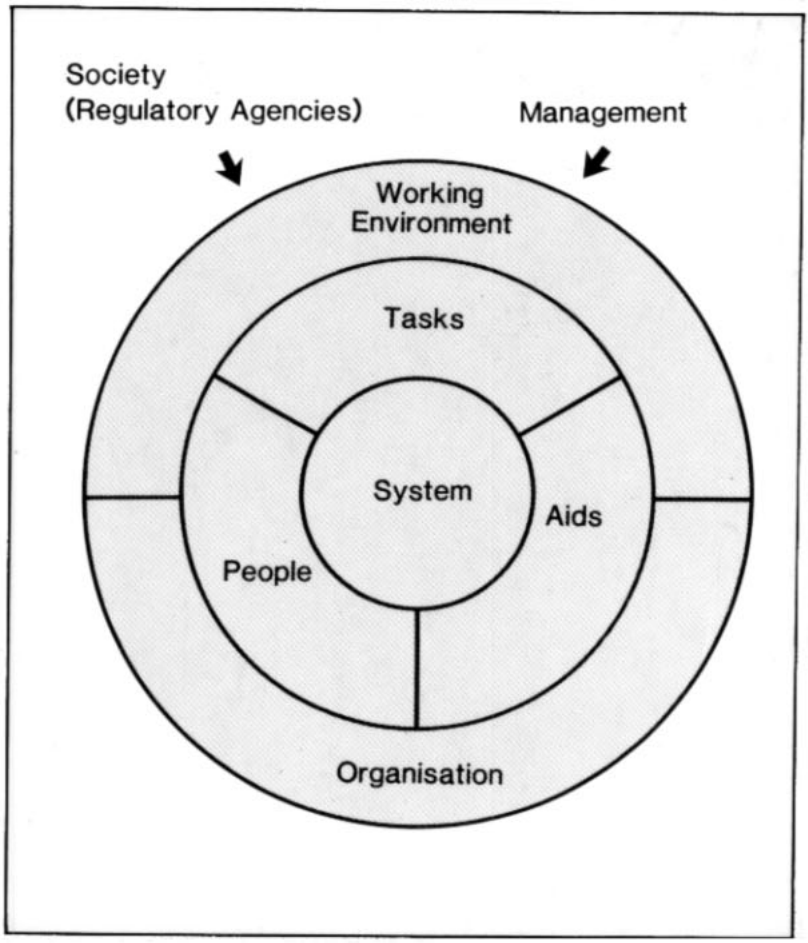
NORD

SEPTEMBER 1985

COMPUTER AIDED OPERATION OF COMPLEX SYSTEMS



nka

Nordic
liaison committee for
atomic energy

nka

Nordisk kontaktorgan for atomenergispørgsmål | Nordiska kontaktorganet för atomenergifrågor | Pohjoismainen atomienergia-yhdyselin | Nordic liaison committee for atomic energy

LIT(85)5
Risø-M-2532

COMPUTER AIDED OPERATION OF COMPLEX SYSTEMS

EXPERIMENTAL TESTING AND EVALUATION

FINAL REPORT OF THE NKA PROJECTS LIT-3.2 AND-3.3

Edited by
L. P. Goodstein
Risø National Laboratory
Denmark

SEPTEMBER 1985

THE NKA/LIT STEERING COMMITTEE

L. P. Goodstein	Risø National Laboratory, Denmark
J. Lindqvist	Swedish State Power Board
B. Liwång	Swedish Nuclear Power Inspectorate
F. Marcus	Nordic Liaison Committee for Atomic Energy
B. Wahlström	Technical Research Centre of Finland
M. Øvreeide	Institute for Energy Technology, OECD Halden Reactor Project, Norway

LIST OF PARTICIPANTS IN THE LIT-3.2 AND 3.3 PROJECTS

Risø National Laboratory	L. P. Goodstein
	J. Hedegård
	K. S. Højberg
	M. Lind
	F. R. Nielsen
	J. V. Olsen
	J. Rasmussen
Institute for Energy Technology, OECD Halden Reactor Project	E. Hollnagel
	G. L. Hunt
	N. Prætorius (KU)
	S. Yoshismura (CRIEPI)

ABSTRACT

Advanced technology is having the effect that industrial systems are becoming more highly automated and do not rely on human intervention for the control of normally planned and/or predicted situations. Thus the importance of the operator has shifted from being a manual controller to becoming more of a systems manager and supervisory controller. At the same time, the use of advanced information technology in the control room and its potential impact on human-machine system capabilities places additional demands on the designer.

This report deals with work carried out to describe the plant-operator relationship in order to systematize the design and evaluation of suitable information systems in the control room. This design process starts with the control requirements from the plant and transforms them into corresponding sets of decision-making tasks with appropriate allocation of responsibilities between computer and operator. To further effectivize this cooperation, appropriate information display and accession are identified.

The conceptual work has been supported by experimental studies on a small-scale simulator.

INIS Descriptors. COMPUTERIZED SIMULATION; CONTROL ROOMS; DISPLAY DEVICES; HUMAN FACTORS; INFORMATION NEEDS; MAN-MACHINE SYSTEMS; NUCLEAR POWER PLANTS; PLANNING; SYSTEMS ANALYSIS.

This report forms part of the safety programme sponsored by NKA, the Nordic Liaison Committee for Atomic Energy, 1981-5. The project work has been partly financed by the Nordic Council of Ministers.

PREFACE

The safety of nuclear power, as for other complicated industrial processes, depends on the accurate and timely execution of planning and operational tasks. However there is always the possibility that human malfunctions either directly or indirectly will initiate an unwanted course of events. The general aim is then to decrease the probability of human errors as well as increase the probability of their detection and correction. In principle this is possible through a careful task design and by giving the human operators appropriate training. In practise, one also has to consider the tools provided for aiding the operator and the operational organisation provided. All of these aspects have been addressed in the Nordic NKA/LIT programme during the period 1981 to 1985.

The Nordic LIT research programme has especially addressed the following questions:

- human errors in test and maintenance (LIT-1)
- safety-oriented organisations and human reliability (LIT-2)
- computer-aided design of control rooms and plant automation (LIT-3.1)
- computer-aided operation and experimental evaluation (LIT-3.2 and 3.3)
- planning and evaluation of operator training (LIT-4)

The fields of activity were based on the results and experience from an earlier Nordic cooperation (Wahlström and Rasmussen (1983)

The Nordic LIT programme has involved a total effort of about 40 person-years of qualified researchers in Denmark, Finland, Norway and Sweden. The programme has been financed partly by the Nordic Council of Ministers and partly by national funding. The LIT project was initiated by the Nordic Liaison Committee for Atomic Energy as part of the Nordic cooperation in the energy production field.

The following organisations have been financially and/or professionally involved in the LIT programme:

Risø National Laboratory, Roskilde, Denmark

Technical Research Centre of Finland, Espoo, Finland

Institute for Energy Technology, Halden, Norway

Swedish Nuclear Power Inspectorate, Stockholm, Sweden

Swedish State Power Board, Vallingby, Sweden

The LIT programme is reported in the following final reports:

- The human component in the safety of complex systems; LIT programme summary report, NKA/LIT(85)1.

- Human errors in test and maintenance of nuclear power plants - Nordic Project work; LIT-1 final report, NKA/LIT(85)2.

- Organization for safety; LIT-2 final report, NKA/LIT(85)3.

- The design process and the use of computerized tools in control room design; LIT-3.1 final report, NKA/LIT(85)4.

- Computer aided operation of complex systems; LIT-3.2 & 3.3 final report, NKA/LIT(85)5.

- Training diagnostic skills for nuclear power plants; LIT-4 final report, NKA/LIT(85)6.

SUMMARY

The introduction of computers in process control has influenced the possibilities for the presentation of information in the control rooms of industrial plants - plants which themselves are becoming more centralized and complex with greater potential risk levels. However, today's displays are still to a great degree based on traditional approaches where each sensor in the plant is represented by its own indicator in the control room. This situation seems incompatible with the increased awareness of the potential effects of human error on plant safety. Yet improved approaches to information presentation and computer-aided support to the plant staff in connection with operation and maintenance are now becoming available.

In addition, computers are being introduced in the design phase of these plants. As a result, design data bases are being established which also will be of great value during the operational phases in connection with planning, writing of procedures, risk management, etc.

Advanced technology has the effect that industrial systems are becoming more highly automated and do not rely on human intervention for the control of normally planned and predicted situations. However, the basis of existence for these systems is still the operating staff which has to maintain the necessary conditions for satisfactory operation. The staff has to cope with all those tasks which have been badly structured as well as the unforeseen events and disturbances in the system. Thus the importance of the operator has shifted from being a manual controller to becoming a ***systems manager*** and ***problem solver.*** Hence the term ***supervisory control*** has become a familiar label for the operating staff's overall function.

The corresponding reduction in the operators' direct involvement in plant control can lead to a deterioration in their "hands-on feel" regarding plant behavior. This may reduce their capability to respond to unfamiliar situations. However operators today are often more handicapped by the lack of adequate information

processing and display. This can affect their decision making in critical situations - decision making which depends on a balance between the operators' insight into design intentions, their plant knowledge, experience and the functioning of the automatic control system functioning.

In poorly designed systems, conflicts are an ever present danger. In unfamiliar and critical situations, the number of involved persons and groups can increase dramatically, and here the decision-making environment can quickly become uncoordinated and fragmented with inadequate information exchange and understanding.

Modern information technology can help meet safety goals and reduce the potential effect of human errors. The introduction of this technology in the control room requires a systematic design approach. It is imperative that designers have an improved understanding of the actual task demands so as to be able to provide appropriate information support to the operating staff. This, in turn, makes it mandatory that suitable **models** or **representations** of human capabilities and limitations be made available to designers. These will guide their allocations of tasks to operators and computers as well as their implementation of specific support facilities.

In this NKA/LIT project, a conceptual basis has been developed for computer-aided operation and supervision of complex industrial process plants. This builds to a great degree on the availability of the original design data base in order to support the operating staff with information on original design intentions and plant performance data. These will be useful when disturbances or other anomalies occur which might require deviations from normal practise and where it is important to have insight into the basis for the original design decisions. The availability of this data base will also insure that modifications can be made on the basis of user experience while still respecting other constraints and limitations, including those of the original design.

The project work included **two lines of endeavor.** The **first** aimed at a formal description of the plant-operator relationship while the **second** consisted of an experimental investigation of some of the conceptual ideas.

With regard to the **first;** the design objective is to achieve a good match or fit between the requirements that the process (power station, chemical plant) imposes for productive and safe control AND the abilities and resources of the total operational system (including the operators and the automatic computer system) to meet these requirements. It should be obvious that there is no single solution to this quest. **The project resulted in a systematic approach** which is logical and well-structured and will assist designers in avoiding an unbalanced result which reflects insufficient attention to all of the elements which constitute an integrated human-machine system. This is especially important when the potential for rare and risky events exists simultaneously with concern about the sensitivity of plant productivity and safety to human errors. Some of the basic ideas are described in the following.

In the project, the technical control requirements as seen from the process side were analyzed and described, in particular with regard to the management of plant faults and disturbances. This analysis of the technical process will lead to information about purpose, function and implementation at various levels of plant description which is consistent with the needs of the operational staff.

The results of this analysis makes it possible to formulate the resulting decision-making sequences which have to take place in exercising the necessary plant control. Examples of elements in these sequences are detection, state identification, evaluation, choice of goal, planning of resource utilisation, task execution and monitoring of results. These, in turn, have to be distributed during the design between the operational team and the computer system in a way which leads to a supportive partner relationship instead of a competitive conflict. Criteria for allocation could include regulatory considerations, available

resources, time constraints, feedback of results, etc. Of critical importance is the need for communication between the two operators and the computer.

In order to carry out the various phases of the decision sequence - be it by computer or through the operator - it is necessary to cope with the fact that they can be dealt with through the use of different strategies and heuristics. Each of these has their particular characteristics such as type or amount of observations required, kinds of knowledge about the process which is needed, amount of information processing required, consequences of error, etc. Thus this part of the design has to analyze the alternatives in order to provide further information for the allocation between the operators and the computer system. In addition, a related objective will be to match the content of the information displays so to stimulate the desired mental representations of the plant and support the strategies which would be effective for the operators and actually preferred by them.

An important phase the design is to draw on the results of cognitive psychology. This should ensure that the resultant interface system with its displays and controls will be **error-tolerant** with respect to the operators' abilities to carry out the assigned control tasks while at the same time enhancing their own detection of and recovery from errors.

To sum up the first area of work, the project explored the operator-process relationship with an eye towards establishing a basis for ensuring adequate computer support in supervisory control. A systematic design procedure for achieving well-balanced error-tolerant operator-computer interfaces in these applications is described.

The **second** area of work was carried out as an experimental program aimed at testing and evaluating certain of the concepts which were generated during the work described previously. There was felt to be a need for a realistic testbed of modest size for carrying out selective studies and, as a result, the

Generic Nuclear Plant (GNP) was developed and utilized in both Denmark and Norway. In addition, GNP has already been exported to several colleagues abroad for use in similar types of research.

In essence, GNP is a simulation of a pressurized-water reactor-like plant into which various types of faults can be introduced. Operators are called upon to carry out certain decision-making tasks which are reasonably realistic replicas from real-life situations. The LIT3 experiments were aimed at testing the suitability of various computer-based display types for assisting them in carrying out these tasks.

Thus, for example, the performance of users was studied during a task to identify the state of the plant. The information was formulated and displayed in functional terms describing the basic **mass and energy flows and states** in the plant. This type of information is normally **not** available in today's control rooms which mostly utilize so-called mimic diagrams of equipment components and their interconnections. It can be noted that the situation seems to be changing - partly as the result of the ideas generated in this project.

The results indicated that, with suitable training and practise, users can learn to search for and utilize information about the plant which is other than conventional equipment-based. This is encouraging in the light of the convictions stated earlier that operators have need for information about the plant which has to do with its purposes and functions as well as physical equipment. Each has its place in the total repertoire of technical support features which should be made available.

To sum up the second activity, the project established a testbed for computer-based support evaluation. This facility should **not** be compared with other full-scope training simulators. Its feasibility for studying selected issues has been tested. A set of mass and energy displays was used to indicate the functional interrelationships within the simulated plant. GNP will now be used for studies of training, the role of expert systems,

integrated display sets, information retrieval, etc. in parallel with continued conceptual studies dealing with **design for error-tolerant operations.**

To **conclude**, LIT3.2 on **computer-aided operation of complex systems** and LIT3.3 on **testing and evaluation**, dealt with the design and evaluation of human-machine systems for use in the operational phase of a process plant (nuclear, chemical, distribution, etc.) when the operating staff takes over the plant. At this point the staff strives on the basis of the delivered design together with accumulated experience to maintain safe and profitable plant performance.

The background for the project's concern with this problem was seen in two features which characterize the current technological development. The first was reflected in the trends towards increasing complexity and centralisation of technical and industrial systems. Such trends can lead to potentially drastic consequences as the result of - (in themselves) - natural and unintentional human malfunctions. The other was the arrival of advanced information technology which has and will have great influence on the form and content of human-work interaction.

In the present context, these developments signify that particular attention must be paid to ensuring that the potentially hazardous "rare event" can be dealt with. In turn, this requires a design strategy that takes into account the capabilities and limitations of the human operator as well as the computer so that a well-balanced solution can be realized. Designers have to pay attention to the actual tasks to be performed and the possible information processing strategies which can be employed as well as the error mechanisms which can be initiated. This is the only way to ensure that suitable facilities with appropriate displays and controls combined with proper training can be implemented so that design intentions can be realized in practise.

The achievement of these goals requires a continuing research effort and the NKA/LIT program has been an important support for

this work. However appropriate couplings to industry are needed for testing and evaluation of the results. Indeed some of the tools and ideas which have been developed during the project have already been utilized by industry. The line of research is expected to continue during the next NKA program. The results of work in artificial intelligence (as exemplified by the many recent references to **expert systems**) will be integrated with the previous work to support the **interactive decision making** which, for example, is the basis for an effective emergency management process.

DANISH SUMMARY

Risikoen for uheld i kraftværker og industri stiger i takt med, at udviklingen går i retning af større og mere komplekse anlæg. Men samtidig har højt udviklet computerteknologi skabt bedre muligheder for proceskontrol, så operatørerne kan få god besked om anlæggets tilstand.

Kontrolteknologi er dog i dag oftest baseret på traditionelle metoder, hvor hvert målested i anlægget er representeret med sin egen indikator i kontrolrummet. En sådan kontrol er næppe i stand til at tage højde for menneskelige fejl i uheldssituationer.

Derfor udvikles nu forbedrede metoder med støtte fra moderne computere til hjælp for personalet ved drift og vedligeholdelse af komplekse anlæg. Computersystemerne bliver anvendt allerede i planlægningsfasen af kraftværker og industri, og de databaser som opbygges under planlægningen, vil derefter kunne udnyttes under driften, f.eks. til planlægning, udarbejdelse af instrukser, risikokontrol.

