

# ***Use of computers to enhance nuclear power plant diagnosis and operator response***

*Report of a specialists meeting/workshop  
held in Manchester, United Kingdom, 15–19 July 1996*



INTERNATIONAL ATOMIC ENERGY AGENCY

IAEA

The IAEA does not normally maintain stocks of reports in this series.  
However, microfiche copies of these reports can be obtained from

INIS Clearinghouse  
International Atomic Energy Agency  
Wagramerstrasse 5  
P.O. Box 100  
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,—  
in the form of a cheque or in the form of IAEA microfiche service coupons  
which may be ordered separately from the INIS Clearinghouse.

The originating Section of this publication in the IAEA was:

Safety Assessment Section  
International Atomic Energy Agency  
Wagramer Strasse 5  
P.O. Box 100  
A-1400 Vienna, Austria

USE OF COMPUTERS TO ENHANCE  
NUCLEAR POWER PLANT DIAGNOSIS AND OPERATOR RESPONSE  
IAEA, VIENNA, 1998  
IAEA-TECDOC-1019  
ISSN 1011-4289

© IAEA, 1998

Printed by the IAEA in Austria  
May 1998

## **FOREWORD**

Over the last ten years there has been a rapid growth in the capabilities offered by computer systems to provide support to the operators of a complex plant under both normal and transient/incident conditions. In particular expert or knowledge based systems have emerged as very powerful tools for providing operators with focused and timely advice.

The nuclear power industry has been at the forefront of these developments and there have been numerous applications of these techniques within it.

Nuclear users of the technology do, however, need to approach it carefully with respect to issues such as validation, verification and human factors. In recognition of this need, the IAEA has organized a number of meetings to discuss the aforementioned considerations.

In recent years, there has been considerable progress in expert system applications within the nuclear industry using by now already well established techniques and associated mature software products. In addition, other techniques such as neural networks, genetic algorithms and hybrid systems have matured to an extent that they can be seriously applied on an industrial scale. Consequently, it is now possible for nuclear utilities to consider a much wider range of applications which represent an acceptable technical risk. However, these more advanced applications put increasing demands on areas such as validation/verification and human factors. These issues were discussed at a specialists meeting held in Manchester, United Kingdom, on 15–19 July 1996, and the main deliberations are summarized in this publication.

## *EDITORIAL NOTE*

*In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscripts as submitted by the authors. The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.*

*Throughout the text names of Member States are retained as they were when the text was compiled.*

*The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.*

*The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.*

*The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.*

# CONTENTS

INTRODUCTION .....	1
1. ADVANCED TECHNOLOGIES FOR INTELLIGENT MANAGEMENT .....	3
1.1. Artificial neural networks .....	3
1.2. Wavelets and neural networks .....	4
1.3. Fuzzy logic .....	4
1.4. Rules .....	5
1.5. Genetic algorithms .....	5
1.6. Chaotic systems .....	6
1.7. Cellular systems .....	6
1.8. Anticipatory systems .....	6
1.9. Case based reasoning .....	7
1.10. Constraint programming .....	7
1.11. Modelling .....	7
1.12. Agents .....	8
1.13. Semantic networks .....	8
2. GENERAL INFORMATION TECHNOLOGY .....	9
2.1. Object orientation .....	9
2.2. Client server technologies .....	10
2.3. Networking .....	10
2.4. Group working .....	10
2.5. Geographical information systems .....	11
2.6. Hypermedia databases .....	11
3. APPLICATION AREAS .....	11
3.1. Signal monitoring of plant maintenance .....	12
3.2. Sensor/signal verification and validation .....	14
3.3. Applications of neural networks in nuclear power plants .....	14
3.4. Emergency response (safety) .....	14
3.5. Accident and emergency support .....	14
4. PROBLEMS AND CHALLENGES .....	15
4.1. Human factors .....	15
4.1.1. Characteristics of human operators .....	15
4.1.2. Preliminary studies .....	16
4.1.3. Human reliability analysis .....	17
4.2. Safety and licensing .....	18
4.2.1. Acceptance, verification and validation .....	18
4.2.2. Acceptance by the regulator .....	19
4.2.3. V&V of AI applications .....	20
4.2.4. Possible approaches .....	20
4.3. Issues of scale-up in KBS .....	21
4.3.1. Methodology .....	22
4.3.2. Robust software tools .....	22
4.3.3. Applying KBS to 'old' and 'new' plants .....	22

5. CONCLUSIONS .....	23
BIBLIOGRAPHY .....	24
ABBREVIATIONS .....	25
PAPERS PRESENTED AT THE MEETING	
Use of on-line fuzzy-logic expert system for water chemistry .....	29
<i>J. Fandrich, W. Metzner</i>	
Intelligent and interactive computer image of a nuclear plant: The ImagIn project .....	43
<i>D. Haubensack, P. Malvache, P. Valleix</i>	
Use of computer aids including expert systems to enhance diagnosis of NPP safety status and operator response: VDU displays in accidents — Interact .....	51
<i>P. Humble, D. Welbourne</i>	
Integrated approach to knowledge acquisition and safety management of complex plants with emphasis on human factors .....	63
<i>K.T. Kosmowski</i>	
Model prototype of information support system for operator approaches and realization .....	73
<i>O.B. Samoilov, V.A. Galushkin, V.V. Drumov, A.V. Kurachenkov, S.L. Shashkin, V.M. Mordvincev</i>	
CONTRIBUTORS TO DRAFTING AND REVIEW .....	79

## INTRODUCTION

In the operation of large complex systems, mechanisms and procedures to ensure the prevention of errors are growing rapidly in significance. There are both safety related and economic pressures to eliminate hazards and periods of suboptimum performance.

There is some concern over the growing application of computer enhanced methods in building human-machine integrated complex systems. In order to ensure reliable, safe and cost effective operation, the dynamics of human-machine interactions needs to be well understood. The situation where a plant is running well without operator intervention and with little or no operator feedback is easy to visualise with the number of automated control, startup and shutdown systems now being developed. It is also easy to imagine that when such a plant goes out of control or develops problems a stressed and ill informed operator is expected to make important decisions in a situation of alarm and panic.

Relevant studies have had various focuses, such as plant-wide monitoring, verification and validation, fault diagnosis and so forth. The important role that artificial intelligence (AI) and related methods can play is to enhance the safe and profitable operation of large human-machine complex systems such as power plants, chemical plants, avionics, transport systems, refineries and manufacturing plants.

Recent catastrophic events in process industries and avionics suggest that the mechanisms demanded to tackle the problems raised by emerging technologies must come from diverse specialisms and must consider the social sciences.

Traditionally AI techniques have included expert systems and neural networks. However, there are more recently developed techniques such as anticipating systems, fuzzy control, and wavelet and cads based methods which, as yet, have not reached maturity and so lack significant applications. It is hoped that the application of these techniques will allow better prediction and control over highly non-linear complex systems and effectively address their two general characteristics, namely time critical behaviour and uncertainty.

Applying intelligent methodologies to complex large systems will enhance:

- (a) plant reliability and safety, and
- (b) the quality of the services together with cost effectiveness.

The disciplines which contribute to the development of the AI-based methods include neural network, pattern recognition, robotics, decision theory, genetic algorithms, advanced signal analysis, real-time learning, adaptive control and fuzzy systems. Fuzzy logic methods enable systems to deal with ambiguity and failures.

Artificial intelligence concepts and methods, as developed for expert systems and knowledge based systems, contribute methods for high level knowledge representation and decision making. Large complex systems typically involve multiple interacting processes and, as a consequence, require interacting knowledge based and decision support systems.

Maintaining and/or bringing a complex system to a desirable state of operation through a human-machine interface involves decision making and enactment. Sufficient information must be available in order to make decisions and this process can be seen to involve three distinct and yet related functions. These are monitoring, diagnosis and control. AI tools have been brought



to bear on each of the functions but it is in the diagnosis of information and in the decision making process that the potential is perhaps the greatest.

Expert systems or AI systems in general have technical and regulatory problems. No reliable method for verification and validation of expert systems has yet been fully developed. Expert systems can be slow as the amount of knowledge which must be used to make a decision increases. This became conspicuous when ES were performing their functions on-line or in real time. Since large complex systems are highly dynamic and have underlying time constants associated with their behaviour, it is essential that the AI system can respond and diagnose within the cycle of these time constants.

The development of time critical approaches to AI implementations is necessary if real time applications are to be practical. Time critical AI allows one to model the time constants, build a time constraint propagation model, and devise knowledge intensive search strategies.

The main problems associated with the real time control of large complex systems can be summarized as follows. At the level of software implementation, real-time control systems typically use procedure oriented algorithms. Existing knowledge representation methods and inference strategies are not suitable for representing dynamic reasoning processes in real time. At the hardware level, under the time stressed environment, a distributed structure is needed for implementation of real-time control, allowing real time reasoning in parallel. Such appropriate hardware structures should be developed and further work is required.

In recent years, neural networks and other AI techniques have gained enormous popularity. They have been developed for a wide range of applications and a variety of technological problems. Pretrained neural networks now offer substantial help as fast and robust computational models that implicitly take into account the non-linear behaviour of a system.

Their use in plant situations is mainly as signal conditioners, error detectors or data compressors. They are typically used in the development of other systems for larger applications, however, and they can also be used as classifiers or problem identifier.

In conclusion, AI tools can assist in verification and validation of both signal and sensor information about the system so that the human operator has an updated accurate global model of the process or plant at any given time. In this respect, the time critical nature of a complex process environment forms the fundamental underlying constraint in the development of intelligent methods to operate complex systems. The critical nature of operation is aggravated by the nature of continuous human-machine interaction and by the decision response characteristics of both the human operators and the semi-autonomous or advisory intelligent controllers. In these situations both human and machine have to operate/be operated in parallel.

## 1. ADVANCED TECHNOLOGIES FOR INTELLIGENT MANAGEMENT

Figure 1 shows how the technologies referenced in this report relate to one another and to AI in general. AI in the nuclear industry is characterized by a set of operational and safety constraints which are not shown.

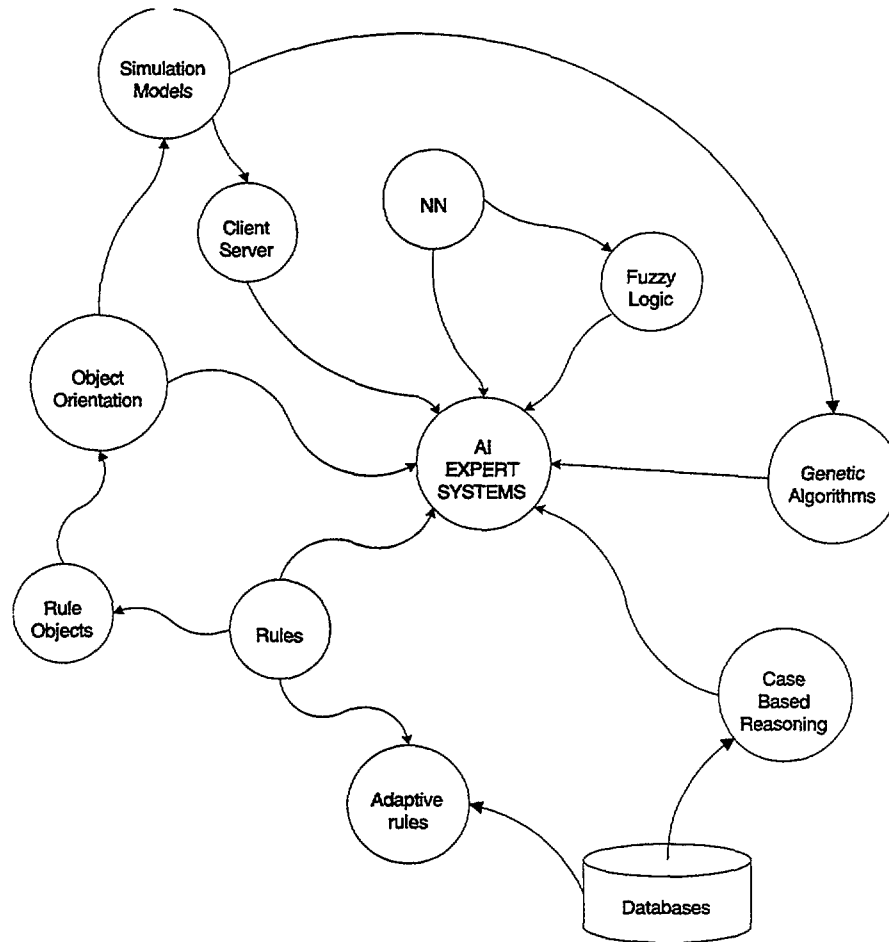


FIG. 1. An AI technology map.

To manage large, complex systems, intelligent management systems must be able to integrate monitoring, diagnostic and control functions. This integration task will provide the basis for enhancing human-machine communications where tasks are to be shared by humans and machines and are extensively executed in parallel. The goal will be to develop representative constructs which facilitate human-machine communication about mutually observed schemes. This will involve translating information perceived or interpreted from images into linguistic format, or using various types of linguistically based information to guide image interpretation. A further extension in this area will be to use linguistically based information in the form of a 'learned' grammar or to describe 'reasons' for system behaviour. The recent work in neural networks and concept graph theory will support this investigation.

