definition and documentation of the PRA coverage, including the search strategies applied, is discussed and aids are proposed such as plant description in terms of a formal abstraction hierarchy and use of cause-consequence-charts for the documentation of not only the results of PRA but also of its coverage. Typical human risk contributions are described on the basis of general plant design features relevant for risk and accident analysis.

With this background, search strategies for human risk contributions are treated: Under the designation "work analysis", procedures for the analysis of familiar, well trained, planned tasks are proposed. Strategies for identifying human risk contributions outside this category are outlined.

INIS Descriptors: FAILURE MODE ANALYSIS; HUMAN FACTORS; INDUSTRIAL PLANTS; NUCLEAR POWER PLANTS; PROBABILITY; RISK ANALYSIS

UDC 614.8

July 1982

Risø National Laboratory, DK 4000 Roskilde, Denmark

ISBN 87-550-0865-8
ISSN 0418-6435

Risø repro 1982

TABLE OF CONTENTS

## INTRODUCTION

Before turning to the more specific topic of this report, a frame-work for the development of formalized search strategies for human risk contributions, we find it practical to describe that concept of Probabilistic Risk Analysis (PRA) into which the search strategies should be fitted. The following aspects of this background will be discussed in more detail:

- relationships between PRA and Risk Management

- analysability as reflected in nuclear plant design

- typical categories of human risk contributions.

## RELATIONSHIPS BETWEEN PRA AND RISK MANAGEMENT

Fig. 1 illustrates how the risk imposed by an industrial process plant, for instance nuclear power plant, is controlled in two ways: Firstly, by a plant construction based on a risk analysis. Secondly, by Risk Management (RM), i.e., administration of the preconditions of the risk analysis which act as requirements for plant construction and operation. In addition, through the plant lifetime, the preconditions for risk analysis can serve as references for inspections, tests and analyses of operational experience. Decisions made from systematic analysis of abnormal event reports can lead to risk management by means of a "feed-back" control function serving to maintain the designer's safety design targets and to reveal oversights and design errors.

The result of a PRA is a calculated risk figure which, if accepted, covers the "accepted risk". If not accepted, the design has to be modified until acceptance has been achieved.

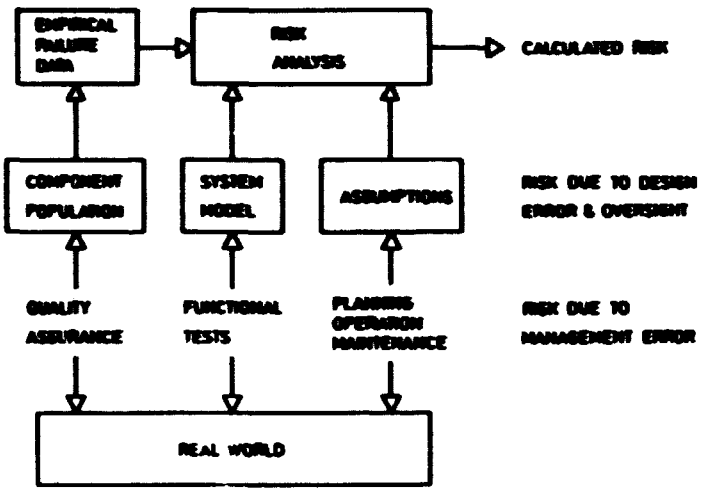



Fig. 1. The risk contributed by the operation of an industrial plant is composed of an accepted risk identified and analysed in advance and a risk due to incomplete analysis and insufficient regard to preconditions for the risk analysis. The latter risk is to be controlled by risk management functions comprising quality control, functional tests, inspection, training and instruction of personnel and including analysis of operational experience as a feedback link. Adopted from Rasmussen, 1982.

Due to incompleteness and errors during performance of PRA, however, an "additional risk" may exist, which is not included in the accepted risk. Contributions to this additional risk can also originate from the fact that the real plant and its operation may depart from the PRA preconditions, e.g.

- because components employed do not belong to the populations providing the PRA failure data

- because the real plant does not correspond with the models of the plant used for PRA

- because the real plant is not operated and maintained according to assumptions made in the PRA.

After the calculated risk has been accepted, the PRA assumptions, models and data sources are to be used as requirements and references for construction, modification and operation during the lifetime of the plant, i.e., as references for the risk management (RM) functions.

Some important means for control in RM in order to make sure that the plant is kept in agreement with these references are

- quality control
- functional tests and inspections
- training of operators
- issuing instructions for operation etc.

In order to close the loop from theory to practice, i.e., from the PRA to the plant in existence, RM should comprise analysis and evaluation of failures and abnormal occurrences by comparison with the references provided by the PRA for deciding whether the abnormalities are included in the accepted risk or whether they indicate circumstances overlooked in the PRA or flaws in risk administration requiring adjustments of practice.

The use of the PRA, including its preconditions as references for RM, obviously requires explicit and user-oriented documen-

tation of the PRA, including preconditions, models and data sources. Particularly, documentation of the coverage of the analysis and search methods, i.e., what has been included in the search for risk contributions, is important for evaluating operating experience as a basis for RM decisions in the feedback control. The well documented model and description of the risk identification strategies of the PRA are necessary to decide whether an individual occurrence falls within the accepted risk and, therefore, should contribute to statistical verification or whether it indicates oversights or operational problems which call for special precautions. In this respect, documentation of coverage is considered more important than attempts to reach high degrees of completeness depending upon the individual creativity of an analyst and, therefore, susceptible to problems with undefined boundaries.

The major part of the human decision making and administrative functions involved in operations management is not accessible to formal analyses with the present state of the PRA art. Errors of management may, however, be significant sources of common mode errors and, therefore, are important candidates for risk management by feed-back control. This feed-back control should not only depend on the formal analysis of abnormal event reports by authorities, but also on the systematic in-house analysis of log-books, repair reports and similar sources by the plant staff itself.

## ANALYSABILITY AS REFLECTED IN PLANT DESIGN

The possibility of accomplishing a credible PRA is supported by particular main design features affecting plant structure and utilizing properties of plant processes in such a way that, viewed from the PRA side, the propagation structure of accidents has limited variability. This means that relevant accident sequences can be ordered and studied collectively in a

fair number of classes. In addition, the accident propagation is subdivided into several subsequent phases by several independent counter-measures, based on different physical principles. This "defense-in-depth" design philosophy makes it possible in a realistic way to achieve very low probability of an accident with moderate requirements to the failure probabilities of each phase under the condition of independence of the different counter-measures. Therefore, the failure probability of the individual phases can be verified empirically, even though this is not the case for the overall risk probability directly.