Under normale driftsforhold er automatiserede industrielle systemer forholdsvis uafhængige af menneskelig indgriben. Operatørerne må dog til stadighed overvåge, om betingelserne for sikker drift er til stede og gribe ind ved uforudsete forstyrrelser i produktionsprocessen. Operatørens rolle har således ændret sig fra at være manuel kontrollør til at være problemløser og tilsynsførende.

Operatørerne har derfor ikke i samme grad som tidligere "fingeren direkte på pulsen", hvilket kan betyde en forringet evne til at gribe ind i uforudsete situationer.

Mere afgørende er det imidlertid, at operatører handicappes af mangler i den måde, hvorpå oplysninger om anlægget præsenteres. Det kan svække beslutningerne i en kritisk situation, hvor operatørens handlemåde er afhængig af hans forståelse af tanke-

gangen bag systemets opbygning og det automatiske kontrolsystems funktion.

Er det industrielle system uhensigtsmæssigt udformet, kan der være en indbygget fare for uheld, og beslutningsprocessen i en kritisk situation kan hurtigt blive forvirret og usammenhængende, også fordi antallet af medvirkende ofte øges drastisk.

Moderne informationsteknologi kan reducere muligheden for menneskelige fejl. Men før den nye teknologi indføres i industrielle kontrolrum, er det nødvendigt, at anlægskonstruktørerne opnår en bedre forståelse af de gældende arbejdsforhold under drift, så de kan forsyne operatørerne med alle relevante oplysninger.

Opgaven kan kun løses, hvis konstruktørerne får adgang til egnede modeller, som beskriver driftspersonalets kunnen og begrænsninger. Det vil sikre den rette fordeling af opgaver mellem operatører og computersystem.

I dette NKA-LIT projekt er der udviklet et grundlag for computerstøttet drift og kontrol af komplekse anlæg. En forudsætning for at bruge metoden er, at operatøren har adgang til den originale database, som er benyttet i opbygningsfasen. Hermed opnår operatøren viden om de oprindelige hensigter med anlægget og dets funktion. En sådan viden er nyttig, når der indtræffer afvigelser fra normal drift. Adgang til databasen vil også sikre, at ændringer, som gennemføres på baggrund af driftserfaringer, tager højde for de begrænsninger, som ligger i det originale design af anlægget.

Projektet havde to hovedformål. Det første var at nå frem til en systematisk beskrivelse af samspillet mellem operatør og anlæg. Det andet mål var en eksperimentel undersøgelse af nogle af de implikationer af det mere formelle arbejde.

Projektets første del: Formålet med anlæggets opbygning er at opnå god overensstemmelse mellem på den ene side de krav, som processen i kraftværker og kemisk industri stiller til høj produktion og sikkerhed og på den anden side de resourcer, som

er til rådighed for drift og kontrol - herunder operatør og computere.

Skønt det er klart, at der ikke findes nogen enkel løsning, viser projektet en systematisk metode til at vurdere samspillet mellem anlæg og operatør. Metoden er logisk og godt struktureret og vil hjælpe systemarkitekter til at undgå fejl i planlægningen, særlig de fejl, som skyldes mangel på opmærksomhed på alle de elementer, der indgår i et integreret menneske-maskine system.

Denne metode er især vigtig, når der er mulighed for sjældne uheld, som til gengæld kan have alvorlige konsekvenser.

I projektet analyseres de krav, som processen stiller med hensyn til kontrol med specielt sigte på, hvordan forstyrrelser og fejl behandles under driften. En analyse af hele den tekniske proces vil give egnede oplysninger om formål og funktion på forskellige niveauer i anlægget.

Analysens resultater gør det muligt at formulere de enkelte trin, som indgår i beslutningsprocessen under kontrollen med anlægget, f.eks. opdagelse af en forstyrrelse, bestemmelse af problemets karakter, valg af løsningsmodel, fornuftig udnyttelse af de givne resourcer, udførelse af arbejdet og overvågning af resultaterne.

Beslutningsprocessens delelementer må under planlægningen af anlæggets konstruktion fordeles mellem operatører og computersystem på en måde, så der opstår et afbalanceret partnerskab. Kommunikationen mellem operatørerne og det støttende computersystem er af fundamental betydning.

For at beslutningsprocessens forskellige dele kan udføres bedst muligt, må både operatører og computersystem være i stand til at arbejde med forskellige strategier. Hver strategi har bestemte karakteristikker som f.eks. arten af de nødvendige observationer, hvilken viden om processen, der behøves, og de følger som

bestemte uheld vil føre til. Krav og strategier må være fleksible og skal kunne tilpasses til operatørernes behov og ønsker.

Når et stort anlæg planlægges bør man trække på forskning inden for den kognitive psykologi, der beskriver menneskelig tankegang samt indsamling og behandling af viden. Hermed kan man sikre, at menneske-maskine systemer bliver tolerante overfor fejl. Det vil sige, at operatøren kan gennemføre en kontrol samtidig med, at han får mulighed for at opdage egne fejl og rette dem.

Sammenfattende kan man sige, at projektets første del har resulteret i et grundlag for at etablere egnet computerstøtte til driftspersonalets overordnede kontrolfunktion.

Projektets anden del: En eksperimentel afprøvning af dele af de modeller for samspillet mellem menneske og maskine, som blev studeret i projektets første del. Til det formål udvikledes en såkaldt Generic Nuclear Test Plant (GNP), som er en simulering af en trykvandsreaktor. GNP er udviklet og anvendt i Danmark og Norge og siden eksporteret til forskere i udlandet.

Forskellige typer fejl kan kodes ind i modellen, og operatører deltog i eksperimentet ved at træffe beslutninger, som er rimeligt realistiske i forhold til lignende situationer i det virkelige liv. I eksperimentet undersøgte man egnetheden af forskellige computer-genererede displays, som skulle støtte operatørerne i at udføre deres opgaver.

Operatørernes handlemåde blev studeret under deres arbejde med at fastslå anlæggets tilstand. Oplysningerne om anlæggets tilstand blev præsenteret i form af grundlæggende strømme af masse og energi i anlægget.

Denne type information er normalt ikke til rådighed i et kontrolrum i dag. Oftest anvendes procesdiagrammer over de enkelte komponenter og deres indbyrdes forbindelser. Situationen ser dog ud til at blive forandret nu - delvis på grund af resultaterne af dette projekt.

Resultaterne tyder på, at operatørerne efter en passende uddannelse kan lære at anvende en sådan information, som går videre end bare at beskrive tilstanden i et kraftværks enkelte komponenter. Resultatet er opmuntrende i lyset af vor overbevisning om, at operatører ikke blot har brug for viden om et anlægs fysiske udstyr, men også viden om dets funktion og formål.

Følgende kan konkluderes: Det katastrofale, men meget sjældne uheld, som kan indtræffe i komplekse anlæg, blandt andet på grund af menneskelige fejl, må kunne håndteres sikkert. Det kræver, at planlægning og opbygning af store industrielle anlæg og kraftværker tager højde for evner og begrænsninger hos både den menneskelige operatør og computersystemet. Planlæggeren må være opmærksom på aktuelle arbejdskrav, mulige strategier for behandling af information, og muligheder for fejl. Således kan man opnå velafbalancerede løsninger, der skal kombineres med en god uddannelse for at sikre, at målsætningerne føres ud i praksis.

En fortsat forskningsindsats er nødvendig, kombineret med et udstrakt samarbejde med industrien, som nu er begyndt at bruge nogle af de metoder, som er udviklet gennem projektet.

I et kommende NKA-program vil det være muligt at integrere udviklingen af "kunstig intelligens"-computere som f.eks. ekspertsystemer i de nuværende resultater. Herved vil der kunne skabes et grundlag for effektiv beslutningstagen i nødsituationer på komplekse anlæg.

TABLE OF CONTENTS

INTRODUCTION

The NKA/LIT project on human reliability included several activities which dealt with the incorporation of appropriate computer aids during various phases of the life-cycle of a complex industrial plant. A separate report from the LIT3.1 project describes the work done on computer-aided **design** approaches for plant monitoring, control and safety systems while this document focuses on the complementary problem area of computer-aided **operations** - as seen both from the conceptual as well as from the experimental and evaluation points of view. The relationship between the **design** and **operation** projects can be seen in Fig.4-1.

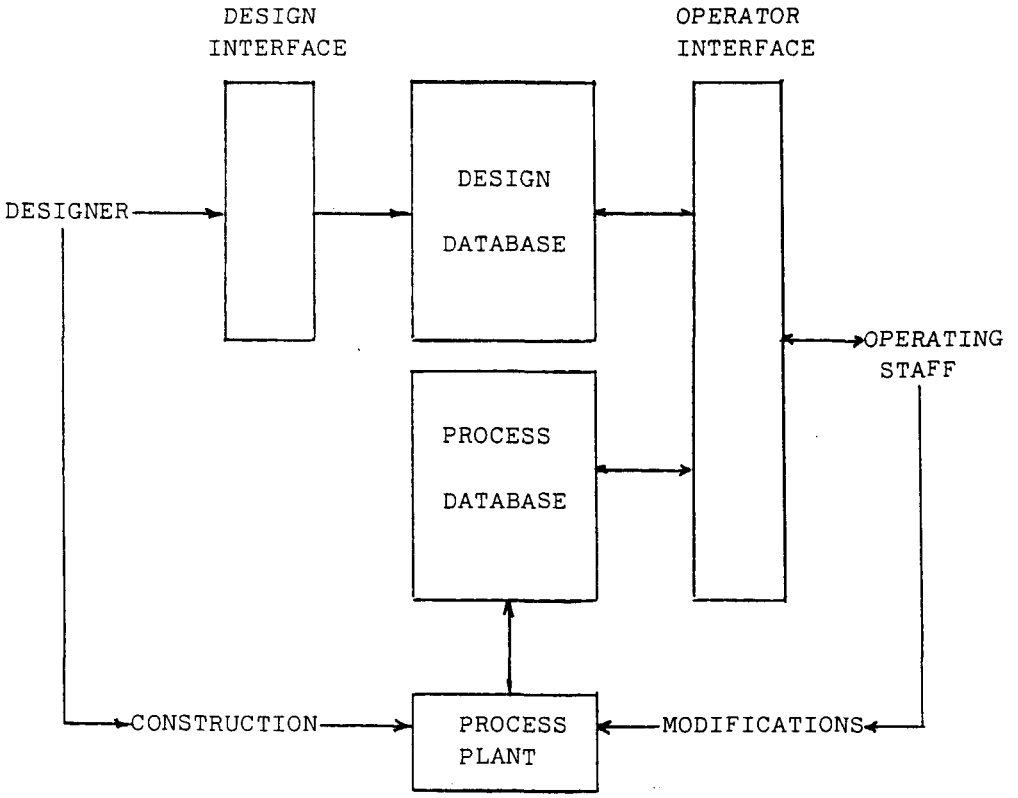


FIGURE 4-1

Thus the LIT3.2 project on **computer-aided operation of complex systems** dealt with ways and means of assisting the operating staff in their task of taking over the plant and striving for stable and safe operation over its lifetime - on the basis of the delivered design (and design database) together with accumulated experience and in the face of revised requirements from management and/or regulatory authorities, etc. In particular, there was an interest in establishing a conceptual basis for using computer-based aids in order to support operators and other members of the staff in dealing with the operational and planning problems which could arise.

The LIT3.3 project concerned itself with experimental testing and evaluation of some of the ideas resulting from this work.

As regards the organisation of these two activities, LIT3.2 was carried out by the Risø National Laboratory in Denmark while LIT3.3 was the primary responsibility of the OECD Halden Project in Norway. In practise, the experimental work was carried out in close cooperation between the two institutes.

PROBLEM CONTEXT

A simplified representation of the elements that make up the total of almost any system is shown in Fig.5-1. At the center of the representation is the **object system** which will produce the electric power, the beer, the oil OR furnish the desired transportation, data processing, communication, etc. In close proximity to this system are the **tasks** which have to be performed in order to properly, safely and effectively control, steer, manipulate, repair, modify, replenish the system. To perform these tasks, it is necessary to provide a suitable combination of suitably qualified **people** equipped with appropriate sets of **aids.** It should be clear that these aids can encompass everything from a pencil to an automated control system. In addition, this inner group of system, people and aids has to function in a given **working environment** and within the confines of a given **organisational structure.** Added pressures and constraints issue from the demands from **society,** (e.g., regulatory authorities) and, not least, from the goals and attitudes of **top management.** Some of these problems have been dealt with in parallel LIT activities - see the final reports from LIT1 on Human Errors in Test and Maintenance, LIT2 on Safety Organisation and Human Reliability, LIT3.1 on Computer-Aided Design of Control Rooms and Automation Concepts and LIT4 on Planning and Evaluation of Operator Training.

In order to treat the requirements for and the design of compatible aids for the operation of complex systems, it is necessary as part of the total design process to take all of these elements into consideration or else risk the danger later of serious and costly modifications. E.g., the Danish Air Force now restricts its candidates to a maximum height and weight in order to ensure that they can fit into the cockpit. Earlier horror stories have indicated less than adequate consideration of human dimensions during design with the result that equipment could not be utilized and/or maintained. The situation is more complicated today where the emphasis is on human cognitive abilities rather than physical dexterity or manual control expertise.

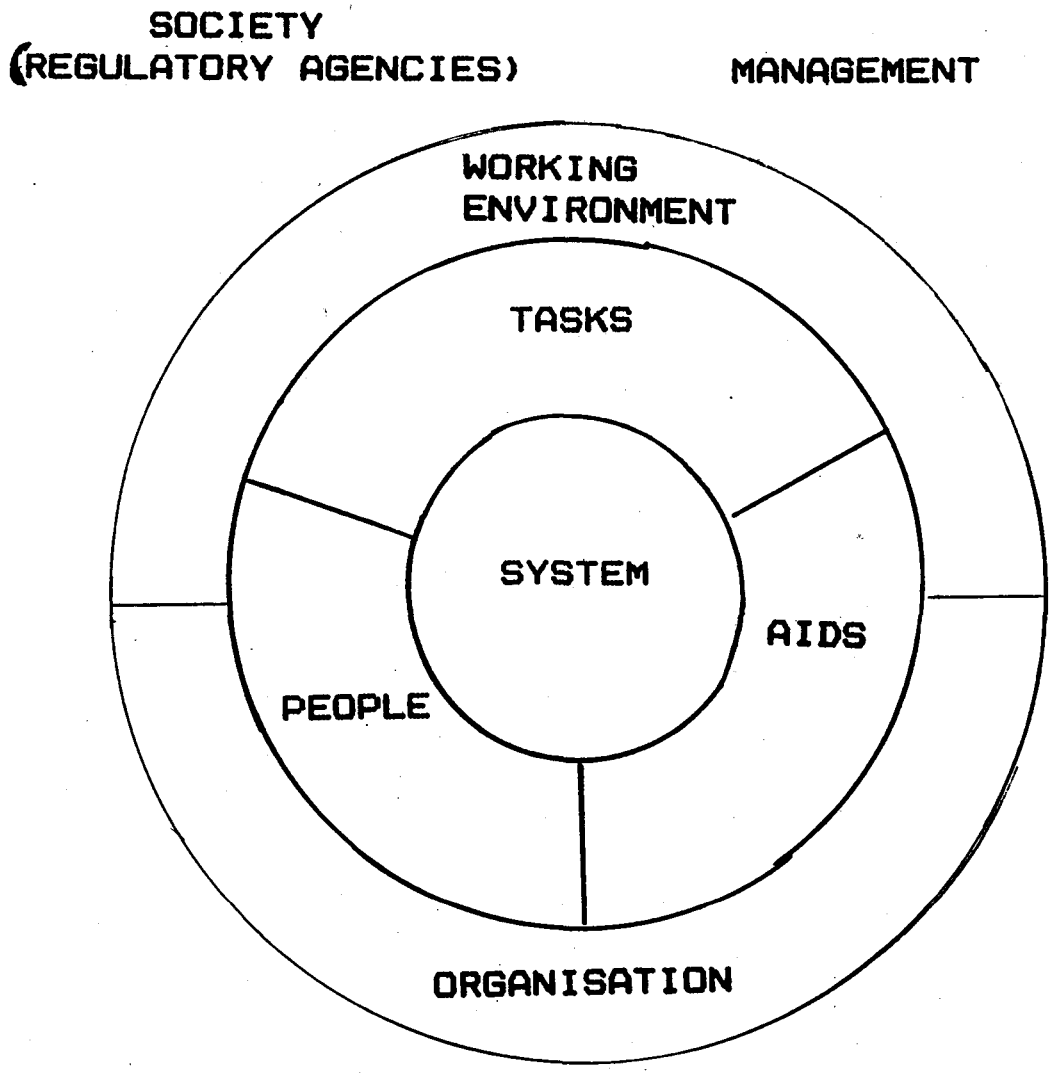

SOCIETY
(REGULATORY AGENCIES)
MANAGEMENT
WORKING
ENVIRONMENT
TASKS
SYSTEM
AIDS
PEOPLE
ORGANISATION

Figure 5-1

This is related to the fact that technical systems are becoming highly automated and do not rely on human intervention for the control of normally planned and predicted situations. However, the basis of existence for these systems is still the operating staff which has to maintain the necessary conditions for satisfactory operation and to cope with all the badly structured and often unforeseen events and disturbances in the system. Thus the importance of the human as a **systems supervisor** and **problem solver** rather than a manual controller is now recognized as an essential factor. However the corresponding reduction in the operators' direct involvement in plant control can lead to a deterioration in their "hands-on feel" regarding plant behavior. On the other hand, the operators are often more handicapped by the lack of adequate information processing and display to help them in making appropriate decisions - decisions which need to be based on a proper balance between insight into plant intentions and goals, knowledge about the actual plant and experience. This balance can easily be disturbed by the fact that, in general, decision-making is a three-way cooperative effort; i.e., between the designer, the operators and the automatic control systems so that, in poorly designed systems, conflicts are an ever present danger.

