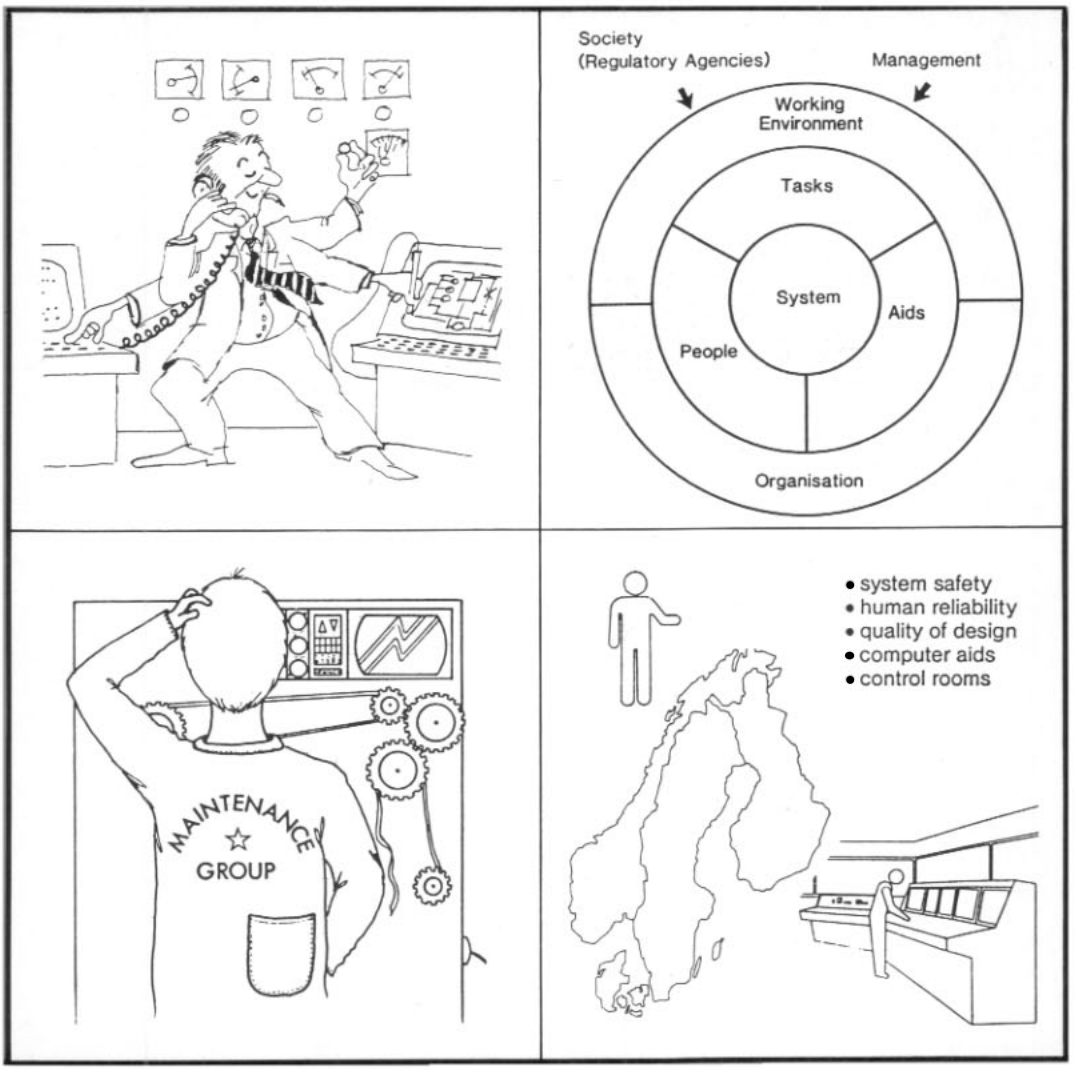
NORD

FEBRUARY 1986

# THE HUMAN COMPONENT IN THE SAFETY OF COMPLEX SYSTEMS




nka

Nordic
liaison committee for
atomic energy

NKA/LIT (85) 1

# THE HUMAN COMPONENT IN THE SAFETY OF COMPLEX SYSTEMS

SUMMARY REPORT OF THE NKA/LIT PROGRAMME
1981-85

BJÖRN WAHLSTRÖM
TECHNICAL RESEARCH CENTRE OF FINLAND
02150 ESPOO

FEBRUARY 1986

Steering committee for the human reliability programme
1981 - 1985 (the NKA/LIT programme)