### 1.1. ARTIFICIAL NEURAL NETWORKS

As an emerging technology, neural networks have received considerable attention in many disciplines. Utilization of neural networks in nuclear power plant operations is being investigated

and a number of conceptual as well as actual applications are reported in the literature. The ANN exhibit characteristics and capabilities not provided by any other AI technology. Generally, the technology developed involved three specific tasks that were undertaken using a variety of methods.

These were:

- diagnostics based on pattern recognition in time records and related representations and variables (e.g. time and frequency domain);
- feature detection based on recognition of patterns in data;
- modelling of phenomena and systems with intersection of input–output relationships.

The characteristics that make ANN systems different from traditional computing and artificial intelligence are:

- learning by example
- distributed associated memory
- fault tolerance
- pattern recognition.

A system with multiple inputs and outputs can be modelled using an ANN by applying the system inputs to the network and using the system output as the desired network responses. After an appropriate number of iterative learning cycles to limit the overall error, the ANN then constitutes a non-structured, non-algorithm model of the process involved. Such modelling can be used in physical systems. Neural computing is at an early stage of development but it is a very fast growing technology in information processing. The results to date have been impressive and they appear to complement expert systems.

## 1.2. WAVELETS AND NEURAL NETWORKS

‘Wavelets’ have proven to be a powerful tool in diverse areas as it is a versatile tool with a high mathematical content and great potential for applications. A wavelets is a ‘small’ wave used to decompose signals in the subbands in the frequency domain so that each corresponding signal component in the bands can be represented with different resolution. The method of analysis is called multi-resolution signal analysis. On the other hand, neural networks can be used as estimator and/or classifier by means of multi-input structure. In this novel signal estimation method using wavelets and neural networks, time series signal components which result from wavelet decomposition are applied to the neural network inputs. The method might potentially be extended for filtering applications, particularly for signal prediction.

## 1.3. FUZZY LOGIC

Fuzzy logic offers a convenient mathematical language for describing a system whose behaviour can be articulated in ‘if–then’ rules. It is primarily concerned with quantifying and reasoning, with the advantage that it uses natural languages in which words have ambiguous meanings.

A number of specialized software shells as well as fuzzy logic hardware are now available offering credible alternatives for rapid development of robust instrumentation and control devices. It is applied to process control, to diagnostics, in many expert system applications and in simulation, and generally offers tools well suited for non-linear and time varying systems. The main difference between fuzzy logic approaches and conventional techniques is that the former

use qualitative information whereas the latter require rigid analytical relations to describe a system. Fuzzy logic has tolerance for imprecision and therefore may offer the mathematical language of choice for the description of systems that are large, non-linear and, by the nature of their high organizational complexity, difficult to manage.

One of the examples, strongly related to fuzzy logic, is the detection and verification of disturbances, which have an impact on water chemistry in NPPs. Because of the complex behaviour of water chemistry processes, it is difficult to develop complete mathematical models. Fuzzy logic is therefore a 'natural' approach to this class of problem.

#### 1.4. RULES

Rules remain a powerful and concise way of expressing knowledge. Backward chaining rule based systems can ultimately be represented as a decision tree whose size can grow enormously and the maintainability of which becomes a major problem. Forward chaining or Demon based rules are in general better suited to object orientation (OO) approaches where the language itself supports event driven programming.

As the complexity of the problems tackled with expert systems increases, a single knowledge paradigm such as rules becomes stretched and more concise mechanisms for the representation of knowledge are required.

Interesting areas of research are in systems which develop their own rules by the observation of behaviour, i.e. how operators gain access to information, or how operating parameters interact. Earlier reports mentioned real time systems where plant personnel were allowed to enter rules concerning causal relationships on the plant. This system resulted in the re-specialization of plant engineers to knowledge engineers, the sort of specialization the system was designed to remove in the first place!

The reasons for this were attributable to three major causes:

1. Complex rule language
2. Elaborate procedures for QA checking of precise rules
3. Poor interface design.

#### 1.5. GENETIC ALGORITHMS

Genetic algorithms (GA) are a useful optimization procedure in large complex systems where it is simply not possible to identify the nature of the interrelationships or to model the processes involved.

The power of genetic algorithms derives from their simulation of nature's principle of evolution over generations of species. A population of slightly different candidates is allowed to evolve over several generations, with the fittest individuals having the best chances of survival by being used in the creation of subsequent generations. Simple operations of reproduction, crossover and mutation of populations are the essence of genetic algorithms.

In a genetic algorithm approach to optimization, a problem is formulated in such a way that any solution can be encoded in a string of binary digits. After evolving over a sufficient number of generations, the encoding process is reversed, and the optimal or near-optimal solution is identified from the binary string that survives. A population of strings is subject to reproduction

and mating to produce a new population of the same size. To avoid local minima and maxima, mutations are introduced during the making stage. Each binary has a small probability of being reversed during the genetic recombination. Studies show that population of 100 individual strings taken through 20 generations have a high probability of including optimal or near-optimal individual strings. By including a random mutation probability of about 0.001 it is adequate to prevent a search from stopping at a local optimum.

## 1.6. CHAOTIC SYSTEMS

Chaos occurs in two steps: random chaos and deterministic chaos. Random chaos has no underlying basis since it arises from a series of independent events or decisions that have no relation to the immediately preceding events or decisions. The only way to relate the state of random chaotic system over an increment of time is through the use of probabilities. Deterministic chaos has an underlying functional relationship between the different qualities involved. Although they are often handled in a statistical manner, this underlying functional relationship is non-linear. As the range of fluctuations grow, the behaviour of the deterministic chaotic system becomes erratic and less predictable. There are two types of non-linear (deterministic) chaos; the Hamiltonian chaos where there is no function (partial beams, planetary motions, etc.), and the dissipative type chaos, which applies for the systems of interest in most systems, in which the system loses energy. In this case the dissipative systems damp out the degrees of freedom, and only a few components of the behaviour remain important. The behaviour is usually determined as much by the initial conditions as it is by the underlying functional relationship, and a special pattern emerges, usually called 'limit cycle' behaviour. This results in a simplification that assists in the understanding of the chaotic system.

## 1.7. CELLULAR SYSTEMS

Cellular automata are a form of dynamic simulation that can be used for many physical, biological and sociological phenomena. In a sense, it is analogous to genetic algorithms, where phenomena are encoded, a biologically based process is imposed, and the resultant is decoded to give the ultimate result.

A graphical programme of this nature is called a cellular automation when it is parallel (independent cell updates are performed independently of each other at the same instant), local (when a cell is updated, its new colour value is based solely on the old colour values of the cell and its nearest neighbours), or homogeneous (each cell is updated according to the same rules).

## 1.8. ANTICIPATORY SYSTEMS

Anticipatory systems (AS) are systems that change state by incorporating in their control strategies information pertaining to anticipated, future states. Thus, in anticipatory control an action is taken on the basis of present conditions as well as a reliable estimate of what the system's performance may be in the near future. It appears that there may be a variety of anticipatory control strategies applicable to a given system. They all fundamentally share the need for an internal predictive model of the system and/or its environment used in a time-scale faster than real time to influence decision taken at the present.

The anticipating paradigm may be particularly well suited for the intelligent management of large complex systems. It allows to view complex systems as systems possessing a variety of descriptions (models), the appropriate one at any given time being chosen on the basis of computational efficiency. It attempts to overcome one of the most serious problems in large

complex systems, that is the lag due to both large size and complexity. One suggests that the idiom of fuzzy logic in conjunction with the mapping abilities of neural networks hold considerable promise for robust anticipatory strategies which may enhance the failure tolerance of large complex systems.

## 1.9. CASE BASED REASONING

A long sought after objective of AI systems is the automatic ability to learn from experience, case based reasoning (CBR) tools deliver easy to use mechanisms for identifying similarities between recorded events and current events. This is a pattern recognition mechanism for the prediction of solutions/outcomes.

This is a good approach where the volumes of data may be very small or there is no underlying mathematical description for the problem domain. CBR systems rely upon scoring and text matches in searches of their case data base. Each question for the system is recorded along with its symptoms and the eventual solution or outcome.

CBR tools may provide an appropriately unstructured mechanism for knowledge archiving. Data is not being encoded as rules but rather as a set of observed causes and effects. The volumes of data collected over time will hopefully reveal any erroneous or indirect causal relationships.

## 1.10. CONSTRAINT PROGRAMMING

Many problem domains do not lend themselves well to descriptions of optimum solutions. It is however relatively easy in some domains to determine what not to do. Constraint programming is such an approach. It eliminates the impossible and reduces the search space for an optimum solution. This approach is especially useful with complex systems where general or specific constraints can be identified. Uses of such an approach include detailed modelling and scheduling. British Nuclear Fuels plc (BNFL) is developing this technology in order to make substantial savings in the scheduling of decommissioning work. These application constraints are of two types, those that are fixed and time varying constraints. C++ is being used as it allows the constraints to be expressed either as a traditional set of AI rules, as a procedure, or a complex time dependent model.

## 1.11. MODELLING

The nature of modern industrial facilities, both nuclear and non-nuclear, is inherently complex. It is likely that in order to understand or to predict the consequences of their interactions with the plant, designers, operators and management each maintain cognitive models of the facility. These models vary in expressibility, detail and applicability. The scope of an individual's model is defined by their level of expertise, and the requirements of their job.

The predictive power of an appropriate model has long been recognized and operational research tools have been developed to deliver such models. However the OO paradigm and the use of NN techniques has made it more feasible to construct models of varying complexity for their predictive qualities.

BNFL Decommissioning for example have developed an OO model of the Sellafield site which describes buildings, their type and structure, their processing or storage capacity, the connections between them and the capacities of the connections. The model has recently been extended to cover the radiological profiles of facilities and their adaptation with time along with

estimations of waste volumes and types for each building. This model is then used to produce cost, manpower, dose uptake and waste arising figures for different decommissioning schedules. Future plans for the system involve the addition of constraint based reasoning where minimum dose uptake, cost and time-scale are parameters.

One of the major problems associated with model building is that of detail or data collection, which must be weighed against the amount of time the model requires to propagate a change through itself. The use of high power servers to run the model is now feasible and very complex models can be operated in usable time-scales. One approach being tried at BNFL is the identification of significant factors for each item modelled and to use NN techniques to attempt to map soft factors such as the crowdedness, or the untidiness of a facility to more quantifiable measures. For instance a small facility which has porous surfaces with a bad containment history is likely to result in many complications over a large facility with a good containment record. The collection and analysis of data for such an approach could be an ongoing process which is used to refine the assumptions the model makes.

### 1.12. AGENTS

As more and more computer systems are being tied together by a medium speed communications infrastructure (>10 Mb/s) a new type of interoperability is coming into play. Conceptualized as intelligent agents, these are autonomous programmes which have access to all networked resources. They are capable of interrogating databases, receiving commands, monitoring situations and communicating with each other.

This approach to expert systems is novel in that it frees them from one location. They are not stand alone systems which wait for users to consult them, they are not embedded within a larger plant control system but they are proactive systems capable of responding to changes in the information environment.

Currently BNFL is undertaking pilot studies focused on implementing agent technology in a distributed processing environment. This work has required an object manager framework to be developed which allows objects in a networked PC environment to be moved from machine to machine as spare processing power becomes available. The object manager development has been successful and now the project is developing agent framework classes in C++. The PCs are all running Windows 3.1 or Windows for Workgroups 3.11. An extension to the environment is planned which will allow objects to be moved to other platforms such as the DEC Alpha 3600s running OSF/1.

The potential for the approach to deal with complexity is high as agents can be duplicated/created/destroyed as required and each agent can be given a broad or specialist area of knowledge. There may be the possibility of merging modelling and agent technologies allowing intelligent agents to roam in a virtual plant environment which is fed with information from the real world. The predictive and diagnostic power of such an approach is attractive.

### 1.13. SEMANTIC NETWORKS

Semantic networks are a way to store information and knowledge using nodes which contain attributes and are connected by relationships to other nodes. In this kind of network, the meaning is contained in the links and much less in the attributes.

This representation is basically very simple and at the same time very powerful and flexible; but on the other hand, this flexibility can generate very complex networks, and various problems can arise (blocking loops, inconsistency, etc.). A very efficient way to stay strict and to assure a correct behaviour is to integrate in this representation an object orientation feature that allows objects to be created from higher level objects (classes, superclasses, etc.). Such generic frameworks are good guides and, if built correctly, they can prevent inconsistency in the system, and can also provide a real possibility of strict validation.

## **2. GENERAL INFORMATION TECHNOLOGY**

### **2.1. OBJECT ORIENTATION**

Object orientation (OO) is an increasingly popular approach to AI. Not only is it a very powerful programming paradigm but ties in well with the questions asked in knowledge acquisition and results in conceptual models which can be used as outline class designs.

- |   |                    |
|---|--------------------|
| 1. What things populate a domain?               | Classes/objects    |
| 2. How do those things behave, what do they do? | Behaviours/methods |
| 3. How do those things affect one another?      | Messages           |

There are OO shells available such as Nexpert Object, Level 5 Object, Kappa and G2, which allow developers to use this paradigm for the representation and interpretation of knowledge. The shells vary in their functionality, flexibility, representation formalisms, maintainability and user interfaces. AI shells are turning out to be restrictive for some developers, and therefore the direct use of the OO languages is becoming increasingly popular.

This has many advantages in the development of AI applications, C++ can deliver a high degree of reuse, it provides excellent encapsulation/modularization and it translates between hardware platforms very well.