Additional important ingredients of this design philosophy can be recognized:

- major risk is related to loss of control of well defined energy and material/mass balances. This implies a transport or integration ("pile up") delay which makes early warnings and protective actions possible. This protection is an active defense against accidental chains of events irrespectively of the initial causes.

- the probability of loss of control is, therefore, determined by the frequency of the typical causes together with the reliability of the protective functions, i.e. this category of accidental chains is accessible to quantification due to the feedback effect of the protective functions. As is the case of feed-back loops in general, the overall properties are largely determined by the properties of the feed-back path.

By elaborating on the generalized accident structure presented above and shown in figure 2, we will discuss in some detail typical human risk contributions.

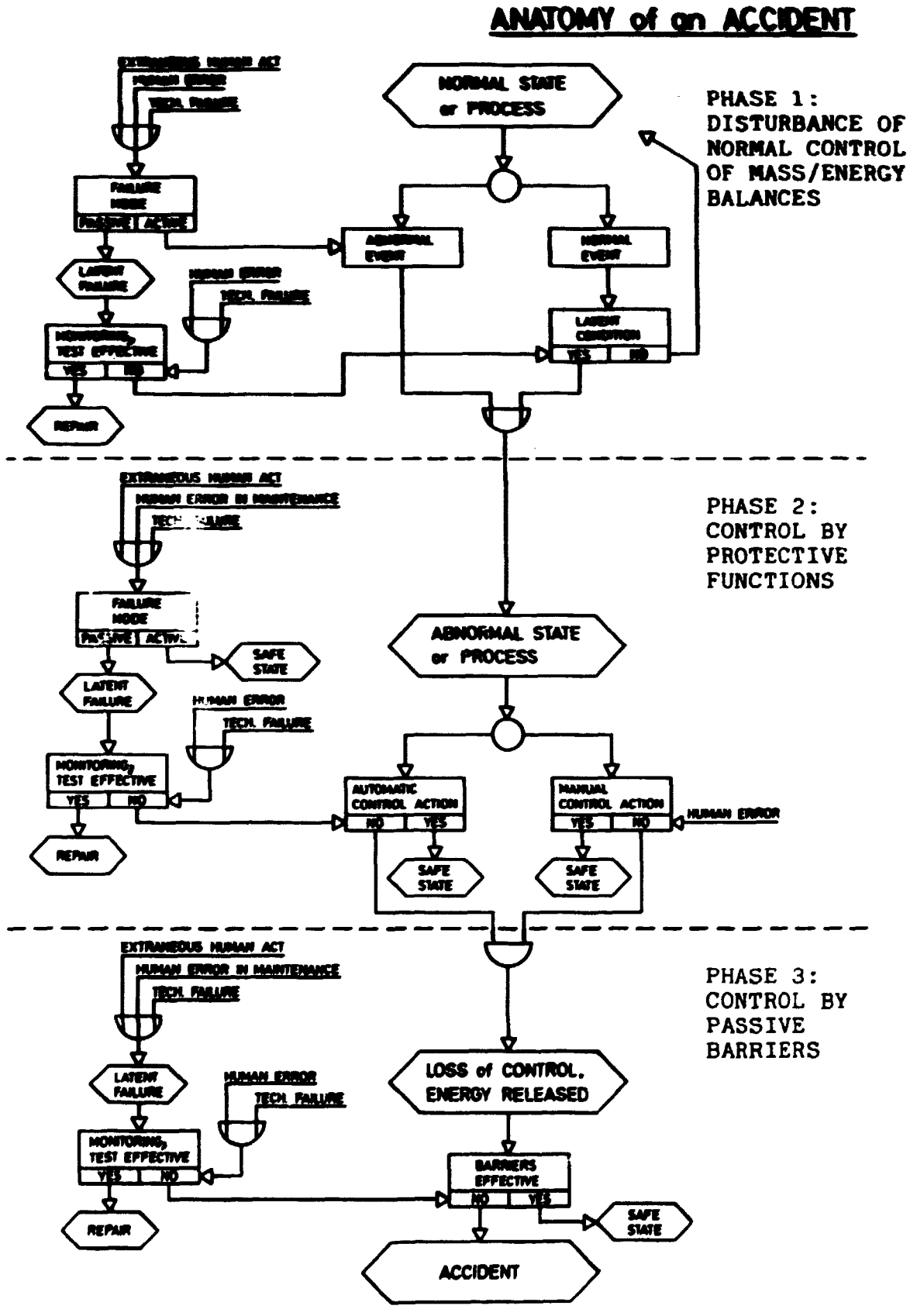



Fig. 2. In nuclear power plants like other industrial processes, major accidents have a common structure of propagation due to the design philosophy applied. Adopted from Rasmussen, 1982.

## TYPICAL HUMAN RISK CONTRIBUTIONS

With reference to the generalized sequence, typical categories of human contributions can be identified.

As causes of accidental chains of events, the simple human errors are generally not very significant for the result of a PRA, because:

- their effects are typically equivalent to technical component failures in the system the human operates.

- their frequencies will not significantly change the overall result based on component data, considering the uncertainty of such data; - or their effects are included in the data on component fault rates.

- human errors performed on active systems are often immediately recognised and corrected.

Special consideration must instead be given the categories of human errors which influence the generic structure of the accident, such as:

- human acts which cause couplings between different phases of Fig. 2. For instance human acts which at the same time initiate a transient and disturb the protective functions.

- errors in the design of protective systems which affect the capability of the protective system to handle a subset of transients. In this category one can also consider errors in work planning and scheduling related to maintenance and refuelling periods.

In all systems based on feedback design principles, the performance is very sensitive to disturbance of the feedback path. For PRA this means that human interaction with the safety

functions is a key problem. Several analytical problems can be identified:

- Estimation of the reliability of protective functions allocated human operators. Since such functions are required under possibly stressing conditions, a meaningful quantitative reliability estimation can only be made under special assumptions regarding interface design and training.

- Estimation of the probability that operators due to misunderstanding or conflicting requirement during emergencies will interfere with the operation of automatic safety functions. Such interference can be caused systematically by high similarity among elements of different tasks or procedures or because the same equipment may be used for different purposes and, therefore, appear in different situations.

- Influence of human reliability on the maintenance, test and calibration of protective systems. Problems are in particular related to systems with extreme technical reliability specifications, such as redundant systems for which complex situations during work planning and maintenance may give rise to "common mode" errors.

## FORMALIZED SEARCH STRATEGIES FOR HUMAN RISK CONTRIBUTIONS

Within the context discussed so far, we will consider a framework for a systematic, proceduralized strategy for identification of the potential for such human interactions with the performance of a technical system, which will significantly contribute to the overall risk and, therefore, must be represented in a risk assessment and risk management system.