Björn Wahlström (chairman)
Technical Research Centre
of Finland
VTT/SÄH
Otsvägen 5 I
SF-02150 ESBO, FINLAND

L.P. Goodstein
Research Establishment Risø
PB 49
DK-4000 ROSKILDE, DENMARK

John Lindqvist
Swedish State Power Board
Fack
S-162 87 VÄLLINGBY, SVERIGE

Franz Marcus
Nordic Liasion Committee
for Atomic Energy
PB 49
DK-4000 ROSKILDE, DENMARK

Else Pettersson
(1.1.1981 - 30.6.1982)
Roger Hagafors
(1.7.1982 - 30.6.1983)
Bo Liwång (1.7.1983 - )
Swedish Nuclear Power Inspectorate
Box 27106
S-102 52 STOCKHOLM, SWEDEN

Magnus Øvreeide
OECD Halden Reactor Project
PB 173
N-1751 HALDEN, NORWAY

ABSTRACT

The safety of nuclear power and other complex processes requires that human actions are carried though on time and without error. Investigations indicate that human errors are the main, or an important contributing cause in more than half of the incidents which occur. This makes it important to try understand the mechanisms behind the human errors and to investigate possibilities for decreasing their likelihood.

The present report presents an overview of the Nordic cooperation in the field of human factors in nuclear safety, under the LIT-programme carried out 1981 - 1985. The work was divided into six different projects in the following fields:

- human reliability in test and maintenance work
- safety oriented organizations and company structures
- design of information and control systems
- new approaches for information presentation
- experimental validation of man-machine interfaces
- planning and evaluation of operator training

The research topics were selected from the findings of an earlier phase of the Nordic cooperation /1/. The results are described in more detail in separate reports. A summary of the LIT programme is presented in /2/.

INIS DESCRIPTORS

CONTROL ROOMS; EDUCATION; HUMAN FACTORS; NUCLEAR POWER PLANTS; ORGANIZATIONAL MODELS; REACTOR OPERATORS; REACTOR SAFETY; SYSTEM FAILURE ANALYSIS.

This report is part of the safety programme sponsored by NKA, the Nordic Lialison committee for Atomic Energy 1981-1985. The project work was partly financed by the Nordic council of Ministers.

LIST OF CONTENTS

## THE HUMAN FACTOR AND NUCLEAR POWER

The importance of the human factor for the safety of nuclear power was demonstrated in a dramatic way by the Three Mile Island incident 1979. Several major and trivial human errors committed during what should have been a minor plant disturbance, were the direct cause of the most spectacular accident of the nuclear industry. Many lessons have already been drawn from this and there may be more to come.

The incident has framed attention on 3 problem areas in relation to human factors:

- control room design
- operator training
- use of procedures

These are general problems encountered in the design of complicated systems, their operation and maintenance. The safety of nuclear power plants and other complex industrial plants depends to a large extent on the quality of human work in design, operation and maintenance, or more generally on the overall management of such plants.

Potential consequences of human errors are determined as part of a risk assessment for a specific plant. Risk assessment evaluates the risks associated with different chains of events. Looking at the risk topography for different nuclear plants, some issues are generic for all plants while others apply only to individual plants. Specific problems evidently have to be resolved locally at the plants but some of the generic issues are suitable for a cooperative research effort.

The present Nordic cooperation has concentrated on generic issues of human factors and nuclear safety. The aim has also been that the results should be applicable more generally to the process industry where complex and potentially dangerous plants are in use. With its broad scope the Nordic project was not designed to solve the most urgent problems in any one country or utility; the projects were rather selected, on the judgement of a number of experts, to include areas where problems are being encountered and where solutions could be suggested as the result of a joint effort.

In defining the projects for the cooperation a number of considerations were taken into account:

- Human errors committed outside the control room make a large contribution to causes of unsafe conditions at nuclear power plants. Errors made during test and maintenance activities can introduce common mode failures in cases where several redundant systems are made inoperational at the same time.

- Another cause of common mode failures could be the work organization when routines are badly structured or have been allowed to deteriorate. Maintaining the ability of a safety oriented organization to handle safety threats is a challenge for industry.

