NKA NORDIC LIAISON COMMITTEE FOR ATOMIC ENERGY

NKA/KRU–(81)13
January 1982

ENLARGED NORDIC COOPERATIVE PROGRAM ON NUCLEAR SAFETY

NKA/KRU PROJECT ON OPERATOR TRAINING, CONTROL ROOM DESIGN AND HUMAN RELIABILITY

TECHNICAL SUMMARY REPORT ON CONTROL ROOM DESIGN AND HUMAN RELIABILITY

A Joint Scandinavian Research Project
Sponsored by

The Nordic Council of Ministers

VTT OFFSETPAINO ESPOO 1982

INTRODUCTION

As discussed in the summary report (Ref(1)), there are trends underway in the areas of technological development related to industrial process installations which, among other things, have serious implications for the design of the process operator's main workplace; i.e. the control room and, in particular, the so-called Man Machine Interface (MMIF). The latter encompasses all transformation and communication of information between the operating staff and the process and, in the light of these trends and their likely rates and weights of influence, its proper implementation in the future will require a careful and more integrated consideration of all the major factors which can affect its design.

The major trends are:

(1) increasing size and complexity of plant where the safety--related implications lie in the potentially more severe consequences of disturbances and the need to prevent or terminate them and/or minimize their effects.

(2) advent of computers which makes all things possible but not necessarily better.

These trends (will) affect

(1) operator roles
(2) operator support (displays, other aids, etc.)
(3) operator selection and (re)training
(4) staff organisation and responsibilities

An increasingly difficult, yet necessary, activity for the designer will be to combine a knowledge of plant behavior and control with a suitable "degree of automation" so as to generate a reasonably well-balanced set of tasks for the operators, which avoids the fragmented and incohesive job spectrum often characterized as "99% boredom and 1% sheer terror", and thus enhances operator readiness for the unexpected. This role optimisation will of course have ramifications for all the other factors listed above.

This situation was the back drop for the portion of the joint Scandinavian project, which will be reviewed here and which dealt with the design and evaluation of computer-based control rooms. The rapidly advancing "state-of-the-art" in instrumentation, displays, etc. has not been accompanied by any corresponding emergence of suitable guides, norms or traditions for the use of these techniques. Thus the project activity described here concentrated on the following important ingredients of a systematic framework for MMIF design and evaluation.

- operator models and behaviour
- operator attitudes
- criteria for MMIF design
- possibilities for computer-based operator support
- experimental methods of validation

Companion volumes to this report are two guidelines for MMIF design (Refs.(2) and (3)). The first is the result mainly of Finnish efforts - based partly on other international work to generate a user-friendly aid for insuring completeness in the design team's treatment of all relevant man-machine questions during the design process. The other attempts to relate the results of the KRU-project to the relevant parts of the Finnish guidelines.

The present technical report summarizes the problems, studies and results for each of the above-mentioned areas and includes references to the appropriate full-length documents.

References

(1) NKA/KRU-(81)11 Summary Report NKA/KRU project - Control Room, Operator Training and Human Reliability

(2) NKA/KRU-P2(81)239 J. Ranta, B. Wahlström and R. Westesson Guidelines for Man-Machine Interface Design.

(3) NKA/KRU-(81)16 Summary Guidelines for Man-Machine Interface Design with Annotated References.

OPERATOR MODELS

Any attempt at a systematic approach to the design of an MMIF must rest in part on a suitable characterisation of human functioning and interaction with the "system". For example, the proper design of displays - both with respect to the total set required as well as the individual formats - requires a conceptual description of operator internal mental processes and decision strategies for dealing with information about the "state of the world".

Thus one objective of this project was to survey the field of human modelling in order to establish the relevance of the work which had been done within the international community to all, or parts of the process operator's work situation - but especially those having to do with the handling of rare disturbances.

The study is reported in Ref(1) and is also summarized in the conference contribution referenced in Ref (2).

In general, the use of models is almost mandatory for purposes such as:

- understanding a process of phenomenon
- communication among interested parties
- as a basis for experimentation
- as a tool for prediction

The main difficulty in modelling the human operator is in his versatility, variability and adaptability, which makes it impracticable to find any all-encompassing model. This means that different roles, functions and capabilities of the human operator need to be modelled separately. The different models will then reflect these different needs, and the use of the model will be restricted to the situation studied. Examples of these are:

- information processing models
- models of visual scanning
- detection models
- decision models
- control models
- reliability models

The information processing models concentrate on human information processing and use information-theoretic measures to explain, e.g. reaction time. The scanning of displays during process monitoring has been modelled using different queueing systems where the operator is considered as behaving rationally while taking into account factors such as information content, workload etc.

The detection models concentrate on human detection of specified cues during the monitoring mode. The decision models have been constructed to account for human decision making in simple game-theoretic tasks where the rationality of the human decision maker has been studied. The control models treat the human operator as a part of a continuous control loop and attempts to relate his/her behaviour to optimal controllers have been made. The reliability models of human actions are often failure trees where the different probabilities have assigned values obtainable from simple task-dependent characteristics.

To a great degree, these models originated within the avionics field, and it has been necessary to develop new models of

behaviour and strategies from real-life studies in actual control rooms and repair shops in order to get a useful basis, e.g. for a more systematic interface design. They are non-mathematical in nature and reflect a striving towards an engineering-friendly framework for describing operator behavior. See Ref(3).

A convenient link for a categorisation of operator behavior can be forged by considering the spectrum of operator tasks - which in order of descending frequency (and increasing risk) - can be sketched as shown on fig. 1.

The model then suggests three relevant categories for coping with this array of tasks. These are shown on fig. 2 and in more detail on fig. 3.

<u>Skilled-based</u> (automatic sensori-motor) <u>behaviour</u>. - Immediate examples from everyday are riding a bicycle, typing, playing a musical instrument. This type of behaviour occurs typically as the consequence of a consciously expressed intention (ride, type) which is thereafter executed as a smooth and highly integrated sequence of movements which does not require attention, synchronized to certain key features extracted from the "surroundings". The result of highly trained performance; this type of behaviour is relevant in the present context for many tracking and control tasks as well as for manual manipulations in connection with familiar tools and equipment.

<u>Rule-based behaviour</u> - rules take the form of either prescribed (written) work instructions or as remembered procedures from earlier successful applications. Thus, this type of behaviour occurs in situations which arise and are recognized as belonging to the set of previously foreseen or predetermined situations. Rule-based behaviour is typical in the control of complex and/or lengthy activities which form part of relatively familiar job activities.

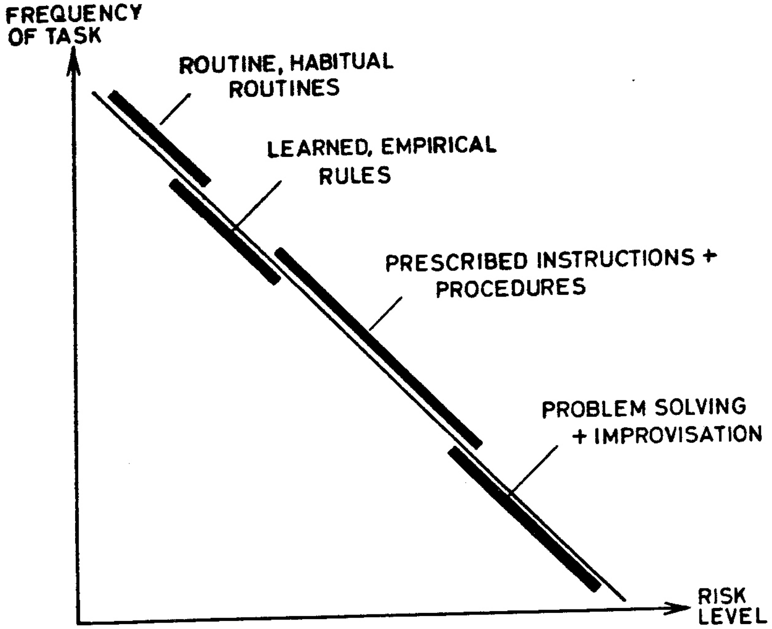

Figure 1. Task spectrum.

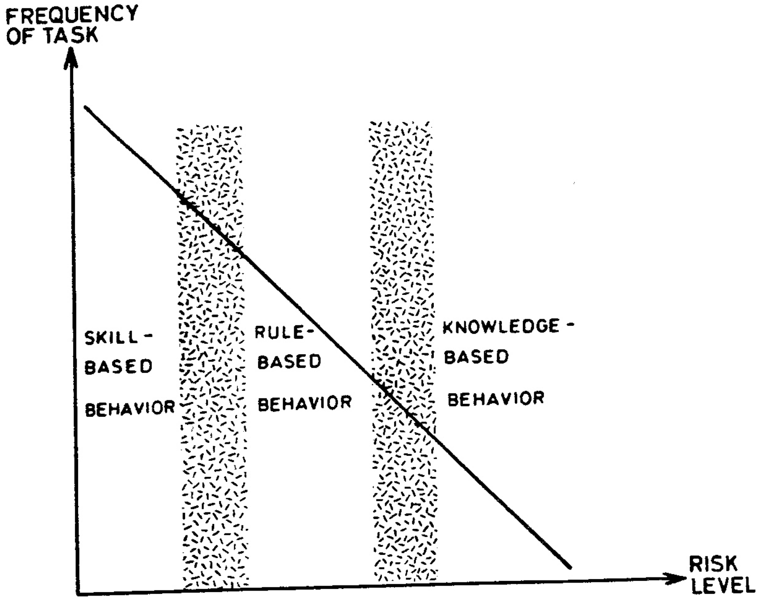

Figure 2. Overlay with behavioral categories.