Several important features must be required for such a proceduralized strategy:

A) It must refer to an overall probabilistic risk analysis (PRA) possessing a boundary of the set of accident mechanisms covered which can be explicitly stated; i.e., the degree of completeness of the search procedure can be explicitly stated conceptually and the structure within which the search is performed can be documented. To form an acceptable reference for risk management, a known degree of completeness is more important than a high, but undetermined degree. In the approach taken here, we base the PRA on a cause-consequence-analysis which is performed by a systematic search for disturbances of vital material and energy balances. To be systematic, this analysis must cover the system as specified by the plant documentation including for instance piping and instrumentation diagrams and formal operating procedures. The analysis will be systematically documented by graphical cause-consequence-charts (CCCs). This analysis will consider as an integrated part only the human influences in terms of the reliability and immediate risk of those activities which are contained in the formalized and instructed operator tasks; i.e., it includes a work analysis for such activities. Therefore, the PRA must also be supplemented with a separate analysis of the potential for human factors interference from activities and decisions which are not represented in the formal work procedures.

B) This analysis for additional human factors interference must likewise be based on a search strategy which can be explicitly specified with reference to the initial PRA. In this respect we will consider search for human interference which may: 1. Affect the frequency of chains of events in the CCC; 2. Change the structure of the CCC by breaking the recovery paths representing safety functions; or 3. Introduce couplings among otherwise independent events.

C) Effective risk management means use of analysis of event and incident reports for a feed-back control of risk potential outside the coverage of the analytical risk assessment. This in theory gives a way of securing completeness of risk

control. The underlying assumption, however, will be that accidents due to chains of events outside the risk analysis depend on stochastic coincidence of several events which can be identified and controlled individually by means of event and incident analysis, as discussed in the previous section. This assumption appears to be realistic due to the defense in depth philosophy, but must be studied carefully.

In the following paragraphs we will discuss the elements of this approach in more detail and sketch a first attempt to proceduralize the search.

## THE BASIC P.R.A.

The development of a proceduralized PRA based on CCC will be described independently of the present work and published separately. However, a brief discussion of the underlying framework will serve to define the interface to the human factors analysis. The structure of a CCC and a heuristic strategy to develop the charts are discussed elsewhere (Nielsen 1974). Briefly, a cause-consequence-chart is a graphic representation of a family of accidental chains of events which has a "critical event" in common, see Fig. 3.

The critical event in a CCC is the focal point connecting an up-stream tree of causal chains of events with a down-stream tree representing the various relevant consequences. A cause--consequence analysis will in general imply a set of CCCs based on various critical events. The size of this set and the possibility for explicit definition of the boundaries of coverage depends very much on the strategy for the selection of the set of critical events to be applied for the analysis. Therefore, a set of formal rules must be developed to choose a consistent set of critical events.

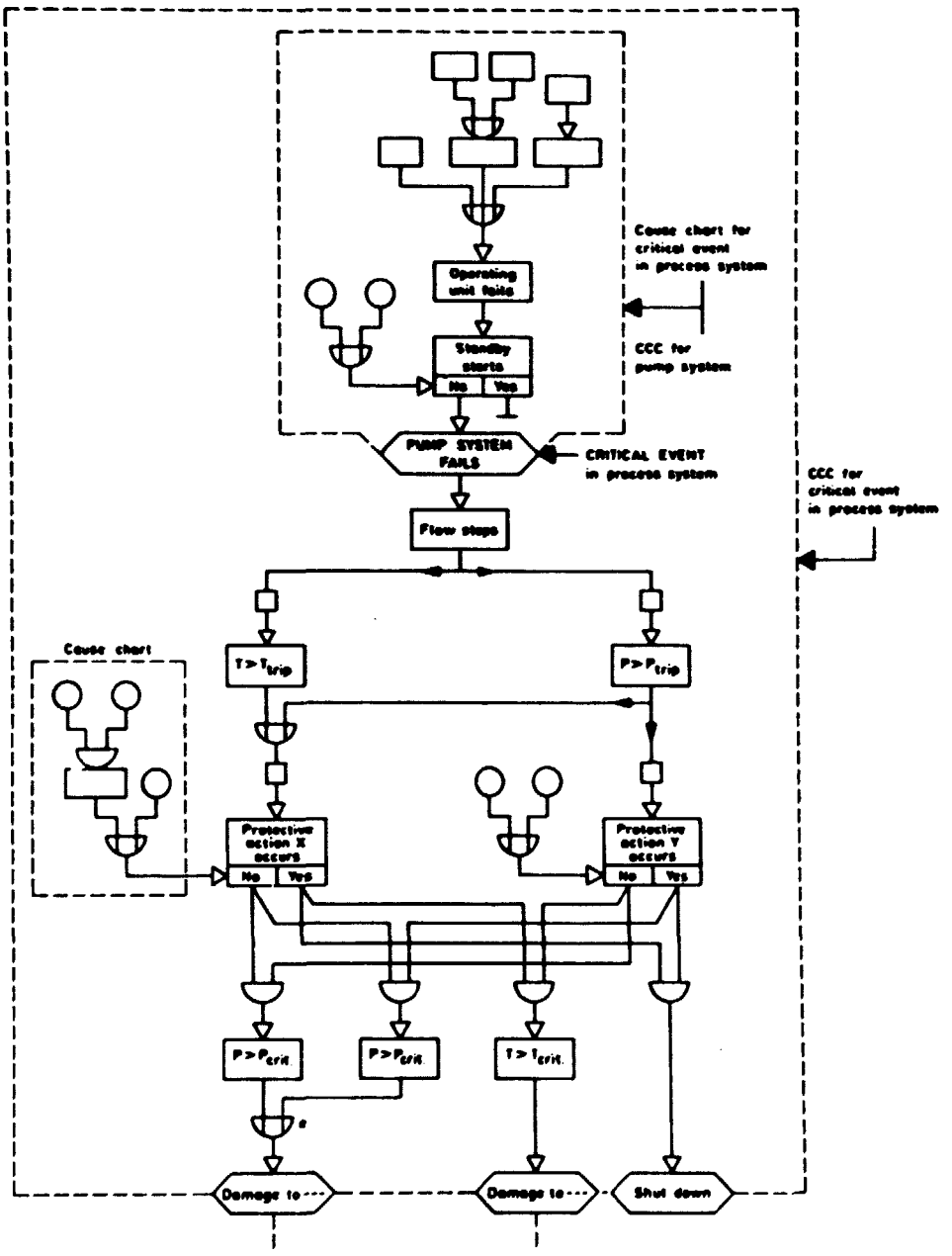



Fig. 3. The structure of a cause-consequence chart for a critical event in a process system. From Nielsen (1974).