The introduction and development of computer-based information systems opens up a tremendous potential for improving this situation. However, there are various prerequisites. In general, use of this technology to support operator decision-making implies necessarily an attempt to match the information processes of the computer to the mental decision processes of the human. This is not to suggest that the two are (or should be) identical. On the contrary, all attempts should be made to utilize in an optimum way the (different) resources of each. However, an effective partnership relation dictates an effective communication between the two and in an appropriate form to the operators in order to assure compatibility with the operators' own thought processes (and vice-versa from operator to computer). If this endeavor is successful, then one can speak of an effective human-computer cooperation; if not, then the new system can be worse than a traditional approach.

GOALS

The two projects aimed at achieving the following results:

- the generation of a suitable conceptual framework for human decision making in connection with diagnosis and planning activities for complex industrial plants

- deriving a methodology for clarifying the relationships between these human activities and the form and structure of appropriate computer-based information presentation and communication facilities

- an experimental evaluation of candidates for computer-based operator aids.

SUPERVISORY CONTROL FRAMEWORK

System function depends on a causal structure. Part of the causal structure of an industrial system is related to energy and mass flows in the physical, i.e., mechanical, electrical and chemical, process equipment. Another part of the causal links depends on information flow paths interconnecting the physical equipment which remove degrees of freedom from system states in accordance with the purpose of system operation. The constraints on system states to be introduced by this controlling information network depend on the immediate purpose or operating mode and will serve to maintain a state; to change operating state in a particular system or subsystem, or to coordinate and "synchronize" states in several subsystems to prepare for systems reconfiguration.

The general aims of the associated information processes which are necessary are therefore: to identify system states, to compare these with target states, to consider goals and purposes, and to plan appropriate actions on the system. In modern, automated process plants and other complex systems, the processing of control information is performed by three parties in a complex cooperation, i.e., the systems designer, the system operator, and the automatic control system. The complexity of this cooperation caused by modern information technology and the requirement for extreme reliability of control decisions in large scale installations now calls for a careful overall design of this information network. The traditional approach is to automate the well structured functions and to ask the operator to cope with the badly structured situations by means of information on system goals and state and education in process fundamentals. This approach is clearly inadequate, even when designers make heroic efforts to assist operators by providing detailed operating instructions for the abnormal situations they have identified and analyzed as part of the design. The usual dichotomy between situations which are analyzed and for which automatic control or detailed procedures are designed and those which are left open by the designer

needs to be replaced by a consistent design of the overall control strategy including an attempt to bring structure to the category of unforeseen situations.

The system designer will have to consider and specify the overall control strategy, which he can do at various levels of detail. He may introduce predetermined links between defined states and relevant actions by means of automatic control loops and sequence controllers or he may introduce control strategies at higher levels by means of process computers with adaptive or heuristic programs. Alternatively, he may ask operators to perform control tasks, either in a preinstructed mode or by problem solving and improvization. In modern systems, all these possibilities are used in various combinations depending upon the actual situation. In order to design the overall control strategy in a consistent way, the designer has to use a model of human performance which is compatible with the models used for design of automatic control systems, together with a consistent description of the actual control requirements of the system in the various operating conditions.

MODEL OF HUMAN INFORMATION PROCESSING

The model of human performance we need for this purpose has several distinct characteristics. First of all, to be compatible with control system design, models of human performance in terms of information processing as they are now emerging within cognitive psychology are most relevant. What we need are not, however, detailed models of human information processes in specific situations, but rather models of the possible categories of human decision strategies which operators will use for various generic types of control tasks. These models will then serve to identify the requirements for psychological models representing the human resources for the types of information processes required and the human performance criteria or subjective preferences which control human choice among possible strategies in a given situation.

Another feature of the models we are seeking is that they should not only cover systematic, analytical decision making used during abnormal situations but also the tricks of the trade and the automated habits used by skilled operators during routine situations. This implies that a model should also include the characteristics of sensori-motor performance, and the output of information processes should be modelled in terms of actions. To be able to evaluate the interference from overlearned routines in performance during unfamiliar situations, it is important to include the two extremes of performance in one conceptual framework. In addition, it is, in general, important that this framework is able to represent also the effects of psychological error mechanisms in terms which can be related to features of the man-machine interface.

The first step in the modelling process is to describe the human information processes required to perform a control task. This should be a description in terms of internal human activities rather than system requirements, i.e., a description of the human decision process from the instant when the need for intervention is detected to the resulting actions.

To develop a model of the possible decision sequences of human operators in industrial process plants, we have analysed a number of verbal protocols (Rasmussen, 1976). As might be expected, this attempt did not reveal much of the human information processes. However, the analysis identified a number of typical statements of "states of knowledge" in the decision process, which can be arranged in a rational sequence, see figure 6-1. These states of knowledge divide the decision process into a sequence of more or less standardized subroutines. This structure appears to be very efficient, since a particular decision problem can be dealt with by a sequence composed from standard routines. Formulation of a "state of knowledge" serves to prepare the result of one routine for application in the following routine. In addition, ready-made solutions from previous cases are easily incorporated. However, the structure also invites by-passes and leaps in the basic rational sequence in the form of immediate associations between states and stereotyped, rule-based transformations. This is

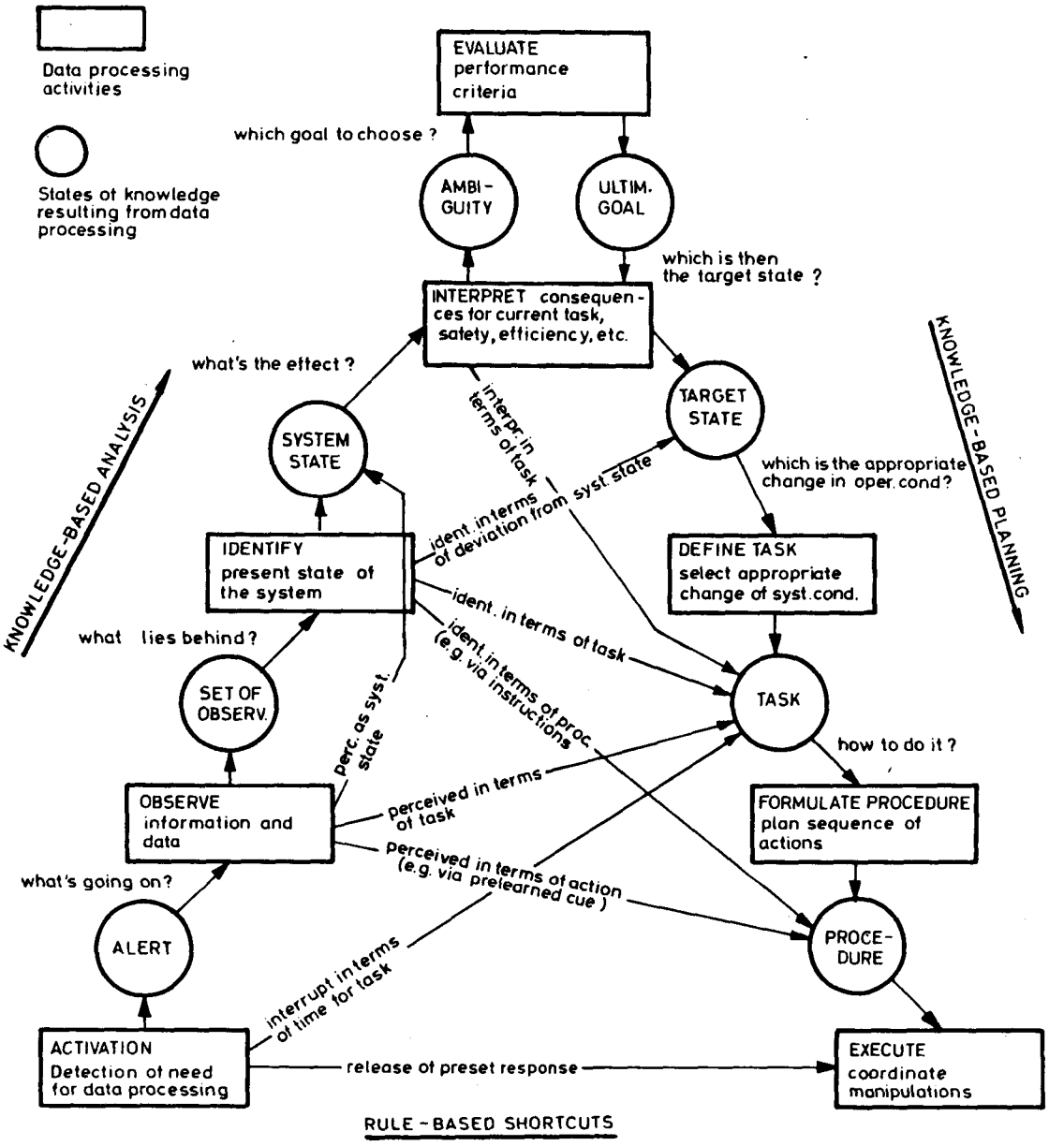


Fig. 6-1 Schematic map of the sequence of mental activities used between initiation of response and the manual action. Rational, causal reasoning connects the "states of knowledge" in the basic sequence. Stereotyped mental processes can bypass intermediate states.

important for reflecting the operators' opportunities for development and use of know-how and skill, but also leads to the potential for "traps" during less familiar situations. In figure 1, different typical by-passes are shown. This model is not a model of human performance but a conceptual framework mapping possible decision sequences which can be used for the same external control task, depending on the know-how of the actual operator. To be useful for interface design, this frame of reference must be supplemented by models of those psychological mechanisms which are used by humans for the subroutines of the decisions process. It is important that these models of psychological mechanisms as they are studied by experimental and cognitive psychology, also represent limiting properties and error mechanisms. As mentioned, the verbal protocols do not in general identify these psychological mechanisms and in well adapted performance they cannot be derived from external performance. Only when adaptation breaks down will properties of the psychological mechanisms reveal themselves and, consequently, we have made an attempt to model the role of internal mechanisms from analyses of human error reports (Rasmussen, 1981) supplemented by findings from verbal reports. The result is shown in figure 6.2. Three levels of human performance are identified with very distinct features, seen from a control theoretic point of view. The skill-based performance represents the highly automated sensori-motor performance which rolls along without much conscious control. The human performs as a multivariable continuous controller, like a data-driven controller for which input information acts as time-space signals and the functional properties of the systems under control are only represented in the controller as dynamic, spatial patterns. The rule-based performance at the next higher level represents performance based on recognition of situations together with rules for actions from know-how or instructions. Input information acts as stereotype signs labelled in terms of states, events or tasks. The functional properties of the system are at this level implicitly represented by rules relating states and events to actions. The activity at the rule-based level is to coordinate and control a sequence of skilled acts, the size and complexity of which depend on the

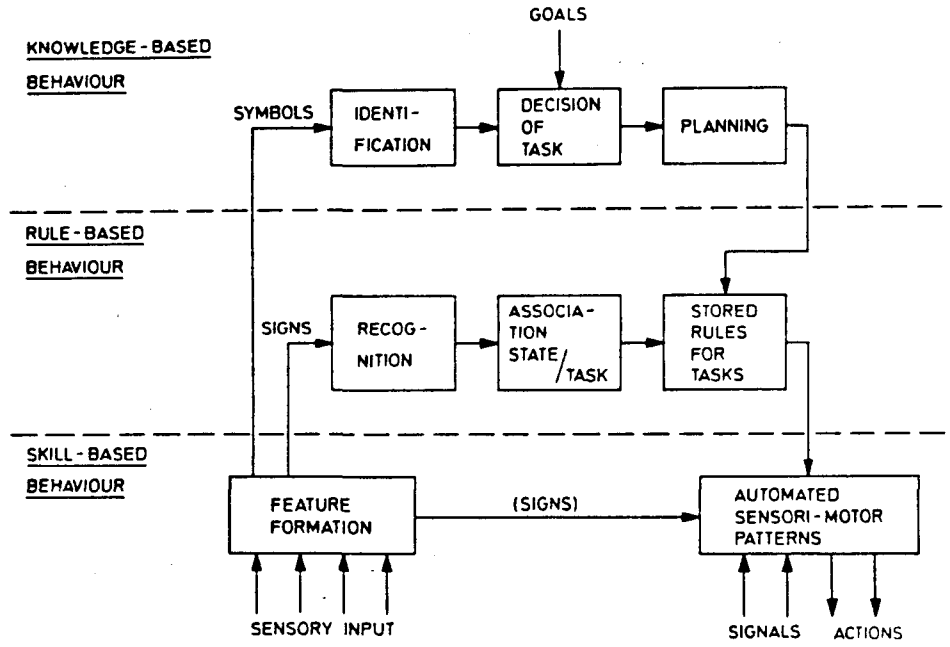


Fig. 6-2. Simplified illustration of three levels of performance of skilled human operators. Note that the levels are not alternatives, but interact in a way which is only rudimentarily represented in the diagram.

level of skill in a particular situation - one single decision to go home for dinner may be enough for driving you there, if the ride is not disturbed.

When proper rules and familiar signs are not available for a situation, activity at the next level of knowledge-based performance is necessary to generate a new plan for action ad hoc. The main feature here is that information is perceived as symbols which are used for information processing characterized by an explicit representation - mental model - of the functional structure of the system to be controlled as well as the related causal relations. The information process used by a person in a specific unfamiliar situation will depend very much on subjective knowledge and preferences and detailed circumstances for the task. It therefore appears to be unrealistic to model the detail flow of information processes in a decision

sequence. Rather, categories of possible prototypical information processes are described by identifying the overall strategy used to control the decision process, which is tightly connected to a specific type of mental model and the related symbols.

A major problem in design of man-machine interface systems is to properly support knowledge-based behaviour in supervisory control tasks. One prerequisite for doing this is to present information in a format structured so as to lead operators to develop effective mental models, and to code the information at a symbolic level compatible with these models and with strategies appropriate for the actual decision task. This is what Norman (1981) calls "cognitive engineering". To do this, however, the control task which the operator is supposed to perform, must be formulated - by the control system designer or by the operator himself - at the proper level of detail and abstraction in the control hierarchy and not in terms of individual instrument readings and elementary actions on equipment (Rasmussen and Lind, 1981).

A control task, and the necessary decision strategies with related mental models, for instance, to be used for state identification and diagnosis, can be formulated at several levels of abstraction, see figure 6.3.These levels range from representation of physical anatomy of the plant through levels of functional descriptions, to a description in terms of design intentions and purpose.

The identification of system state, which is most frequently the critical phase of a supervisory control task, is in general facilitated by the fact that we are not asking for an absolute, isolated identification but rather an identification in terms of deviation from a target state, i.e., a normal, specified or forbidden state. In this way a kind of structure can be imposed on the category of unforeseen events. In the abstraction hierarchy, the discrepancy can be identified at each of the levels and so can, therefore, the control task. Disturbances, i.e., actual states, are propagating bottom-up in the hierarchy whereas target state in terms of topological configuration and

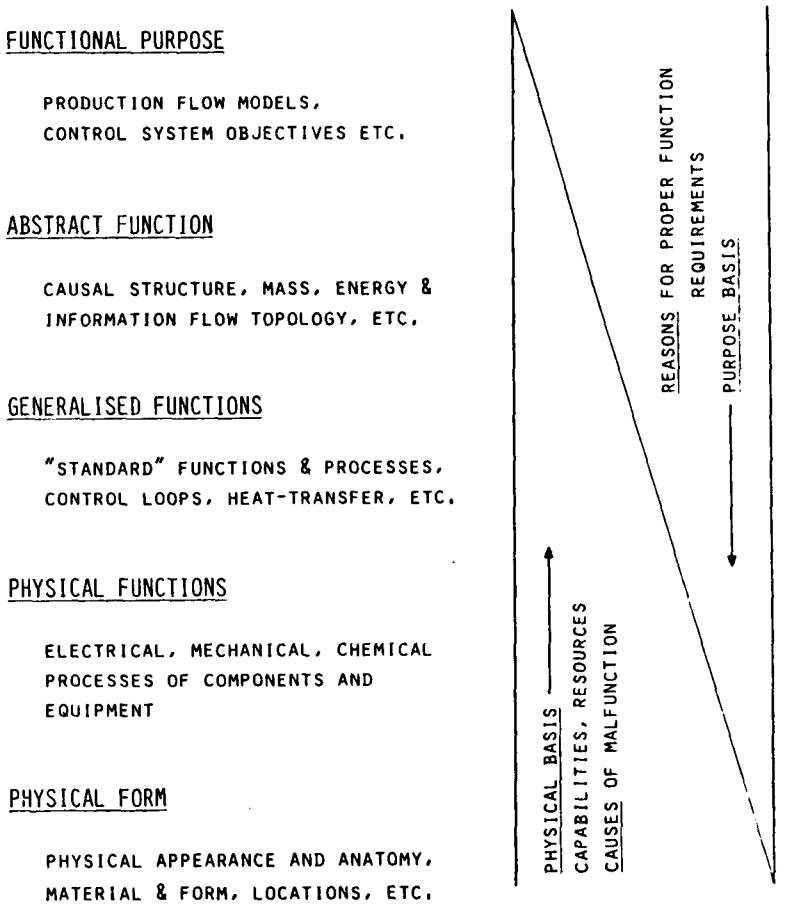


Fig. 6-3. The abstraction hierarchy used for representation of functional properties of a technical system.

boundaries for allowed and specified states can be developed top-down from consideration of production and safety requirements derived from the purpose of system operation.