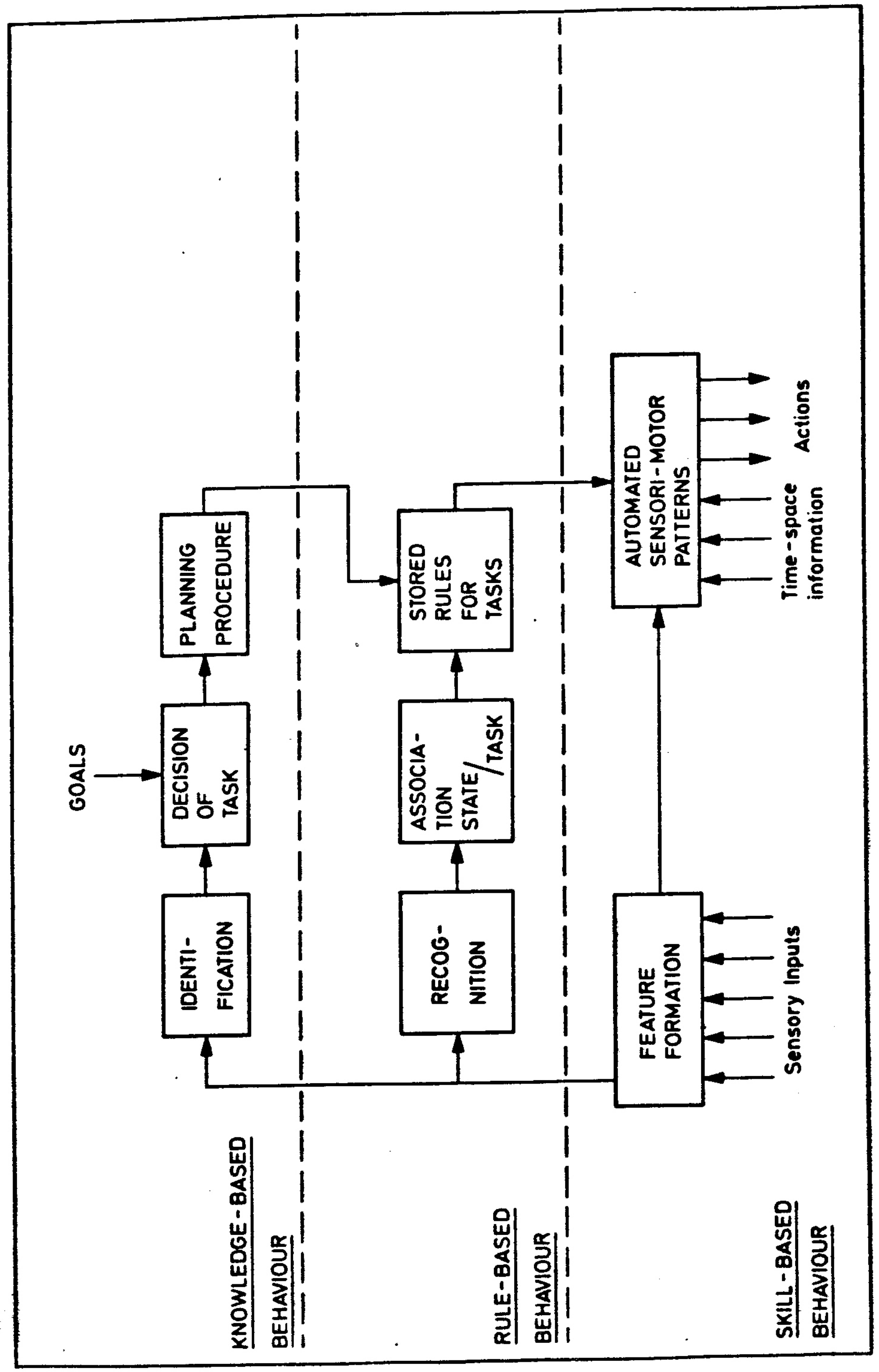

Figure 1. Schematic illustration of categories of human data processes.

Knowledge-based behaviour - this type of behaviour becomes actual (as a last resort) when skills and rules are neither available nor adequate and the situation therefore calls for problem solving and perhaps improvisation. Elements of data processing thus include observing, identifying, deciding and planning, and these involve causal and functional reasoning based on a knowledge of the functional properties of the system including the potential means for and effects of making corrective changes in order to counter an undesirable state or trend.

Under knowledge-based behaviour, there are two important sub-concepts which have significance, e.g., for display design. These are:

Field of attention - a concept which can be likened to photographic "zooming" where the amount of system coverage and detail is variable and depends on the desired field of attention which, in turn, depends on the current activity. For example, in the initial phases of a diagnosis, the coverage would be wide and the detail probably restricted to the most critical primary parameters. In the final stage where a corrective action is identified, the coverage would be limited and the detail concentrated on the location and operation of the selected control.

Level of abstraction is a more subtle concept which reflects human ability and tendencies to speculate consciously about the world (or bits of it) in different ways depending on needs and abilities. See Ref(4).

Another element in a representative framework of operator interaction with the plant - and one which has special significance in responding to disturbances - is a description of the operator's mental strategies when searching in the system in order to identify state, cause or the appropriate action. As such, strategies are high-level mental concepts which relate goals to relevant sets of plant models, data and technical rules for carrying out a diagram. Refs(5) and (6)

deal in detail with this question. The study has led to a kind of typology of diagnostic strategies and an identification of some of the performance criteria guiding the operator's choice of strategy.

For example, a diagnostic search can be performed in two basically different ways. A set of observations representing the abnormal state of the system - a set of symptoms - can be used as a search template in accessing a library of symptoms related to different abnormal system conditions to find a matching set. This kind of search will be called symptomatic search. On the other hand, the search can be performed in the actual, maloperating system with reference to a template representing normal or planned operation. The change will then be found as a mismatch and identified by its location in the template. Consequently, this kind of search strategy has been named topographic search. The difference between the two kinds of search procedures is related to a basic difference in the use of the observed information. Every observation implies identification of an information source and reading the content of the message. By symptomatic search, reference to the identity of system state is obtained from the message read; by topographic search, reference is taken from topographic location of the source, while the messages are subject to good/bad judgements which are used for tactical control of the search.

A typical diagnostic sequence would involve many shifts back and forth between the two strategies.

The above has necessarily been a cursory description of the conception of the operator as an information processing system which has been used as the basis for the work an interface design, computer aids and human reliability. These are discussed in the subsequent sections.

References

(1) NKA/KRU-P2(79)217 Juhani Timonen
On the Control Theoretic Modelling of Human Process Operator.

(2) NKA/KRU-P2(80)221 Juhani Timonen, Björn Wahlström, Leena Tuominen
On the Modelling of the Tasks of Operators in Automated Process Plant.

(3) NKA/KRU-P2(79)11 J. Rasmussen
Man as a System Component
"Man-Computer Interaction" H. Smith, T. Green (eds.)
Academic Press, 1980.

(4) NKA/KRU-P2(79)21 J. Rasmussen
On the Structure of Knowledge - a Morphology
of Mental Models in a Man-Machine System Context.
(Also Risø-M-2192).

(5) NKA/KRU-P2(78)1 Jens Rasmussen
Notes on Diagnostic Strategies in Process Plant Environment
(January 1978).

(6) No number Jens Rasmussen
Models of Mental Strategies in Process Plant Diagnosis.
"Human Detection and Diagnosis of System Failures". J. Rasmussen, W.B. Rouse (eds.).
Plenum Press 1981.

OPERATOR ATTITUDES AND PREFERENCES

Operator models and operator attitudes are complementary concepts. The models of operator performance described previously are intended to represent human cognitive functioning and, as such, depict the human as a kind of "systems component" by

indicating what people can do. In reality, we all function under the influence of a surrounding environment - on shift, under training, at home, etc. - which, in turn, gives rise to a host of so-called "performance shaping features". These factors have a great effect on what an operator will do in a given situation. A stressful task environment, a disharmonious family life, a poorly coordinated operating team are examples of environmental factors which can interact with the more cognitive functioning described by the models.

In addition, expectations and/or experience, built up over a lifetime, give rise to many subjectively and emotionally based values and preferences which, when expressed, reflect the person's attitudes towards "such and such".

In this project, there was interest in investigating the attitudes and preferences of operators and others towards various aspects of computer-based communication and display systems. Several methods were employed to study these.

For example, the Norwegian team had the opportunity of conducting a running study at a pulp and paper mill in which a computerized control, instrumentation and display system had been installed. They contacted management and operating staff at regular intervals starting prior to the installation, and via questionnaires and interviews attempted to gather information about current attitudes to computers in general and about the particular system which had been installed. In addition, the investigation sought to trace any changes in "process feeling" and problem solving behaviour which had developed over the period. See Ref(1).

The introduction of advanced communication equipment was sometimes received with doubts. Two of the often mentioned issues were that the operators would lose their contact with as well as their overview of the process. According to the experience gained in this study, neither of these opinions was supported. On the contrary, the general impression was that the operators got a much better overview of the process and a more intimate relation to it than they obtained with conventional instrumentation.

In particular, the immediate feedback was appreciated. The pictures which seemed rather crowded for an outsider were handled without difficulty. Those who were a bit sceptical about the new communication devices were also more negative about the use of computers for automation in general.

In this study, a majority of the operators thought the advanced communication devices made it easier to control the process and to get process information. At the same time they were of the opinion that this type of system placed greater requirements on the operator's attention and accuracy.

Of relevance is the fact that most of the operators had transferred from an older, conventionally instrumented plant. There was also a considerable span in age (over 40 years) and this was reflected in the information collected. Before the system was installed, the older operators were more reticent with regard to the need for going over to a new technique while the younger people were eager to use the new system. They saw the new job as a challenge while the older operator had some fears about not being able to cope with the new approach and not having the same opportunities to use their own "personal control system".

After installation, the very positive attitude seemed somewhat cooler although the differences in opinion as illustrated above persisted. In addition, the attitudes of newly employed operators seem to be quite similar to those expressed by the older operators in the initial study.

On the whole the operators still thought that the work environment would be better in this installation, with a better contact with their fellow-worker. Some of them became more sceptical about the use of computers in industry. The older operators also became more doubtful about the reliability of

computers, while the younger operators thought that they were still quite trustworthy.

The younger operators seemed to have maintained their opinion that "It is easier to run the process with a computerized control room compared with traditional instrumentation". The older operators, who were of the same opinion in the beginning, changed sides. The work did not seem to be quite as meaningful and important as before for these operators, but they still thought that it could give some opportunity to get higher salaries. They did not change their opinion about the expected intensity and monotony in the job, but there seemed to be a slight trend towards the impression that the tasks would be less difficult, demanding and tiring than first expected. They seemed to be afraid of more trouble with their eyes than before. In the first study, the medium time in front of the CRT-display was estimated to about 3 hours, a figure that is a bit lower now. Concerning the amount and fault frequency of the information and the ease of getting information, the opinions were the same.

Refs(2) and (3) describe a parallel study which concentrated on characterizing the operator's own conception/description of his job, the process, etc. and seeing how this developed with time and experience. The following table illustrates how such a "process feeling" evolves - as called from this study.

Of course there are large individual differences. It should also be clear that the development of a process image has ramifications for training, information displays, organisational structure, etc.

Colour Preferences

The advent of the colour CRT in the control room requires in the long term that suitable standards for colours be developed and maintained. At present, there are advisory recommendations from the 1930's, application guides from ISO regarding safety as well as a host of individual company practices and some

The Development of a "Process Feeling"

Phase	Knowledge	Performance
1) Task-orientation	Tasks & procedures (normal operations)	Psychomotoric activities "doing"
	Physical layout & working tools	
2) Evaluation	Events/process malfunctions	Motoric activities
	Reliability & validity estimates	"Trial & error performance" (emotionality)
3) Differentiated process feeling	Cause-consequence relations (criteria deviation-action to take)	Non-emotional, context-independent
	Consequence-cause relations (symptoms, faults)	Problem solving & decision making
		"Thinking"
	Strategies for fault allocation and problem solving	

uncertainty about the applicability of all these in the modern control room. See Refs(4) and (5).

Among the problems are:

- Number of hues in a display taking into account the physiological accommodation limitations of the eye.

- Selection of colours for information transfer in the light of needs, established practices, etc.

For watching TV at home, some illumination recommendations can be given, the illumination being set once and for all as a compromise among the family members. However, in a control room a relatively great number of individuals will have to be served, and therefore illumination there must be adjustable to fit various needs because a compromise may be undesirable and downright unprofitable. Two additional requirements must therefore be set for control room illumination:

1) The illumination should not enhance the flickering of CRT displays; i.e. use incandescent bulbs rather than gas-discharge tubes.