Furthermore, a set of principles to guide the path tracing identifying the causal propagation through the system must be formulated for the development of the individual CCCs. As it has been previously argued (Rasmussen, 1982) the documentation of the search strategies behind a risk analysis is a very important part of the result of the assessment. A fault-tree is only a logical combinatorial record of the result of an analysis; a CCC in addition records the causal chains considered; but neither of them represents the identification procedure applied.

The present approach depends on the conception of an accident as a loss of control with accumulated material or/and energy in a system (Rasmussen, 1982) and upon a systematic use of a description of the system in terms of a formal abstraction hierarchy (Rasmussen, 1979a; Rasmussen & Lind, 1982), see Fig. 4.

The strategy for development of CCCs will be a top-down search for disturbances in this hierarchy. The critical events are typically chosen at the level of "abstract function" in terms of the identification of those material and energy accumulations which have potential for unacceptable consequences at the "purpose level", i.e., for plant availability and safety, judged alone by magnitude and content of accumulations, and not at this stage by probability of mechanisms of release.

At the next lower level of "generalized functions", the functions which are intended for control of the accumulations - in the considered operational mode and during emergencies - are identified. These are then the generic functions which should be analysed further for sensitivity to disturbances. The consideration at this general level of functions involved in control of mass and energy accumulations is important since there seems in this way to be a possibility for the systematic analysis of the problem of "system interactions" (which has been identified as a major safety problem, cf. USNRC 1980-1981. A potential source for such interaction of a non-random nature

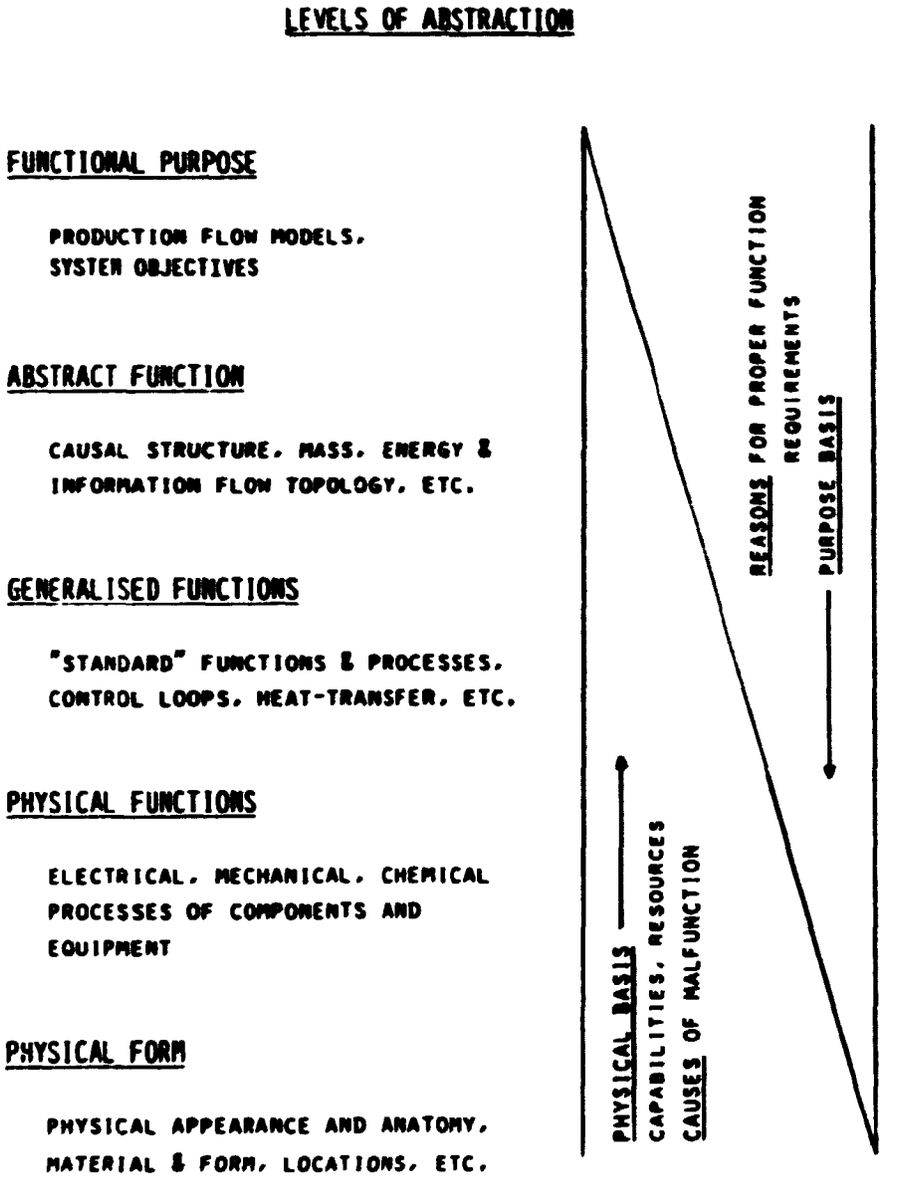



Fig. 4. The abstraction hierarchy used for representation of functional properties of a technical system.

is related to the fact that the same general functions can be served by different physical systems and parts which in addition may serve various other functions. See figure 5 and 6. This lack of one-to-one correspondence between functions and systems requires a stringent analysis involving both levels of descriptions in order to identify the potential for systematic "functions-interference" during certain situations.

From the generalized functions, the implementation in terms of the physical function of related equipment is identified and the bottom-up propagation of changes, faults or disturbances of the equipment is analysed. The search strategy will be a proceduralized iteration among the description of the plant properties as represented by the abstraction hierarchy.

In addition to the strategy, the causal structure of the plant in which the search is performed, must be documented in a stringent way. This not only implies an identification of the plant documentation which is taken as representative, such as P and I diagram, process descriptions, and formal operating procedures, but also that the consistency of the information related to the various levels of the abstraction hierarchy must be documented. For this purpose, application of the mass/energy flow graph representation of the total system as suggested by Lind (1982a, 1982b) seems to be promising. (See also Rasmussen & Lind, 1981, 1982).

In this basic analysis is included only those human activities which are formalised in written work instructions and for which a work analysis as described below is performed. This means that manual protective functions not specified in the formal instructions are not given credit and erroneous human acts not related to those specified activities are not included.