The appropriate level of identification depends on the actual circumstances. Identification of disturbances in terms of mass-energy flow topology at a high level of abstraction is appropriate for compensation of production disturbances. In

order to remove the cause of disturbance by repair or replacement, identification in terms of physical anatomy is of course necessary. There is, therefore, a circular relation in the choice of appropriate level of identification which depends on the goal which, in turn, depends on the state to be identified. It is, therefore, necessary to consider a reasonable strategy for search through levels and for prioritizing. Although the functional properties represented at the various levels of abstraction are basically different, it appears to be important to seek a common language in which generic control tasks can be formulated for all levels. For this purpose a representation of causal relations at all levels has been formalized on the basis of energy-, mass-, and information flow topology.

INTEGRATED CONTROL SYSTEM DESIGN

During design of the process plant itself, the functions of the system and its physical implementation are developed by iteratively considering the plant at various levels of abstraction and in increasing degree of detail, see Figure 6-4.

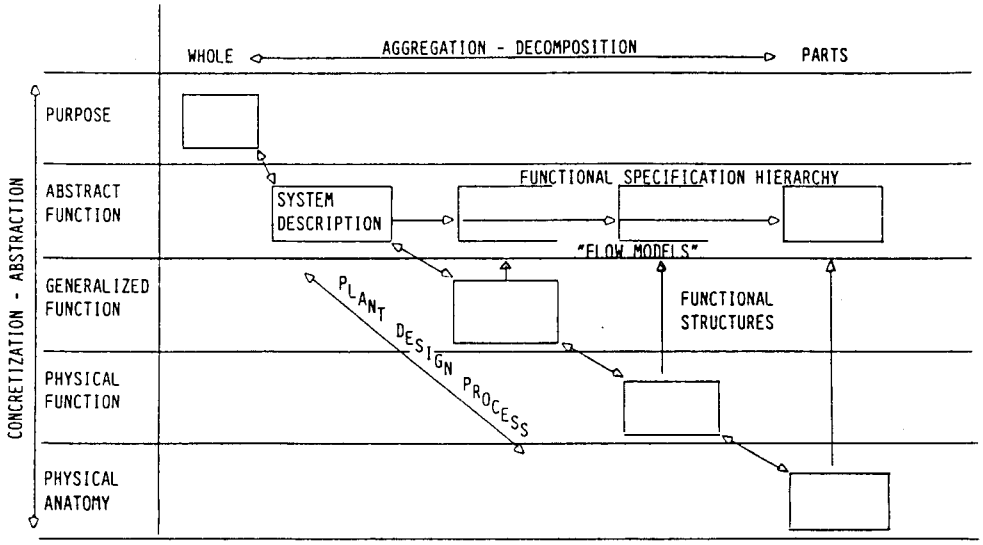


Fig. 6-4 Derivation of goals and functional specifications during the design process.

During this design process the physical system is identified, i.e., the implementation of those causal structures depending on mass and energy relations. However, as the degree of physical detail increases during the design process, so does the number of degrees of freedom in functional states. Therefore causal links by means of control paths relating desired states with necessary control actions must be introduced to constrain the possible operational states.

In this way, the desired states of functions and equipment will be identified during design at different levels of abstraction, and the necessary information or control constraints will be identified in terms of the conceptual framework related to these levels. In general, a skilled designer will immediately be able to identify suitable and familiar control system concepts. It is, however, the aim of the present paper to demonstrate that a consistent systems design including operator control functions can be performed more systematically by means of the generalised decision model and the flow modelling concept.

The system's control requirements are derived from the necessary relations between the actual states, the desired states or changes of states, and the required actions on the system. This means that planning of control actions involves the rational decision sequence of figure 6-1 covering state identification, goal evaluation, and prioritizing, in addition to the planning itself. Depending upon the control task allocation, the decision sequence - or parts of it - will be performed by the designer himself, the plant operator or the process computer. The conceptual framework within which decisions are taken, will usually depend on the background of the person, i.e., designer or operator, and upon the immediate context of the decision. However, to have a consistent overall-design and to be able to formalize the decision functions to be performed by the computer, ad-hoc decisions throughout the design process should be replaced, or at least reviewed, by considerations based on a uniform description of the necessary constraints and the related control requirements which are expressed in a suitable language. For this purpose, we consider a transformation of the

desired functional states and the necessary conditions, supplies, and constraints emerging during the various phases of design specification into a uniform description of specified functional states at the level of energy and mass flow structure - the abstract functional level of Figure 6-4. The result is a consistent hierarchical description of target states and intended functions - i.e., a goal or specification hierarchy as shown in Figure 6-5(Lind, 1982).

The importance of dealing with different types of hierarchies in the description of complex systems has been discussed by Mesarvoic and his collaborators (Mesarovic et. al. 1970). In their terminology, our abstraction hierarchy is an example of a stratified system description. The decision making hierarchy introduced in op. cit. is related to our specification hierarchy in the sense that system control requirements specified in the hierarchy are the basis for choices of decision making strategy in control of the system. Mesarovic et. al. do not distinguish clearly between the hierarchies of decision making and of system goals. However, this distinction is essential to the present discussion of control task allocation between the operator and the computer. The allocation strategy leads to the specification of the structure of the decision making processes in control.

Hierarchical Control and Generic Control Tasks

A multi-level model as depicted in Figure 6-5describes mass-and--energy flow topology at different levels of functional decomposition of the plant. It can be used to define plant control requirements on any level in a uniform way (Lind, 1982). Three generic control tasks can be identified using this framework. Two categories of control tasks relate to the constraints in plant variables necessary to remove excess degrees of freedom in order to maintain specified state or to change state within a regime of operation. The third category relates to the changes in variable constraints which are necessary to coordinate the state in two separate flow structures during plant reconfiguration, as, e.g., required during

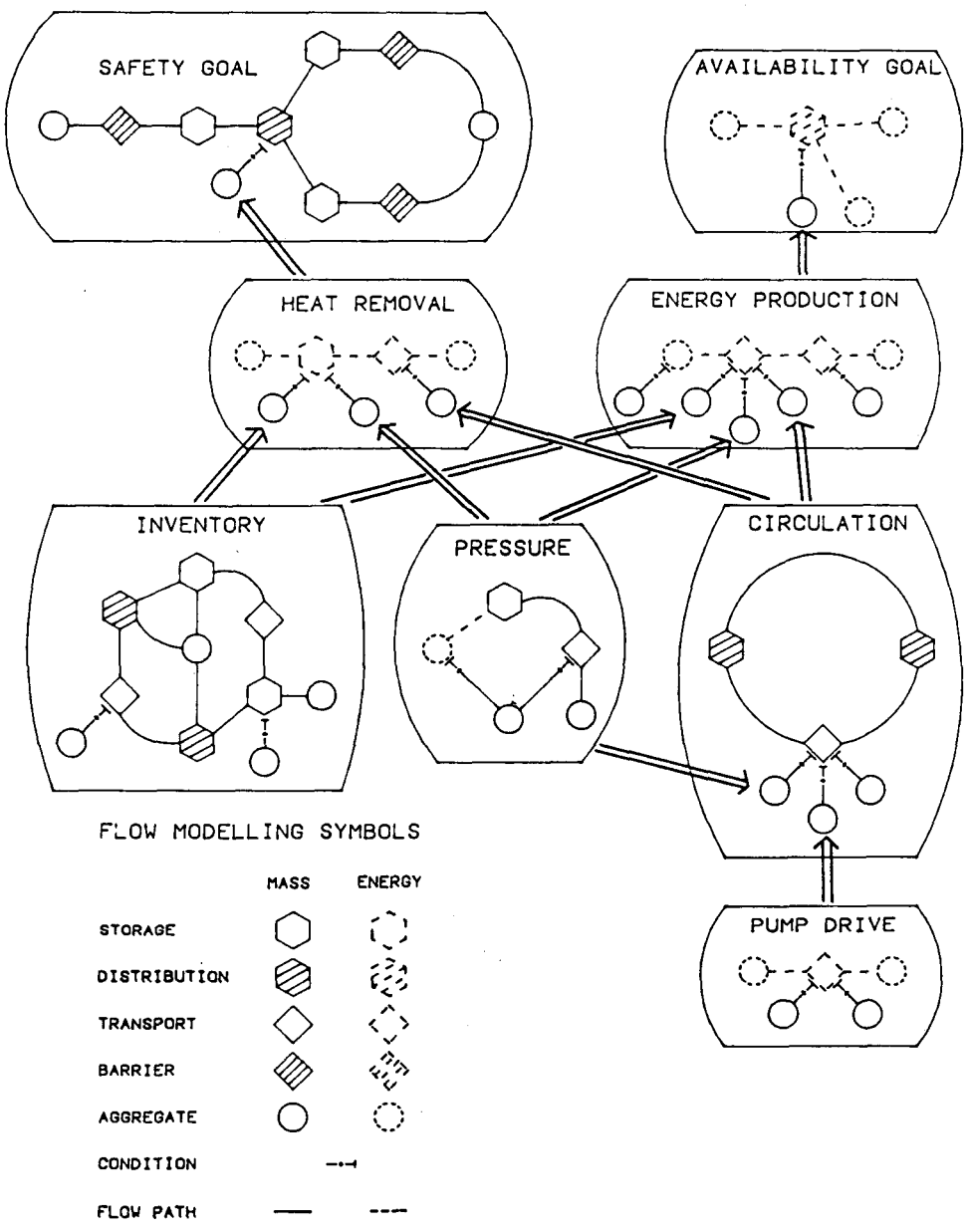


Fig. 6-5. Multilevel flow model of a nuclear power plant (PWR).

start-up and shut-down (Lind, 1979). The flow modelling framework leads to a systematic identification of plant control tasks at any level of functional decomposition in terms of these generic types and plant control can be systematically planned in generic flow model terms before allocation to operator or automatic equipment is considered.

This planning phase of the decision task for known or specified states is, perhaps, the least problematic part. The difficult part will frequently be the analytical state identification part, necessary to cope with disturbances. Since the energy--and-mass flow models represent the causal structure of the physical system in a uniform way, they are well suited to map the propagation of disturbances through the system. This means they can support a systematic state identification in terms of changes or deviations from specified or normal states in the flow topology by means of logic inferences based on measured variables. This is precisely the diagnostic task necessary for systems control. The systematic or consistent structure of diagnosis with reference to specified state and not to known fault patterns is mandatory for automation of the identification of unforeseen disturbances (Lind, 1981). A model based on a description of the mass-and-energy flow structure thus appears to be an efficient tool for an integrated design of the control hierarchy in device-independent terms as well as for a stringent formalization of these analysis and planning processes for computer implementation. The allocation of the decision task to operators or computers will be considered in more detail in the following.

Man-Computer Allocation of Decision Functions

Man-computer allocation of the different parts of the decision sequence is the last stage in a formal control system design process which has several distinct steps.

First, the functional properties of the process plant as identified during the design process at the various levels of abstraction are transformed into a hierarchical description in

terms of mass-and-energy flow structures, i.e., into a functional specification hierarchy for each of the relevant operating regimes. Then the bottom-up propagation in the abstraction hierarchy of disturbances from faults in the system is examined and the measured physical variables necessary to identify the disturbed state and to plan proper control actions, are determined by means of the flow model.

Second, the control or information paths necessary to maintain or change the states in this flow structure are determined together with the decision process necessary to identify the need for and plan execution of control actions in terms of the general decision sequence of figure 6-1. Furthermore, it is evaluated to what extent stereotype bypasses in the decision sequence can be utilized by the designer to simplify the decision function in the actual operating situation for the foreseen and well specified conditions.

Third, the information processing strategies which can be used during plant operation for the various phases of the decision sequence are identified. In general, strategies with very different structures and resource requirements can be used for a given decision phase. As an example, we can consider the identification of a disturbed state of the plant. This identification or diagnosis can be performed by various search strategies related to different representations or models of system properties (Rasmussen, 1981). An abnormal plant state can be identified by a symptomatic strategy implying search through a set of symptom patterns labelled in names of states or actions. The symptom patterns can be stored in a library of symptoms in the memory of an operator or a decision table of a computer, or they can be generated ad-hoc in a hypothesis--and-test strategy by an operator and/or a computer with access to a proper functional model of the control object. These strategies depend on symptom-patterns or models related to known failed functions, which is not the case for the topographic search strategies. In these strategies, search for the deviation from normal state is done with reference to the normal function, which eases the problem with identifying unforeseen states. In return, labelling in predetermined tasks is not feasible and ad-hoc planning may be necessary.

These strategies have very significant differences with respect to the type of model, the symbolic interpretation of data and the amount of information which is required and with respect to the necessary data processing and memory capacity. Consequently, they match the capabilities of computers and people differently.

Therefore, the fourth step in the systematic design will be to evaluate the match between the requirements of the various possible strategies and the resources available for the decision makers, i.e., designers, operators, and process computers.

To a large extent, this allocation procedure will lead to traditional designs in the clear-cut choices. The control decisions to serve the majority of necessary control links required to maintain specified states in the equipment will be analysed by the designer and implemented by standard control algorithms. Likewise, the control sequences necessary for planned, orderly coordination and reconfiguration for start and stop sequences will be analysed by the designer and the necessary sequences transferred to operators as instructions or to automatic sequence controllers as decision tables. However, in designing for disturbance control the systematic consideration of possible strategies for state identification, prioritizing and planning along the line discussed here will support the search for a consistent overall design.

For more complex emergency situations, a "once-and-for-all" allocation of the decision functions is difficult because demand/resource match will depend on the specific situation and may change several times during the decision processes. A kind of cooperative strategy in which operators and computer in parallel consider the same decision problems may be preferable. It will then be possible to let the role of decision maker and that of monitor and guide shift back and forth between man and computer depending upon the immediate situation. Consider, for example, the use of various diagnostic strategies for system identification. An expert trouble shooter will start using symptomatic search based on recognition of familiar symptoms -

this strategy utilizes all his experience and skill and may rapidly lead to the result. However, the expert is characterized (Rouse, 1981) by his ability to recognize when symptoms are unreliable with the result that he will switch to a careful, topographic search. This requires a high capacity for remembering and inference and can be efficiently supported by a computer. For a computer diagnostician, the reverse will be an appropriate strategy. Thus a consistent, topographic search in the flow topography at several levels with conservative careful inference and data transformation will be more suitable followed, when no more resolution is available, by a seeking of assistance from a human operator for additional knowledge, symptoms, locations of recent repair of the plant etc. In this way, complementary approaches can be used by man and computer, but planning of a successful cooperation depends on an overall structuring of system function, control requirements and decision functions which is device independent.

Even though the overall control structure and task allocation are developed in terms of the abstract flow-topology, the operators may choose to implement their allocated control decisions a conceptual framework at another level of abstraction closer to the physical anatomy level. This may affect the demand/resource match and must be considered when tasks are allocated since, for example, iterations between descriptions at different levels of abstraction may be required. Furthermore, the conceptual framework that operators will tend to prefer as the basis for the actual task will depend on the framework used for the display formats and data conditioning, which therefore should be considered concurrently with the decision task allocation (Goodstein, 1982a & b). See also section 7.

In this way, the abstraction hierarchy is used to design the control system while the specification hierarchy at the abstract function level is used to coordinate the structure of the total control strategy.

IMPLICATIONS FOR INFORMATION DISPLAY

The advent of computers does not seem to have given rise to any significant advances in the information display design philosophy employed in control rooms of industrial plants. Instead computer-based presentation techniques in many ways preserve the **one sensor-one indication** approach from traditional installations. Thus the relatively restricted area on the display screen is used to display information in ways which reflect both pre-computer practises as well as the influence of digital computer-inspired alphanumeric presentations as the basis for the display repertoire which is utilized.