- The design of automated systems and the lay-out of the control room are important factors; errors can cause serious deficiencies in the man-machine interface. Efficient management of the design process and the use of computer aided design methods have potential benefits for improving the quality of design and operation.

- The actual methods for presenting information are based on conventional approaches regardless of the technology used. The advent of cost efficient computers will make it possible to introduce completely new approaches for the man-machine interface.

- It is necessary to validate experimentally the systems proposed for the man-machine interface in nuclear power plants before full scale implementation. The problem here is to establish a measure of the performance of the control room and to collect and analyze the data from the operability experiments.

- Human error data collected during simulator training can be used to improve the feedback given to the trainees. Diagnosing complicated transients is a critical task and therefore it is important to develop the ability of operators to make correct diagnoses of such transients as a part of the simulator training.

TEST AND MAINTENANCE ACTIVITIES cf. LIT(85)2.

Test and maintenance activities are designed to ensure the operability of components and systems. The tests should provide early detection of cases where components and systems have developed faults. The maintenance activities can be divided into corrective and preventive maintenance, for correcting observed faults and trying to prevent faults from occurring. Human error may influence the result of the test and maintenance activities in the ways as indicated in Figure 1. Although the aim of test and maintenance activities is to ensure operability of the systems, possible human errors may actually introduce a new fault in a component or system which was previously operating properly.

| | Test interpreted by maintenance crew as: failure | Test interpreted by maintenance crew as: no failure |
|---|---|---|
| fault in component or system | correct interpretation | failed component or system not detected |
| component or system operable | maintenance initiated unnecessarily | correct interpretation |

Figure 1. Possible errors in test activities and their consequences.

A fundamental question in planning test and calibration activities is the selection of an appropriate test interval for critical components. Too long a test interval will potentially increase the unavailability due to various time dependent failure mechanisms. On the other hand too short a test interval may result in unnecessary wear on the component or system and will also increase the risk of unavailability due to human errors.

Another point is the identification of error-prone tasks within the test and calibration activities. If such tasks can be identified precautions can be taken to ensure that the activity is carried out in a correct and timely manner.

Specific studies on these topics carried out within the NKA/LIT-project include:

- an overview of test and maintenance practices at nuclear power plants

- an optimization of test intervals for components and systems in nuclear plants

- a study of test and maintenance of diesel generators

- the collection of case histories in which human errors in test and calibration have played an important part

- a comparison of national practices for test and calibration at Swedish and Finnish BWR plants

- the development of a method for identifying error prone tasks within test and calibration activities

- an assessment of the development of improved test and calibration procedures in a BWR plant

Some general conclusions from the different studies are mentioned below.

The test and maintenance activities at the plants rely on a formal system of work orders and procedures. This system makes it possible both to obtain a certain structure in the activities and the necessary assurance that the tasks are carried out as they should. The case histories, however, indicate that the formal procedures are occasionally bypassed and that such improvisation always introduces a risk of human errors. The use of formal procedures for test and maintenance activities are influenced by several factors such as work practices, lay-out of procedures, and organizational attitudes.

The optimization of test intervals cannot be carried out by mathematical methods alone but must always include some degree of engineering judgement. There is insufficient

data to construct a mathematical model of unavailability, as a function of the test interval, which takes into account all relevant phenomena. This means that the determination of the test interval has to be based on a simpler model for unavailability for which enough data can be obtained. A sensitivity analysis gives a basis to judge if a test interval is either in the lower or upper range.

The search for error-prone tasks in test and calibration activities has to rely on a probabilistic risk assessment (PRA) study performed with a sufficient degree of detail. This should be supplemented with a task analysis, where the tasks of persons carrying out activities which are associated with the relevant chains of events are investigated in more detail. In such analyses special attention must be given to those tasks where earlier errors may make it impossible for the tasks to be completed. Without such check points in the test and calibration procedures there is always a potential risk that errors might be left in the component or system.

In addition to carrying out a PRA study the assessment of potential risks from chains of events involving human errors must also take a risk management approach into account. In this the assumptions in the PRA are compared with information obtained from analyzed incidents. This feedback make it possible to check the completeness of the PRA analysis and to ensure that the assumptions of the PRA are well-founded.