2) The illumination colour should not impair the display colour perception.

So far, in the work with colours, some control room monitor quality criteria have been found:

1) The stability of colour (convergence) has to be high. Since colour is used as an information carrier, the message has to be unambiguous to be expedient. Frequent change of the hues through recurrent colour recalibration of the convergence cannot be tolerated.

2) The same input signal should generate the identical hue on all monitors in the installation. When colours are

used as information carriers, the colour has to be the same regardless of which monitor it is displayed on. It can absolutely not be tolerated that any display is bound to a specific monitor in order to be shown with the correct (i.e. the designed) hues.

3) The CRTs have to be of a quality class such that the display is influenced only to a bare minimum by the ambient illumination.

In addition it is not yet fully known how the following particulars may influence the use of colours in man-process communication:

- age
- physical fitness
- mood and mental attitude
- task diversity
- stress imposed by task
- stress imposed by supervisors
- stress imposed by unknown consequences of erring
- fatique of 8-hour shift duty
- fatigue of many years of shift work

Some experiments were run to establish sets of CRT colours which could be readily discriminated. A subsidiary step is to adapt these colours to a particular industrial process; e.g. the nuclear power plant. Colours will be needed for long term monitoring - i.e. be comfortable to view for long periods of time - as well as for alerting the operators in an "alarm" situation.

Some conclusions are reported in Ref(6). Very briefly, these include the following:

In a specific environment, specific concepts will be associated with specific colours. Therefore, be specific in the use of colours; one colour should identify only one thing, thus ambigui-

ties and frustrations are limited and safer operator performance enhanced. Be careful with intensity; too high intensity may produce eye fatigue. Leave the overall intensity to personal preference.

Use safety colours as recommended internationally; do not apply safety colours for any other purpose.

The medium in the piping is a good colour identifier. Inactive circuitry can be grey. The number of colours in a display depends on the purpose of the use of colours. If each colour has an independent information content, we have experienced that eight different colours in a display does not seem unreasonable. If possible, avoid use of colours of very different frequencies (hues) in one display, otherwise it may be easy to impose eye fatigue.

To avoid flickering, refrain from the use of large coloured areas. The black screen is an excellent background colour.

References

(1) NKA/KRU-P2(79)111 M. Holmgren & J. Ø. Hol
Attitudes to Computer Control Systems - an Industrial Application.

(2) NKA/KRU-P2(80)104 M. Holmgren
The Development of "Process Feeling" and Problem Solving Behaviour in Computer-Based Control Rooms.

(3) NKA/KRU-P2(80)102 M. Holmgren
Performance of Unexperienced Subjects in a Computer Based Control Room.

(4) NKA/KRU-P2(78)105 M. Holmgren, J. Ø. Hol
Use of Colours as Information Carrier in Computer-Based Control Rooms. (1978-11-29)

(5) NKA/KRU-P2(79)106 M. Holmgren
A Working Paper on the Usefulness of Standards for CRT-Colours.
June 1979.

(6) NKA/KRU-P2(80)103 J. Ø. Hol, Gunnar Øhra
Development of Guidelines and Recommendations for Colour Display Based Information Presentation Systems.

GUIDELINES AND CRITERIA FOR CONTROL ROOM DESIGN

Due to the flexibility of process computers, system designers have great freedom in their choice of the general strategies as well as specific solutions for facilities to support process operators in coping with the complexity of modern plants. However, since there is neither an established theory nor a proven design practice based on empirical rules for carrying out a design for a computer-based man-machine system, other forms for assistance must be found, and there is a widespread activity in industrial and professional organizations to create relevant design aids and guides.

These aids take on two forms - both of which have been dealt with in this project. The first has to do with design guidelines and the second with design criteria.

Guidelines aim at leading the designer through a more or less structured consideration - based on the design process itself (Ref(1)) - of all the relevant areas and points of concern which can influence the ultimate man-machine system design and implementation. As such it is a kind of "flag-waver" intended to alert the design team - at as early a stage in the design as possible - of potential problems which need to be considered and decided about with regard to the control room design.

Within the project, the general question of guidelines has been approached in two steps. First, a questionnaire dealing with

the state of the art and the predicted trends within control room design was distributed to utilities within the Scandinavian countries and the Halden project signatories. See Ref(2).

The results were a useful input to the activity connected with the generation of a guidelines document. This document is available separately (See Ref(7)) and is essentially a Finnish effort based in part on similar work being carried out in international circles under the auspices of the European Workshop on Industrial Computer Systems (EWICS).

Result of the Questionnaire

Staffing

There is less manning in the fossil fuelled plants than nuclear, on the average 1-2 persons less per shift, and 4 shifts compared to an average of 7 in nuclear plants. The operator licensing body is in the majority of cases the plant management itself; i.e. only one nuclear plant has a government body, and another a mixed government and plant management body.

Well into the future, the manning on shift will be the same for both fossil and nuclear plants. Nor will there be any change in the formal education requirement, at least not for the first 10 years. The main arguments given are that instrument refinements will handle any increased process complexity. In the first 5 years, management will still retain the operator licensing responsibility, but later on the body will be a composite of government and management: a purely governmental body is highly unlikely.

Today, operator qualification is maintained through work in fossil fuelled plant. In nuclear plants, "brush-up" courses are used in addition to on-site training and in 4 of 5 plants simulators are used. In one nuclear plant, the work itself was considered sufficient. Thus simulators are on the move for operator training. Regular re-certification (24 months) of operators is done in only 2 nuclear plants.

In the coming 5 years or more, the efficiency of simulators in operator training is assumed to be moderate to high by the nuclear industry. Fossil plants do not indicate any such use of simulators; their approach is to use brush-up courses for maintaining operator qualification.

Operator Role

Control takeover

In the majority of plants, the operators can take over almost all control when automatic control fails to function. Even though there is some scattering in the concept of automatic control failure, it can be said that today the crew is authorized rather extensively to take control. One may assume, however, that the automatic control systems of new plants are very reliable, which means that the crew may not be ready for a takeover unless they are trained by other means, and that the design criteria of procedures and the man/process communication systems need to take due consideration of such unpreparedness.

In the coming 5 years there will be no change in the manual portion of supervision and control, but in a 5 to 10 years time this portion will be reduced. The reduction will be due to instrument refinement and computer applications. In more than 10 years the manual portion may increase again for legislative reasons.

Responsibility structure

Without exception the responsibility structure is a vertical hierarchy from assistant to operator. Oral reports and log books are the general form of reports to management of shift activities. In 4 of 10 cases, completed forms are used for operational information to management. There seems to be a rather high potential for (already developed) computer "mailing and conference systems". This goes for not only the shift-to--management reporting, but also for shift-to-shift information.

Task distribution between operator and control system

In the majority of cases, the operating crew is not assigned to any additional significant tasks other than supervision and control. Additional work like statistics, fire guard and simple periodic testing is mentioned.

Automated control of discrete loops alone is found only in one plant; the rest have in addition automated plant monitoring, automated sequence control of interconnected plant units, and sequence control including arithmetic operations (load follow). In 7 plants, computers are used for plant status monitoring.

The present structure of the operators' main tasks will apparently be maintained in the first 5 years. Thereafter there will be less routine tasks and more planning. The overwhelming reason for the change is the impact of use of computers, effective in about 5 years.

Control rooms

Those who work in control rooms have little or no influence on control room design. In only 1 case of 10 did a shift supervisor take part in a design process. The main mode of arranging the man/process communication is according to a combination of operator tasks and plant lay-out. A few arrangements are, however, purely according to plant lay-out.

In half of the plants the main mode of information presentation is by graphic panels with conventional instrumentation. The other half have a combination of conventional and computer--based information presentation.

It is believed by 8 of 9 answerers that conventional instrumentation will be retained in control rooms for safety instrumentation in the foreseeable future. A smaller majority (6) thought that control instrumentation would remain conventional. The probable operator influence on control room design seems to be almost as meagre as today.

Design Criteria

Guidelines for design as defined above, while a necessary aid for ensuring a more systematic treatment of important factors with relevance for the control room situation, are not of as great a value in assisting the designer in choosing among possible alternative solutions to the design questions which are raised. In order to aid this process, an appropriate set of criteria is necessary in order to identify and define various critical attributes, which need to be compared and evaluated.

The importance of criteria as judgement aids increases directly with the variety of solutions available as well as the degrees of difficulty in establishing quantitative specifications for performance - and it is clear that this is exactly the situation existing when incorporating computers and people in a system.

Actually more than one set of criteria is required.

1) Criteria related to the consideration of man as a system component and thus connected with the characteristics of behaviour discussed in this report.

2) Criteria related to consideration of the system as a man's environment. Locally in terms of "working life quality": e.g. increasing levels of automation create a need for criteria to counteract the situation when the tasks left to system operators are a scattered set which cannot be packaged into an integrated profession. Globally, large, centralized systems mean potentially large consequences from maloperation and thereby create the need for criteria to protect people in general and to formulate responsibilities of system operators in particular.

A set of design criteria belonging to category (1) and based on the operator model discussed previously has been proposed. A comparison of the consequences of employing these criteria on the presently accepted view of "quality of life" attributes (2) has fortunately indicated no immediate conflict.

If the discussion is thus restricted to a consideration of "man as a system component", then the criteria listed below are considered to be important. For further details, see Refs (8) and (9) as well as the next section.

a) To insure proper activition of the operators

Discrimination - cues for activating the operator must be weighed and presented according to their importance in order to "alert" the operator to the full significance of the change and thus avoid hasty and inappropriate decisions and/or actions. Thus discrimination = detection + preliminary identification + proper activation of skill-, rule- or knowledge-based behaviour.

Sensitivity - information must always be presented which will keep the operator's "feel" (or, in other words, his subconscious plant model) updated and synchronized so it can serve as a reliable reference for detection of changes or preparation for coming events or tasks.

b) To also insure proper information transfer and control the fit between system demands and operator resources.

Compatibility - information must be transformed into a set of symbols consistent with the needs of the operator in his current behavioral mode or level of abstraction, i.e.

- skill-based support
- rule-based support
- knowledge-based support (including information at physical, functional and intentional levels of abstraction)

Flexibility - operators must be able to shift strategies and behavioral modes dynamically without losing support from the interface.

Pacing - operators must be able to take over pacing when resource/demand conflicts arise so as to be able to reduce stress effects and possible resource deterioration.

Preparedness - normal activities, tasks and support facilities must serve to prepare the operator for the demands which can arise during infrequent and unfamiliar situations.

c) To insure adoption of the proper goal.

Responsibility - competence follows responsibility:

- the designer is responsible for the effect of the automatic features - therefore either present clear statements and orders or automate their activation.

- the operator must be in control when he is responsible. In these instances, support his needs and preferences.

Trustworthiness - operators must be able to trust the information presented. Data transformations, extrapolations, predictions, etc. must not be carried to a point where correctness and consistency cannot be verified. The operator must understand the basis for these transformations, etc.

d) To support system analyzability for reliability and safety

Reversibility - the effects of errors and mistakes must be clearly observable and reversible. Design for operator self-monitoring and correction.