The occasional user is unlikely to see all of these benefits. However, organizations which have moved to an object oriented approach soon develop a set of classes which allow systems to be built quickly.

This approach raises issues of verification and validation. OO systems tend to display a behaviour which is combinatorial in nature. As objects interact, it is impossible for one object to 'know' what the effect of its actions are. The use of private and protected functions can limit this, but a holistic approach to the testing of OO systems is bound to be difficult. Another approach is to test the classes in isolation. This relies upon an appropriate class design which well partitions the knowledge domain. This is very much the preferred approach as it reduces the complexity of the testing. It also means that a partial test may be all that is required if the only changes made to a system are in a single class.

System behaviour in the above example is defined by the behaviour of individual objects and the interaction between classes. The experts of the verifying group are thus in a better position to conceptualize an overall model.

It is now possible to purchase C++ classes for the rapid development of an interface, e.g. Microsoft's MFC, but more importantly third party vendors support more complex system functions such as geographical information systems, complex graphing, scheduling as well as



classes for the generation of neural networks, genetic algorithms and the resolution of complex constraint based reasoning.

It has always been recognized that no single representation of knowledge would suffice for all application areas and that integration of knowledge paradigms was an important capability. It would appear that at present the expanding use of C++ is the best mechanism for the integration of different AI techniques.

## 2.2. CLIENT SERVER TECHNOLOGIES

The use of centralized servers and remote clients in order to ensure synchronization of data, and move computer intensive tasks to more appropriate hardware, is now common. The next challenge is to use the technical infrastructure in order to deliver better AI systems. The use of object orientation, or some similar approach, will allow the distribution of a single computing task across network resources and the construction of an AI system architecture which can operate in this way will avoid many of the complexity and speed/performance problems which have hindered the real time application of expert systems.

## 2.3. NETWORKING

Early advisory expert systems were able to operate off line, that is on a stand alone hardware platform. Traditional real time expert systems received their data from the plant instruments either directly, or by using the data streams for the plant control & monitoring computers.

The use of general purpose networking for the interconnection of computer systems was not widespread in a plant environment. The situation is changing and wireless/non-electrical very high speed networks are now available. These networks are capable of transmitting instrumentation data, computer data and video data across an organization, and they have changed the relationship between real-time and off-line expert systems.

## 2.4. GROUP WORKING

As outlined in the introduction to this TECDOC, an element of social science should be brought into the design of human machine systems. Group working is a set of concepts gaining favour in the general IT community. Historically the focus of large IT departments was on either plant or corporate systems. There was in parallel to this a development of systems, known as groupware, designed to increase personal productivity, including spreadsheets, word processors, graphing tools and expert systems.

Economic pressures are now forcing organizations to look at their business processes and the mechanisms which support them. The result of this is that businesses require an IT infrastructure which facilitates organizational change. It is no longer permissible to have a dichotomy in the application of computing; systems must contribute to the business processes and business processes are people working in groups. Groupware therefore is a mapping between individuals and the processes to which they contribute.

It is currently difficult to see how this approach will be specifically applicable to AI in the nuclear industry. However, it could be an appropriate technique for the delivery of multimedia operator support systems or for the production of safety procedures, as they can be electronically joint authored, approved and distributed, and it can be used to implement complex procedures

where the flow of information and the level of notification requires changes in the data being recorded.

## 2.5. GEOGRAPHICAL INFORMATION SYSTEMS

Much information is best associated with its place or origin, so it is appropriate to see demographic charts overlaid on a map of the region from which the data is taken. This is an increasingly popular class of IT systems which can be of real use in the nuclear industry. BNFL is using GIS components in their Strategic Planning Systems, allowing users access to multimedia data in the form of numeric information, text and pictures by simply pointing to the thing they want to know about. It is being used as the front end to the physical model of the site to be decommissioned. It allows plants and their interconnections to be simply displayed and the information concerning them to be readily entered.

One other potential use of GIS is in the planning of emergency response. AI systems can interact with the components of the map, give attributes and behaviours to map objects, and then intelligent systems can make decisions or give recommendations concerning the speed of response for the requisite emergency service.

## 2.6. HYPERMEDIA DATABASES

Hypermedia is an approach to information management in which information is organized as the network of nodes connected by links. Nodes may contain text, graphic, audio, video and general software for operating on numerical and/or symbolic data. The essence of hypermedia is that linking is machine supported. At the development level most hypermedia environments feature control bottoms (link icons) which can be arbitrarily embedded within the content material by user. Hypermedia allows for easy and intuitive access to documents and programs by linking dispersed yet integral information throughout the document, a program or a series of documents/programs. Hypermedia is non sequential, i.e., there is no simple order that determines the sequence in which text is to be read, which sometimes leads to user disorientation (in the process of moving through hypermedia information) and even confusion. Navigational tools need to be further developed.

## 3. APPLICATION AREAS

Within the nuclear industry, as in other process industries, it is in the area of operator support that many expert system applications are being developed. It is the aim of these systems to:

- reduce cognitive load
- maintain awareness of the plant
- provide appropriate information and assistance at all times.

For the foreseeable future the operator will remain the key decision making component in complex human-machine systems. The non linear and often counterintuitive behaviour of such systems makes their control and optimization a difficult process. Figure 2 shows the inputs to a typical plant operator, and makes explicit the operators' use of their own model of the plant. This is constructed over time by their experience, training, interaction with other operators and knowledge of procedures. The quality of a person's predictive model, and his or her ability to transfer that into decisions and actions, is the distinction between a good and an indifferent operator.

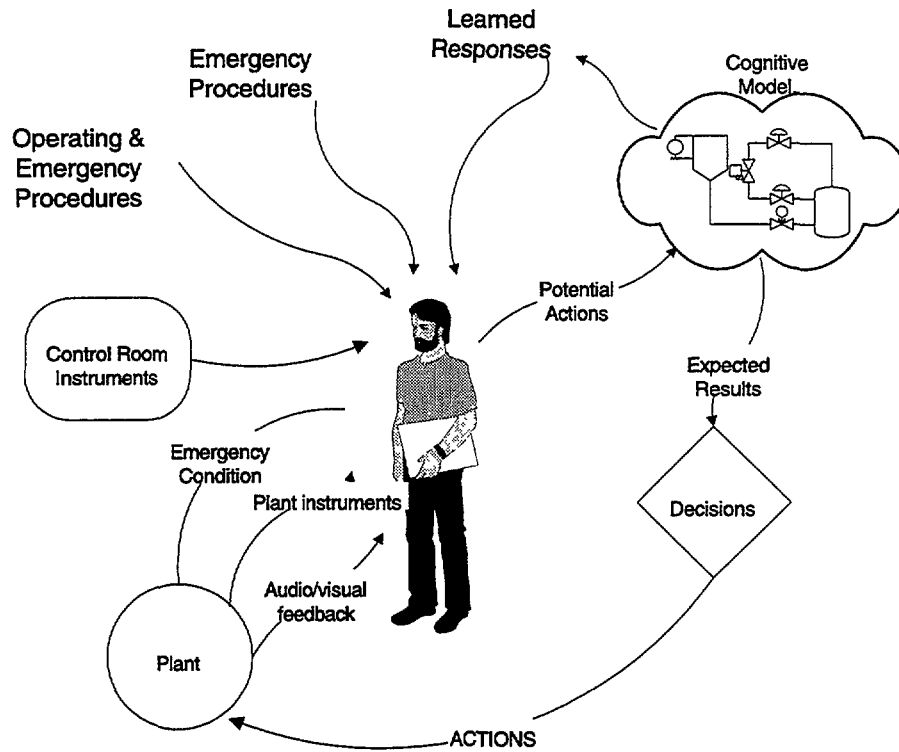


FIG. 2. The role of the operator in the control room.

The significance and quantity of information with which the operator is expected to deal with can vary greatly. When the process is under control there is a danger of under-stimulation; when an unexpected event occurs there may be too much information for effective and safe decision making.

Figure 3 shows in more detail the relationship between operator, plant and automatic and manual control/safety systems. The diagram also shows how AI tools have been and may be applied.

Real time modelling tools and techniques gives the AI practitioner the ability to build components which hold a demonstrable dynamic view of the plant or process. This recognizes a key ability in good decision makers and presents an exciting challenge to developers for the further automation of decision making behaviour.

### 3.1. SIGNAL MONITORING OF PLANT MAINTENANCE

Reliability of safety equipment in power plants is an important issue in operation. The role of maintenance in increasing nuclear power plant reliability and availability is an important concern for nuclear utilities. An effective maintenance procedure for this purpose is reliability centred maintenance (RCM), which is based on systems and/or subsystems reliability considerations. RCM is a systematic approach for developing a maintenance strategy (equipment, interval, etc.) which takes into account system safety, its ability to function as desired, and economics so that the design reliability of the system is satisfied (or even improved). Equipment reliability and mean-time between failures can be quantified.

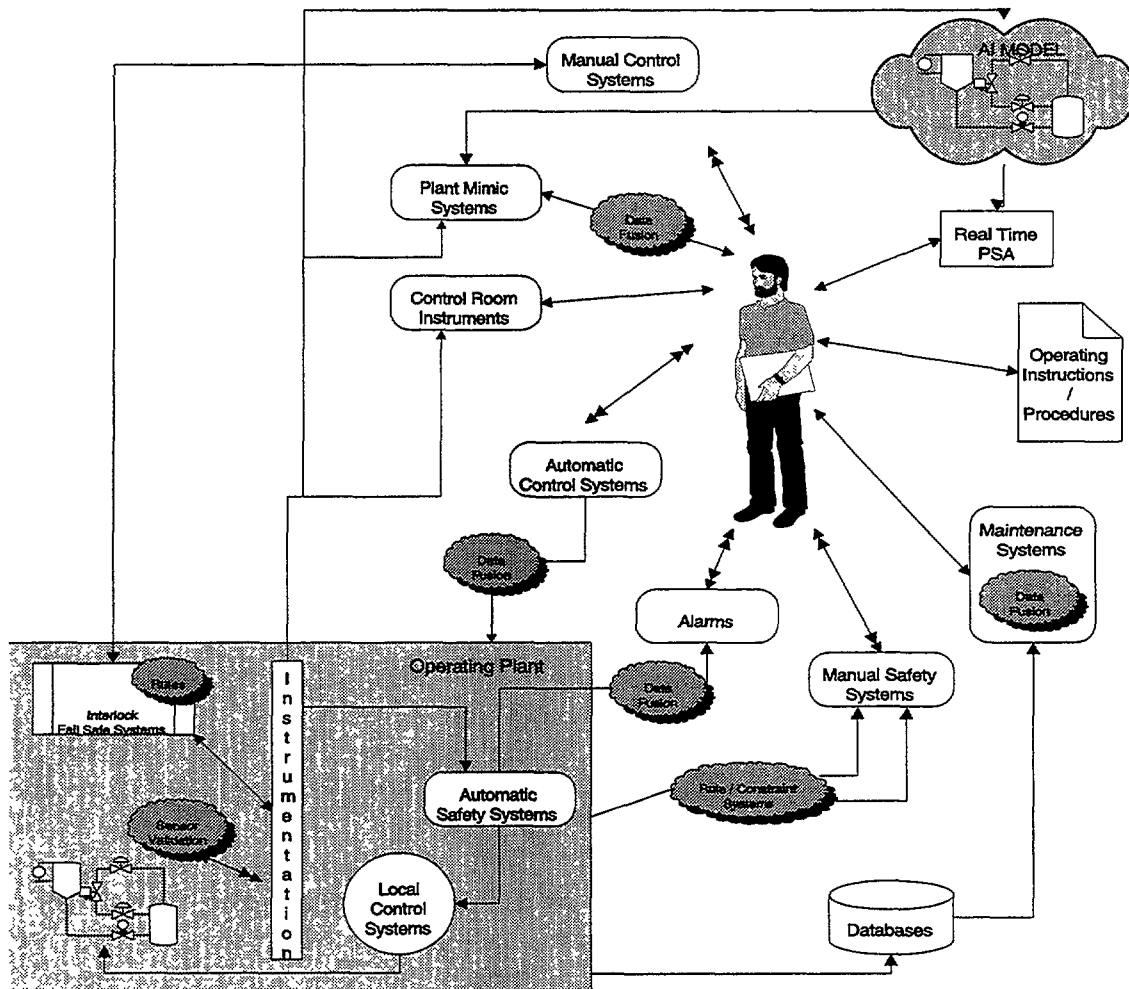


FIG. 3. AI tools in a complex human-machine system.

Referring to the RCM program as a systematic approach for the implementation of an effective preventive maintenance programme, with the developments in the computer technology in the last decade, the on-line real-time monitoring and fault detection and identification (FDI) should be integrated in this maintenance scheme as a part of preventive maintenance programme. By these means, system reliability, safety and availability are enhanced. The integration of the preventive maintenance (PVM) task selection into RCM is accomplished together with the PVM task selection.

Making use of the advancement in computer technology, real-time monitoring and fault detection for preventive maintenance can be carried out by means of modern workstation and/or enhanced single-user based computers known as WS and PC. By means of real-time plant surveillance methods, predictive maintenance is exercised through the plant in the form of:

- continuous monitoring of component conditions and plant operation by diagnostic monitors and sensors;
- use of on-line analysis tools that utilize updated plant data, equipment records and databases;
- automated assessment of components' remaining life, wear and tear and specification of different operational condition limits.