One of the themes of the work being reported is the need for a **multi-level** approach to information display which is based on the conceptual ideas on plant representation and control discussed earlier. For example, Fig.7-1 illustrates the two-dimensional problem space which serves to structure the information which is needed. Thus the horizontal axis denotes **whole-part** considerations; i.e., the degree of plant detail that is in focus. The vertical axis reflects the different **levels of abstraction** or ways of thinking about the plant; i.e., about goals, functions or equipment. In an actual plant situation, the operators' information needs will shift dynamically around in this plane - e.g., from considerations about overall system goals all the way to detailed speculations about individual components.

An illustration of a related information **display** concept is shown in Fig.7-2. Essentially it consists of five displays each of which is aimed at supporting particular aspects of the operators' total needs for information. The concept is based on the human capabilities for functioning in three behavioral categories - **skill**, **rule** and **knowledge**-based - as discussed previously. See also Goodstein & Rasmussen 1980, Rasmussen 1980,1983; Goodstein 1981,1982a,b. These can be characterized briefly as follows:

VARYING NEEDS FOR INFORMATION

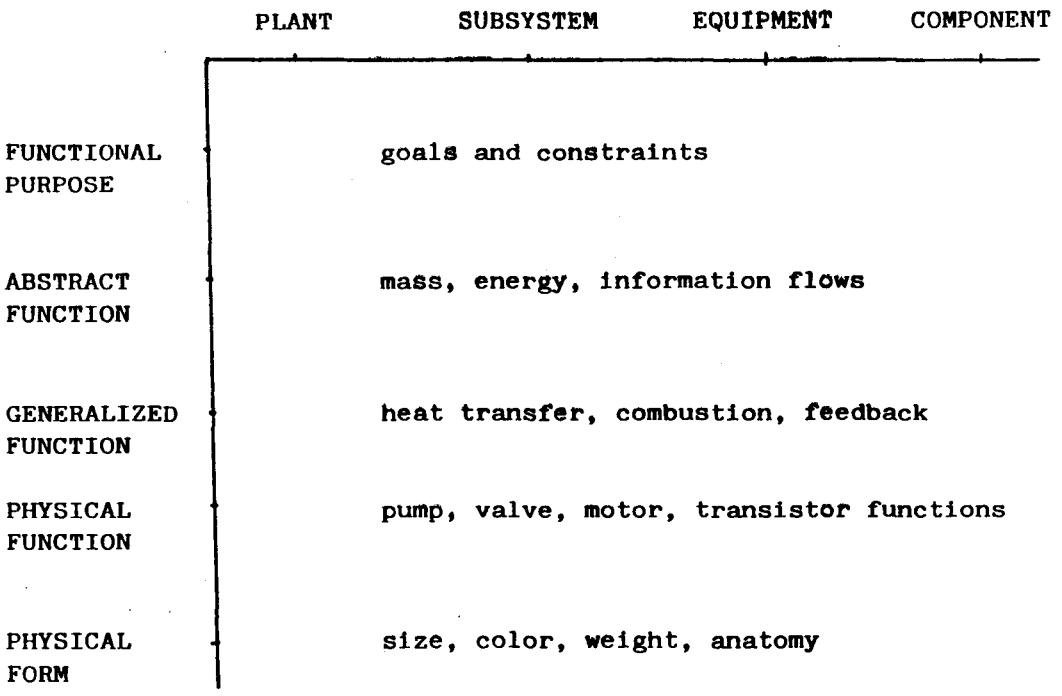


FIGURE 7-1

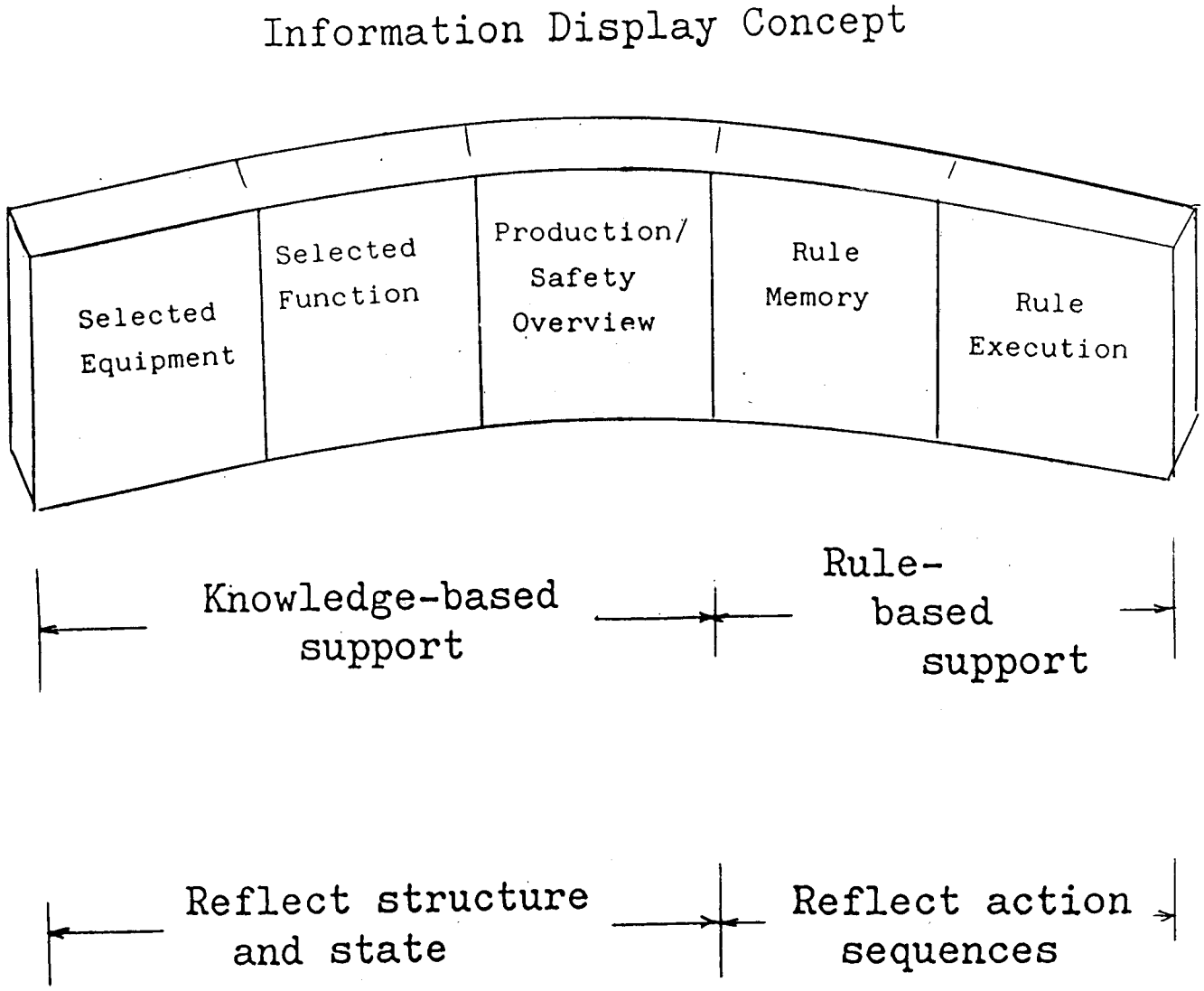

Information Display Concept
Selected Equipment
Selected Function
Production/ Safety Overview
Rule Memory
Rule Execution
Knowledge-based support
Rule-based support
Reflect structure and state
Reflect action sequences

Figure 7-2

Skill-Based Behaviour

Exercised in sensori-motor tasks involving steering, driving, tracking as well as manipulative tasks of all kinds. Examples are:

Setting process variables and set points;keeping process variables within limits; finding and operating controls, switches, etc.

Rule-Based Behaviour

Applies in the broad spectrum of procedurisable tasks in which a set of learned/prescribed rules is followed in order to achieve a given goal/purpose. Executing the rule will probably involve skill-based subroutines. Examples range from

When lamp X lights, turn on Y and check for Z to

Complete plant start-up procedure.

Knowledge-Based Behaviour

Becomes necessary when skills and/or rules are not available. Thus more of a conscious thought process comprising **identification** of state, **decision-making** regarding a remedial strategy and **planning** of the necessary procedures/rules for implementing this strategy is involved.

Information Requirements

Information requirements for achieving compatibility with these three modes of behaviour differ considerably. As illustrated below, elements of display support should consist of:

Support knowledge	-why		
	- what		
	- how		
Support operators' own deliberations	- strategies		search
	- goals		identify
	- priorities	in	decide
	- values	order	:
		to	:
Support operator actions on the plant			:
	- what to		execute
	- howto		check

These will be discussed in a little greater detail.

Support Knowledge

Rasmussen & Lind (1981) discuss how people are able to cope with complexity. Among the tools used are the abilities for abstraction and for decomposition/aggregation which play important roles in making it possible to restructure/reformulate a new or unfamiliar problem in order to enhance its solution. For example, an operator's top-down diagnostic search through the system in response to a disturbance will be subject to a given stop criterion. This will be a function of the current goal - e.g., keep the plant running by finding the appropriate compensating action to remedy/bypass a defective function - or - identify, repair/replace a defective component. Thus the need for information can be quite varied and indeed range from considerations at the overall system level to speculations about single loops or components. At each of these levels, there can

be a requirement for different kinds of information - depending on the needs of the moment, operator experience or just personal preferences. These consist of:

- Main purpose, reason for the (sub)system's existence in the overall process; what performance can one reasonably expect from such a system, etc

- Fundamental behaviour - energy/mass transport, storage and/or information flow together with the conditions for maintaining/supporting these.

- Functional structure and state.

- Physical structure and state.

- Component characterisation.

In simpler terms, this is equivalent to saying that, when working at any of the above levels, there are generally three relevant degrees of abstraction:

- The intention behind this (sub)function/process = WHY

- The (sub)function/process under consideration = WHAT

- The implementation of this (sub)function/process = HOW

The relationships can also be seen from Fig.7-3 for a subprocess (X) which is located at some given point in the overall system hierarchy. If we keep our attention on this subprocess, then, at the WHAT level, information on its structure and behaviour should be made available to indicate that all the conditions (supplies, etc.) for supporting the subprocess are satisfied, the appropriate paths are activated, the degrees of freedom are under control and that therefore the subfunction (X) is realized. If this is not the case, then the disturbance has to

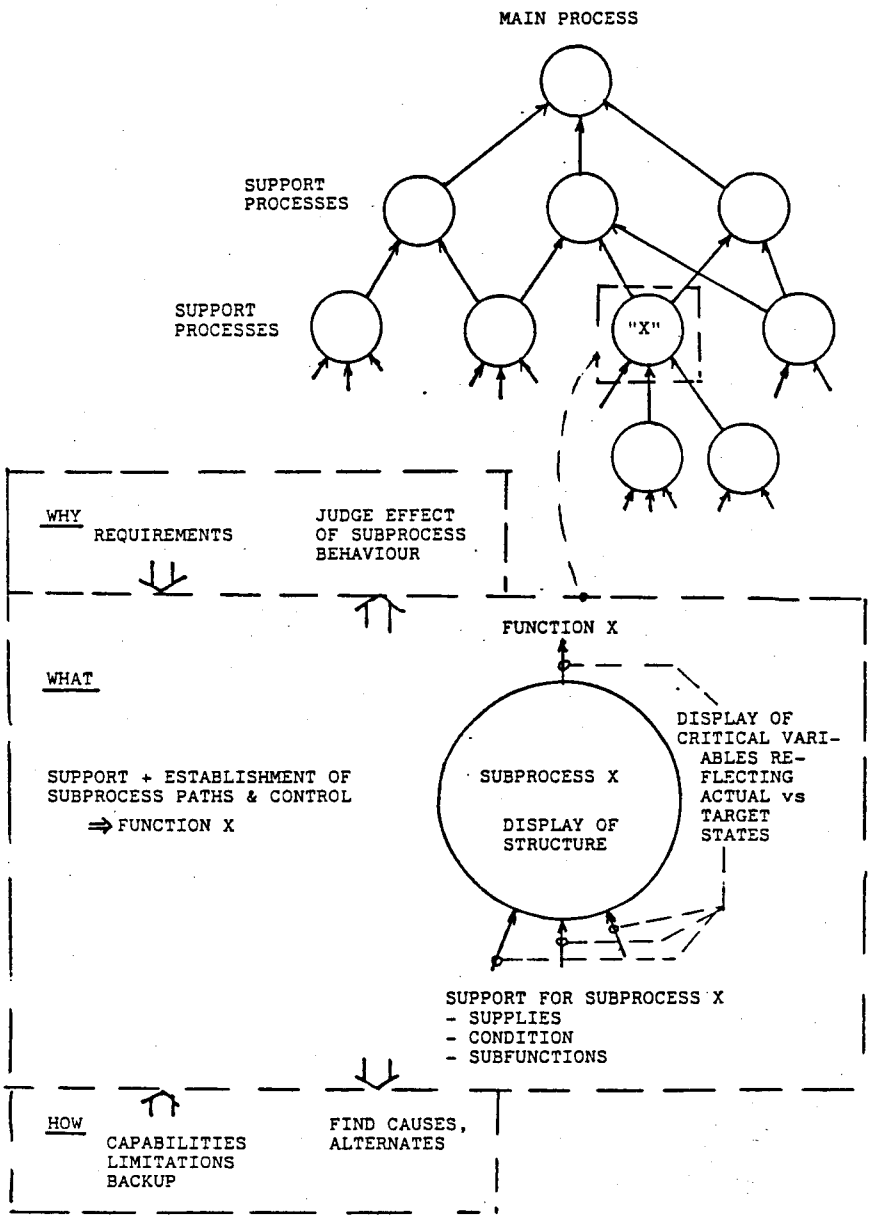


Figure 7-3 WHY,WHAT,HOW Relationships

be isolated to one or more of these; i.e. conditions, path, control - and a suitable corrective task devised. The remedy may be immediately apparent - e.g. increase flow. However, information at the HOW level may be needed - either to narrow down further, to find an alternate, to find a cause, etc. In addition, it is important that the WHY level be consulted - in order to keep a check in the higher level implications of the disturbance as well as the possible effects of the alternate modes of operation which could be considered.

The iterative nature of the associated thinking process should become apparent. For example, if the HOW question is raised about the support features, then the resultant shift in level and attention may actually reflect a desire for a description of WHAT the support subprocesses are/do so that the cycle described above is repeated for the new subprocess.

The philosophy behind Figs.7-1 to 3 can be reflected in a display WINDOW concept as shown in Fig.7-4 which gives a consistent structure for a set of displays which holds for each functional element in the system.

Window 1 (WHY)

It is not customary to specifically include WHY information on control room displays. The assumption is that if operators will just follow procedures, the WHY'S will be taken care of implicitly. This, however, is not compatible with the notion of operators as competent knowledge-based problem solvers who are capable of recognizing the unexpected and dealing with it. It therefore follows directly that any planning for recovery from an identified disturbance must represent an acceptable compromise between the capabilities of the actual physical plant (possibly in a disturbed state) and the design intention/goal as reflected in the functional requirements and constraints.

Thus Window 1 is an instance of an "interface" betwen the particular (sub)process and its "users" - (a) where the adequacy

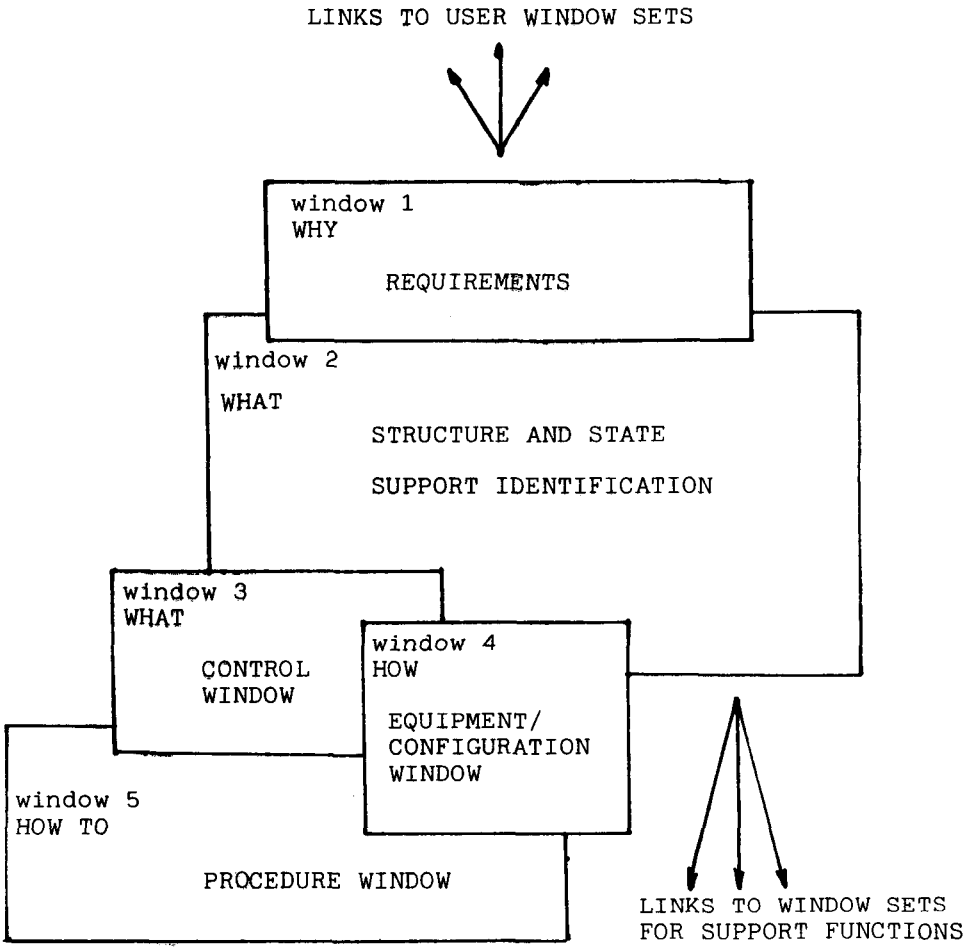


Figure 7-4 Multi-window Approach to information Display

of the delivered function can be judged against requirements coming down from above, and (b) where the effects in an upwards direction of deviations, alternate possibilities for recovery in the event of a disturbance can be evaluated on the basis of considerations of intention, span of tolerances, co-functioning constraints, etc.