Error tolerance - if the effects of errors, mistakes and extraneous acts will be irreversible and unacceptable, then protect personnel and equipment by the use of barriers, interlocks and/or automatic safety features.

References

(1) NKA/KRU-P2(80)220 Björn Wahlström
Om planering och konstruktion av man-maskin-system.

(2) NKA/KRU-P2(78)101 J.Ø. Hol
Questionnaire.

(3) NKA/KRU-P2(78)100 J.Ø. Hol, K. Netland
"State of the Art" of Control Room Design.
(1978-02-10).

(4) NKA/KRU-P2(79)104 J.Ø. Hol
State of the Art - Status of Questionnaire Response.
June 1979.

(5) NKA/KRU-P2(79)113 J.Ø. Hol and E. Edsberg
Recommendations and Guidelines for Design of Future Control Rooms - Analysis of Questionnaires 1978/79.

(6) NKA/KRU-P2(80)101 J.Ø. Hol
Analysis of Questionnaire 1978-79.
Questions from the Answered Questions.

(7) NKA/KRU-P2(81)239 J. Ranta, B. Wahlström and R.Westesson
Guidelines for the Design of Man-Machine Interfaces.

(8) NKA/KRU-P2(78)7 Jens Rasmussen
Notes on Human System Design Criteria.
(September 1978).

(9) NKA/KRU-P2(80)27 Jens Rasmussen
Some Trends in Man-Machine Interface Design for Industrial Power Plants.
Risø-M-2228, March 1980.

SPECIFIC SUPPORT SYSTEMS

General Structure

One of the specific goals of this project was to investigate the use of process computers for the improved design of data presentation and operator support systems - especially for disturbance analysis and diagnosis during infrequent plant abnormalities. In particular, there was an interest in using the computer as an integrated display generator with all the potential such an approach could provide for satisfying the varying needs of the operator for information. These needs had come out of the related studies of the work situation in the control room as well as the operator's methods and strategies for coping with the control tasks which were involved. This interest was in keeping with the point of view which has been expressed repeatedly in these reports that the advent and ultimate incorporation of computer-based technology will place new demands in systems designers. In order to derive the maximum benefit from the almost unlimited technical possibilities which are available, designers will have to be aware of the details of operator tasks and operator behaviour. Essentially this requires an identification of the operators' tasks and information requirements on the basis of a multi--level consideration of the process system and the states in which this system can lie or be put into. Such a multi-level approach should consider:

- over-all purpose and goals of system (operations, safety ...).
- main plant production "path" from source to sink with all transformation, transport and storage processes together with the necessary supply, support and conditioning parameters for maintaining production.

- the individual supply and support functions as made up of "standard" (sub)processes.
- the corresponding physical equipment with its functional properties and limitations.

The above corresponds to viewing the system at several different "levels of abstraction". See Refs(1)+(11). To each level corresponds a set of possible states which when in their target (or design) condition "enables" the next higher level to function. An important requirement thereafter is to determine the corresponding set of information which is necessary/sufficient to characterize these states and also be sensitive to deviations in <u>actual</u> state from <u>target</u> or <u>intended</u> state. Operator control tasks arise from a consideration of state transitions - e.g. "start-up" which describes how the physical components must be combined to result in subfunctions which condition higher-order functions which ultimately enable production <u>or</u> "automatic shutdown" which describes how the plant (should) "disintegrate" into identifiable stable subprocesses meeting target state requirements. Using such an approach enables some general remarks to be made about the operator's need for information as a function of level of system consideration and control task. These are summarized in fig. (4).

To this discussion about operator tasks and information requirements need to be added the constraints imposed by human functioning - especially in diagnostic situations - which have been described in a previous section. Thus, e.g., any display set must be made up of subsets of data presentations which compare actual and target states at the level corresponding to the operator's immediate control task. Furthermore, the information presented and the coding used must match the three levels of operator performance discussed earlier - skill-, rule- or knowledge-based.

In this connection, the following representation of information needs can be useful:

MULTILEVEL DESCRIPTION OF SYSTEM	GENERIC TYPES OF INFO REQUIREMENTS
OVERALL PRODUCTION STRUCTURE OF ENERGY, MASS, INFO FLOW	- QUANTITATIVE DATA ON LEVELS OF PRODUCTION - QUALITATIVE INFO ON STATES/MARGINS FOR CRITICAL CONDITIONS, SUPPLIES AND BARRIERS - POSSIBLE CONTROL POINTS
SUBPROCESSES AND FUNCTIONS TO SUPPORT PRODUCTION AND ENSURE SAFETY	- QUANTITATIVE INFO ON CRITICAL VARIABLES VS REFERENCES/LIMITS - QUALITATIVE INFO ON SUBPROCESS STATE AND CONDITIONS - I.E. AS REQUIRED, DISTURBED, FAILED - CAUSAL FLOW STRUCTURE WITH POTENTIAL CONTROL POINTS
PHYSICAL EQUIPMENT CONNECTIONS/PROPERTIES	- QUANTITATIVE INFO ON PHYSICAL VARIABLES VS REFERENCES/LIMITS - QUALITATIVE INFO ON OPERATION - EQUIPMENT AND COMPONENT CHARACTERISTICS

Figure 4.

Level	Info used as	To assist in	Goals
Knowledge-based	Symbols	Problem solving ⇒	Plan what how
Rule-based	Signs	Recognition ⇒	Task ⇒ Set of rules
Skill-based	Signals	"Keeping on course"	Manipulation

Thus, for skill-based manipulations of control rods, test equipment, etc. the information feed-back should act as <u>signals</u> which define the space-time relations, deviations, variations, margins between the controlled object and the environment. On the other hand, when monitoring, the operator must rely on the displayed information to serve as <u>signs</u> about the state of plant - either to identify the situation and be able to associate to the appropriate set of rules, or to check the progress of the execution of the rules. Thus the presented signs must be sufficient indicators of system state. In tasks where skills and rules are unavailable or inadequate, the required problem solving activity will have to be supported by information in the form of <u>symbols</u> which can be directly utilized and manipulated within the frame of the mental representation of the plant currently being used by the operator (i.e. the levels mentioned above).

All of these have strong implications for the depth and breadth of the display coverage, and the earlier mentioned criteria of discrimination, compatibility and flexibility will be especially relevant, in order to

- optimize the operator's ability to recognize the full significance of plant behaviour and help him to distinguish between situations where rules and procedures are adequate and must be followed, and situations where this is not the case and the operator must think and decide for himself. See Ref(2).

- follow his immediate needs for display support as his mental representation of the plant shifts among the various abstraction levels.

- influence his willingness to offer resources in a knowledge-based activity to decide on a course of action as well as check on the consequences of his corrective actions.

One of the points of this approach is that most attention to date in designing VDU displays for search support has been given to lower abstraction level aids in the form of mimic diagrams of plant (sub)systems which in reality are structured around the more physical aspects of the system such as components. However, there is a need, especially in the early diagnostic phases, for depicting system structure and behaviour at a higher device-independent level of abstraction and for supporting operator thinking at this level by incorporating suitable tranformations of the basic process data. Thus, at these higher levels, it is felt that operator attention should be centered around fundamental process behaviour related to the mass and energy in the system and their status with respect to normal. This requires that pressures, temperature, and valve positions, which on typical mimic diagram are visualized as pressures, temperatures and valve positions, have to be converted to flows and inventories and suitably represented within a suitable system flow structure. See Ref(2).

Procedural Support

Written procedures are an important ingredient in the control by management of costly and potentially hazardous facilities. E.g., in the U.S. nuclear field, there exists a legal requirement for this kind of documentation which, in turn, has created the need for extensive implementation and control mechanisms for generating, reviewing, approving, auditing and updating procedures. Procedures represent a desire on the part of their designers for a formal and standardized conduct of affairs so that tasks will be performed in the same way every time in accordance with an approved method. However, as an analysis of event reports such as the American LER's will confirm, conflicts often arise between these goals and actual practice. Reasons for this are:

- Involvement of humans in carrying out procedures.

- Existence of a process environment which is highly dynamic in nature and not always foreseeable.

It seems also evident from experience in the field that apparent misconceptions often lead to the attempted use of procedures in non-procedurizable tasks - i.e. expecting of rule--based behaviour in a knowledge-based task situation. This is discussed in more detail in Refs(3)+(4).

Of particular interest to the project was the possibility of using the process computer as a means for supporting the generation and use of written procedures.

A transformation from conventional paper-based procedures to a computer-based implementation with VDU's opens up, of course, a vast spectrum of possibilities. The most obvious are connected with the facilities which become available for on-line preparation, editing, storing or retrieval of procedural material. A second advantage is connected with the possibilities for administrative control which can be incorporated - for example, in recording the usage of procedures. The third important feature is the direct availability of the process data base which can be accessed during the actual execution of procedures, checklists, etc.

In using the computer with VDU's for procedural support, there are two aspects which need to be considered:

- support rule memory
- support rule execution

Operator memory for rules is notoriously poor in general so that the prescribed sequences themselves should be displayed for convenient reference. Secondly, the series of state-action--check routines which constitute a typical procedure need appropriate support in the form of displays which allow the operator to check and verify that the prerequisites for the step are as required, that the proper action has been taken, and that the results of the action are as intended. Illustrations of this can be seen in Ref(5) which builds on two samples of procedures used at the Halden simulator.

Generation of Procedures

Some thought has also been given to the systematic design of procedures based on plant requirements for the proper sequencing and coordinating of the prescribed actions for moving the plant from one state to another. This approach makes use of the flow modelling concept discussed elsewhere as an aid in structuring the plant and decomposing the given control task into a consistent set of subtasks. The results of this analysis are combined with suitable heuristics for task sequencing as well as other considerations of the time dimension as well as material and energy resource requirements, etc. in a way which is analogous to a project planning activity. For further details, se Ref(6).

Automatic Diagnostic Support

The use of computer-based control and instrumentation systems makes the idea of incorporating some form for advanced automa-

tic diagnostic assistance attractive - indeed, the complexity of process plant almost requires that this be done. Problems in implementing such a scheme have to do with assuring that a satisfactory allocation of roles and responsibilities between the automatic system and the operating staff can be defined, accepted and maintained. In addition, management, regulators, designers have to be convinced that the necessary effort will reduce the probability that the spectre of the rare unforeseen, potentially catastrophic event can become a reality to an even more remote level than is claimed for it today. However, the pressures are real and there is a great deal of activity going on in the area of computer-aided diagnosis - in particular, with the aim of supporting the operator's detection and identification of disturbances in the system. Within the confines of the KRU-project member organisations, the following can be reported:

1. Alarm handling

It is obvious that present day conventional alarm systems cannot cope with the complex situations which arise. Actual alarms can often be hidden by the abundance of less important alarms. True alarms are mixed with less urgent status indica-Order of occurrence can be difficult to ascertain and, most importantly, the operator can risk not being able to see the "forest for the trees".

Thus a VTT study (Ref(7)) looked at various kinds of alarm inhibition schemes such as "event" alarms, dynamic priority assignments, blanking of stationary alarm patterns etc. as well as the implications of these for presentation to the operator.

Halden has proposed a computerized logical and filtering scheme for alarms (Ref(8)) with facilities for alarm display, alarm journals, and user documentation of the underlying basis for the implemented filtering.