Processing sensory information is the essential task of control and instrumentation in power plant operation. Processing of this information can be accomplished on different levels. Modern signal analysis technology uses real-time computer systems with advanced signal processing algorithms with optimal estimations. Added to this, AI-based technologies can also be utilized. Among these, expert systems and neural networks are the outstanding technologies, but are not yet mature enough to be used in critical situations such as emergency/accident cases.

### 3.2. SENSOR/SIGNAL VERIFICATION AND VALIDATION

Safe, reliable and cost effective operation of a plant is mainly dependent on the quality of signals obtained from the sensors and/or measuring instrumentation where, after the initial phase of data and single processing, the information processing systems pave the way for optimal decisions. In this respect, before the sensory information is used in major time critical functions, i.e., monitoring, diagnostics and control, it has to be verified and validated. Although verification and validation (V&V) is a rather comprehensive concept, in simple terms verification is to provide confidence in the resulting information processing subject to the recognition of the plant's operational conditions. Validation is to provide confidence in that the implemented techniques and methods are right to perform the independent function. The terminology implies that verification provides confirmation to the design, on one hand, and validation provides confirmation to the specifications and the requirements, on the other. The reliability of the verification and validation method is enhanced by the implementation of the concept of redundancy together with diversity in this process so that the monitoring basically serves for obtaining confidence in the integrity of the sensory information.

There are several approaches to the design of instrumentation systems to ensure their reliability in spite of eventual sensor failures. Instrumentation failure detection (IFD) or, with inclusion of redundant sensors, instrumentation failure detection and isolation (IFDI) are known as hardware redundancy. Another sensor failure detection method is known as functional or analytical redundancy known as Kalman filtering methodology. It is extensively used in time recursive algorithm for prediction and estimating non-measurable state variables.

### 3.3. APPLICATIONS OF NEURAL NETWORKS IN NUCLEAR POWER PLANTS

The following section outlines actual implementations of NNs in the global nuclear industry. It is categorized into five application areas, and example applications are given in each.

### 3.4. EMERGENCY RESPONSE (SAFETY)

Intelligent agents, combined with a plant model which was fed in real time from plant monitoring instruments, could be used to demonstrate safe or 'lowest dose' evacuation routes in the event of a radiological incident.

### 3.5. ACCIDENT AND EMERGENCY SUPPORT

The safety of nuclear power plants is elaborated and analysed in various reports such as Final Safety Analysis Reports (FSAR), Probabilistic Safety or Risk Assessment (PSA/PRA) and extensive generic studies on reactor risk and on safety issues. There is a challenge for the nuclear community today in making the insights from these studies useful especially for accident management. An advisory computer programme can be used to monitor and analyse an ongoing incident in a nuclear power plant. An example is the Accident and Incident Management Support (AIMS) program, developed for the United States Nuclear Regulatory Commission, which focuses on processing a set of data as transmitted from a nuclear power plant to an operational team during the incident.

TABLE I. A CATEGORIZATION OF NEURAL NETWORK APPLICATIONS IN THE NUCLEAR INDUSTRY

APPLICATION AREA	EXAMPLE APPLICATIONS
Monitoring of NPP sensors and systems	<ul style="list-style-type: none"> <li>•Sensor validation</li> <li>•Plant-wide monitoring</li> <li>•Loose parts monitoring</li> </ul>
Monitoring of thermodynamic behaviour	<ul style="list-style-type: none"> <li>•Monitoring of performance and efficiency</li> <li>•On line thermal margins (DNBR) estimation</li> </ul>
Diagnosis of NPP transients	<ul style="list-style-type: none"> <li>•Training on simulation transients</li> <li>•Prediction of plant parameters</li> <li>•Identification of abnormal events</li> <li>•Severe accident management</li> <li>•Hybrid neural and fuzzy systems for transient identification</li> </ul>
Neural control systems	<ul style="list-style-type: none"> <li>•NN for adapting power plant control for wide range operation</li> <li>•Normal control during PWR startup</li> <li>•Adaptive control as diagnosis</li> </ul>
Diagnostics	<ul style="list-style-type: none"> <li>•Machine fault diagnosis</li> <li>•Bearing fault diagnosis using vibration sensors</li> <li>•Core vibrations to detect interference</li> </ul>
Virtual instrumentation	<ul style="list-style-type: none"> <li>•Fuzzy and neural systems for virtual instrumentation</li> </ul>

## 4. PROBLEMS AND CHALLENGES

### 4.1. HUMAN FACTORS

#### 4.1.1. Characteristics of human operators

In designing and implementing computer aids, including expert systems, to enhance diagnosis of nuclear power plant status and operator response it is important to consider the human and computer factors of the control room 'system', i.e. the relationship between the operator, control and protection systems, and computer aids in different states of the plant. To achieve the correct balance between computer and human actions, the design process must consider each control room activity as a human task, a computer task, or a task requiring a combination of human and computer solutions. The process of assigning control room activities is known in the ergonomics literature as the 'task analysis' and 'allocation of functions'.

There are many factors influencing human performance. Different groups of factors can be distinguished, e.g. cognitive, physiological and organizational. The analysts and designers of the computer system should consider the influence of more important factors on human performance in abnormal and emergency situations.

Generally, functions allocated to the computer are those functions that exceed the capacity of humans, including the processing of large quantities of data, and tasks requiring high accuracy or repeatability of performance. Functions that require heuristic or inferential knowledge, flexibility, etc., will need human involvement. In addition, there may be practical or technical constraints that make a computer solution impractical, and thus require human operation. Human flexibility and judgement are essential for extreme fault or accident situations. Under these conditions, the extraordinary nature of the task makes the specification of computer solutions very difficult or impossible.

To develop computer aids for operations staff, it is essential to understand the mental process of the operators working in the control room. The distinction of three categories of human behaviour was proposed by Rasmussen. His conceptual framework assumes three cognitive levels of human behaviour:

- skill-based, i.e. highly practised tasks that can be performed as more or less subconscious routines governed by stored patterns of behaviour;
- rule-based, i.e. performance of less familiar tasks in which a person follows remembered or written rules;
- knowledge-based, i.e. performance of novel actions when familiar patterns and rules cannot be applied directly, and actions follow the information processing with the inclusion of diagnosis, planning, and decision making.

Generally, when operators detect abnormal situations, a simple, timely response will initiate a set of automatic actions to restore the plant to its normal state. This can be referred to as **skill-based control**. If the situation is more complex, the operators have to assure themselves of the status of the equipment by validating the signals, and follow the operating procedures to restore the plant. In such situation the performance of operators can be referred to as **rule-based control**. However, if the situation is complex and not obvious from monitoring, e.g. due to multiple failures including faulty sensors, the operators will have to evaluate the whole plant status, predict the possible next state of the plant, and define tasks to achieve restoration. Such complexity of actions is referred to as **knowledge-based behaviour**.

Given the information flow in a control room is known different modules of computer aids may be developed according to the need of operators in the different modes of their control functions.

#### 4.1.2. Preliminary studies

It is important to involve the end user during the overall design process of expert system and computer aids to the operator.

This implies that the knowledge based system will be useful for the operators in their activity ('utility' criteria), and also that the human-machine interface (HMI) makes the system accessible to the users ('accessibility' criteria).

For example, these points require attention during preliminary studies:

- The consistency of the knowledge based HMI and the other systems' HMI when they are used together, e.g., in control room.
- Design process must involve designers, users and human factors specialists in order to identify the needs and requirements for the system.

- At the beginning of the project, some task analysis has to be carried out on existing systems to collect the data about the behaviour of the operator; this data is necessary for designing new system:
  - what kind of help to give the users;
  - which are the goals and tasks of the operator, and what are the tasks and activities he or she effectively performs in real situation to achieve these goals;
  - this implies collecting data about different levels, especially cognitive and organizational aspects;
  - for which users (operators, supervisors, managers)
  - needs of the users: information to present about the process, about the system itself, alarms, data entries, navigation in the software, etc.;
  - the context: environment, time constraints, performance, viability required.

It is important to get a precise knowledge of what the operator really does in some work situations where he or she uses some heuristics, some specific 'ways of use' which are not prescribed but which permit the user to operate with best performances, or at a low cost for him. The operator must be able to apply these ways of use with the new system.

Knowledge based systems may have some impact on operators (performance, competence, mental load, decision making process, etc.), and also on the team organization (co-ordination, co-operation, etc.).

The task analysis involves necessarily the users: different methods are available including interviews, observations of users in real or simulated work environments, questionnaires, incident analysis, etc. It has to take into account the different working situations concerned: normal operation, transients, etc.

This analysis has to be done at the first step of the design process. If required for some particular aspects, some more analysis can be performed later.

Care needs to be taken to involve the real end user in the design process, and to place these operators in situation where it is possible for them to give appropriate information about their work.

Data collected during this analysis constitute some basis for identifying requirements, especially for the HMI. Data also provide some basis for the allocation of functions between human and machine, in order to decide which tasks have to be performed by the operator.

The impacts of the future system on the existing situation of work have to be analysed and evaluated at an early stage of the project. The differences between the existing system and the proposed one will most probably have some impact on the task of the user, but it is also important to take into account the impact on the organization: co-ordination with other members of the team, with management, etc.

#### **4.1.3. Human reliability analysis**

For the assessment of the allocation of functions between control systems and human operators, it can be useful to carry out human reliability analysis (HRA). Human reliability analysis is often performed in the context of probabilistic safety analysis (PSA). Human reliability is understood as a quality of human performance interacting within a complex system. There are several methods/ techniques useful for the evaluation of the human reliability.



## 4.2. SAFETY AND LICENSING

### 4.2.1. Acceptance, verification and validation

The issue of verification and validation (V&V) for all complex safety critical systems, such as in avionics or the nuclear industry is a persistent problem. V&V is a formal aspect of acceptability at the other end are issues of usability and working practice. In the case of the nuclear industry there are three groups for which acceptance is an issue. These are:

- |                               |  |
|-------------------------------|--|
| 1. The regulatory authorities | This group is mainly concerned with demonstrating compliance to existing regulations and procedures, The aspects of V&V and Safety are critical to acceptance by this group. |
| 2. The plant owners           | This group is also concerned with safety but in addition they are aware of requirements to achieve competitive advantage through optimum performance.                        |
| 3. The plant operators        | This group will be required to interact with AI systems on a daily basis and it is usability as well as safety and performance issues which concern them.                    |

In view of the very wide nature of AI as a science and the amenability of different approaches to external evaluation, it is likely that acceptability for some systems will be easier to achieve than for others.

In general, acceptance by the regulatory authorities of AI technology will always lag development. The authorities are conservative in nature, and the scope and diversity of AI tools and techniques is increasing, as is the difficulty in proving their operation, or even the applicability of one technique over another. This situation can be made worse by the introduction of autonomous AI components and systems utilizing chaos theories; a place for such developments within the nuclear industry remains to be proven.

As can be seen from the brief coverage afforded to each of the technologies in this report, AI is a wide and multispecialized area. As technologies are developed there is an increasing trend to view them as separate entities; an approach that may benefit the technology but is likely to hinder its application and integration.

Whilst the intelligent control of large scale complex systems is an issue for the more distant future, AI methods and related tools are essential intelligent aids in nuclear plant operation. They can provide considerable help in decision making for human-machine systems in real time operating conditions. The critical nature of a nuclear power plant environment forms a fundamental underlying constraint in the development of intelligent methods to operate it. An important feature of NPPs is that they are dynamic; that is, the operating environment changes without the operator's intervention. Safety critical operation is aggravated by the characteristics of both human operators and the semi-autonomous or advisory intelligent controllers. This generates the requirement for systems which are also capable of dealing with a large dynamic range or operating conditions and which respond appropriately.

It is hoped that the amalgamation of real time modelling and AI systems supported by powerful distributed processing architectures will have the power not just to advise, monitor or diagnose, but to predict. This will give tremendous benefit to NPP operators in emergency situations or as training tools where actions can be rehearsed and optimum solutions sought.

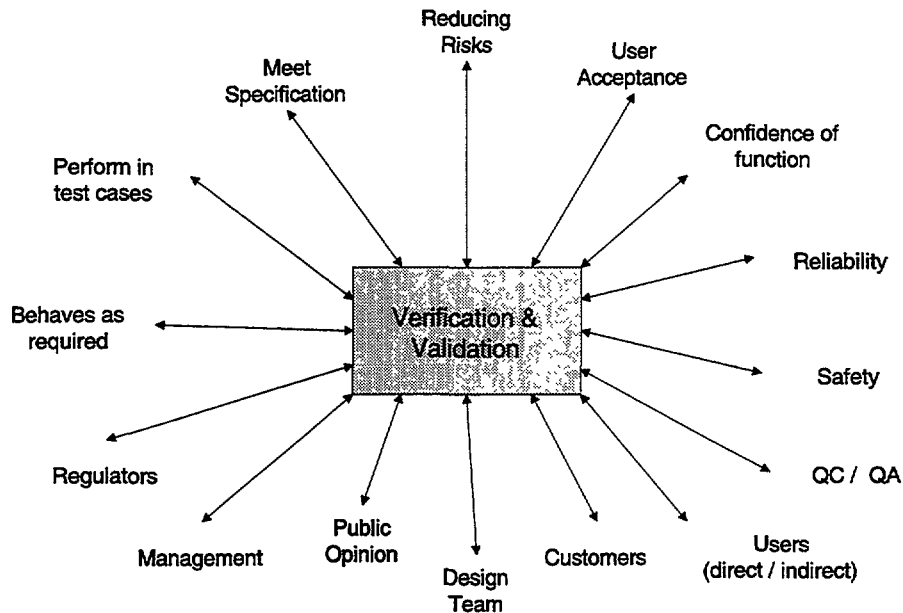


FIG. 4. Factors influencing the acceptance of AI in the nuclear industry, and the groups for whom acceptance is an issue.