SAFETY ORIENTED COMPANY STRUCTURES cf. LIT(85)3.

The responsibility for the safety of a complex industrial plant is ultimately borne by the industrial company both with respect to its own personnel and to the society. This means that management practices, which are directed to promote the safety of the plant, have to be developed. The task of the management is to ensure that it is possible to

maintain necessary knowledge and skills within the industrial company, that work practices are efficient, that necessary information is distributed to and from members of the company, and that appropriate attitudes to safety are ensured. In so far as any problems in maintaining safety levels then arise they are indicative of deficiencies in the organization.

The NKA/LIT-project investigated the organizational aspects of safety and a method for identifying organizational deficiencies has been developed. The method is intended to be used by the company itself and provide a framework for compiling specialized checklists at the plants in question. The tasks in the project have included:

- analysis of cases where evidence of deficiencies in system planning were found

- development of a theoretical framework for the analysis of management system and organizations

- development of procedures for organizational surveys

- testing of the developed procedures

The study has concentrated on the management function and the information system (cf. Fig. 2). Another important concept is the existence of formal and informal structures, which interact to form the real organization. Some of the more general conclusions from the project are indicated below.

In order to understand some of the phenomena observed in different bodies it is useful to analyze the interactions between various components of the organization. This is facilitated through a formalized discussion of the structural concept which was worked out as a part of the