2. DAS studies

In recognition of the fact that there no doubt are limitations in how far more complex processing of individual conventional alarm signals can be carried, the DAS concept has been introduced in Europe as well as in the U.S. In particular, Halden and its signatory partners (especially GRS in Germany) have been involved in designing and evaluating this approach. While not directly a component in the KRU-project, it is mentioned here as representing one school of thought regarding computer-aided disturbance analysis against which the KRU-approach can be compared.

The DAS method in question uses preconstructed disturbance models containing the anticipated flow of events for the given disturbance. These form the reference data base against which actual evolutions detected in the plant are compared in order to aid in an identification of prime cause, present status, possible propagation and recommended corrective action. The aim is to give the operator an early warning with better information in advance of conventional annunciator systems and thus more time to avoid a possible automatic safety action. More details can be found, e.g., in Ref(9).

3. Flow modelling andautomated plant diagnosis

Automatic, computerized diagnosis can be based on several different search strategies, e.g. a search for a match between a pattern of measured data and some stored symptom patterns, as illustrated by the DAS approach, or a search to locate a change in the system's functional state with reference to a stored model of normal or specified plant state. The latter strategy has a number of basic advantages: it is independent of the prediction and analysis of specific faults and events; the reference for search, the normal state, can be derived from actual plant operation by the computer; the strategy can be based on invariant relations such as conservation laws; etc.

In the project, the use of conservation laws of mass and energy for diagnosis of plant malfunction has been explored; see Ref. (10). An advantage of this approach is that it is possible to

diagnose unforeseen plant disturbances; this is due to the general nature of the conservation laws. Furthermore, accumulation of mass and energy is a potential source of risk in plant operation, and the identification, counteraction and location of unbalances is thus an important aspect of process plant diagnosis. The plant flow model which has been developed describes the topology of mass and energy flows and represents qualitative aspects of plant function in a given operational mode.

Diagnostic strategies based on these flow models can be used in the design of automatic disturbance analysis and control, but they can also be used for organising the available measured plant data in a meaningful way for an operator and for supporting him in the need for rapid "zooming in" on the relevant details in a complex situation. As a corollary, this approach can be used to determine the adequacy of the instrumentation to measure all relevant parameters needed for diagnosis.

References

(1) NKA/KRU-P2(80)23 — L.P. Goodstein and J. Rasmussen
Man-Machine System Design Criteria in Computerized Control Rooms.
N-7-80. February 1980. (An abbreviated version will appear in the proceedings of the IFIP/IFAC "Assopo 80" Conference, Trondheim 16-18 June 1980).

(2) — L.P. Goodstein
Discriminative Display Support for Process Operators - in "Human Detection and Diagnosis of System Failures". Jens Rasmussen, W.B. Rouse (eds.).
Plenum 1981.

(3) NKA/KRU-P2(79)13 — L.P. Goodstein
Procedural Support.
February 1979.

(4) L.P. Goodstein
Procedures for the Operators - Their Role and Support - IWG/NPPCI Specialists Meeting on Procedures and Systems for Assisting an Operator .... 5-7 December 1979.
Munich FRG.

(5) NKA/KRU-P2(81)37 L.P. Goodstein
Suggestions for Incorporation of Procedural Support.

(6) NKA/KRU-P2(79)26 M. Lind
The Use of Flow Models for Design of Plant Operating Procedures.

(7) NKA/KRU-P2(80)224 Björn Wahlström and E. Rinttilä
Inhibition of Alarms during Nuclear Power Plant Operation.

(8) NKA/KRU-P2(80)106 B.B. Thomassen and J. Augustin
Alarm Generation - A Concept Based on Logical Filtering.

(9) W. Bast and L. Felkel
Disturbance Analysis Systems - in "Human Detection and Diagnosis of System Failures". J. Rasmussen, W.B. Rouse (eds.).
Plenum 1981.

(10) M. Lind
Use of Flow Models for Automated Plant Diagnosis - in "Human Detection and Diagnosis of Systems Failures". J. Rasmussen, W.B. Rouse (eds.).
Plenum 1981.

PROCESS MODELLING

During a period of changing level of automation and control room design, an important basis for planning of the roles of the operation staff, for design of specific tasks involving availability and safety, and for choice of appropriate operator support, is a systematic description of the technical system, its different operating modes, and the control requirements for maintaining as well as for transition between operating modes. In the project, two separate approaches have been taken to this problem.

First, the operating modes of the plant, which are generally used in operational planning such as hot and cold shutdown, power production, disturbed operation, etc., have been defined, and the implications in terms of the state of subsystems and equipment have been analyzed. Then control requirements and the related operator tasks have been determined partly by technical analysis and review of operating procedures, partly by interviews of the operating staff. This approach has been used mostly in connection with the Swedish and Finnish program on operator competence and training and is described in greater detail in Ref. (1).

Secondly, an attempt to develop a consistent, formal description of the functional states of the system, based on energy and mass flow structures and formal rules for decomposition in subsystems and functions, has succeeded in establishing a formal framework for deriving target states or normal states for subsystems from overall plant goals as well as identifying the related actual states by information integration from measured data. The framework also appears to be promising as a tool for synthesizing control programs for sequential control and, as was mentioned earlier, for designing operating procedures and ascertaining the adequacy of the instrumentation. Se Refs (4) + (5).

In addition, the relevance of the flow model approach for automatic diagnostic support has been mentioned previously (see also Ref(6)), as has the importance of the concept for information display. See Ref(7).

References

(1) NKA/KRU-(81)12 — Technical Summary Report on Operator Training.

(2) NKA/KRU-P2(78)206 — B. Wahlström and J. Timonen
Notes on a State Description for the Combined System Process, Instrumentation and Operator.

(3) NKA/KRU-P2(78)201 — L. Tuominen, B. Wahlström and J. Timonen
A System and Task Description for the Operating Personnel of the LOVIISA Nuclear Power Station.

(4) NKA/KRU-P2(79)26 — M. Lind
The Use of Flow Models for Design of Plant Operating Procedures.

(5) NKA/KRU-P2(79)216 — Sauli Päkkilä
Working Paper: Mass and Energy Balance Analysis of LOVIISA I Plant.

(6) M. Lind
Use of Flow Model for Automated Plant Diagnosis - in "Human Detection and Diagnosis of System Failures".
Plenum 1981.

(7) L.P. Goodstein
Discriminative Display Support for Process Operators - in "Human Detection and Diagnosis of System Failures".
Plenum 1981.

Analysis of Work Situations

There are (at least) two lines of approach available for studying the operator's interaction with the plant. The one - described in a companion report (Ref.(1)) - produces as one result a set of typical tasks which could form the basis for training, competency ratings, etc. It is thus possible to consider these tasks as isolated elements which the operator must be equipped to handle by giving him the necessary knowledge and skills.

However, as a basis for control room design and evaluation, operator interaction needs to be analyzed more from a situational point of view in order to describe/evaluate such things as:

- workload - fx, from simultaneous tasks.
- information flow requirements.
- situational factors affecting human reliability.
- manning.

Such a situational analysis was performed as part of the project in the form of a study of a PWR startup which was based on the startup procedure itself complemented with comments from the operational staff of the plant in question. See Refs. (2) - (5). One of the outputs of this study was a "time-line" description of the operator's work situation over an approximately 48 hour period. This graphical representation indicated the distribution vs. time of the operators' tasks as specified by the procedure in eight process-related areas (e.g. reactivity, chemical and volume system, secondary system, etc.). An excerpt is shown in Fig. (5). This work has been used, among other things, in connection with the design of displays for procedural support - see the previous section.

These analyses have also aided the design of the experimental situations used in the simulator studies of computer-based displays. See Refs.(6) - (8). The situations had to preferably

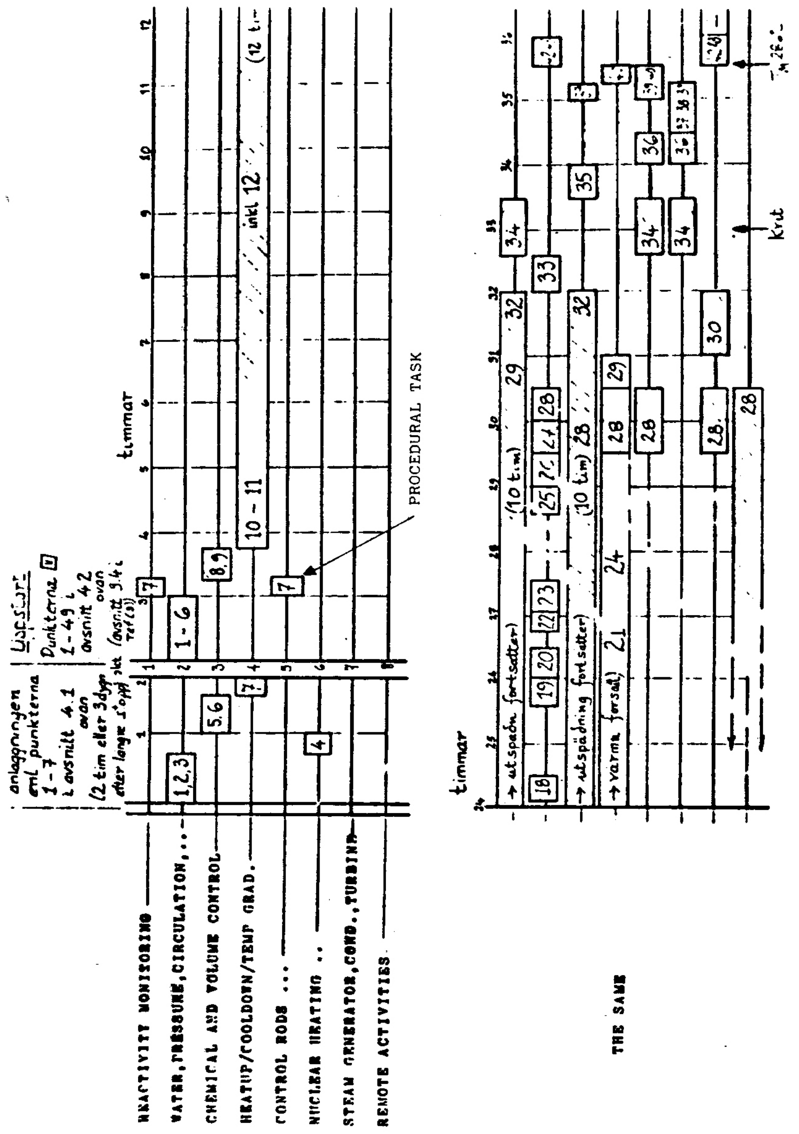

Figure 5.

- be simulatable,
- be based on actual operating experience,
- be of suitable duration and complexity,
- incorporate task elements of control, sequencing, optimisation, diagnosis, monitoring and safety backup,
- include episodes which offered a realistic possibility for operator intervention and recovery.

However, the lack of post-trip features in the available simulator has until now restricted the spectrum of disturbances to either less dangerous (initially) or more slowly developing situations where the operator has a chance to interact before a trip condition is reached.