It is our feeling that the advent of computer-based methods for design and documentation will make it feasible to record and store the bases for design decisions made regarding safety and availability. In this way,the design base will be available (years) later in connection with commissioning, training, procedure generation, dealing with disturbances and/or modifications, etc. and then enhance, for example, the possibilities for incorporating Window 1 WHY-type information.

Window 2 Causal Information (a WHAT component)

Window 2 is intended to give information on the causal structure of the particular (sub)process as well as its current operational state. What is needed here is a high level representation which is relatively independent of implementation details and yet can serve as an effective visualisation of state and, hopefully, also of task. Thus there is a good justification for using a flow modelling approach - be it for energy, mass, information - and a high level symbolic flow language for depicting the basic flows in the process has been described earlier. (See also Lind 1981,1982; Rasmussen and Lind 1981,1982)

Window 2 would thus supply operators with the following types of information about WHAT:

- Topological flow diagrams of the processes reflecting actual paths, distribution of flow, deviations from target values, etc.

- Quantitative information on the state of the "critical

variables" which comprise the defining set to indicate whether the function is/is not normal.

- An identification of the set of support conditions which are required to be satisfied in order that the (sub)process can be operable, together with appropriate information on their state and interrelationships.

Window 3 - Control (a WHAT component)

In general, there are three major requisites to proper functioning - the necessary **support functions** and **supplies** are available, the appropriate **flow paths** are activated and the degrees of freedom are under **control.** Thus the control system is equivalent to a kind of "finishing touch" condition which overlays the physical system with a web of interrelated constraints. These then serve to restrict (sub)process behaviour to an allowable - preferably optimal - region compatible with higher level requirements in spite of variations, drifts, etc. Since operators can have greater difficulty in understanding the control system than other more directly process-related aspects, the need for appropriate control information seems to be quite high.

However, it seems important that the possibilities for taking a control action first be identified on the flow schema of the process itself (e.g., Window 2) if these actions can affect the overall flow. Identification of control actions at this level would thus be more likely to be compatible with operator speculations about process behaviour including the possibilities for making corrections and adjustments. However, the additional Window 3 providing information such as the following would give a better basis for selecting, performing and checking a control action.

- Control requirements

  . modes

. transitions

. limits

. constraints (interlocks)

- Operation

. control organs

. actual vs. target state

. dynamics

- Backup/alternate forms/means for control

- Access to relevant procedures for manipulating the various control systems.

It is also at this window that implementation-dependent HOW details can begin to arise - e.g., if the system actually consists of two or more loops operating simultaneously - each of which is under separate control.

Window 4 - Implementation (HOW)

It is first at Window 4 that the more familiar view of the plant at the mimic diagram level appears. Configuration monitoring and control are tasks related to the particulars of a given plant and require support which can facilitate a search and localisation activity within an equipment-based structure. Information which is important at this level relates to:

- Physical paths and connections - prescribed, actual and alternate
- Actual vs. target state in terms of the variables reflecting equipment operation.

- Equipment capacity and limitations.

- Access to relevant procedures and checklists at the equipment level.

The capability of an advanced display system to perform "windowing and zooming" should be particulary applicable in the physical world represented here.

Windows 1-4 are thus intended to support operators in knowledge-based operations of observing, weighing, deciding and planning while meeting requirements for maintaining relevant overviews, reducing memory overloads and encouraging the use of top-down search strategies through an orderly and easily accessible display hierarchy. In terms of Fig.7-2, they make up the three left-hand displays.

Window 5 - Procedures (HOW TO; DID IT)

Window 5 is aimed at supporting procedural (rule-based) tasks connected with the particular (sub)process - either as prescribed for the operators or for automatic sequential control equipment. As described elsewhere (Goodstein 1979, 1982), these aids are composed of two components:

- Support of memory - what is in the procedure

- Support (feedback) regarding the execution of the procedural steps themselves - e.g., "check state, do action, check result".

The possibilities for combining computers and displays for this purpose are of course quite obvious.

To summarize this section, an integrated information structure based on a multi-level representation of the process AND the concept of abstractional shifts in human thinking in order to cope with complexity has been proposed. A generic set of "windows" has been described which can be applied to each process/function in the plant to inform about its WHY, WHAT and HOW - i.e., its interface with higher order requirements which set goals, its own flow structures, the relevant conditions necessary for satisfactory functioning, any associated control systems and, lastly, details about its physical implementation. This knowledge-based foundation is supplemented by a procedural and checklist window to support rule-based plant manoeuvering.

GNP TESTBED FOR EXPERIMENTAL STUDIES

The GNP activity is an outgrowth of the conceptual work described earlier in the areas of system representation, human modelling, etc. - particularly with an eye towards problems with diagnosis and decision making in connection with complex technical systems. There was felt to be a need for a realistic test bed of a reasonable (and variable) complexity for evaluating and studying these concepts by means of a suitably designed and executed experimental program. The test bed which resulted can be considered in various ways:

- a plant family based on a PWR-like process (thus the name **G**eneric **N**uclear **P**lant; i.e. GNP)

- running simulator programs for two members of this family

- an experimental "control center" with computer-based displays and controls

- a scenario generator for placing the subjects in diverse types of decision making situations in connection with simulated faults of various kinds

- a data collection and analysis facility for recording and studying the behavior of the experimental subjects

- a training and testing activity

One of the important requirements regarding the choice of the GNP was that it had to reflect different aspects of system complexity met in modern production systems. These include:

- a component or subsystem can be part of the implementation of several functions

- correspondingly, a plant function can have several alternative implementations

- plant and subsystem goals can be multiple and partially in conflict
- the functional structure is dependent on the operating mode

In terms of operator involvement, this means that GNP is (or can be) "realistic" enough to support tasks where information about **goals, functions** and **equipment** must be available in order to cope, for example, with "ends"-oriented situations having to do with power and/or inventory control through the management of the available resources or "means".

Of course the implementation of GNP does not of course have to represent all of these aspects in a given application; therefore a certain amount of flexibility and modularity was called for. The type of fidelity which was desired is related more to functional diversity considerations than to achieving close agreement with the operating specifications and/or data of any particular plant. Thus the component models are not (necessarily) very accurate replicas of actually existing components but rather describe prototypical characteristics and properties based on the use of fundamental physical laws. See Lind (1983).

Two versions of the power plant selected are shown in Fig.8-1. Each is a very simplified nuclear power station of the PWR type and the difference between the two can be seen in the primary circuit where the version currently being used includes a pressurizer together with an associated makeup/letdown system. The control systems include primary pressure, pressurizer level, secondary pressure, steam generator level and turbine-generator control. Protection systems have not yet been included.

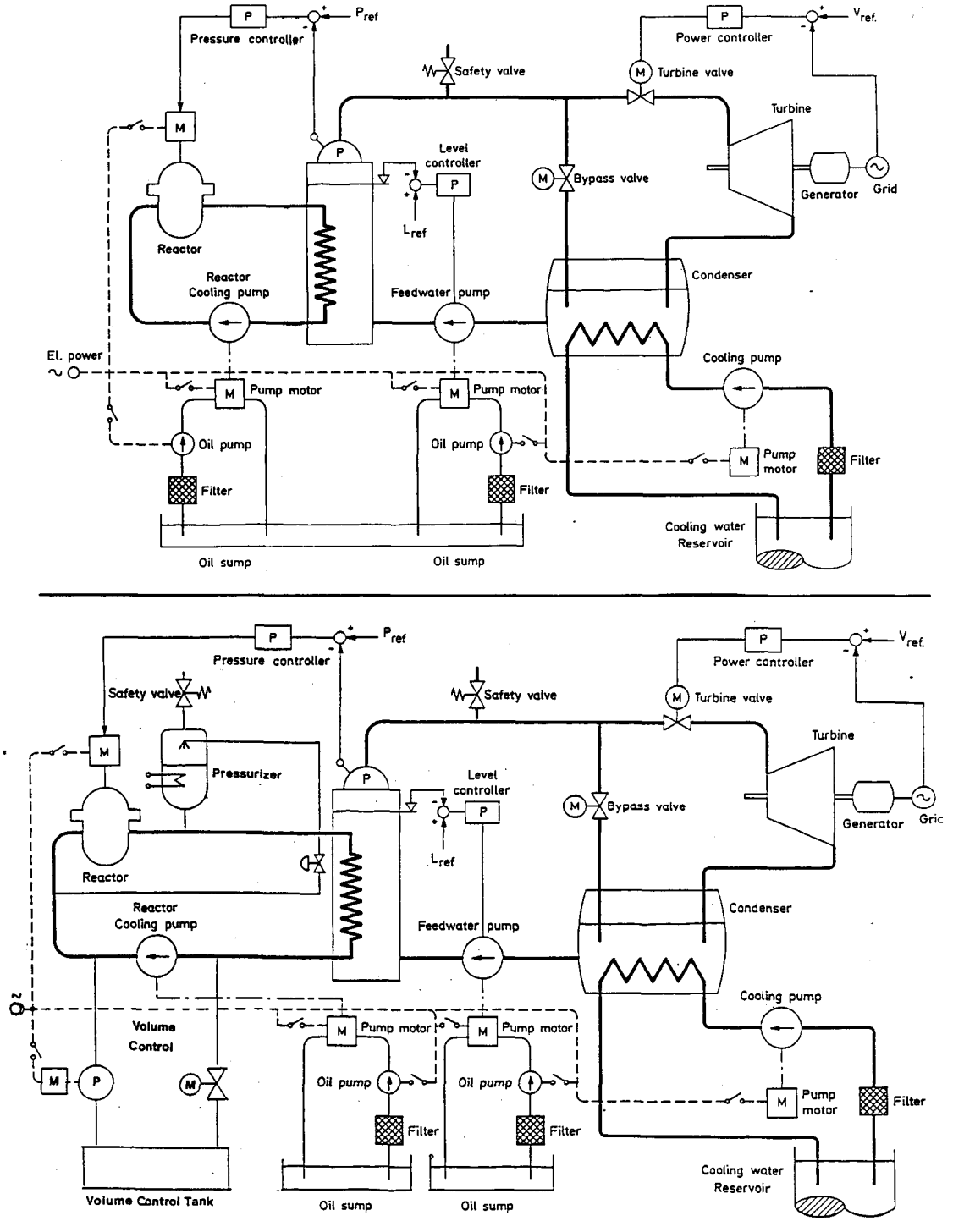


Fig.8-1 TWO VERSIONS OF GNP

Uses of GNP

General Remarks

The key areas towards which the GNP program was aimed had to do in general with supporting the operators in their supervisory control functions. Earlier portions of this report have dealt with the more conceptual ideas behind the experimental work. Among other things, these have involved the use of the **multi-window** approach to information presentation based on a representation of the plant as a hierarchy (almost) of functionally-based entities coupled together in order to achieve given top goals concerning, e.g., availability and safety. For each entity, the connotations reflected in operators' questions about **WHY, WHAT and HOW** are essential factors in deciding on a relevant display structure. The basic idea was illustrated in Fig.7-3 where, for any selected element in the hierarchy, top-down information about goals, requirements and target states (=ends) can be compared to actual structure and state and to equipment status and capability (=means) with appropriate access to relevant procedures, control information, etc.

This integrated approach thus attempts to tie together the various loose ends which often characterize computer-based solutions for control rooms. In this way, the equivalents of extra DASS displays, SPDS, alarming and other separate (e.g. procedural) aids for use in "special situations" reappear as basic elements within the integrated concept in order to assist with the various phases of the operating staff's decision-making.

The First Study

With this introduction in mind, the use of GNP to investigate specific points can be discussed. One of the important extensions proposed here to traditional approaches on information display is the multi-level display structure

approach. This is felt to be essential in order to aid decision-makers in ascertaining any mismatch between functional goals and requirements and the actual state of affairs at the appropriate level of abstraction where a suitable control task can be identified and carried out.

Therefore the first exploratory experiments were concentrated on the **abstract functional** level (i.e., which deals with mass and energy in the system). A set of fifteen displays based on a functional analysis of the first version (GNP1) was generated. This analysis, based on the multi-level flow modeling (MFM) method (See Lind 1981,1982) produced in diagrammatic form the result of a top-down goal-directed functional identification and description of the plant in terms of mass and energy flows. The result is shown in Fig.8-2. Thus the top goals of safety and production give rise to a multi-level arrangement of functional entities - each with its own sub-goals, targets, conditions, etc. and conformed and constrained so as to satisfy the requirements of the "user" functions at the (usually) higher levels. Thus for each function a **goal** can be identified, as well as a **control task** and a set of **critical variables** the state of which reflects whether the goals indeed are being met. The variables are/should be compatible with the level of abstraction and, in general, suitable algorithmic transformations from the "raw" transducer data will be required.

The most interesting (and provocative) feature of this implementation was the employment of the set of flow symbols defined by Lind (and used as part of the modelling exercise itself) to depict the mass and energy flow structures on the displays. These symbols have no resemblance whatsoever to familiar pumps, valves, etc., but instead represent various functional elements such as **transport, storage, source/sink,** etc., coupled together as required to achieve the desired mass/energy function.

The use of these symbols was a deliberate attempt to represent the higher levels of information within the two-dimensional space described earlier in a distinctive fashion which would