Although validation of such a complex system is, in an absolute sense, a difficult task and will not be achieved in the near future, this does not mean that AI is currently unusable in a NPP environment. Applications and prototypes have consistently shown that AI tools and methods can yield increased safety and reliability in plant operation. By their application to sub-systems V&V is simplified and consequently the NPP system's safety is enhanced.

#### 4.2.2. Acceptance by the regulator

The complex nature of the processes in expert systems is such that it will be some time in the future before an acceptable case is made for their use in safety critical applications. The use of expert systems in safety related roles will require justification in the form of a safety case. Some of the components which the regulator is likely to seek assurance on before making a regulatory decision are:

- What is the role of the system?
- What reliance or integrity is required of the system?
- Is this the single source of information/advice available to the operator?
- If the proposed system is ill-conceived, specified or implemented, what are the implications if the operator acts on the advice presented?
- Is any numerical claim made on the integrity of the system?
- If so, how are these claims justified?

When the designer has addressed these initial questions, the V&V and QA aspects must be addressed at a level consistent with the regulatory requirements. The designer of a safety-related application of an AI or KBS should be aware of the importance of establishing principles of V&V and of regulatory acceptance early in the design process. Without this awareness, design methods and documentation may not be prepared or may not be available in a suitable form. The regulator will normally require clear evidence that:

- the system has established and defined requirements;
- suitable QA has been applied;
- there has been appropriate V&V of the system;
- the requirements are, where possible, traced to the documentation and the testing done on the final system.

The regulator generally requires this evidence in the form of a safety report, which should be provided in a preliminary and in a final form, with suitable revisions when changes are made in service.

#### **4.2.3. V&V of AI applications**

The use of AI and of KBS is still not fully developed, and the technology is not yet fully mature. Therefore, it is unlikely that a safety regulator would accept such a system for safety system application. There are, however, many potential applications where safety may be improved or enhanced by the use of AI and KBS.

Possible applications which have been developed in some countries are:

- alarm display with alarm processing logic;
- specialized plant monitoring applications such as detection and location of loose parts, chemical monitoring and diagnosis, and detection of barrel vibration in the reactor core;
- accident monitoring and methods of determining the characteristics of an accident.

A problem arises where a commercial software system is used to develop and operate the knowledge base, in whatever form it is held. The regulator and the user will require suitable evidence that the software is of proven quality in service, or that it has been developed under suitable discipline with well-defined documents, V&V and testing.

Established and defined requirements are needed for any computer based system, if defects and faults in the system are to be properly controlled. The requirements for an AI system may have two components: those of the commercial software package used, and those of the application. Evidence of suitable QA will be needed both for the commercial package and its development, and for the AI application information, rules, etc.

The demonstration that the requirements of the application are implemented and can be traced may be gained by some V&V methods. Some commercial tools exist to assist this process. Sufficient confidence that the requirements are implemented may be reached by suitable validation of the final implementation.

#### **4.2.4. Possible approaches**

Some approaches to presenting evidence of the integrity of an AI or KBS could be as follows:

- (a) The information in the KB must be traceable to a source in the design documents or the knowledge of an expert. This may be done by drawing and document references, and possibly by reference to the experts concerned, using a Traceability Matrix.
- (b) The information in the KB must be able to be preserved and placed under configuration management. Preferably it should be preserved in magnetic form with the ability to print it and record information such as level, date, originator, etc.

- (c) Learning systems, such as neural nets, must be able to have their learnt state recorded and controlled, similarly to (a).
- (d) Information and advice presented to operators must be able to be recorded for analysis after any adverse experience report, and correlated with the state of the AI system at that time.
- (e) The verification steps of the information held in the AI or KB system should be defined before the information is assembled, and the steps should be controlled by a suitable QA system, with inclusion of signatures for completion of verification of each step.
- (f) Validation may be an ongoing process, or an open ended process for a KB or learning system, and therefore, may not be totally possible to achieve. Some method of validation of the performance of the software functions should be done. Standard logic or knowledge could be placed in the system and the performance checked and recorded.
- (g) Validation of standard logic modules could be done comprehensively in the design offices or the factory, and the verification of that these functions had then been configured for specific logic could then be done later.
- (h) Validation of application knowledge may be possible by direct injection of plant states in some systems, or by simulated injection of states in others. Simulated injection will need support by a method of showing that the injected states are correctly simulated.

#### 4.3. ISSUES OF SCALE-UP IN KBS

Many KBS applications have been developed using a rapid prototyping technique. This approach typically involves a single knowledge engineer building a system directly from information supplied by a domain expert, i.e., without an explicit design stage. A key advantage is that the end users or experts can quickly see how the system is developing and whether it is meeting their requirements. User feedback is used to drive further cycles of development until eventually a system is produced which fulfils user needs in terms of functionality and performance.

While rapid prototyping has been successfully used for a number of mainly small scale KBS applications, it may not be appropriate for larger applications. The reasons for this include:

- As the size of (number of inputs) of the problem increases, there may be an exponential increase in the problem complexity and knowledge (rule or rule equivalents) required to handle it.
- More human resources may be required to meet the project time constraints, and these resources must work effectively together.
- The project will be more difficult to plan and to cost.
- Maintenance of the system will be more difficult without a set of formal requirements.

In addition:

- The capacity of the hardware or software tools used may be exceeded.
- Real-time performance may no longer be achieved.
- Recommendations should be established for effective scale-up.

In order to overcome the problems outlined above, a general purpose method is required to assist knowledge engineers to manage and control the development of KBS applications, supported by KBS development tools which can handle the problems associated with larger applications.

#### **4.3.1. Methodology**

A standard approach to building KBSs, using accepted notations and conventions, should enable knowledge engineers to work effectively together on larger applications. The method should ideally:

- provide a general purpose framework, which is configurable for different problem tasks;
- provide support to the full project life-cycle, from initial application selection through analysis, design and implementation;
- include some support for iterative development;
- be easily integrated with other, more conventional methodologies;
- be teachable;
- be widely accepted;
- have tool support with links to existing development environments.

#### **4.3.2. Robust software tools**

The following functionality is required within KBS development environments which are targeted at larger applications.

- a means of inspecting the knowledge within the system;
- support validation and verification;
- support for debugging applications;
- support to partition/modularise applications so that they can be constructed (and reused) in manageable chunks;
- for real-time applications, a means of focusing knowledge in response to events; only a small proportion of the knowledge base should be active at any one time during ‘normal’ operation;
- for real-time applications, a means of prioritising activities within the knowledge base.

For real-time KBS applications, guaranteed response times cannot be achieved using existing commercial tools, although this may not be a problem if the system is designed to act in a purely advisory role, with ‘read-only’ access to plant information. KBS are not currently recommended for closed-loop operation in safety related situations.

#### **4.3.3. Applying KBS to ‘old’ and ‘new’ plants**

The problems associated with scale-up are equally relevant when attempting to apply KBS to old, established plants, or when the KBS is being developed/deployed during a plant commissioning phase (or soon thereafter). However, it is usually found that:

- New plants have up-to-date information on plant design/operation which can be more easily accessed. There may also be more opportunities for KBS developers to influence the design of, for example, plant control systems to expand the potential operational scope of a KBS. Access to personnel can be a problem however, especially during the commissioning phase itself.
- Old plants suffer from a loss of design/operational information as time passes. This is particularly true of smaller changes, which may not be adequately recorded and stored.

## 5. CONCLUSIONS

AI methods and related tools can be essential intelligent aids in NPP operation. Essentially, these methods and tools have three major functional tasks: monitoring, diagnostics and control. In each part of these tasks, AI tools provide high level of automation as well as operational and/or diagnostic information. They can provide considerable help in forming decisions in human-machine interface systems in real time operating conditions. This is important because an important feature of NPP is that they are dynamic, that is, the operating environment changes without the operator's intervention.

The critical nature of the working environment of a nuclear power plant forms the fundamental underlying constraint in the development of intelligent methods to operate the plant. The appropriate V&V and QA for all systems, including AI based solutions, and their component parts, is essential. In each of these systems, the critical nature of operations is exacerbated by the nature of continuous human-machine interactions, and by the decision-response characteristics of both human operators and the semi-autonomous or advisory intelligent controllers. As a result of these concerted actions, safety and reliability of the plant can be further improved.

Although validation of a complex system is, in the absolute sense, a difficult task, the efforts yielding increased safety and reliability in plant operation by subsystem V&V procedures supported by AI based methodologies would consequently enhance the NPP system's safety.

The complex nature of the processing within expert systems is such that it will be some time in the future before a case can be made for their use in safety *critical* applications. The specification, design and use of KBS in safety *related* roles must be consistent with the safety requirements for such application.

It is recommended that end users are involved from the outset of the project to ensure that they own the system, and are fully aware of the system's capabilities at all stages. Ergonomic issues of the implementation are crucial to the acceptance of the system.

## BIBLIOGRAPHY

- CIFTCIOGLU, Ö., TÜRKCAN, E., Sensor Failure Detection in Dynamics Systems by Kalman Filtering Methodology, ECN-RX-91-025, Netherlands (1991).
- CIFTCIOGLU, Ö., TÜRKCAN, E., Sensor Signal Monitoring and Plant Maintenance, ECN-RX-93-121, Netherlands (1993).
- CIFTCIOGLU, Ö., Intelligent Management of Large Complex Systems, Real-Time Computing, NATO ASZ Series F Vol. 127 (1994) Springer Verlag (Wolfgang A. Halang and A.D. Stoyenko, Eds).
- CIFTCIOGLU, Ö., TÜRKCAN, E., 'Wavelets' Understands Neural Networks, ECN-RX-94-31, Netherlands (1994).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Expert Systems in Nuclear Safety, IAEA-TECDOC-542, Vienna (1990).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Expert Systems in the Nuclear Industry, IAEA-TECDOC-660, Vienna (1992).
- INTERNATIONAL ATOMIC ENERGY AGENCY, The Potential of Knowledge Based Systems in Nuclear Installations, IAEA-TECDOC-700, Vienna (1993).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Current Practices and Future Trends in Expert System Developments for Use in the Nuclear Industry, IAEA-TECDOC-769, Vienna (1994).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, Vienna (1995).
- MALLAT, S., A Theory for Multi-resolution Signal Decomposition the Wavelet Representation, IEEE Trans. Pattern Anal. and Machine Intelligence **31** (1989) 679-693.
- MILLER, L., GROUNDWATER, E., MISRSKY, S., Development of Guidelines for the Validation and Verification of Expert Systems, Trans. 19th Reactor Safety Instrumentation Meeting, NUREG/CP-O119, Washington, DC (1992).
- NATO ASI, Verification and Validation of Complex Systems: Human Factors Issues, (John A. Wise, V. David Hopkin and Paul Stager, Eds), NATO ASI Series F: Computer and System Sciences **110**, Springer-Verlag, Berlin (1992).
- NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Final Report, NUREG-1150, Washington, DC (1990).
- UHRIG, E.R., "Artificial Neural Networks and Potential Applications to Nuclear Power Plants", Conference on Structural Mechanics in Reactor Technology, held in Konstanz, Germany, August 23-25, 1993, University of Stuttgart (1993).
- YAGER, R.E., ZADEH, L.A. (Eds), Fuzzy Sets, Neural Networks and Soft Computing, Van Nostrand Reinhold, New York (1994).
- ZADEH, L.A., Outline of New Approach to the Analysis of Complex Systems and Decision Process, IEEE Trans. Syst. Man Cybernet. SMC-3 (1973) 2844.

## ABBREVIATIONS

AI	artificial intelligence
AIMS	accident and incident management support
ANN	artificial neural networks
AS	anticipatory systems
C++	computer language used in AI
CBR	case based reasoning
ERDS	emergency response data systems
ES	expert systems
FDI	fault detection and identification
FSAR	final safety analysis report
GA	genetic algorithms
GIS	graphical information systems
GUI	graphical user interface
HMI	human-machine interface
HRA	human reliability analysis
IFD	instrumentation failure detection
IFDI	instrumentation failure detection and isolation
IT	information technology
KBS	knowledge based systems
NN	neural networks
OO	object orientation
PC	personal computer
PSA	probabilistic safety assessment
PVM	preventive maintenance
PWR	pressurized water reactor
QA	quality assurance
RCM	reliability centered maintenance
V&V	verification and validation
WS	work station

**NEXT PAGE(S)  
left BLANK**



**Annex**

**PAPERS PRESENTED  
AT THE MEETING**

**NEXT PAGE(S)  
left BLANK**



## USE OF AN ON-LINE FUZZY-LOGIC EXPERT SYSTEM FOR WATER CHEMISTRY

J. FANDRICH, W. METZNER

Siemens AG – Bereich Energieerzeugung (KWU),  
Erlangen, Germany

### Abstract

The requirements for availability and operating economy of power plants have become steadily more stringent over the last few years. In addition to technological advances (e.g. in the form of new design measures, processes and materials), manufacturers have also increasingly applied secondary measures to enhance the safety and operating economy of power plant units. These include ever more sophisticated process monitoring and analytical systems and, (in recent times) diagnostic systems which perform continuous assessment of the plant condition to allow imminent changes that can lead to damage and faults to be detected at the earliest possible time. The following paper presents an expert system, based on Fuzzy logic, which is used to perform a wide variety of tasks in the field of NPP water chemistry diagnostics. Thanks to the general nature of the approach selected, the system kernel is identical for all solutions which were implemented despite the wide variety of tasks and their diverse needs. This would not have been possible without the development and application of powerful and flexible engineering tools which can provide solutions to different types of problems at no extra effort. It will be shown in which way the system builds up diagnoses from the collected on-line data via a system – specific and easy-to-learn language and several tools. The presented module DIWA (Diagnostic System of Water Chemistry) was directly derived from the DIGEST system (diagnostic expert system for turbomachinery), which was developed over the last few years at the Power Generation Group (KWU) of the Siemens AG.