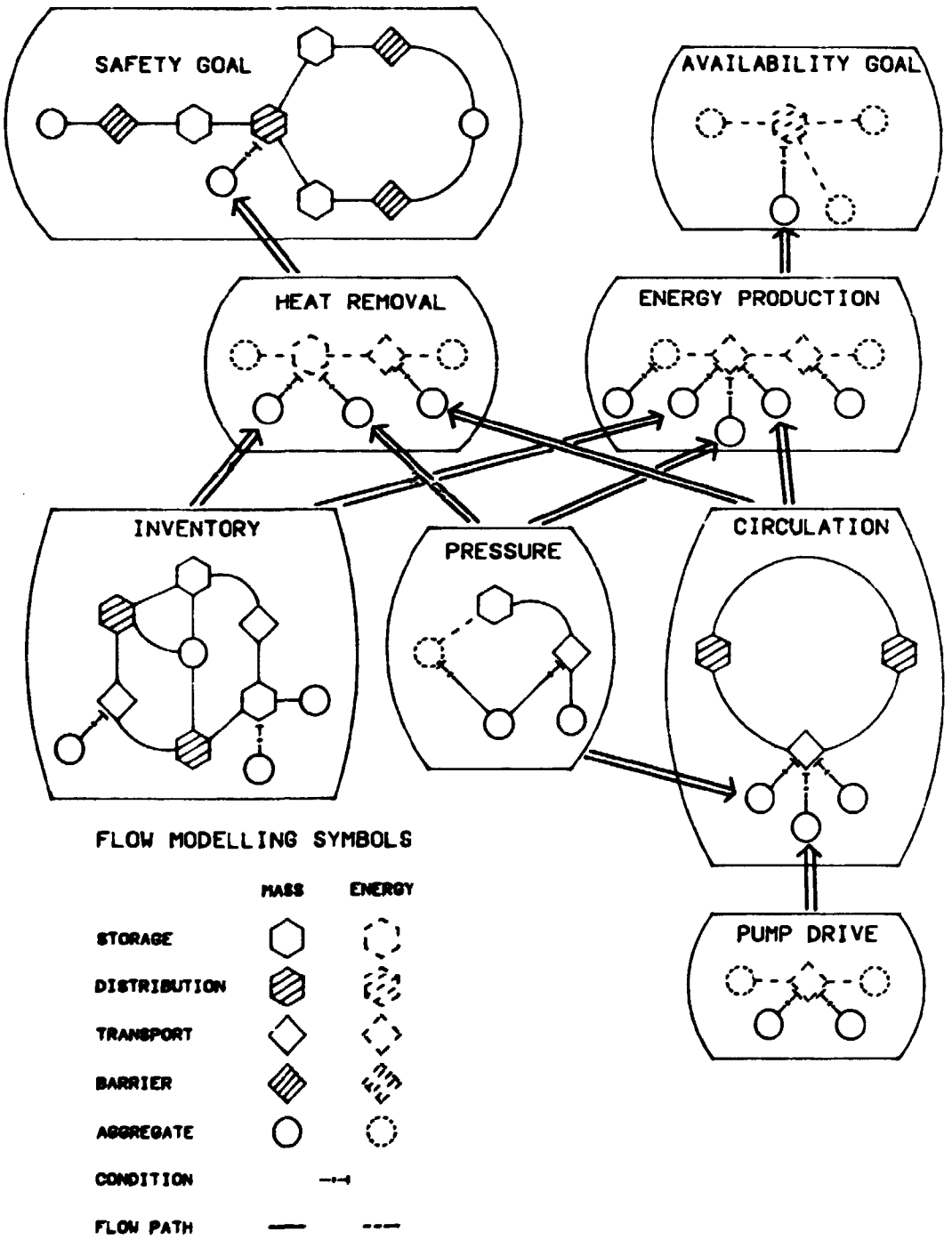



Fig. 5. Multilevel flow model of a nuclear power plant specifying goals and functions. From Rasmussen & Lind, 1982.

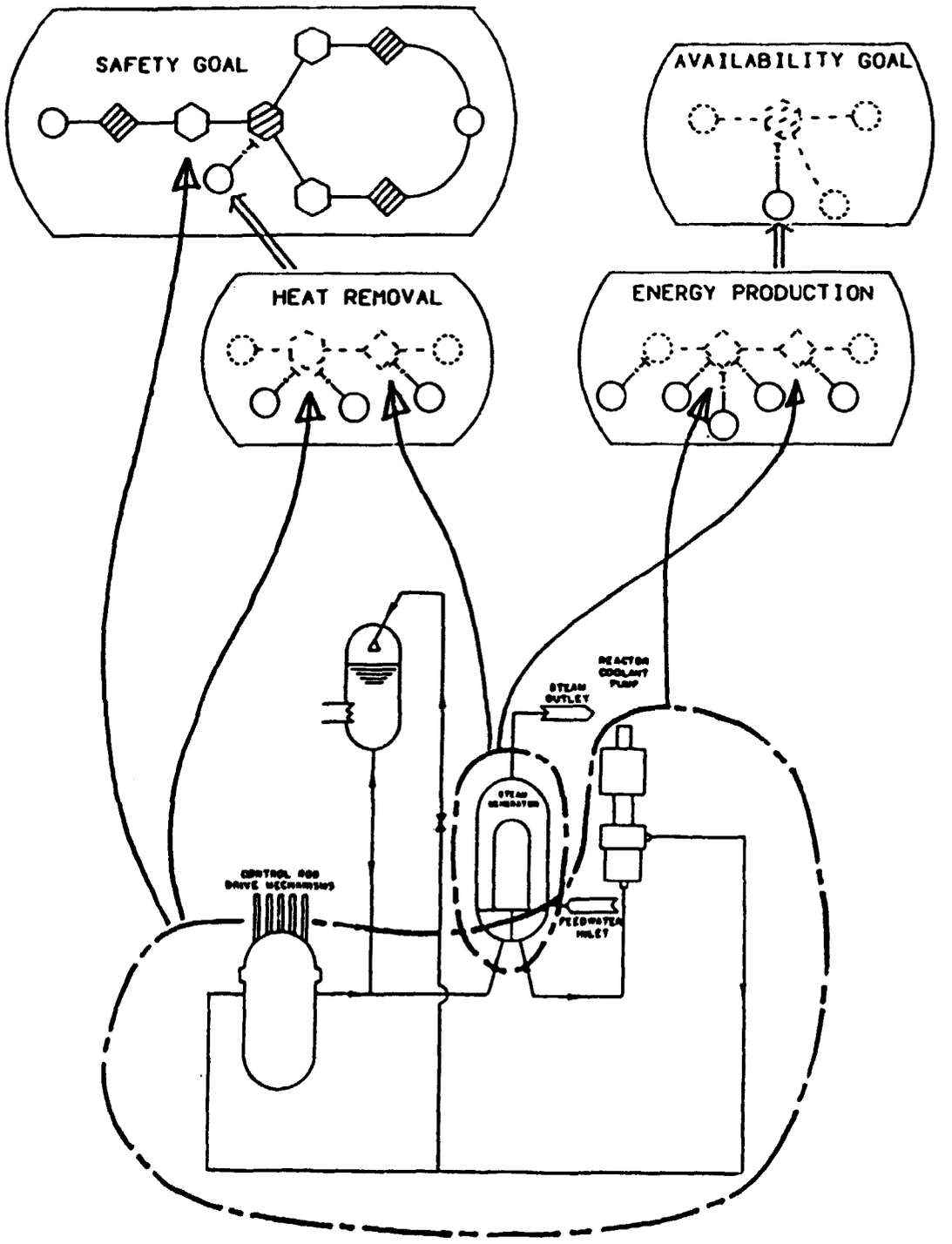



Fig. 6. Example illustrating one to many relations between physical structure and functional structure in a complex process plant. From Lind, 1982a.