The use of reference situations for studying operator behaviour requires that the process behaviour must be defined, controllable and repeatable in order to provide a well specified and stable environment. A typical KRU scenario consists of

- a background task based on normal, expected situations.
- an episode in the form of an abnormal unexpected disturbance.

To these could be added a repertoire of embellishments such as interruptions, telephone calls, log book activities, etc. This has not yet been done.

References

(1) NKA/KRU-(81)12 Technical Summery Report on Operator Training.

(2) NKA/KRU-P2(78)308 Helge Tuxen-Meyer Arbetssituationer för kontrollrumsper-

sonal vid värmning av reaktorsystemet och uppkörning genom kritikalitet till 5% reaktoreffekt.

(3) NKA/KRU-P2(78)310 Helge Tuxen-Meyer
Arbetssituationer för kontrollrumspersonal vid värmning och uppkörning av en tryckvattenreaktor PWR typ R2.
(1978-12-07)

(4) NKA/KRU-P2(79)313 H. Tuxen-Meyer
Sekvensanalys PWR typ Ringhals 2.
Värmning och uppkörning.

(5) NKA/KRU-P2(79)315 E. Forsyth och H. Tuxen-Meyer
Sekvens- och time-line analyser för PWR typ Ringhals 2.

(6) NKA/KRU-P2(78)9 L.P. Goodstein
Reference Situations and a Proposal for an Experimental Program.
(September 1978).

(7) NKA/KRU-P2(78)307 A. Bhattacharya
Simulating "Scenerios" of a PWR Plant for Operator Task and Reliability Analysis and New Control Room Concepts.

(8) NKA/KRU-P2(79)112 J.Ø. Hol
Episodes for the First Experiment.

THE EXPERIMENTAL PROGRAM

Introduction

The primary aim of the program was to investigate the effectiveness of computer-based displays as an aid for operator response to plant situations including disturbances. This

activity was a natural extension or continuation of the more conceptual work carried out on operator behavior and strategies, task requirements and system characterisation (see other sections) and led to the establishment of a "test bed" facility for pursuing an experimental verification of the ideas which had been developed.

There were several basic ingredients required in order to set up and operate such a test facility:

- simulation of the process to serve as the "test vehicle" in sufficient breadth and detail.

- implementation of the advanced man-machine interface system with colour VDU's, keyboards, etc.

- establishment of the necessary methods and facilities for recording and evaluating the performance of the experimental subjects.

- selecting and training of the subjects.

These will now be treated in a little more detail.

Experimental Simulator Facilities and Control Room Interface

A power reactor simulator facility for studies of operator performance has been developed and implemented at the OECD Halden Reactor Project, Halden, Norway, and based to a great degree on the Swedish STUDS-development at Studsvik Energiteknik AB. The chosen setup is a continuance of the on-going research in man/process communication started about ten years ago. A prototype computer-based control room was developed and used for many years for intermittent supervision and control of the Halden Boiling Water Reactor. The experimental facility is thus a realisation of the experience gained through these years and with extensions to cover the presently planned research. See Ref(1).

Viewed by an operator, what is represented is a simplified Pressurized Water Reactor (PWR) plant, controlled and supervised from a computer-based control room with no so-called "conventional instrumentation". While the operator(s) works on a predefined task, e.g. to raise the reactor power from 35% to 100% of full power, the experimentalist may introduce a malfunctioning or a set of malfunctions in the process. These should be detected and identified, and proper counteractions found to avoid plant shutdown. Any period of operator task performance can be logged on file, including operator-process interactions and associated plant data. Additionally, all operator actions and some main process parameters are logged on-line on a hard-copy printer (line-printer). The complete process history, or selected parts of it, with the concurrent operator actions can be reproduced/replayed in detail from file. This includes the use of the buttons on the operator console keyboards so that the displays shown on the VDU's (colour CRT is used as Visual Display unit in the operator console) are repeated in the same real-time sequence as during the original run.

There are two operator consoles, each console holds a VDU with a display controller, a function keyboard, an alphanumeric keyboard and a tracker ball. The function keyboard is used to request displays and to manoeuvre plant elements such as switch pumps on/off, open/close shut-off valves and position modulated valves. An additional feature are the so-called "dead man's" buttons. These are buttons that are active for as long as they remain pushed; in the present set-up they are used for control rod positioning. The function keyboard holds also trip buttons for turbines and reactor. The alphanumeric keyboard is mainly used for input of control parameters and display specifications such as process variable selection and periods in trend displays. A third console is dedicated for alarm presentation and includes an alarm handling keyboard. Except for alarm presentation, all information is presented on operator's request only.

The operator controls the process that is simulated, but the experimentalist controls the simulator. This is done through a standard b/w VDU terminal. A set of commands is available for start of simulation at a selected reactor power level, initiation of the logging facility, run a real-time simulation, implement process malfunctions; and for freeze, restart and stop of the simulation.

The simulation can be done in either of the three modes: simulation, experimental-run and playback. In the simulation mode, control and supervision of the simulated process is done without any logging. All time notations are in real-time. The experimental-run mode gives the same possibilities for process control, but in addition the logging is operative. All time notations are now given as seconds, minutes and hours after start (elapsed time). In the playback mode, the logging of the experimental run is displayed on the keyboards and VDU on the operator's consoles without any logging. Any selected period of process history can be replayed with a resolution of 15 seconds.

Playback of the process history starts with initializing the simulator with the set of logged static and dynamic data nearest to the given starting time. From then on, the simulation proceeds as if in simulation mode; e.g. no more filed process data are introduced. The reproduction of the process history is taken care of by playback of the operator activities. Each second, the simulator is acted upon by the filed actions as during logging; hence the operating history is exactly repeated, at least in principle. Due to technical problems during the first experiments, the reproduction of the operating history was only approximate.

Experimental Methodology

There were several factors which weighed heavily in the selection and implementation of a suitable experimental methodology.

The first factor selected for the goal of evaluating display support as an operator aid. This cannot occur by taking an isolated display out of a set and testing its function in the operator's decision making by means of a traditional limited scope and well-defined psychological laboratory experiment. Such approaches are only realizable for testing, e.g., specific perceptual coding features such as colours, symbol size and shape, brightness, etc. This is because displays play different roles according to the specific situation, and the total set of display must therefore be tested in the complete context including possible interference in rare situations with the stereotypes and habits formed during familiar routines. If we to this add the difficulty of getting a reasonable number of results from experimental "rare events", the conclusion was that the traditional way of getting quantitative, hard data to prove the value of a new design had to be replaced by experiments aiming at a qualitative understanding of the function of the displays in the context of situations based on real-life scenarios. The method required also special features in the simulator for such scenarios as well as special tools for observation, recording and analysis.

This approach was suppported by the desire to employ an experimental technique which enabled the experimenter to follow in detail each individual behavior profile and to relate this profile to the conceptual framework for human information processing which had been generated. This is described in the earlier sections. See also Ref(3). Such a requirement was not compatible with the normal statistical approach.

Thus the decision was made at an early stage to perform a limited number of analysis-in-depth experiments in a "real--life" situation rather than a large number of a more restricted nature. The approach is described in Ref(4). In essence, this states that the use of computers for simulation and data handling means that a complete description of an experimental situation and the operator's response to it can be obtained, stored and recalled. Having this complete record permits the

use of the technique of so-called self-confrontation; i.e. confronting the operator with the behaviour which he actually demonstrated and having him comment on that (rather than his recollection of it). This is best served by replaying for him the actual situation together with a record of his response.

Through this possibility of replication of the way the experiment progressed, one may confront the operator with episodes of particular importance and have him explain what went on in his mind, i.e. what he thought and why he acted the way he did. This, of course, does not guarantee that he will be able to express exactly what he thought or experienced at the moment, either because he cannot completely remember it or because he is distorting his report in order to justify himself, but it is probably the least objectionable way of doing it.

In this way, it was expected that information of the following type would be derivable.

- The effectiveness with which the provided interface activates the appropriate intention or goal within the operator. Which information is used to update his internal model, to direct his attention and activate his value system?

- The extent to which the operator will be willing to or can use his normal resources and the resources offered by the system without his performance being impaired by negative attitudes, stress or distrust.

- The freedom given the operator to develop and use a repertoire of data processes which allow efficient trade-offs in resource/demand conflicts. This freedom strongly depends upon the selection, preconditioning, coding and formatting of the information presented to him.

An experiment thus consisted of the following phases:

Phase.0 - Preparations
Phase.1 - Experiment
Phase.2 - Preliminary analysis
Phase.3 - Self-confrontation
Phase.4 - Final analysis

At this date, a pilot experiment and three subsequent experiments have been carried out. There are reported in Refs (5) - (8). However, development of the methodology and its implementation and testing have delayed the experiments in which specific display sets aimed at achieving compatibility with the operator's varying needs for information were to have been evaluated.

Selection of Subjects

The selection and training of experimental subjects was and is the critical "cog" in the total experimental "wheel" - especially when the question of the validity of results is raised. See Ref (9). This is an important point since, in general, the subjects who participated were (mostly) not the same (type of) persons who work in control rooms, and therefore the impression might be that the immediate relevance of the results would be rather limited.

In answering that question in general, one should keep in mind what the purpose of the simulator study was. In the present context, the purpose was to study the influence of a specific factor (or set of factors) on, e.g. the subject's problem solving, decision-making, diagnosis, etc. The influence is, of course, observed in the performance of the subject, specifically in the way in which the performance is organized. And it goes without saying that it is an advantage if the influence of a factor has an easily discernible effect on the performance.

As described elsewhere in this report, the performance may be characterized by means of the categories of skill-based,

rule-based, and knowledge-based behavior. Since skill-based behavior is characterized by not requiring attention, by being readily available, and by being carried out automatically and efficiently, it is clear that the influence of a factor will be hard to detect if the performance is largely skill-based. Skill-based behavior is an integrated whole which depends on an immediate recognition of the situation as being highly familiar, leading to the automatic activation of a well-learned activity. It is therefore literally a contradiction of the definition to assume that a specific factor can have an influence on skill-based behavior, since if that happens the behavior will no longer be skill-based. What may happen, of course, is that a new skill gradually develops. But in that case it is misleading to talk about the influence of a specific factor, since it is no longer considered in isolation.

Consequently, the performance which is observed in a simulator study should not be predominantly skill-based but rather rule-based and/or knowledge-based. That, however, means that very experienced, hence highly skilled, subjects are not required. Since the influence of a specific factor is best established when the performance is rule-based or knowledge-based, simulator studies will benefit from using experimental situations (tasks) which require such behavior. And if we use highly experienced subjects, such as reactor operators, we will have to design experimental situations which are outside the range covered by their skill-based behavior. This may be difficult. For example, highly skilled operators should not be used to test displays different from those related to their skill, since their habits and biases will influence the result in an uncontrollable way.

Thus although highly experienced subjects are not necessary, this does not mean that the subjects should not be familiar with the system (the simulator). If everything is completely new, the performance will be no more interesting than if everything is completely familiar. The simple functions, such as regulating a valve, changing a setpoint etc. must not present a problem to the subject, i.e. that must be within his repertoire of skills. To say that a performance is rule-based does, of course, not mean that it does not contain skills. Any performance and any type of behavior is based on skills. The difference is whether the organization of the behavior is skill-based or rule-based/knowledge-based; i.e. whether the skill covers the whole situation or only a part of it. As mentioned earlier there was interest in studying the organization of the performance and how it is influenced by specific factors.