## 1. Introduction

The requirements for availability and operating economy of power plants have become steadily more stringent over the last few years. In addition to technological advances (e.g. in the form of new design measures, processes and materials), manufacturers have also increasingly applied secondary measures to enhance the safety and operating economy of power plant units. These include ever more sophisticated process monitoring and analytical systems and, (in recent times) diagnostic systems which perform continuous assessment of the plant condition to allow imminent changes that can lead to damage and faults to be detected at the earliest possible time – well before levels are reached at which a protection trip is initiated.

The economical aspect is reflected in fewer outages, increased operating reliability and longer component service life. Plants which are fully equipped with such systems can achieve a medium-term goal of replacing the standard practice of periodic maintenance (which is time and cost-intensive) with condition-oriented maintenance for certain components. The following paper presents an expert system, based on Fuzzy logic, which is used to perform a wide variety of tasks in the field of NPP water chemistry diagnostics. Thanks to the general nature of the approach selected, the system kernel is identical for all solutions which were implemented despite the wide variety of tasks and their diverse needs. This would not have been possible without the development

and application of powerful and flexible engineering tools which can provide solutions to different types of problems at no extra effort.

The presented module DIWA (Diagnostic System of Water Chemistry) was directly derived from the DIGEST system (diagnostic expert system for turbomachinery), which was developed over the last few years at the Power Generation Group (KWU) of the Siemens AG [1, 2]. Although the DIGEST system was originally designed for steam and gas turbine—generators, the application area has been extended to include global diagnostic activities at hydroelectric and nuclear power plants.

## 2. Analysis and Diagnosis

For marketing reasons, solutions which are at best analytical systems are often sold today as diagnostic systems. The dividing line between analysis and diagnostics is, in fact, not always straight and narrow. However, when diagnostics is understood and accepted as a new quality, it is relatively easy to define.

The main distinguishing factor is that analysis embraces all the activities performed by applying numerical mathematics in the broadest sense. In particular, this includes the calculation of characteristic parameters or setpoints, the comparison of setpoints with actual data, and the detection of deviations and limit violations. Also included is the broad task of visualizing information which has been measured or calculated. In addition to displaying numeric values in tables, for example, one of the main tasks is to present the information intuitively in optically enhanced graphics, trend plots and other presentation formats. The methodology is based on familiar, step—by—step solution procedures, i.e. algorithms. If the algorithms are known, they are relatively easy to implement in conventional computer programs.

In addition to the above tasks, diagnostic systems are expected to actually interpret the information, in order to assess a process in relation to particular properties and requirements. In analytical systems, this more demanding task is left to the operator. Diagnostic systems must also be capable of explaining the process used to derive the diagnosis, so that the operator can understand it. Finally, the presentation of a forecast for subsequent process events, and the recommendation of countermeasures are features which must also be included in the performance spectrum. The above work is

TABLE I. ANALYSIS/DIAGNOSIS DELIMITATION

	Analysis	Diagnosis
<b>Function</b>	<ul style="list-style-type: none"> <li>• Calculation of characteristic values</li> <li>• Calculation of setpoints</li> <li>• Setpoint / actual data comparison</li> <li>• Detection of deviations and limit violations</li> <li>• Visualization</li> </ul>	<ul style="list-style-type: none"> <li>• Interpretation of information</li> <li>• Derivation of diagnoses</li> <li>• Explanation of cause and effect</li> <li>• Prognosis</li> <li>• Recommendation of measures</li> </ul>
<b>Basis</b>	<ul style="list-style-type: none"> <li>• Numerical mathematics</li> <li>• Graphics, trends and charts</li> </ul>	<ul style="list-style-type: none"> <li>• Logic</li> <li>• Natural language</li> </ul>
<b>Methods</b>	<ul style="list-style-type: none"> <li>• Algorithms</li> <li>• Programs</li> </ul>	<ul style="list-style-type: none"> <li>• Empirical knowledge</li> <li>• Knowledge base, rules</li> </ul>

based mainly on mathematical logic, often combined with the processing of statements in (quasi-)natural language. Both technical and, especially, empirical knowledge, which cannot generally be expressed directly in algorithmic terms, are required from the experts providing the input. A suitable method is to use a knowledge base in which the knowledge is set out in the form of rules.

For a long time, diagnostics was regarded as the "task of identifying possible fault causes from the incorrect behavior of a component or system" (see [3], for example). This definition can no longer be considered appropriate in many areas. A more up-to-date interpretation of the term is *preventive* diagnostics, which detects and reports changes, through continuous monitoring and assessment of events, before any damage or fault can occur. This is the concept which the diagnostic component of the DIWA system seeks to implement.

### **3. Reasons for a Fuzzy-Logic Expert System**

#### **3.1. "Knowledge incorporating uncertainty"**

It has already been mentioned that every type of problem needs an appropriate method of solution. The attempt to develop diagnostic systems in an environment such as DIWA is inevitably faced with. This has been proven in a wide range of projects. However, the fact that the state of the art does not allow an "exact" algorithmic representation a large number of expert system projects have also failed. In many cases, the reason was that the uncertainty incorporated in the knowledge was inadequately represented. An expert system must provide special mechanisms in cases where a problem is characterized by knowledge incorporating uncertainty. During the history of expert systems, a range of methods has been developed for this purpose, from which probabilistic models and confidence factors have acquired a certain degree of acceptance. More recently, Fuzzy logic has become an increasingly popular means of solving the problem.

Expert systems which are based on Fuzzy logic not only allow the implementation of expert knowledge, but also provide a method of representing knowledge incorporating uncertainty and of modeling the uncertainty in the decision-making process.

Knowledge incorporating uncertainty can occur in many forms, which can be characterized as fuzziness, incompleteness, inaccuracy or uncertainty. An important role is played by so-called linguistic uncertainty, which arises from the inaccuracy of natural language. When an expert is assessing the steam generator conductivity in a diagnosis, he might refer to a "*high conductivity*" or an "*low pH*". It is obvious that these phrases cannot be generated and manipulated by software straight from the measured data. This is precisely where Fuzzy logic comes into its own.

#### **3.2. Fuzzy Logic**

In the context of the problems encountered in nuclear power plant water chemistry diagnostics, it is significant that Fuzzy logic presents a method of expressing and processing knowledge incorporating uncertainty in quasi-natural language. One of the main aspects is that Fuzzy logic is not merely a logic calculation for combining statements, but rests on the foundations of an exact mathematical formalism. The result of a diagnostic process is thus not confined to naming the diagnosis, but includes the specification of a confidence factor with respect to the accuracy of the diagnosis. It is important for the expert providing the knowledge that he can concentrate solely on the formulation of the rules, without the need to consider the underlying mathematics. Fuzzy logic thus makes it considerably easier to develop a diagnostic system, and hence promotes the acceptance of such systems.

## **4. Operating Principle of the Fuzzy–Logic Expert System**

### **4.1. The Structure and Operating Principle of the System**

Fig. 1 shows the overall structure of the system. The operating principle is evident from the diagram. After performing plausibility checks, calculations of characteristic and additional values, which can't be measured directly, all of the measured data are directly accessible to the expert system kernel. From these values symptoms are derived (fuzzification). This task is performed by the help of parts of the knowledge base of this system.

After creating symptoms the system accesses another part of the knowledge base, where the rules of the expert knowledge are to be found. After running through all the rules the expert system creates one or more diagnoses. Basing on the operator connections within the rule base the system calculates confidence factors for every created diagnosis, which represent the safety level for the diagnosis. This workflow is directly related to the work an expert is doing.

All diagnoses which are created by the expert system kernel are stored together with the related measured data within the data base of the diagnostic system. The user has access to the results via a graphical user interface.

The user has the choice of the following functions within the graphical user interface:

- Overview of all created diagnoses,
- History of all diagnoses
- Technical description of all diagnoses and further recommended activities
- explanation component of the expert system.

The following chapters give a detailed view of the working principle of every component of the expert system kernel.

### **4.2. Measured values processing and visualization**

The starting point of data processing is the cyclic sampling of measured values. The problem related cycles range from 1 second to 30 minutes.

The concept of the analytical part of the diagnostic system takes into account, that more than one input source can be available. In the case of power plant water chemistry it is the normal case, that some of the measured data are collected online via installed sensors. Most of the data which have to be collected are measured at power plant laboratories via special analytical methods and equipment and therefore have to be input into the system "off–line".

The analysis part of DIWA performs the following tasks based on the specific data input:

- Plausibility check of all measured data. The data check is performed with respect to limit violations, characteristic changes within the trend and their affinity in relation to other values. All results of these checks are stored in a quality identifier and are accessible to the diagnostic part of the system.

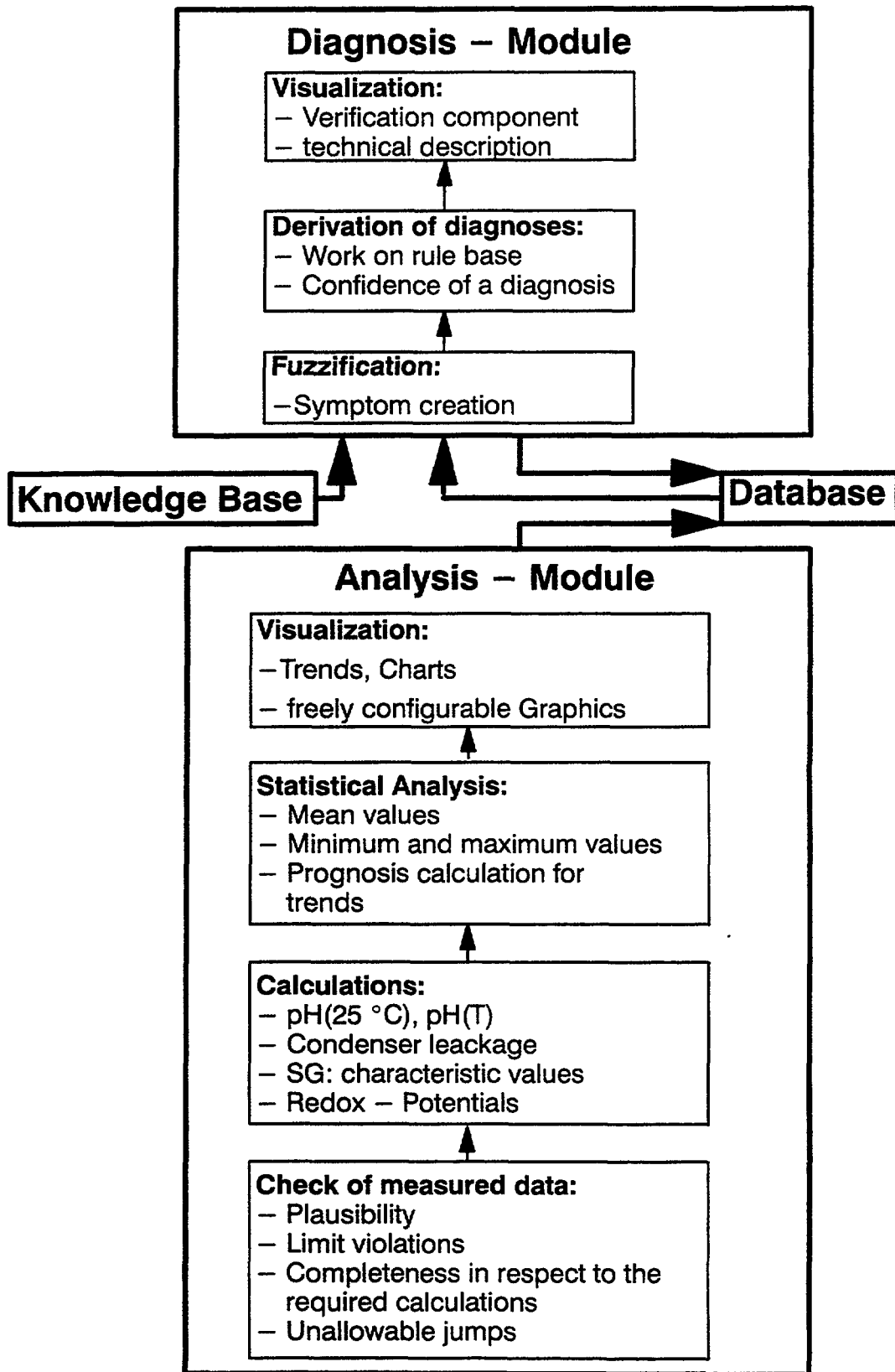
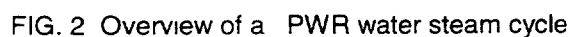


FIG. 1. Structure and working principle of the DIWA diagnostic system.