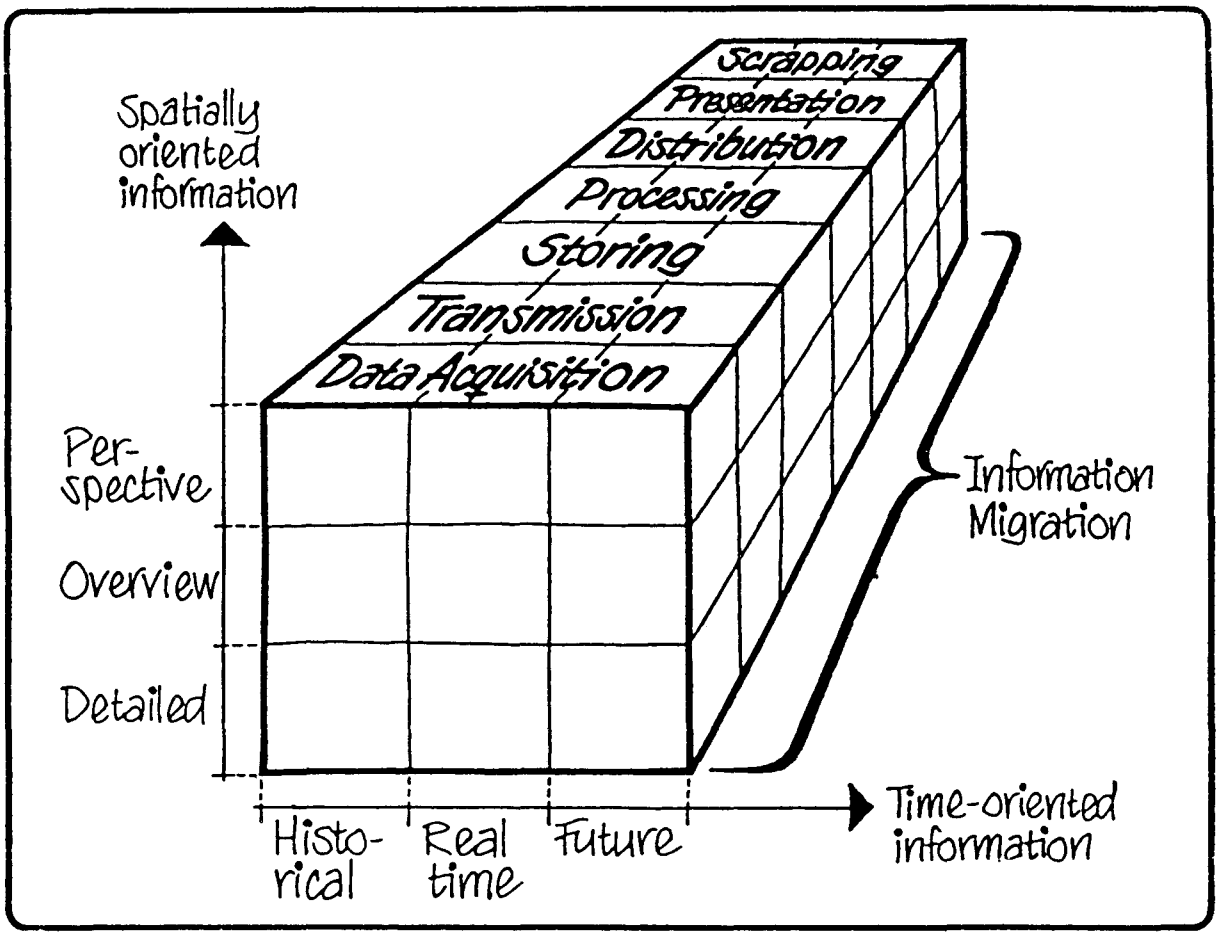



Figure 2: Matrix the completeness of an information system.

project. The understanding which is obtained is essential in the classification of deficiencies observed in actual case studies.

In attempting to illustrate structural deficiencies, an investigation was made of disturbaces that have occurred and have been reported, but not many good examples could be found. One reason is that the disturbances seldom are analyzed with respect to organizational problems, which implies that some important questions are never asked. It is also difficult to obtain an accurate account of all the details behind a specific chain of events, as there always will be either conscious or unconscious cover-up actions. Another problem is the confidentiality necessary towards the persons involved. On an anecdotal level, however, many

cases are referred to in the nuclear community, which clearly point towards generic issues.

In the NKA/LIT-project three field studies were carried out; an event which occurred in the dispatching area of the electric grid system; a reorganization at a nuclear power station; and an investigation of how a stress corrosion cracking problem was handled at a nuclear power plant. The field studies indicate the benefits of the method developed and also show that it is possible for the method to be adopted by the utility company itself.

COMPUTER AIDED DESIGN cf. LIT(85)4.

The quality of the control room design has an important influence on the human errors that can be committed in controlling a complex industrial process. From looking at possible design deficiencies it is evident that they, to a large extent, are caused by deficiencies in the management of the design process itself. Such errors may be avoided by a proper design management and by using proper design tools.

In the design of control rooms it is important to consider the projected life time costs of the plant. When it is realized that industrial processes are often designed for a projected lifetime of 20 - 40 years it is clear that the yearly operational costs are far more important than the costs of the initial design. This applies especially to the case where a small design omission could lead to unavailability or even safety problems in the plant.

Any errors in the design should evidently be caught and corrected at the earliest possible stage. In control room design as in all design work it is the rule that with time the costs of design changes will go up and the design freedom will go down (cf. Fig. 3). This means that proper attention should be paid to assuring the quality of the design.

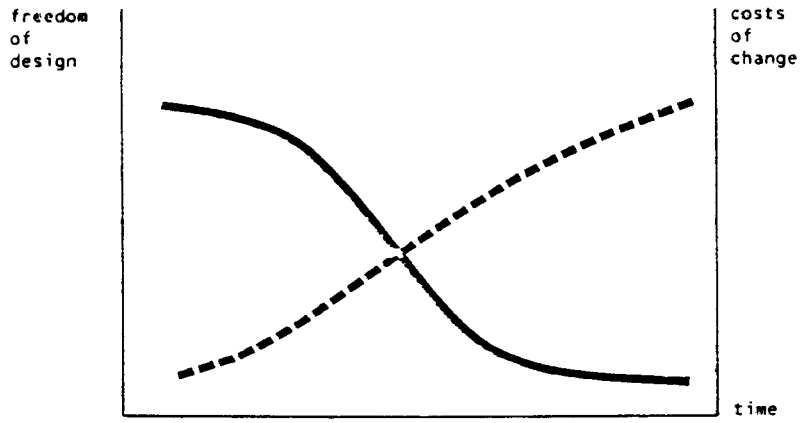



Figure 3: The freedom in the design decisions will sink gradually with time and the costs of changes introduced will increase correspondingly

The following design errors were considered

- that an important design requirement has been omitted
- that the quality of the selected design is not high enough.

Generally, the first type of error is the most important because it could cause serious deficiencies in the subsequent design. This type of error also points to problems in the design management. It is evident that the second type of error also could cause deficiencies in the design, but it could also be introduced through a compromise between conflicting requirements on the design.