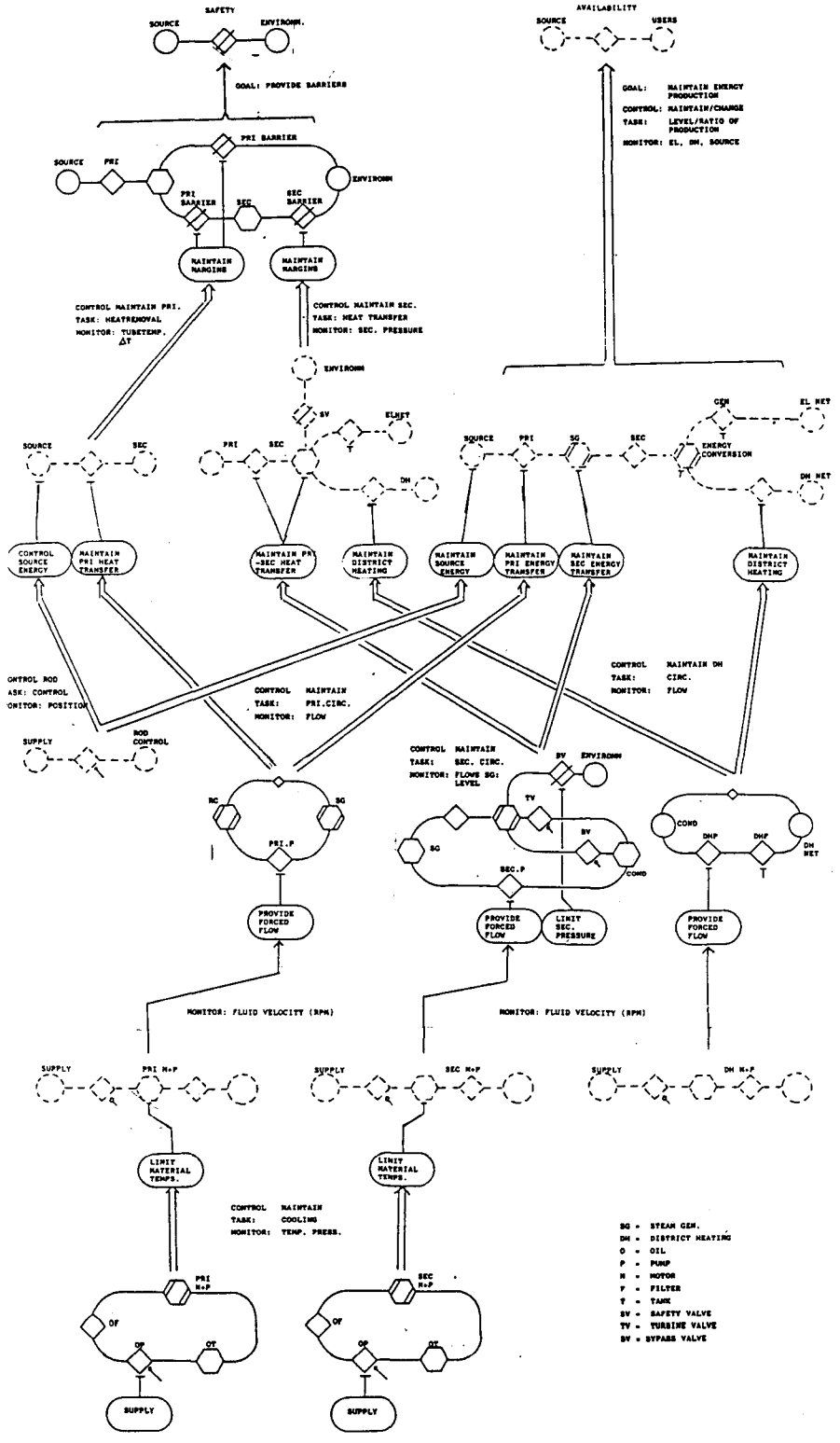

SAFETY
SOURCE
ENVIRONM.
GOAL: PROVIDE BARRIERS
PRI BARRIER
SOURCE
PRI
ENVIRONM
PRI BARRIER
SEC
SEC BARRIER
MAINTAIN MARGINS
MAINTAIN MARGINS
CONTROL MAINTAIN PRI.
TASK: HEATREMOVAL
MONITOR: TUBETEMP. ΔT
CONTROL MAINTAIN SEC.
TASK: HEAT TRANSFER
MONITOR: SEC. PRESSURE
AVAILABILITY
SOURCE
USERS
GOAL: MAINTAIN ENERGY PRODUCTION
CONTROL: MAINTAIN/CHANGE
TASK: LEVEL/RATIO OF PRODUCTION
MONITOR: EL, DH, SOURCE
ENVIRONM
SV
EL NET
SOURCE
SEC
PRI
SEC
DH
SOURCE
PRI
SG
SEC
GEN
EL NET
ENERGY CONVERSION
DH NET
CONTROL SOURCE ENERGY
MAINTAIN PRI HEAT TRANSFER
MAINTAIN PRI -SEC HEAT TRANSFER
MAINTAIN DISTRICT HEATING
MAINTAIN SOURCE ENERGY
MAINTAIN PRI ENERGY TRANSFER
MAINTAIN SEC ENERGY TRANSFER
MAINTAIN DISTRICT HEATING
ONTROL ROD
ASK: CONTROL
ONITOR: POSITION
CONTROL MAINTAIN
TASK: PRI.CIRC.
MONITOR: FLOW
CONTROL MAINTAIN DH
TASK: CIRC.
MONITOR: FLOW
SUPPLY
ROD CONTROL
CONTROL MAINTAIN
TASK: SEC. CIRC.
MONITOR: FLOWS SG: LEVEL
BV
ENVIRONM
RC
SG
PRI.P
TV
BV
SG
SEC.P
COND
COND
DMP
DMP
DH NET
PROVIDE FORCED FLOW
PROVIDE FORCED FLOW
LIMIT SEC. PRESSURE
PROVIDE FORCED FLOW
MONITOR: FLUID VELOCITY (RPM)
MONITOR: FLUID VELOCITY (RPM)
SUPPLY
PRI M+P
SUPPLY
SEC M+P
SUPPLY
DH M+P
LIMIT MATERIAL TEMPS.
LIMIT MATERIAL TEMPS.
CONTROL MAINTAIN
TASK: COOLING
MONITOR: TEMP. PRESS.
PRI M+P
SEC M+P
OF
OF
OT
OF
OF
OT
SUPPLY
SUPPLY
SG = STEAM GEN.
DH = DISTRICT HEATING
O = OIL
P = PUMP
M = MOTOR
F = FILTER
T = TANK
SV = SAFETY VALVE
TV = TURBINE VALVE
BV = BYPASS VALVE

Fig. 8-2

discourage operators from making possibly interfering associations to lower level implementation-related knowledge/experience. An interesting question in this research is to determine a desirable distribution within the display network of the flow symbols and the more traditional. The multi-window approach retains both at all levels but may be difficult to manage, seen from a display accessing point-of-view.

At any rate, there was considerable interest in investigating whether users could learn to identify GNP state on the basis of this kind of "abstract" information. Some of the preliminary results are given later.

An example of these displays is shown on Fig.8-3b, which is one of the fifteen displays and represents "removal of heat from the secondary". Fig.8-3a indicates the generic layout for all of the displays.

Thus, each display actually consists of two parts:

(1) the **functional array**, common to all displays, is a miniature replica of the total functional network for the GNP (as shown in Fig.8-2) where the letters represent the various functions and the lines the connections between functions. It fulfills two purposes:

By means of color coding, it indicates the **current choice** of display as well as its relation to the rest of the display set (and there fore to the plant itself). I.e., "where are we now and where can we go to get more information?"

By means of color coding and blink, it serves as an **alarm tableau** at the abstract-functional level to indicate whether each of the fifteen functions is meeting its goals with respect to maintaining given conditions regarding mass/energy. It is clear that corresponding alarms can be defined and the associated data transformations specified at all levels of the abstraction hierarchy. They appear to be

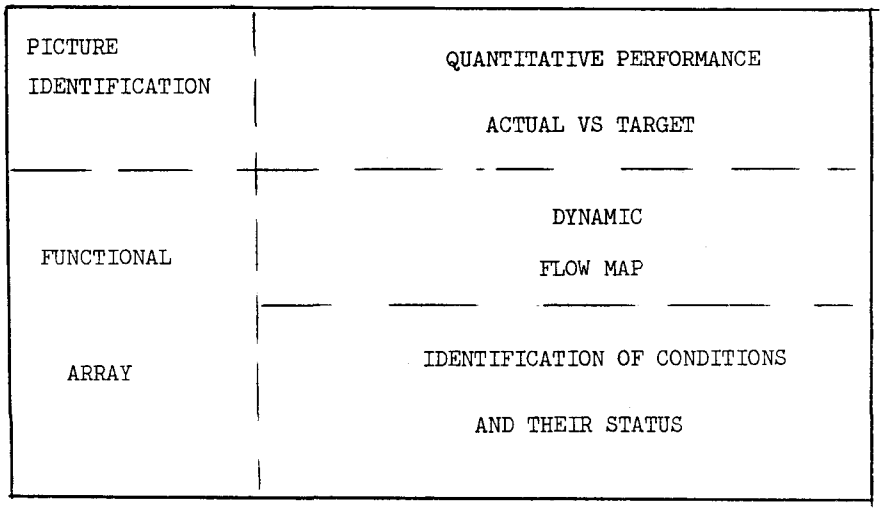


Fig.8-3a Generic Display Layout

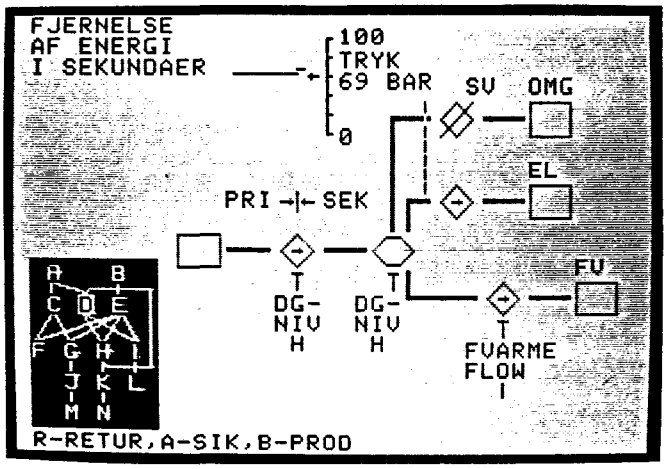


Fig.8-3b Sample Display - Removal of Heat from Secondary

particularly appropriate at the abstract-functional level because they are few in number (perhaps 60 for a full-blown plant compared to thousands at the physical-functional level), richer in structure and content and thus suited to help the operators "see the forest for the trees" - at least in the initial phases of dealing with a disturbance. In particular, many cases of multiple failure combinations can be seen more clearly.

(2)- the **flow structure** for the selected function - color coded according to whether the function deals with mass or energy, together with relevant **state** and **condition-related** information. State information on the associated critical variables is given in digital and analog formats - including a trend indication. This diversity is intended to help operators treat the information as **signals**, **signs** or **symbols** (Rasmussen 1983) depending on their task, training, experience. The state of the flow network is updated dynamically by means of indicators for "too high/too low" flow, changes in flow function (i.e. barrier to transport), etc. Lastly, the conditions necessary to maintain the given function are identified with an abbreviated name together with the letter corresponding to the function (and associated display) which "supplies" the condition. This facilitates an orderly movement from picture to picture in searching for relevant information. The condition "buttons" (letters) change color and blink in case of a fault.

Thus searching in the system can be carried out via these condition "buttons" or through the "buttons" comprising the functional array. The actual request on GNP1 occurred through the keyboard (by typing the appropriate letter) but the newer versions will use a touch panel thus permitting a more direct access.

Preliminary Results

The first version of GNP was used to evaluate the response of subjects being subjected to a state identification task on the basis of the information presented in the set of flow displays. Experiments were run on two separate versions of GNP 1 - one at Risø and one at the Halden Project. Details of the training, etc. are given in Goodstein et al (1984) and Hollnagel et al (1984) and the discussion here will be limited to some preliminary conclusions and observations.

The strategies used by most subjects to search in the set of displays to find the source of disturbances seemed to be structured (as was intended) more or less by the displayed relationships between the flow functions - either via the functional overview or through the state of the condition "buttons". That is, the subjects used the various dynamically updated functional indicators to guide their choice of displays in order to narrow in on the one(s) where the fault(s) occurred. Performance of course was quite dependent on background knowledge and experience with technical systems. Particularly for novices, problems often arose in connection with understanding the meaning and implications of the information regarding the individual flow elements and there was a widespread tendency to "think physically" about the presented information and its significance.

It is clear that the incorporation of a multi-level display support which is intended to help operators keep track of goals, functions and equipment requires suitable symbol (icon) and data sets to which they can relate at the various levels without interference. It is also obvious that appropriate trade-off or allocation strategies for assigning these symbol and data sets are required - i.e., when should they change to match the operators' needs during a diagnostic search or a planning task, etc. Again, the multi-window approach seems to be a suitable framework for investigating these questions.

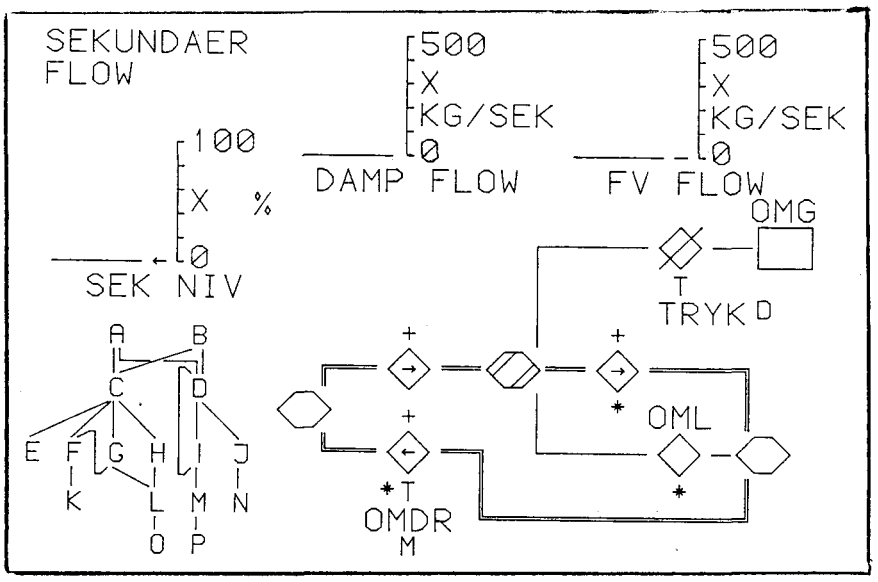
Further Developments

Further work has been done to expand the available display set to include information at a second level of the abstraction (means-ends) hierarchy; i.e., the **physical functional**, corresponding to the more familiar mimic-type of presentation in which process diagrams showing physical components and their respective interconnections are depicted together with appropriate state information. Thus the first set of displays - as described above - has been retained but the user/operator has the additional possibility of calling up the equivalent of a **HOW** display for any selected function, thus making available information on the **mapping** of functions to equipment for the particular operating mode.

Conversely, the possibility is provided for performing the reverse mapping of displays at the mimic level to displays of associated function(s) in which the particular selected piece of equipment is involved.

As was discussed above, these transformations are important to overcome possible confusion on the part of operators arising from the **many-to-many mappings** between goal, function and equipment which characterize the type of systems under consideration. Thus, for example, in planning a control action, it is important to be aware of possible side effects due to the fact that the resources/equipment chosen for carrying out the action already may be in use to implement another function with the result that a conflict can occur. Or, in carrying out a diagnosis, it can be vital to be aware of the current implementation of a particular function.

Thus, for the latest version of GNP, it is possible for the user to make use of display mappings such as those illustrated in Fig.8-4. Seen in terms of the two-dimensional information space described earlier, a function- equipment mapping would be equivalent to taking a vertical dive from a selected location on the abstract level to the physical→functional level. In the current implementation, this mapping is shown as an accentuating or



FUNCTION

TO

EQUIPMENT MAPPING

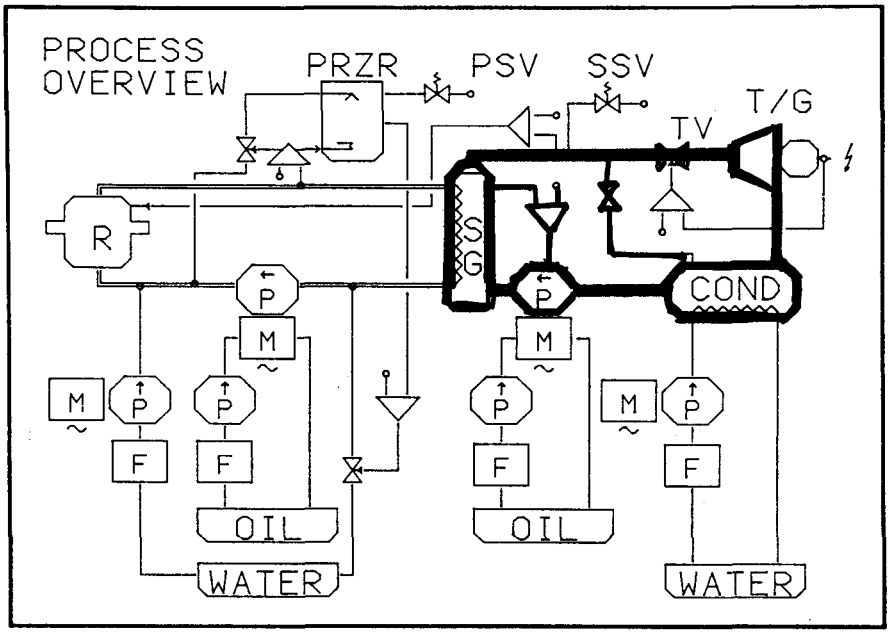


Figure 8-4

mass/energy display set. At the same time, appropriate state or other information can be displayed in the immediate vicinity. In terms of the multi-window concept of Fig.7-4, the two possibilities correspond to windows 2 and 4 for the selected function.

The reverse mapping, from equipment-_function, is also possible, although a little more complicated because of the many-to-many situation. See Fig.8-5. Thus, selecting a particular piece of equipment, the pressurizer, for example, first results in a version of the functional array which identifies the functions which directly utilize this component (but not necessarily all those which in turn are dependent on these functions. This information appears on the functional array). Thereafter, the user chooses one of these functions (in the example, function G) and the corresponding flow display appears. A toggling mechanism then allows the operator to directly switch back and forth between the mimic with the highlighted pump and the selected function - assuming a single display system.

It seems to be characteristic for GNP that there are many function-_equipment mappings which involve all or much of the physical plant. This highlights the beauty of the functional approach and the difficulties which can arise in wandering around the physical plane and trying to keep track of utilisation and performance.

At the present time, the implementation of this two level system is being completed prior to starting a new round of experiments. The plans are to give groups of subjects either functional or equipment-based training and therefter access to functional and/or equipment-based displays, in different combinations. The interest lies in tracking each subject's development and his/her use of the provided display set(s) while performing decision-making tasks. Different forms for performance monitoring coupled with other tests will strive for a better understanding of the mental models and strategies employed by the subjects in their climb up the novice-to-expert ladder.