- All of the collected and derived data can be accessed by the user through DIWA's graphical user interface. DIWA provides this service in several ways: process displays (figure 2), trends, tables (figure 3), protocols and the ability to freely configure diagrams.



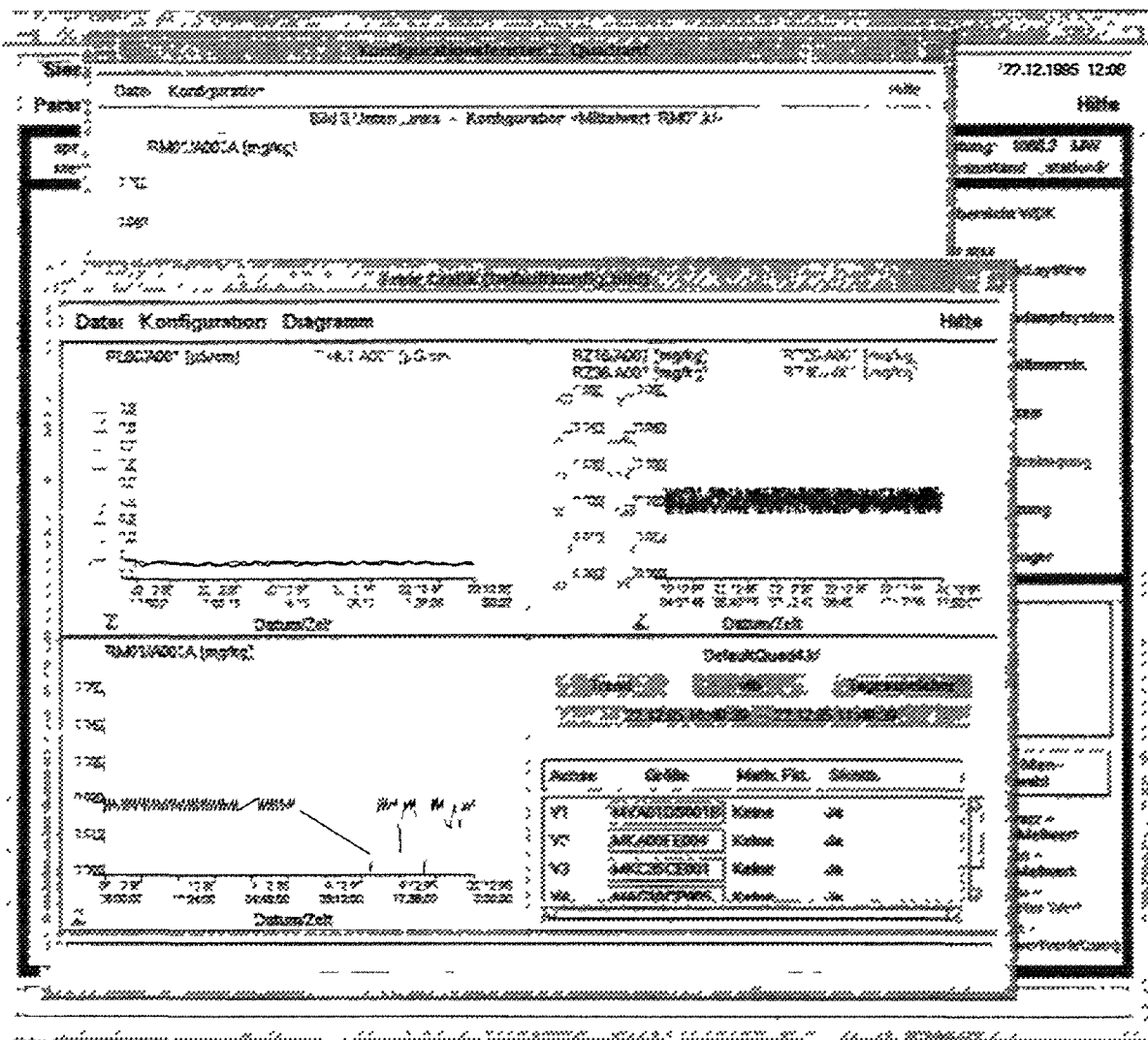


FIG 3 Analysis of trends and interesting operational states with the help of the graphics component of DIWA

### 4.3. Symptom Generation

The next step consists of the actual symptom generation. This requires answers to the following questions:

- What symptoms are relevant for a diagnosis and how can they be formulated?
- What measured data and characteristic parameters are suitable for symptom generation and what linguistic properties are appropriate for the diagnosis?



The actual warm gas gradient plays a part in the hydrogen sealing, for example. It is appropriate to classify the temperature profile as "falling", "constant" and "rising". The gradients generated from the warm gas temperature are assigned to these terms by means of membership functions, whereby the confidence factors are normalised within the range of 0 ... 1. Fig. 4 shows two examples.

Diagrams must be created for all variables which could be of interest.

#### 4.4. Representing Empirical Knowledge in the Form of Rules

The knowledge is represented in the form of "if...then..." rules. The symptoms are used in the "if" clause. The result of a rule, i.e. the statement in the "then" clause, can be an intermediate or final result. A final result is a finished diagnosis.

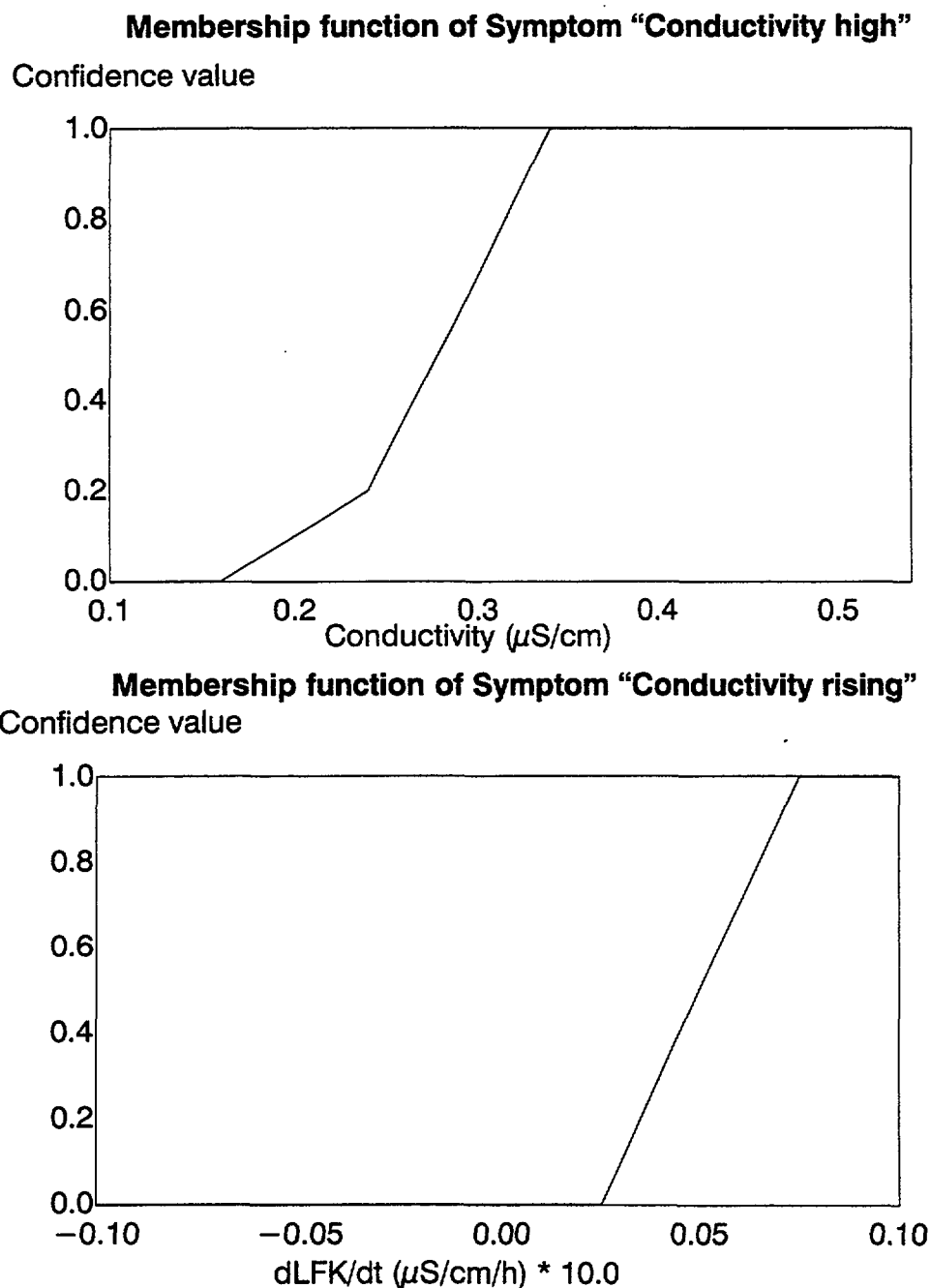


FIG. 4. Membership functions of two example symptoms: conductivity high and conductivity rising.

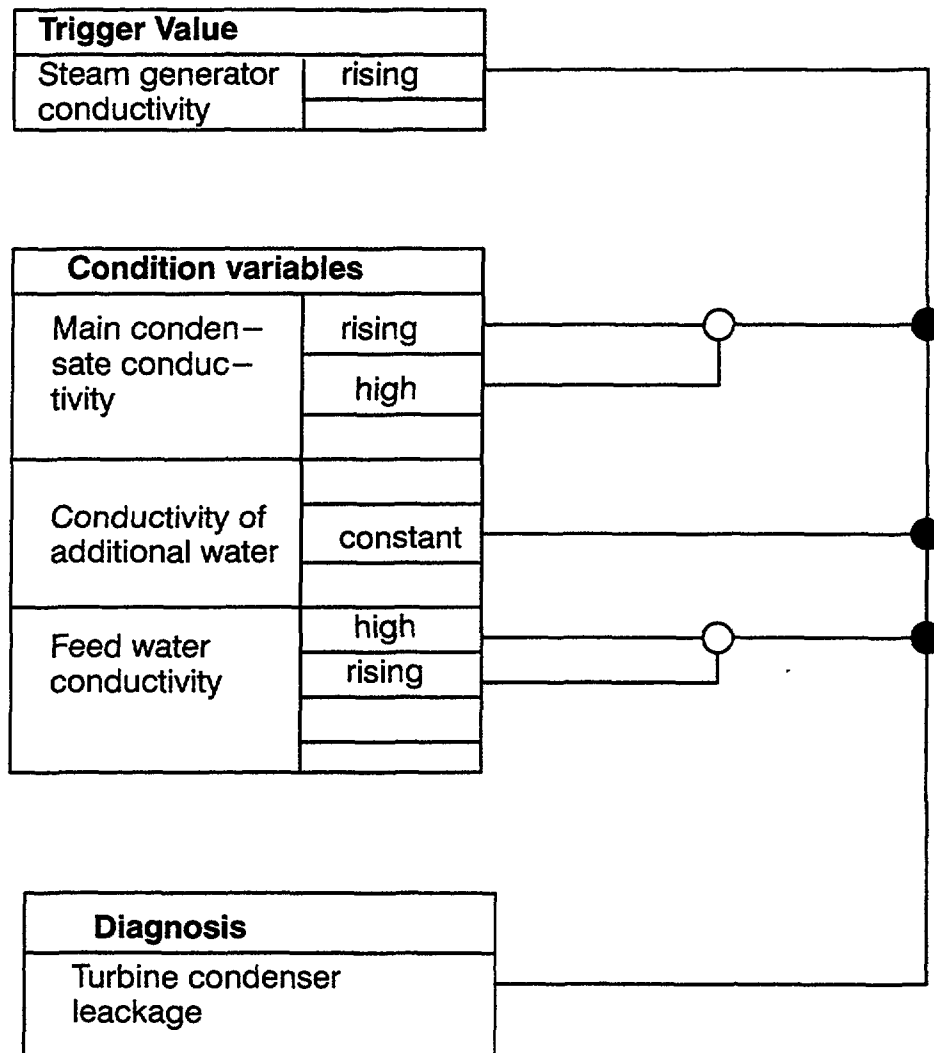


FIG. 5. An example rule.

An intermediate result can be input as a symptom to other rules, with the result that the entire rule base has a net-type structure. Since reference is often made to the same symptoms within the rules, the rules can be represented graphically, and rules which refer to the same symptoms can be combined in a group. The following example shows one rule.

This rule, corresponding to the whole path in the example is read as follows:

If the steam generator conductivity is rising and the conductivity of main condensate is high or rising and the conductivity of additional water is at a constant level and the conductivity of feed water is rising or high then a condenser leakage must be the result.

A specific language was created for the formulation of these rules in a form that can be processed immediately by a program. This language is called FCRSL, the "Fuzzy and Crisp Rule Specification Language". The notation in this language is quite similar to the formulation in natural language shown in the above example. The mechanism for integration into the program is to specify all rules in an external fileset (knowledge base). Rules can thus be changed or added as desired, without the need to modify the program.