The choice of subjects for simulator studies is therefore made easier. We do not have to have highly experienced subjects. The only requirement is that the subjects are so familiar with the system that the handling of it does not present a problem. But it is, on the other hand, an advantage to use subjects with different backgrounds and different degrees of experience. In that way one may ascertain with greater certainty whether the assumed influences really exist. And that means that the validity of the study will be increased. If, for example, one can show that a display of a certain type improves the performance for subjects with various levels of practical experience, assuming subjectively similar tasks, then one is on safer ground than if it was only done for one type of subject. The use of subjects of various backgrounds reduces the probability that the results are an artefact of the characteristics of a single group. Therefore one should never just use highly experienced operators or non-experienced persons, but rather a mixture of as many types as possible.

In the experiments to date, the subjects can be grouped in three different categories with regard to formal education and professional experience. The first group were students from a nearby college with a main curriculum in computer science (administrative data processing). Only a few had professional experience prior to their enrollment and if so, very little in process control. Their age ranged from about 20 to 30 years.

The second group were students from a technical college (Ingeniørhøjskole). All of them were engineers in a one-year extra course in process engineering. A few had professional experience in process-related work and some had pre-educational experience. Their ages were the same as for the first group.

The third group were licenced operators and operator assistants from the Halden Reactor (Boiling Water Reactor). They were either technicians or licensed skilled workers, with additional theoretical training as reactor operators. Their control room experience ranged from about 4 to 20 years and some of them were in process related work prior to their engagement at the Halden Reactor.

In anticipation of a continuation of the experimental program, Halden is considering the establishment of an "in-house" group of subjects to serve as a pool of persons for use in future experiments. The requirements which one must pose to such a group are (1) that they are sufficiently knowledgeable in how a nuclear reactor functions, specifically a PWR, (2) that they are sufficiently trained in the use of the communication system for the simulator, and (3) that they are readily available for participation in experiments. See Ref(10).

Training

The content of the compendium for the theoretical training was partly a joint Studsvik/Halden work (Refs (11) - (14)) and the designed training scheme a joint Risø/Halden work. The aim of the training scheme was to enable the participants to act as operators in predefined operational situations and to master sufficiently the ways and means of a computer based control room communication system. The original scheme was adapted to the college students and can be revised in accordance with the knowledge level of the ensuing groups.

Because of time allocated from the educational institutions, the training had to be concentrated to one week with an additional day for experimentation. The first day was used for introducing the purpose and performance of the experiment and for an excursion to the control room of the Halden Reactor itself as well as a computerized control room of a neighbouring pulp and paper plant. In the remaining 4 days, theoretical and practical training were allocated equal time.

The theoretical training aimed at a crude functional understanding of the nature of a Pressurized Water Reactor. This included nuclear physics and a plant description to give a reference to the control systems. In the control system description, plant behaviour was explained together with the various manual and automatic systems. A survey of the different plant elements (pumps, valves, etc.) and their functions aimed at a basic comprehension of the dynamics of the process. The coding system for the process variables was explained to enable identification of process element variables. The principles behind the various procedures were elaborated, and related to exercises in the practical training. This included the most common plant malfunctions and process anomalies that could be simulated.

The practical training started with an introduction to the presentation techniques on colour CRT's of the computer data used in the experimental set-up, and a crude sketch of the signal handling from simulator to CRTs. Furthermore the display design procedure was explained with the strategy behind the keyboard design and tracker ball functioning, and how these elements function in the man/process communication. The instruction was rounded off with an introduction to the symbolism and information content in the display hierarchy. However, the main portion was used for exercising operational tasks and problem solving.

During no part of the training was the episode (problem) to be handled during experimentation revealed, but problems of the same nature as the episode were trained on.

Training Modification

The training scheme was revised somewhat for the process engineers in that the process control theory was reduced to only what was related to the simulated process. The same was done with the theory of plant element functioning. This was partly compensated for with an expansion of reactor physics and the nature of nuclear plant operation, the man/process communication system, and more practical training. A third revision for the reactor operators reduced the nuclear and process parts even further than for the engineers, and compensated for this with more practical training and operation exercises.

For half of the reactor operators, the theoretical training was given in a conventional classroom manner. For the latter half, it was given in the simulator control room using the man/process communication system, the displays and the running simulator as instructor aids.

Conclusion

The theoretical training of the subjects was not sufficient for a detailed understanding of the nature of a Pressurized Water Reactor and its supervision and control. But it was sufficient for a crude understanding of observed phenomena during execution of simple operational tasks. For some persons the episode to handle during experimentation may have been too complex to fully comprehend, but others performed successfully.

The practical training was sufficient for learning to use the man/process communication system, but not sufficient for attaining skilled proficiency in its use. Because of this, the previous experience of a subject could be decisive for his performance. Although this was not fully anticipated, it could be captured by the experimental method. But it would have provided a serious obstacle for a traditional statistical method.

Preliminary Results

The experience from the experiments which have been carried out so far is that even in the case of trained operators - who may be assumed to possess a thorough knowledge on the theoretical level - the actual handling of the system proved difficult. In all cases there was a wish for more practical training (hands-on training) so that one could "feel more familiar" with the simulator.

Therefore one of the lessons learned was that future subjects will have to have greater opportunities for "on-line" practice so that the use of the available facilities will not be a stumbling block in the subjects' surveillance and control of the process.

The other main result corroborated the usefulness of the experimental method and analysis to give a detailed description of the operator's performance. While being a very craving and laborious technique, there are indications that the essential parts of the method could be incorporated in a training simulation evaluation system.

In addition to this, a detailed analysis has been made for the performance of each subject in three of the four experiments. While it is almost impossible to give a brief summary of this (since that would be against the whole idea behind the methodology), a few comments may be in order.

1) It was clearly demonstrated that the conceptual background for the experiments was useful for describing and analyzing the performances. That goes for the skill, rules, knowledge distinctions as well as the general description of diagnostic strategies and decision-making. It was also shown how one could "identify" the operator's model of the system, and how this made it possible to give a coherent interpretation of his performance. In other words, knowledge of how the operator saw the system made it possible

to understand apparent "human errors"; they were errors from an observer's point of view, but they were consistent, hence correct, with the operator's interpretation of the system.

2) It was further found how the operator's performance could be categorized in terms of some characteristic traits. Examples of these are:

   a) Tactical vs. strategical performance, i.e. whether the performance was a sequence of smaller parts with no essential coordination (tactical), or whether it was well integrated and constituted a whole (strategic).

   b) Surface control vs. control in depth; i.e. whether the operator relied basically on the system as it was represented in the displays, or whether he used additional knowledge. In general, the subjects controlled the system from the surface; i.e. as it was presented to them.

   c) Functional fixation vs. openness. This refers to the well-known phenomenon that a person may become so fixated by, e.g. a specific solution to a problem or a specific interpretation of a situation, that his behavior becomes stereotyped. This is typically an effect of stress, combined with insufficient proficiency in handling the system. It was observed in a number of cases how the structure of the display could heavily influence the subjects' performance.

References

(1) NKA/KRU-P2(80)105 R. Stokke, J. Augustin, O. Falmyr
Simulation Facilities for Operation Performance Experiments.

(2) NKA/KRU-P2(79)121 K. Netland
Measurement of Operator Performance - an Experimental Setup.

(3) NKA/KRU-P2(80)25 E. Hollnagel
The Role of Conceptual Structures in Analyzing Operator Behaviour.
Risø-M-2217, February 1980.

(4) NKA/KRU-P2(79)23 E. Hollnagel
The Methodological Structure of the KRU-Experiments. Notes on the Nature of Qualitative Research.

(5) NKA/KRU-P2(80)28 E. Hollnagel
Report from the NKA/KRU Pilot Experiments - an Evaluation of the Use of a Qualitative Methodology in the Investigation of Operator Performance.
N-18-80, April 1980.

(6) NKA/KRU-P2(80)30 E. Hollnagel
Report from the Second NKA/KRU Experiment: The Performance of Non-Professionals in Controlling a Complex Process.

(7) NKA/KRU-P2(81)36 E. Hollnagel
Report from the Third NKA/KRU experiment: The Performances of Control Engineers in the Surveillance of a Complex Process.

(8) NKA/KRU-P2(81)34 E. Hollnagel
Report from the Third NKA/KRU Experiment - Tape Transcripts and Diagrams

(9) NKA/KRU-P2(80)33 E. Hollnagel
On the Validity of Simulator Studies: Problems and Preliminary Precepts.

(10) NKA/KRU-P2(80)32 E. Hollnagel
Suggestions for the Training of the In-House Group of Persons at the Halden IFE.

(11) NKA/KRU-P2(79)114 J.Ø. Hol
Operator Training for the First Experimental Series.

(12) NKA/KRU-P2(79)117 B.B. Thomassen
Kompendium i reaktorteknikk for STUDS-20 PWR.

(13) NKA/KRU-P2(79)118 G. Ohra
Kompendium for praktisk opplaering om STUDS-20 PWR.

(14) NKA/KRU-P2(80)100 J.Ø. Hol
Kompendium i sikkerhetsfilosofi for STUDS-20 PWR.

HUMAN RELIABILITY

The previous sections of this technical report have treated the portions of the NKA/KRU-project which dealt with the establishing and testing of a conceptual structure of human performance as applied specifically to the monitoring and control of a nuclear power plant (but, in fact, of a more general nature) - a structure which hopefully could assist the designer in utilizing modern information technology in the creation of a well-balanced work situation in the control room. Of similar importance, however, is the growing need for being able to document the significance of the human for overall safety by including the operators in quantitative risk assessments of complex process plants. This means not only analysis of existing installations but also predictions of human errors in future designs - and especially in connection with "rare events" with high risk potential.

The requirement for prediction implies, among other things, that any empiric human error data must be so well founded - both psychologically and with respect to relevant system characteristics - that they can be transferred to other task situations than the original source task.

Little work has been done on such generic psychological error mechanisms, probably because human errors have been considered to be a weakness of operators which could be cured by improved training and better instructions, and because the pace of change of work situations has been slow enough to allow for purely empirical methods. Typically, some of the early attempts to find generic psychological error mechanisms from analysis of professional task performance are from aviation research in order to improve cockpit designs.

In a further pursuit of these goals, work has been carried out within the NKA/KRU framework and in cooperation with the OECD/CSNI Group of Experts on Human Error Analysis. The approach has included an extensive analysis of event reports (mostly from U.S. nuclear power plants issued as Licensee Event Reports (LER's) in a sufficient quantity and as deeply as the detail allows in order to characterize the human errors which occur in practice. See Refs(1) - (3). For example Fig (6) illustrates the breakdown of error modes as a function of the operator's mental task. The table clearly indicates that, in the daily, familiar task environment, most of the errors by far are connected with the planning, recall and/or execution of procedures. However, other analyses have shown that in the rare, unforeseen and unfamiliar situations, operator errors occur mostly during the detection, observation and identification phases.