## WORK ANALYSIS

In the basic PRA is included a work analysis covering the reliability and the immediate risk from human errors during performance of formally instructed activities. A set of criteria must be established to guide the decision as to whether a given task design is acceptable for formal analysis and it is assumed that identification of necessary human activities not corresponding to such criteria will lead to modification of the system design. In our view, with the present state of the art, only scheduled, familiar tasks are considered to be accessible to formal analysis. Fig. 7 gives an overview of the content of a work analysis and its relationships to the risk analysis.

The phases of work analysis which are shown in Appendix 1 are tentatively proceduralized for evaluation by application in trial analyses of event reports and other actual case stories.

## AUGMENTATION OF BASIC PRA BY ANALYSIS OF LESS STRUCTURED HUMAN INTERFERENCE

As a supplement to the basic PRA as documented by CCCs, an analysis is performed of the possible modifications of the content of the CCCs due to errors during human activities in general. The aim is an explicit documentation of the search strategy and the field of search for such analysis so as to create the basis for systematic risk management through feed-back from event report analysis.

Due to human acts the content of the CCCs can be modified in the following ways:

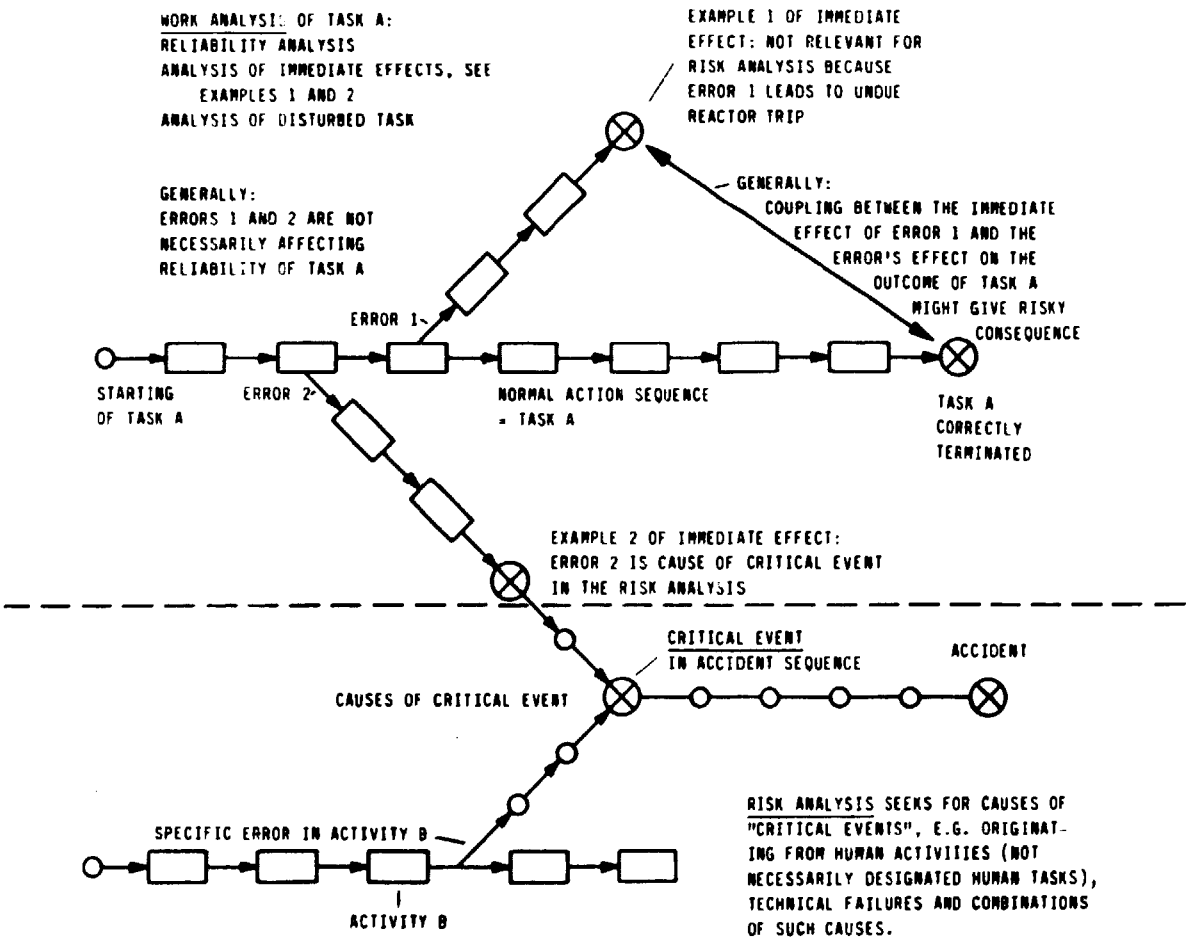



Fig. 7. Illustrates the difference between work analysis: with starting point in normal work sequences and seeking for the effects of errors; and risk analysis: with starting point in a critical event seeking for its possible causes among technical failures and human activities and errors.

Increase of frequency of chains of events

Human errors and acts may increase the probability or frequency of events already contained in the basic cause-consequence--charts. For each of the CCC-decision boxes, therefore, it is judged whether human errors will be significant contributors. For sensitive decision boxes, for instance those found in recovery paths related to protective functions, a work analysis is performed of topographically and functionally "close" activities.

Change of structure in the CCCs

One type of critical human act will be to break a recovery path related to a safety function. Interference due to unreliability of instructed human safety functions is covered by the work analysis included in the basic PRA. Interference in a recovery path due to decision errors and undue interaction during emergency situations requires an independent systematic analysis. In particular, a formal analysis must be able to identify possible decision errors which may provoke systematic interactions due to the existence of instructions for activities aiming at different purposes for the same system. An unacceptable act can be the result of a mistake caused by similiarities between the actual situation and another task context of which the act is a natural part. This similiarity may be found at any level of the abstraction hierarchy of figure 4; i.e., the mistake may be caused by a similiarity in terms of location or appearance of equipment, of the physical function, of the purpose of the systems in overall plant goals or in terms of action sequences. A way to specify the kinds of systematic interference ("systems interaction") caused by the existing many-to-many mappings among purposes, functions and equipment, which are taken into account in an analysis, can be to base the analysis on a proceduralized search in a consistent and documented description of plant properties at the various levels of the abstraction hierarchy.