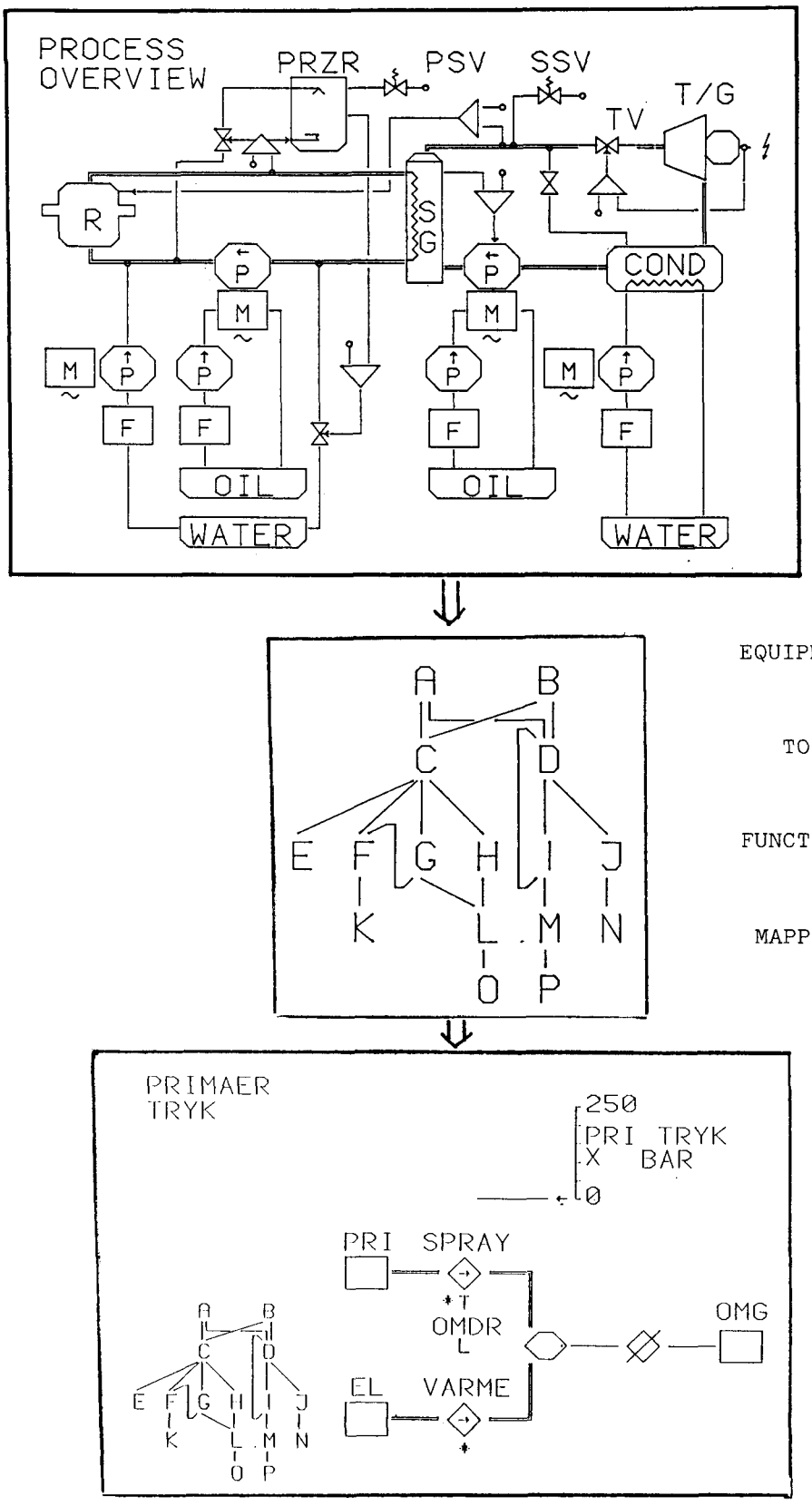

PROCESS
OVERVIEW
PRZR
PSV
SSV
T/G
TV
R
S
G
COND
P
M
F
OIL
WATER
EQUIPMENT
TO
FUNCTION
MAPPING
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
PRIMAER
TRYK
250
PRI TRYK
X BAR
0
PRI SPRAY
T
OMDR
L
OMG
EL VARME

FIGURE 8-5

their climb up the novice-to-expert ladder.

CONCLUSIONS

To briefly summarize the context; there are two trends which characterize the state of the world under consideration.

Current technological developments are leading to increased complexity and centralisation in administrative, technical and industrial systems. Abnormalities in these systems can lead to potentially drastic consequences. These abnormalities can come from technical failures and/or from (in themselves) natural and unintentional malfunctions by users and operators.

In parallel, these technological developments - especially in the area of information technology - are impacting on the work situations of the same users and operators of these increasingly complex systems. Solutions employing this technology are unlimited in number and possibilities. How do we choose among them so as to ensure (a) that system goals, e.g., regarding production and safety in the case of power generation, are met and (b) that the users and operators are assigned roles and responsibilities and are supported with appropriate aids in a way which is compatible with their capabilities and limitations and also is tolerant with respect to errors. How do we design human-machine systems for rare and perhaps risky situations which we cannot predict beforehand but expect operators to identify and manage.

The LIT 3.2-3.3 effort dealt with these problems through a parallel program of conceptual development and experimental studies which is described in some detail in the body of the report.

The project work resulted in the establishment of a framework for the systematic design of human-machine systems. This is composed of a sequence of steps beginning with a description of plant control requirements - seen especially from the point of view of fault and disturbance management - which integrates information at various levels of plant description in terms of

goals, functions and realisation. The so called multi-level-flow modelling technique which was generated represents a milestone in methodology development. This description is then used to formulate the corresponding decision-making sequences in plant-independent terms. With this basis, one can determine the information requirements necessary to support diagnosis, planning, task execution, etc. Thereafter allocations of functions between automatic systems and the operational staff have to be established so as to support the wish for a cooperative relationship between the two partners. This then gives a basis for the implementation of the required operator interface facilities, training, etc. The exercise is multi-disciplinary and requires expertise in engineering and operational analysis, human factors, cognitive psychology.

Another conclusion of the LIT3.2-3 project is the confirmation of the value of small-scale simulators such as the GNP system for selected studies of human-machine interaction.

It is clear that this area is in constant development. Research programs must be combined with running dialogues and contacts with designers and operational staff in industry. The research is necessary to further develop the basis for human-machine system design. The cooperation with industry is vital to encourage applications and evaluations. Incorporation of new information technology will affect the design process. It will have to become more "top-down" (goal-to-function-to-equipment) oriented and less limited to making incremental changes to existing designs in order to meet a new requirement. Indeed, in the end, design and operations will become more integrated.

Designers will have to become more versatile and their knowledge-base broadened in order to deal with the human-machine environment. Trends towards combined technical and humanistic curriculae in universities are signs of increased attention to these problems.

To conclude, the line of research carried out in the LIT project represents the result of an early realisation of the importance

of the human factor for safety and reliability. This effort is expected to continue. Programs under the European Common Market, in Scandinavia as well as national endeavors are current. To give an idea of the breadth of the field, the results of work in artificial intelligence (for example, in connection with expert systems) will be integrated in the next NKA program in order to support the interactive decision making which characterizes the operation and management of complex industrial systems.

REFERENCES

Goodstein, L.P., 1979, Procedures for the Operator - Their Role and Support, IWG/NPPCI Specialists' Meeting on Procedures and Systems and Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operation Situations, Munich, F.R. Germany.

Goodstein, L.P., and Rasmussen, J., 1980, The Use of Man-Machine System Design Criteria in Computerized Control sRooms, IFIP/IFAC ASSOPO 80 Symposium, Trondheim, Norway.

Rasmussen, J., 1980, Some Trends in Man-Machine Interface Design for Industrial Process Plants, ibid.

Goodstein, L.P. (1981) Discriminative Display Support for Process Operators; in Human Detection and Diagnosis of System Failures, J.Rasmussen and W.B.Rouse (eds), Plenum Press

Rasmussen, J., 1981, Models of Mental Strategies in Process Plant Diagnosis, ibid.

Lind, M., 1981, The Use of Flow Models for Automated Plant Diagnosis, ibid.

Goodstein, L.P. (1982) An Integrated Display Set for Process Operators; in IFAC/IFIP/IFORS/IEA Conference on Analysis, Design and Evaluation of Man-Machine Systems; G.Johannsen and J. Rijnsdorf (eds)

Goodstein, L.P. (1982) Computer-Based Operator Aids; in DESIGN 82, Birmingham, UK; IChE/Pergamon Press; Symposium Series No. 76

Goodstein, L.P. et al (1984) The GNP Testbed for Operator Support Evaluation - Risø-M-2460

Hollnagel,E. et al (1984) Report from the Pilot Experiment on Multilevel Flow Modelling Using the GNP-Simulator, OECD Halden Reactor Project, Report HWR 114.

Lind, M. (1982) Multilevel Flow Modelling of Process Plant for Diagnosis and Control; in Proceedings of International Meeting on Thermal Nuclear Reactor Safety, Chicago - ANS

Lind, M. (1983) GNP - A Power Plant Model for Man-Machine Experiments - NKA/LIT-3.2(83)122

Mesarovic,M.D. et al (1970) Theory of Hierarchical, Multilevel Systems; Academic Press

Norman,D. (1981) Steps Toward a Cognitive Engineering; Systems Images, System Friendliness, Mental Models; paper presented at Symposium on Models of Human Performance, ONR Contractor's Meeting, La Jolla, Ca. (UCSD)

Rasmussen,J. (1976) Outlines of a Hybrid Model of the Process Plant Operator; in Monitoring and Supervisory Control; T.B.Sheridan and G.Johannsen (eds); Plenum Press

Rasmussen,J. (1980) What Can Be Learned from Human Error Reports; in Changes in Working Life; K.Duncan et al (eds); John Wiley.

Rasmussen, J. & Lind, M., (1981) Coping with Complexity, Risø-M-2293.

Rasmussen, J. and Lind, M. (1982) A Model of Human Decision Making in Complex Systems and its Use for Design and System Control Strategies; in Proceedings of American Control Conference, Arlington, USA.

Rasmussen, J. (1983) Skills, Rules and Knowledge; Signals, Signs and Symbols and other Distinctions in Human Performance Models; in IEEE Transactions on Systems, Man and Cybernetics - vol.SMC13 no.3.

Rasmussen, J. (1984) Strategies for State Identification and Diagnosis in Supervisory Control Tasks and Design of Computer-based Support Systems; in Advances in Man-Machine Systems Research; W.B.Rouse (ed)

Rasmussen, J. (1985) The Role of Hierarchical Knowledge Representation in Decision Making and System Management - IEEE Transactions on Systems, Man and Cybernetics, Vol. SMC-15, No. 2.

Rouse,W.B. & Hunt,R.M. (1981) A Fuzzy Rule-based Model of Human Problem Solving in Fault Diagnosis Tasks; in Proceedings of the Eighth Triennial World Congress of the International Federation of Automatic Control; Kyoto, Japan

Wahlstrøm,B. & Rasmussen,J. (1983) Nordic Cooperation in the Field of Human Factors in Nuclear Power Plants - IAEA-CN-42/247;

LIST OF PROJECT REPORTS

NKA/LIT-3(81)

101 Erik Hollnagel
Guidelines for Observations of Operator Decision Making, Risø N-27-81.
July 1981.

102 Erik Hollnagel
Inductive and Deductive Models of Decision Making as the Background for Observation and Analysis of Operator Operator Decision Making, Risø N-28-81.
July 1981.

103 Erik Hollnagel
On the Use of Generic Baseline Descriptions, Risø N-32-81.
September 1981.

104 Jens Rasmussen & Morten Lind
Coping with Complexity, Risø-M-2293.
June 1981.

105 Jens Rasmussen
Human Errors. A Taxonomy for Describing Human Malfunctions in Industrial Installations, Risø-M-2304.
August 1981.

106 Erik Hollnagel
The Methodology of Man-Machine Systems: Problems of Verification and Validation, Risø-M-2313, August 1981.

107 Erik Hollnagel
Simulator Training Analysis Directions for Using the Decision Analysis Scheme, Risø N-39-81. October 1981.

108 Erik Hollnagel
Verification and Validation in the Experimental Evaluation of New Designs for Man-Machine Systems, Risø-M-2300. July 1981.

109 Erik Hollnagel & Jens Rasmussen
Simulator Training Analysis - A Proposal for Combined Trainee Debriefing and Performance Data Collection, Risø-M-2301. August 1981.

NKA/LIT 3.2(82)

111 Goodstein, L. P.
Computer-Based Operator Aids
February 1982.
Paper presented at DESIGN 82 Conference, Birmingham, UK.

112 Rasmussen, J.
Skills, Rules and Knowledge; Signals, Signs and Symbols and Other Distinctions in Human Performance Models.
March 1982.
In IEEE Transactions on Systems, Man and Cybernetics, Vol SMC-13 no 3 1983

114 Hollnagel, E.
Report from the IEOP Pilot Study of Training Simulator Analysis Methods.
March 1982.

115 Goodstein, L. P.
An integrated Display Set for Process Operators.
March 1982.
Paper presented at IFAC/IFIP/IFORS/IEA Conference on Analysis, Design and Evaluation of Man-Machine Systems, Baden-Baden, F.R. Germany.

116 Hollnagel, E.
An Outline of a Series of Diversified Process Simulation (DIFOS) Experiments.
April 1982.

117 Lind, M.
Artificial Intelligence Techniques in Process Plant State Identification.
April 1982.
Paper presented at SAIS-82 Workshop on Artificial Intelligence - Uppsala, Sweden.

119 Lind, M.
Generic Control Tasks in Process Plant Operation.
JUNE 1982.
Paper presented at 2nd European Annual Manual Conference, Delft, Holland.

Rasmussen, J. and Lind, M.
A Model of human Decision Making in Complex Systems and Its Use for Design and System Control Strategies.
April 1982.
Risø-M-2349. Paper presented at American Control Conference, Arlington, USA.

120 Lind, M.
Multilevel Flow Modelling of Process Plant for Diagnosis and Control.
August 1982.
Paper presented at International Meeting on Thermal Nuclear Reactor Safety, Chicago, USA.

121 Højberg, K. S.
Power Plant Model for Display Experiments.
September 1982.

NKA/LIT 3.2(83)

122 Lind, M.
GNP - A Power Plant Model for Man-Machine Experiments.
March 1983 (also Risø N-23-82).

123 Lind, M.
Some Experiences in Application on the Multi-level Flow Modelling Method.
June 1983 (also Risø N-12-83).

Presented at Enlarged Halden Programme
Group Meeting, Loen, Norway and Third
European Annual Conference on Human
Decision Making and Manual Control, Risø

124 Lind, M.
A System Modelling Framework for the
Design of Integrated Process Control
Systems.
June 1983.
Presented at IASTED Conference on Applied
Control and Identification, Copenhagen,
Denmark.

125 Goodstein, L. P., Hedegaard, J.,
Højberg, K. S., and Lind, M.
The GNP Testbed for operator Support
Evaluation.
June 1983 (also Risø N-16-83)
Presented at Enlarged Halden Programme
Group Meeting, Loen, Norway and Third
European Annual Conference on Human
Decision Making an Manual Control, Risø.

126 Rasmussen, J.
Strategies for State Identification and
Diagnosis in Supervisory Control Tasks
and Design of Computer Based Support Systems.
April 1983 (also Risø N-6-83).
Published in "Advances in Man-Machine
Systems Research", Vol. 1,
W. B. Rouse (ed.) 1983.

127 Højberg, K. S.
On-Line Program for Multilevel Flow Model
Man-Machine Experiment.
August 1983 (also Risø N-19-83).

128 Højberg, K.S.
Off-Line Programs for Multilevel Flow Model
Man-Machine Experiment.
August 1983 (also Risø N-20-83).

130 Højberg, K. S. and Suusgaard, C.
Power Plant Model with Failure Extensions
for GNP Man-Machine Experiments.
December 1983 (also Risø N-26-83).

131 Goodstein, L. P.
GNP Display Processing.
December 1983 (also Risø N-27-83).

NKA/LIT-3.2(84)

132 Goodstein, L.
Functional Alarming and Information.
Retrieval (also Risø N-3-84).

133 Lind, M.
Information Interfaces for Process Plant
Diagnosis. (also Risø M-2417).

134 Goodstein, L.
GNP III Display Set Working Paper I.
(also Risø N-7-84).

135 Goodstein, L.
GNP III Display Set Working Paper II.
(also Risø N-10-84).

136 Goodstein, L.
GNP III Working Paper III.
(also Risø N-12-84).

137 Goodstein, L.
GNP III Working Paper IV.
(also Risø N-13-84).

NKA/LIT-3.3(81)

300 Forslag til eksperiment i 1982 til
"LIT3.3 Experiment med foreslagne løsninger".

NKA/LIT-3.3(82)

309 The NORS Research Simulator and the Associated Control Room at IFE, Halden.

310 Polygonpresentasjon av Prosessinformasjon.

311 Halden Man-Machine Systems Laboratory - Experimental Programme.

NKA/LIT(83)

311 Yoshumura, S. et al
Man-Machine Interface Design
using Multilevel Flow Modelling.

Reports from 100-199 can be ordered from the Library, Risø National Laboratory, DK-4000 Roskilde, Denmark.

Reports from 300-399 can be ordered from the Institutt for Energiteknikk, P.O.Box 173, N-1751 Halden, Norway.

LIT final reports:

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

These reports are available at the following organizations:

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

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