Fig (7) illustrates the relation between these "generic" error modes and the three layer model described earlier which reflects the operator's various behavioural modes for interacting with the process. Thus problems with procedures fall into the rule-based or the skill-based domain while planning de-

11	12	17		5		117	36	2	Distribution across mental task phase	200
Detection of demand	Observation - communication	Identification of system state	Goal - strategic decision	Target - tactic system state	Task - Determine, select	Procedure - plan, recall	Execution	Various	MENTAL TASK PHASE / ERROR MODE	Distribution across error modes
•	1	1	•	•	•	•	1	•	Absent-mindedness	3
•	•	5	•	1	•	•	•	•	Familiar association	6
6	2	•	•	•	•	1	1	•	Alertness low	10
1	•	•	•	•	•	65	2	•	Omission of functionally isolated act	68
1	2	•	•	1	•	12	1	•	Omissions - other	17
•	1	•	•	•	•	1	9	•	Mistakes among alternatives	11
•	4	3	•	•	•	3	•	•	Expect, assume - rather than observe	10
•	•	1	•	1	•	13	•	•	Side effect not adequately considered	15
•	•	5	•	•	•	15	•	•	Latent conditions not adeq. cons.	20
•	•	•	•	•	•	•	10	•	Manual variability, lack of precision	10
•	•	•	•	•	•	•	10	•	Topographic, spatial orient. weak	10
3	2	2	•	2	•	7	2	2	Various; not mentioned	20

Figure 6. Distribution across mental task phase and error mode of 200 reports of "operational problems" in nuclear power plants.

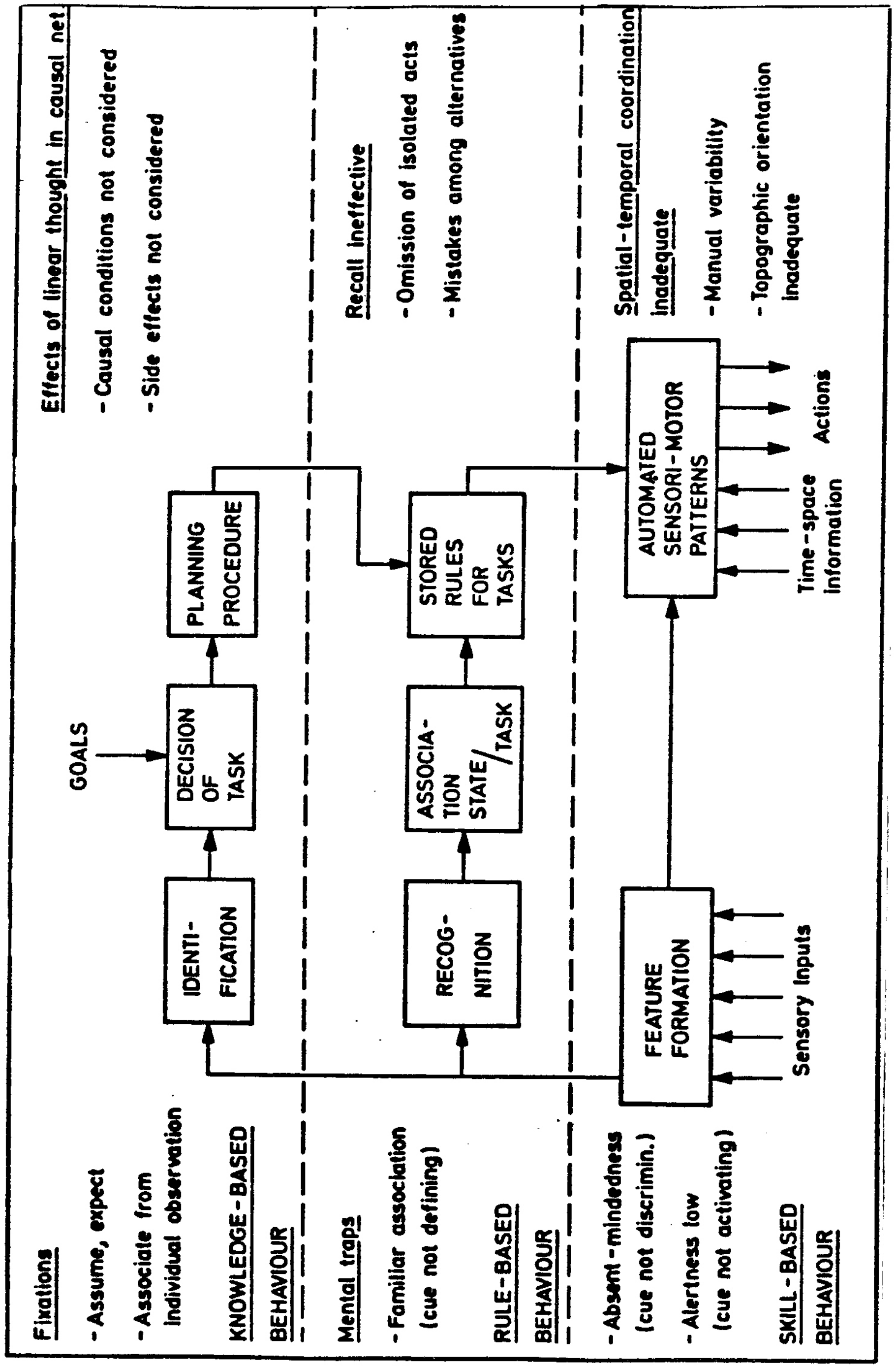

Figure 7.

ficiencies would indicate difficulties in the knowledge-based domain, etc. These sorts of results have significance for the design of the control room displays and controls and were expressed in the form of criteria in an earlier section of this report.

They also have implications for the design of the system as seen from the analyzability point-of-view.

Thus when a task is designed to follow a normative procedure, the elements of the sequence should be cued individually to counteract systematic changes and "optimization" and to identify separate task elements as categories for data collection.

When a task is allowed or expected to be goal-controlled, this is presumably because adaptation and learning are advantageous (and desirable). The task sequence will then be flexible and will depend upon the particular circumstances. In this case, identification of task elements for data collection is generally irrelevant since they cannot be separated from their context in a meaningful way. Analysis of goal-controlled tasks is more realistic if a feedback concept is realized. The task is designed so as to make the effect immediately observable and reversible; then the reliability of the task can be evaluated from the frequency of opportunities for error together with an analysis of the reliability of the error detection act.

Finally, if human mistakes and extraneous acts are found to be significant contributors to irreversible and unacceptable effects, the system should be made error tolerant by introduction of interlocks or barriers, since reliable data on the probability of such human acts cannot be obtained in practice.

Generally, criteria for analyzability will act in unison with design for error tolerance. It will force designers to consider more carefully the distinction between situations where he takes control by normative instructions and where he leaves control to the operator. He will also have to consider in detail the conditions for observability, reversibility and error tolerance.

Returning to the question of data evaluation in the form of event reports, the choice of suitable data categories is important. These, in turn, depend in the uses envisioned for the data. The multi-facet taxonomy (Ref. 4)) shown in Fig(8) has been generated as a scheme for describing and analyzing events involving human malfunctions. This covers "what" went wrong, "how" it went wrong and "why" it went wrong. The total result takes on the form of a causal chain from "why" to "what". How far back from the externalization of the malfunction one needs to go to determine the "cause" for data collection depends on the actual application. For example, to judge reliability of an existing task, it is only necessary to consider the external mode of failure; to judge training and interface design for improvement, the mechanism of failure must be considered; and to evaluate the work situation, the external causes must also be identified.

It is intended that this taxonomy will eventually form the basis for an exploratory international data collection program.

References

(1) NKA/KRU-P3(78)1 Jens Rasmussen
Operator/Technician Errors in Calibration, Setting and Testing Nuclear Power Plant Equipment.
(March 1978).

(2) NKA/KRU-P2(79)15 Jens Rasmussen
Preliminary Analysis of Human Error Cases in U.S. Licensee Event Reports.
March 1979.

(3) NKA/KRU-P2(79)18 Jens Rasmussen
What Can Be Learned from Human Error Reports.
June 1979.

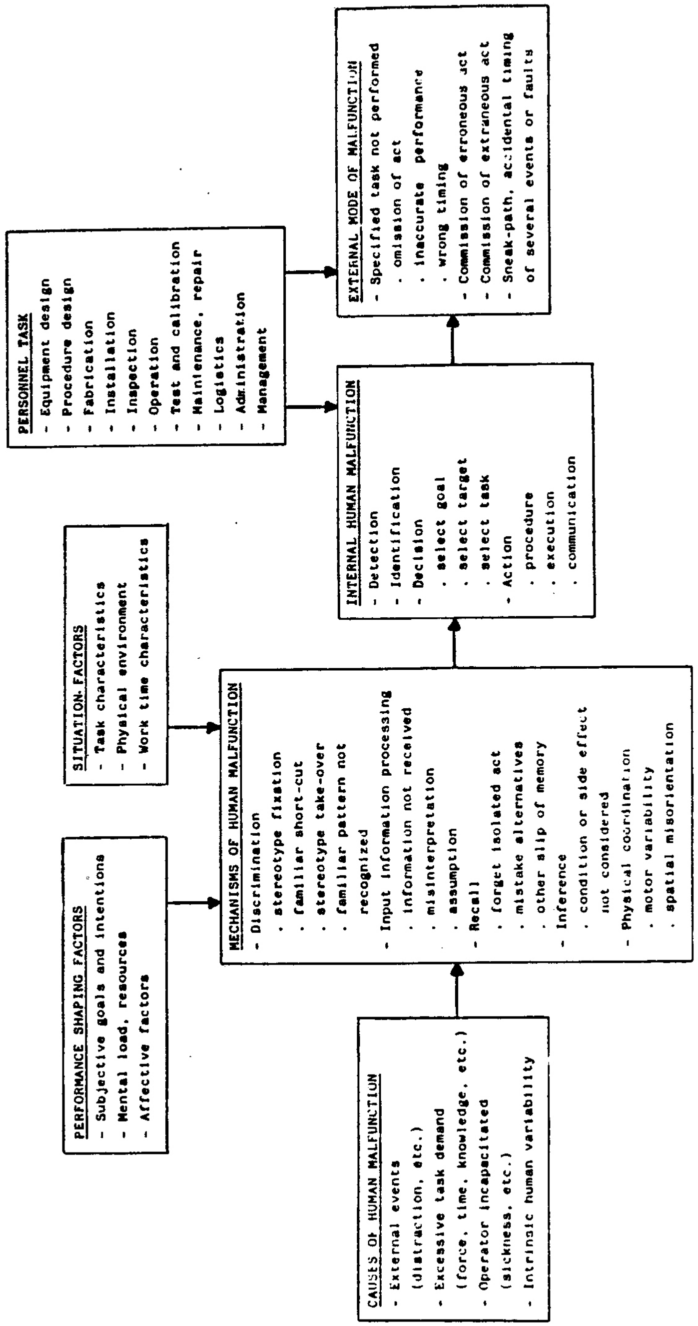

Figure 8. Multi-facet taxonomy for description and analysis of events involving human malfunction.

(4) NKA/KRU-P2(80)29 M. Griffon et al.
Classification System Proposal for Reporting Events Involving Human Malfunction.
N-15-80, March 1980.