Another way in which the structure of a CCC can be changed by human interference is by introduction of causal coupling between events which are otherwise independent, in particular between events initiating a transient and events leading to interruption of a recovery path. The extent to which such couplings can be identified by formalised strategies looking for events, functions and equipment in critical parts of the CCC must be examined. Such strategies may be based on the topographical or functional closeness of equipment or psychological similarities of acts, leading to errors of intention or action. Identification of critical activities for which the potential for a decision error should be analysed or a work analysis performed, must be studied in relation to the abstraction hierarchy in order to develop formal morphological search strategies. Again, such a strategy will be a proceduralised search through a data-base representing the properties of the plant at the various levels of abstraction to identify systematic relations between an unacceptable act - for instance to interrupt a safety system - and intentions or acts related to other goals, systems or operating modes, which may systematically lead to the unacceptable act through connections in the many-to-many mapping between equipment, functions, and purposes.

The practical feasibility of such an approach should be judged with the present evolution of computer supported design data bases in mind.

A fundamental weakness of the search strategies considered so far is that multiple errors are included only to a limited degree. In addition, the analysis of complex situations, for instance during major overhauls and refuelling periods, is difficult to include due to their less structured character.

For this reason attempts are also underway to develop morphological strategies which look directly for risky patterns of faults and disturbances as a supplement to the previous strategies which consider the chain of events by means of causal forward- or backtracking.

A morphological method involving a birds-eye-view search for accidental patterns has previously been discussed briefly (Rasmussen, 1979b), in terms of sneak-path analysis. A heuristic strategy to identify such situations resembles a design algorithm: First, the potential for accidents such as high energy accumulations, toxic material concentrations etc. are identified together with potential targets for accidental release such as people, environment etc. Then possible accidents are designed; i.e., the technical (mal)-functions and human actions which are necessary to form the route from source to target are determined. Finally, it is determined how changes in the normal system together with coincident normal and abnormal human activities will coincide with the designed accident pattern. Such accidents are sometimes due to "sneak paths" which are formed by minor mishaps or malfunctions in simultaneous human activities which only become risky in case of very specific combinations and timing.

The close relation to design procedures invites immediately an attempt to base a formalization on the abstraction hierarchy of Figure 4. The procedure involves a top-down search through the levels of the hierarchy but, unlike the search in the basic PRA, the normal functional links among the elements are not used to structure the search. Instead, the plant is considered as a collection of elements or parts at the various levels which can be connected to form accidental chains in the process of design for an accident. Subsequently, the changes in the normal structure needed to release the accident are identified in order to judge its probability. Again, judgement of the feasibility of such an approach must be done with the recent developments within data basis for computer aided design in mind.

## CONCLUSION

The present report is an interim report presenting the basic structure of an approach to an integration of a formal, probabilistic risk analysis and the practical administration of preconditions of an analysis, this integration being necessary if the risk calculated is to have any relation to the risk imposed by the actual, operating plant. The aim of the report is to serve as a discussion which can serve to coordinate the impact on PRA from various studies on system modelling, human performance analysis and risk analysis in the group at Risø and in the joint Scandinavian NKA/LIT study. The work has been funded partly by the Nordic Board of Ministers.

## REFERENCES

LIND, M. (1982a). Generic Control Tasks in Process Plant Operation. Paper presented at the European Annual Manual, FRG, June 2-4, 1982.

LIND, M. (1982b). Multilevel Flow Modelling of Process Plant for Diagnosis and Control. Paper to be presented at the International Meeting on Thermal Nuclear Reactor Safety, August 29 - September 2, 1982, in Chicago, Illinois, USA.

NIELSEN, D. (1974). Use of Cause-Consequence Charts in Practical Systems Analysis. In: Reliability and Fault Tree Analysis. Theoretical and Applied Aspects of System Reliability and Safety Assessment. SIAM, Philadelphia, 1975, pp. 849-880. Also in Risø-M-1743, 1974.

RASMUSSEN, J. (1979a). On the Structure of Knowledge - a Morphology of Mental Models in a Man-Machine System Context. Risø-M-2192, 1979.

RASMUSSEN, J. (1979b). Notes on Human Error Analysis and Prediction. In: Apostolakis, G. and Volta, G. (Eds.): Synthesis and Analysis Methods for Safety and Reliability Studies. Plenum Press, London, 1979.

RASMUSSEN, J. (1982). Human Factors in High Risk Technology. In: High Risk Safety Technology, E. A. Green (Ed.). John Wiley & Sons Ltd., London, 1982.

RASMUSSEN, J. and LIND, M. (1981). Coping with Complexity. Risø-M-2293. European Annual Manual. Presented at the European Annual Manual Conference on Human Decision and Manual Control, Delft, 1981.

RASMUSSEN, J. and LIND, M. (1982). A Model of Human Decision Making in Complex Systems and Its Use for Design of System Control Strategies. Presented at the American Control Conference, Arlington, Virginia, USA, June 14-16, 1982. Also in Risø-M-2349.

TAYLOR, J. R. (1982). Risk Analysis of a Distillation Unit. Risø-M-2319.

USNRC (1980-81):

NUREG/CR-1321 (SAND 80-0384), Final Report - Phase I, Systems Interaction Methodology Applications Program, U.S. Nuclear Regulatory Commission, Washington, D.C., April 1980.

NUREG/CR-1859, Systems Interaction: State-of-the-Art Review and Methods Evaluation, U.S. Nuclear Regulatory Commission, Washington, D.C., Jan. 1981.

NUREG/CR-1896, Review of Systems Interaction Methodologies, Nuclear Regulatory Commission, Washington, D.C., Jan. 1981.

NUREG/CR-1901, Review and Evaluation of System Interactions Methods, U.S. Nuclear Regulatory Commission, Washington, D.C., Jan. 1981.

APPENDIX 1

# PROCEDURE FOR WORK ANALYSIS

Analysis of reliability and immediate risk from performance in a familiar, well trained task which is part of a planned work schedule. This means: the goal or target of the activity is generally accepted; the cues to start of the task are known and, therefore, no errors of intention are considered.

## A. ANALYSIS OF TASK SEQUENCE

Use instructions and manuals as well as interviews and observations.

A.1. Define a sequence of phases or subtasks which is determined by functional requirements of the system and which cannot be modified without interrupting the task.