In order to ensure an appropriate design quality computer aided design (CAD) methods, if properly realized, may prevent many of the difficulties involved in purely manual methods. CAD methods offer the following potential benefits for control room design:

- easy design changes
- automatic generation of documents
- automatic verification of design
- automatic production of software
- easy access to design information
- easy use of internal design standards
- better quality of design data base

The construction of computerized design aids involves a thorough analysis of the information needed by different users during the design project. The construction of the design data bases means also that a formalization of the design process has to be carried through.

As a part of the NKA/LIT-project a demonstration system was built, where emphasis was laid on the documentation of a formal model of requirements and their relation to the technical solutions. This helps to resolve the problem of keeping track of the reasons behind the design which is one of the largest problems with the present design practices. The system has been tested using a case from a BWR plant.

The results indicate that it is possible to get the benefits listed above by using computers in the construction and verification of the design data base. Computerized methods are recommended not only for new designs, but it could also be beneficial to computerize parts of the design data base for old plants.

The introduction of new operator aids in the control room would provide a suitable opportunity to carry out such computerization. The realization of a computer aided system should clearly be based on available commercial systems, adapted so as to include modules of the type developed in the demonstration system developed in the present project.

COMPUTERIZED OPERATOR SUPPORT AND EXPERIMENTAL VALIDATION
cf. LIT(85)5.

The increasing use of computers for information presentation in control rooms offers new possibilities but also introduces new risks. The new system makes it necessary to consider concurrently operator roles, system functions, operator training etc. in order to arrive at better solutions of the problems of the interface between man and machine.

As the present design of both conventional and computerized control rooms relies to a large extent on conventional concepts it is necessary to make a more detailed re-evaluation of the new concepts underlying the construction of operator aids. Taking into account the required safety and the high costs involved with a full scale implementation of a new system, it is clear that proposed concepts should go through several stages of experimentation and validation.

When considering the supervisory and control tasks in a nuclear power plant, it is evident that the process operators need a clear and well structured understanding of the operational goals and restrictions of the plant. It can be noted that operational goals and restrictions often only are implied in the operational instructions and not directly deducible from the plant information system. One of the aims of future system would thus be to make these goals more explicit and to structure the information in such a way that it becomes easier to determine whether the goals are attained and the requirements satisfied.

Similarly it is necessary to support the operators in matching plant goals and functions to available equipment and vice versa as an aid in diagnosis, planning, resource management etc. This can be expressed as the operators need for information about the plants "WHY, WHAT and HOW".

In a power plant, one of the most important operations is to control the transfer of mass and energy in the process. The NKA/LIT -project shows that the operational goals and requirements can be described in terms of balances and transfer of mass and energy. In order to pursue this concept, a formal system has been developed for describing the plant, using symbols of mass and energy flows. This makes it possible to construct abstract functional models of the plant on several levels (cf. Fig. 4). This formalism has been described as multi-level flow modelling (MFM).