A.2. Define the necessary acts of the different alternative, functionally acceptable action sequences for each subtask, (i.e., also possible short-cuts, tricks of the trade, which lead to an acceptable result.)

## B. ANALYSIS OF TASK RELIABILITY

B.1. Define acceptance criteria for task product. (Criteria for task process are related to analysis of risk).

B.2. Define error recovery points; i.e., define points in the sequence in which previously committed errors will be immediately observable - either directly or by breaking task sequence, making action difficult. (Such recovery points may correspond to links between subtasks of A.1.).

B.3. Define those acts or action sequences for which the influence on task product is not covered by error detection and recovery; i.e., errors will not be observable and reversible.

B.4. For these acts, identify the human error modes which will lead to uncorrected, unacceptable task product. This error-mode-and-effect analysis can be performed by postulating errors in terms of external acts (Taylor, 1982) or internal error mechanisms, (Rasmussen, 1982). The first is the simplest; however, if risk analysis is to be made, the latter is preferable. See figure 8.

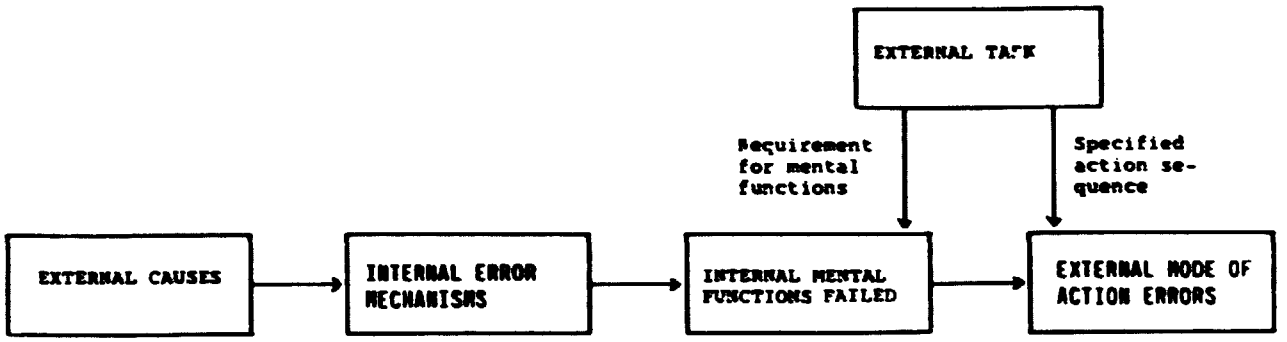
B.5. Evaluate conditions for error detection and correction at the states found in B.2. Define error modes which will cause unsuccessful error recovery.

B.6. Apply human error rate estimates to evaluate total task reliability, considering errors and modes found in B.4. and B.5.

B.7. Judge whether the reliability of the error recovery at the recovery points of B.2. is in fact sufficiently high to ignore errors in the preceding sequence. If not, repeat B.3. for these sequences.

## C. ANALYSIS OF IMMEDIATE RISK

C.1. Define the topographically nearest as well as the structurally and functionally connected systems which can be affected by erroneous human acts.




| HUMAN ERROR MECHANISM ANALYSIS | HUMAN ACTION ERROR MODE ANALYSIS |
|---|---|
| - Based on model of man, task and system function. | - Based on model of task and system function. |
| - Search through generic human error mechanisms. | - Search through generic action error modes. |
| - Relates effect of each error to success of task and erroneous chains of event. | - Relates effect of individual errors to success of task and chains of event in system. |
| - Includes human coupling of chains of events. | - Coupling of chains of event due to human traits not covered. |
| - Includes some types of "errors of intention". | - Errors of intention not covered. |

Fig. 8. The figure illustrates how error-mode-and-effect can start by postulating error modes at different links in the causal chain of events involving human activity.

C.2. Define the set of error modes which should be used in a error-mode-and-effect analysis. Use modes in terms of internal error mechanisms in order to be able to perform C.5.

C.3. Apply this set of postulated errors for each of the steps in the applicable task sequences of A.2.

C.4. For each action and error mode, identify possible unacceptable effects on the system worked on, as well as those identified in C.1.

C.5. Evaluate the significance of the possible simultaneous presence of an erroneous act and an unacceptable task product, i.e., a possible, systematic coupling between two abnormal chains of events.

C.6. Judge potential for error detection and recovery for each relevant error mode from C.4.

C.7. Categorize unacceptable effects found by C.4. and C.5. in relation to the overall risk analysis as given in the CCC.

C.8. Apply human error estimates for the significant contributors in C.4. and C.5.

## D. ANALYSIS OF TASK DISTURBANCES

Task disturbances may lead the performer to re-evaluate the task conditions. This may result in decisions which, if erroneous, may give human "errors of intention".

D.1. Evaluate sources of disturbances. Define the categories to be analysed in an explicit way. Formulate assumptions in order to facilitate "risk management" of those not included in the analysis.

Examples of typical sources of disturbances:

- personnel/work planning and scheduling
- tools/equipment; materials, spareparts
- latent, faulty conditions in system worked on.

D.2. Identify for each of the task steps not covered by error recovery and for the error recovery path, the possible lack/degradation of planning/tools/material-/information which will affect task conditions.

D.3. Identify the normal, typical, easy alternative replacements or improvisations of the particular profession and work setting.

D.4. For the improvised task sequences identified in D.3., repeat analysis under A., B., and C. If effects are unacceptable and conditions too unstructured for analysis, modify system or specify risk management.

**Risø National Laboratory** **Risø-M-2351**

Risø-M-2351

Title and author(s)

# Formalized Search Strategies for Human Risk Contributions: A Framework for Further Development

J. Rasmussen and O. M. Pedersen

Date July 1982

Department or group

Electronics

Group's own registration number(s)

R-9-82

NKA/LIT-1(82)101

pages + tables + illustrations

**Abstract**

For risk management, the results of a probabilistic risk analysis (PRA) as well as the underlying assumptions can be used as references in a closed-loop risk control; and the analyses of operational experiences as a means of feedback. In this context, the need for explicit definition and documentation of the PRA coverage, including the search strategies applied, is discussed and aids are proposed such as plant description in terms of a formal abstraction hierarchy and use of cause-consequence-charts for the documentation of not only the results of PRA but also of its coverage. Typical human risk contributions are described on the basis of general plant design features relevant for risk and accident analysis.

With this background, search strategies for human risk contributions are treated: Under the designation "work analysis", procedures for the analysis of familiar, well trained, planned tasks are proposed. Strategies for identifying human risk contributions outside this category are outlined.

Copies to

**Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark**
**Telephone: (03) 37 12 12, ext. 2262. Telex: 43116**