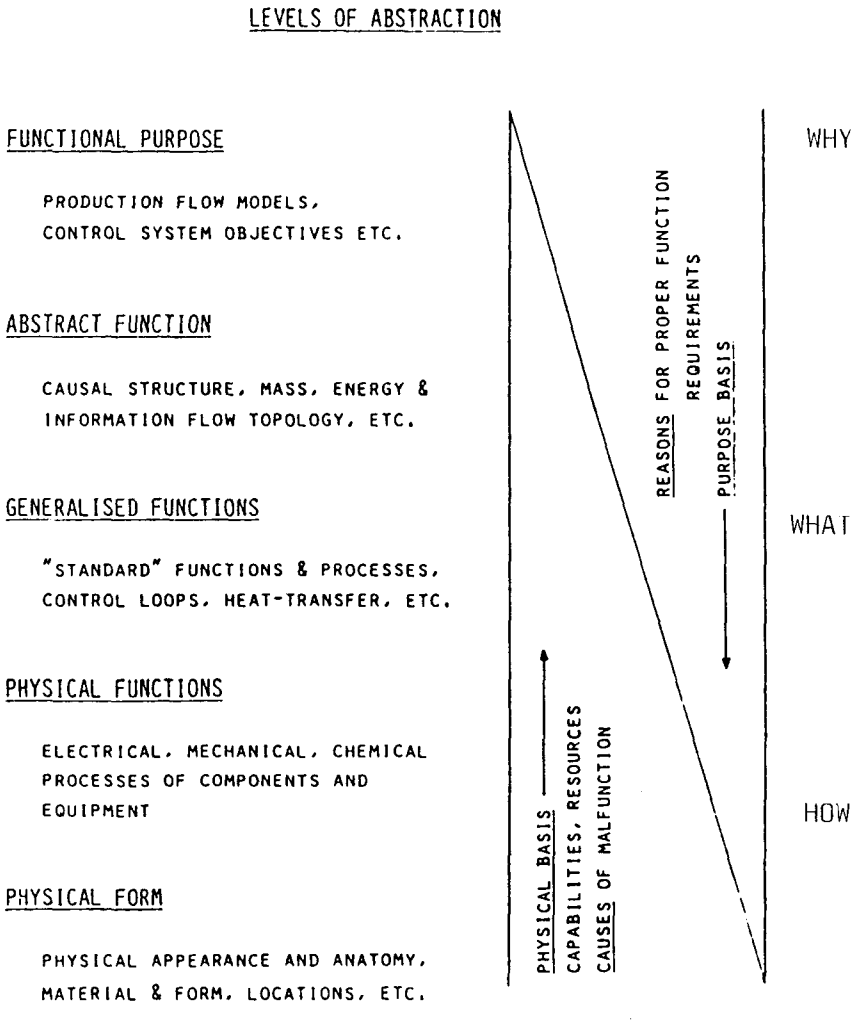



Figure 4: The abstraction hierarchy used for representation of functional properties of a technical system.

The possible uses and benefits of multilevel flow models have been assessed. Using a simple experimental tool, a generic nuclear power plant (GNP) simulator, their acceptance as a means of information display has been studied and it seems that the approach is viable. Several versions have been installed for experimental and demonstration purposes. Experiments using GNP with display systems built on the multilevel flow model approach have been carried out and show that it is possible to diagnose faults in a plant on a more general level in terms of production and safety goals.

The experience obtained with the multilevel flow models indicates that they are particularily useful in plant design. Efficient use of this system for practical problems requires good process knowledge and training in the symbolism and in thinking in terms of abstract functional models. It seems, however, to be relatively easy for persons with a technical process background to acquire the necessary skill in using the symbols.

The experimental validation of the proposed displays turned out to be time consuming and costly. The construction of an experimental facility and its modification for a specific experiment is an effort which easily could take several years and involve a considerable amount of manpower. If it is to be used to build real systems for nuclear power plants it will be necessary to develop a method by which the concepts could be checked in several stages during the design.

PLANNING AND EVALUATION OF OPERATOR TRAINING
cf. LIT(85)6.

The requirements for proficiency of nuclear power plant operators have lead to the use of simulators for the training of control room operators. The simulator is operated in the same way as the plant from the control

room and the training sessions are devoted to manoeuvres which the operators have little or no possibility to perform during routine plant operation. The simulators are used on a continuous basis to ensure that the operators have the required abilities.

One of the problems in planning the training is to judge the relative importance of different training sessions in terms of task difficulty and operator experience. One solution is to systematically collect the results from earlier training sessions in order to identify areas where deficiencies in the knowledge of the operators have been noted. Such information could also be used to direct the attention to possible problem areas in control room design and in the operation instructions.

One method of collecting information during the training sessions, developed and used in the NKA/LIT-project, can provide feedback to the planning of the training. Experience with the method also shows the importance of a detailed preparation of the training session in terms of what the operators should do and what they might do. To recognize the causes of observed errors during the training session it is important to arrange for a detailed discussion analysis after the training session. Experience also indicates that it should be the instructors who collect the error data.

On a more general level one of the important questions in the planning of operator training is to determine the qualities that are needed for a good operator. The good operator should have a "process feel", but how such a feel could be developed and what it involves is by no means clear. One possible explanation is that a good process operator has been able to structure his knowledge into an easily manageable set of rules which directs his attention at all times to the most relevant issues of the operation.

One of the aims of the NKA/LIT-project has been to investigate the applicability of such rules to nuclear power plant operation. Some of the rules proposed are self-evident from an operational point of view, but it was possible to identify how the internal model of the operators develop by giving them the task of writing down such rules. It was seen that the rules generated became more general as the profiency of the operators increased.

Another question is the extent to which training in such rules can influence the acquirement of "process feel" and whether this could be measured. For isolated tasks and items of knowledge it seems possible to define the minimum requirements necessary for operation. The difficulty, however, is to assess whether the operator has been able to integrate all the separate items into a working model of how the process should be operated. At present the tests given to the operators, e.g. by the authorities as a part of the licencing practices, are based more on judgement and sound engineering practice than on a systematic evaluation of the requirements of operator proficiency.

Considering rules of thumb used by control room operators of a process plant, it is possible to distinguish between context-dependent and context-free rules. The former are directly associated to the plant in question and are not transferable. Context-free rules provide more general aids for problem solving, indicating e.g. how causes and consequences should be diagnosed. An interesting question is then to what extent it is possible to transfer operator skill in using context-free rules from one task to another. This could have important implications in planning operator training.

## CONCLUSIONS

The NKA/LIT-project has confirmed the importance of the human factor as a component in the safety of nuclear power

plants. The different parts of the project have also generated specific suggestions on how the quality of the human work could be improved. Discussions and observations within the nuclear industry have indicated that some of the problems are well known and have already been handled on an ad hoc basis. There could, however, be benefits to be derived from a more systematic approach in the treatment of human errors. In order to apply available theoretical knowledge it is important to arrive at a working dialogue between researchers and those engaged in practical work in the industry.

In spite of the large effort (nearly forty personyears) during the four year NKA/LIT-project it is clear that another phase of follow up work will be needed before the ideas proposed can be utilized in practice. Application oriented follow up projects would need to be performed on a national basis in view of the varying field of interest in the Nordic countries, but the cooperation established offers the possibility of involving several parties in such application projects.

The project has also indicated areas where additional research efforts will be needed. One such problem is to make quantitative assessments of the probability of human errors in different tasks. At the present level of knowledge and with present data available it does not appear possible to identify any valid and reliable method for the calculation of human error probabilities. Therefore it is important to continue the work to establish a suitable basis for the design of error-tolerant systems.

The design and operation of nuclear power plant relies on the contributions of a large number of human experts. One of the crucial questions is how this expertise can be made available to the operators. The increasing complexity of the nuclear plants also poses problems where

connections between several areas of expertise are required. This generic problem could be addressed by using methods from the field of artificial intelligence and build up so-called expert systems. At present there are diverging opinions on the possible benefit of such systems and fears have even been expressed that an increasing use of expert systems could tend to undermine human expertise. Regardless of the diverging opinions it is, however, clear that additional research efforts are needed before such systems could be utilized. Questions in this connection are addressed in a new Nordic Cooperation programme in the period 1985 - 1989.

REFERENCES

1. Wahlström, B., Rasmussen, J., Nordic cooperation in the field of human factors in nuclear power plants. IAEA-SN-45247, Nuclear Power Experience, IAEA Vienna 1983.

2. Wahlström, B., Human factors in nuclear power systems - activities in the Nordic Countries, ANS/ENS topical meeting, Knoxville, Tennessee, April 20 - 23, 1986.

## LIT final reports:

| | |
|---|---|
| LIT(85)1 | The human component in the safety of complex systems. |
| LIT(85)2 | Human errors in test and maintenance of nuclear power plants - Nordic project work. |
| LIT(85)3 | Organization for safety. |
| LIT(85)4 | The design process and the use of computerized tools in control room design. |
| LIT(85)5 | Computer aided operation of complex systems. |
| LIT(85)6 | Training in diagnostic skills for nuclear power plants. |

These reports are available at the following organizations:

| | |
|---|---|
| Technical Research Center of Finland, VTT/INF<br>Vuorimiehentie 5<br>SF-02150 Espoo 15 | LIT(85)1 & 4 |
| Studsvik Energiteknik AB<br>S-611 82 Nyköping | LIT(85)2 |
| Statens Vattenfallsverk<br>Fack<br>S-162 87 Vällingby | LIT(85)3 |
| Risø National Laboratory<br>Postbox 49<br>DK-4000 Roskilde | LIT(85)5 & 6 |

**Handling charge USD 10,- per report to be forwarded with order.**

***gotab*** Stockholm 1986