## 4.5. Operators in FCRSL

As shown, symptoms are combined with each other within the rules. Various operators, which mathematically process the weightings resulting from the membership functions, are used for this purpose. The standard logic operators AND, OR and NOT are represented, according to Fuzzy logic conventions, as Minimum, Maximum and Complement. It became apparent at a very early stage that these operators are insufficient for a complete and authentic representation of the expert knowledge. Conditions occurred where the existence of a symptom strengthened or weakened the diagnosis, but where non-existence had no effect. Two new operators were introduced for this purpose: an amplification and weakening operator. The following table summarizes the operators and their mathematical representation.

TABLE II. FCRSL OPERATORS

Operator	Symbol	Mathematical definition
<b>AND</b>	●	$\min(a, b)$
<b>OR</b>	○	$\max(a, b)$
<b>NOT</b>	X	$1 - a$
<b>weighted AND</b>	◆	$k \cdot \min(a, b) + (1-k) \cdot (a + b) / 2$ k: weight factor
<b>weighted OR</b>	◇	$k \cdot \max(a, b) + (1-k) \cdot (a + b) / 2$ k: weight factor
<b>Strength</b>	■	$\min(1, a \cdot (1 + b/2))$
<b>Weakness</b>	□	$\max(0, a - ((1 - a) \cdot b/2))$
<b>weighted Strength</b>	■	$\min(1, a \cdot (1 + k \cdot b/2))$ k: weight factor
<b>weighted Weakness</b>	□	$\max(0, a - k \cdot ((1 - a) \cdot b/2))$ k: weight factor

Further operators can be added as required, and have since also been implemented.

## 4.6. Visualisization and Verification of Diagnoses

The verification component, with which the user can analyze the generated diagnosis, is an important component of the expert system. The complete rule tree involved in the diagnosis analysis is presented graphically on the screen. All graphical elements are mouse-sensitive: when the user positions the mouse on any of the symbols for rules, symptoms, operators or diagnoses, the associated values (names, states, weightings) are displayed. Elements are also highlighted in color, wherever possible. Since the rule trees can, in certain circumstances, cover large areas and may not fit completely onto the screen, it is possible to expand and collapse rule symbols simply by clicking them with the mouse. This enables context-sensitive navigation through the rule base, allowing the operator to concentrate on specific areas of relevance within the analysis. Fig. 6 shows a snapshot of the explanation component.

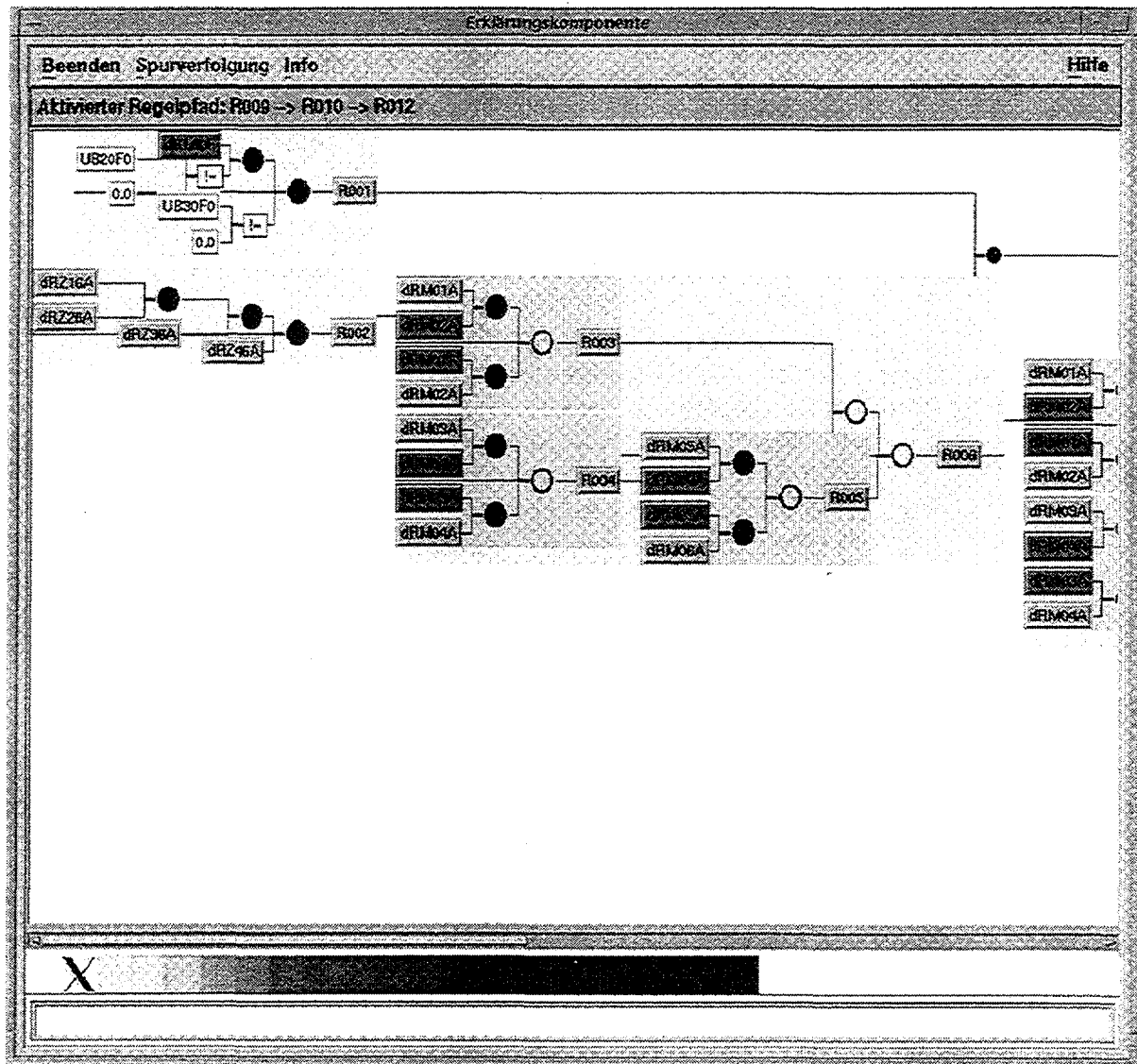


FIG. 6. Partly view of the rule tree of the diagnosis "Condenser leakage".

With these features, the explanation component presents a powerful tool with which even less experienced users can rapidly trace the path of the diagnostic system from the measurement of the data to the generation of the diagnosis, and thus pinpoint the causes.

## 5. Further applications of the Fuzzy expert system kernel

### 5.1. RF Diagnostics (HFD)

The task of this module is the detection and evaluation of conductor and insulation faults on the generator. Potential electrical faults frequently manifest themselves in the form of partial discharges or sparking in the generator or its leads, inclusive of the associated transformers. The RF signals are acquired by the RF monitor and displayed in analog format. In the off-line version of the module, the user enters the observed symptoms in a computer, and the expert system generates the diagnoses. In the online version, the digital signal conditioners connected to the RF monitor calculate characteristic parameters, which are subsequently interpreted by the expert system. The capability

of this module includes detection of the following hazards and avoidance of potential consequential damage for the following: destruction of the high-voltage insulation, breaks in grounding strips and damage to the generator bearings, as well as static discharges in the generator transformer and faults in the exciter system. See [4] for further information.

## **5.2. Hydrogen Sealing (WAD)**

The WAD module is used on gas-cooled generators to detect leakages of hydrogen, which is used as the coolant in a closed circuit, as well as faults in the function of the generator shaft seals. The detected leakage points are localized approximately. The problems associated with identifying a leakage result from load-dependent temperature and pressure fluctuations and the fact that hydrogen is also used for other purposes. The module is thus required to establish, under the given conditions, whether the current  $H_2$  consumption is normal or whether it points to a leakage. The relevant regulations require that uncontrolled losses must be limited to minimum rates. The monitoring of the  $H_2$  cooling system is therefore geared to preventing the uncontrolled escape of hydrogen to atmosphere, into the primary and secondary water cooling circuits and, in the event of a shaft seal fault, into the turbine building. Continuous monitoring also facilitates the planning of maintenance and repair work.

## **5.3. Moisture Ingress (FEW)**

The main objective of the FEW module is to detect and prevent primary water leakages in the hydrogen cooling circuit. The monitoring is performed by measuring the humidity of the  $H_2$  cooling gas. Water leakages which penetrate the gas space of the generator or are taken up in absorbers can lead to an increase in the steam pressure and, if the dew point is exceeded, to the wetting of components. Steel parts can corrode and the withstand voltage for insulating parts can be reduced, resulting in hazardous operating conditions. In this case, diagnostics has a mainly preventive character. The humidity of the gas can be measured directly. Part of the moisture is extracted via a gas drier filled with gel. Since the gel has only a limited capacity for storing water, it must be regenerated from time to time, i.e. it is only active for a limited time. The measured humidity and the operating time of the gas drier are the main indicators for the diagnostics. The FEW module is also used to control the operating modes of the gas drier (operation, regeneration).

## **5.4. Cooling System Faults (KÜSTE)**

Hydrogen and water are used as cooling media in large generators. Faults in these cooling systems can result in serious damage, such as overheating and destruction of insulating parts or melting of active metal parts. The module is used primarily for the early detection of flow disturbances brought on by operating errors, or of blockages in the subsidiary circuits of the cooling system. Damage to the bushing seals on the shaft pump is detected before trip of the generator protection system takes place in response to pump failure. The relevant pressures, volumetric flow rates and temperature increases are continuously monitored and analyzed for this purpose. An analysis of the chemical conditioning of the water is also performed. The early detection and localization of faulted zones in the cooling system prevents damage from spreading and often even allows operation to continue at an appropriately modified power level.

## References

- [1] W. Zörner, H. Müller, K.–H. Andreae, H. Emshoff: Diagnostic System for Monitoring the Operation of Steam Turbine Generator Sets  
VGB Kraftwerkstechnik, Vol 6, pp 487 – 496, 1991
- [2] W. Zörner, R. Denkes: The DIGEST On–Line Diagnostic System reduces costs in Power Stations  
Joint Venture Power Generation Conference, San Diego,  
7. 10. – 10.10. 1991
- [3] C. Weisang, "Methoden der Prozeßdiagnose in Kraftwerken",  
ETG–Fachbericht 48, October 1993
- [4] P. Grünewald, J. Weidner, "HF–Überwachung für Kraftwerke",  
CIGRE SC 11, March 1993



# INTELLIGENT AND INTERACTIVE COMPUTER IMAGE OF A NUCLEAR POWER PLANT:

## *The ImagIn project*

D. HAUBENSACK, P. MALVACHE, P. VALLEIX  
CEA/CEN Cadarache,  
Saint-Paul-lez-Durance, France

### Abstract

*The ImagIn project consists in a method and a set of computer tools apt to bring perceptible and assessable improvements in the operational safety of a nuclear plant.*

*Its aim is to design an information system that would maintain a highly detailed computerised representation of a nuclear plant in its initial state and throughout its in-service life. It is not a tool to drive or help driving the nuclear plant, but a tool that manages concurrent operations that modify the plant configuration in a very general way (maintenance for example).*

*The configuration of the plant, as well as rules and constraints about it, are described in a object-oriented knowledge database, which is built using a generic ImagIn meta-model based on the semantical network theory. An inference engine works on this database and is connected to reality through interfaces to operators and captors on the installation ; it verifies constantly in real-time the consistency of the database according to its inner rules, and reports eventual problems to concerned operators. A special effort is made on interfaces to provide natural and intuitive tools (using virtual reality, natural language, voice recognition and synthesis).*

*A laboratory application on a fictive but realistic installation already exists and is used to simulate various tests and scenarii. A real application is being constructed on Siloe, an experimental reactor of the CEA.*

This paper describes a research project of the French CEA, concerning evolutions in plant operation apt to bring perceptible and assessable improvement in the operational safety [ref.1].

Many mistakes in plant operations are due to a discrepancy between the "mental representation" of the plant by the operators and the actual plant status : this is often due to lack of information provided to operators, particularly on the modifications of the plant, either temporary or definitive. This can also originate in an inconsistency between the operational procedures and the actual status of the plant, due to these modifications. The maintenance of a coherent and unique representation of the plant for all the actors (human or computerised) of plant operations is the main objective of the ImagIn project [ref.2,3].

## 1. ELEMENTS OF SPECIFICATION

The aim of ImagIn project is to design an information system that would maintain a highly detailed computerised representation of a nuclear plant in its initial state and throughout its in-service life.

Each actor working around the plant uses his own database (equipment database, documentation, regulations, supplier database for instance), needs information from other actors and has to know current and past status of the plant. Some of them, e.g. operators in the control room and maintenance operators, directly operate on the plant configuration.

The role of the computerised representation system is :

- to provide a unique and accurate description of the whole plant for all the actors.
- to be a central node of communication between these actors.
- to record any modification of the plant.
- to verify the consistency of the plant within respect to regulations.

To reach these objectives an ImagIn system must :

- provide a database containing the specification and the current status of the installation (components, systems, spaces, staff ...), and all the available documentation (drawings, procedures and instructions, regulations...),
- restore, at any time, these informations in a comprehensible and reliable form exempt of any ambiguity,
- follow up each modification occurring on the plant and update the plant database (memorising how, when and what was done), without any unbearable additional constraint on operators,
- always verify the coherence of these modifications with the requirements and regulations, and point out any discrepancy.
- manage although any temporary modification involving a non compliance with requirements, during extraordinary maintenance operations or transient alarm situations for instance.
- take into account changes occurring on regulations,
- always inform actors about modifications of any type that concerned them.

The ImagIn program is based on two main tasks :

- build a prototype which will be a full-size illustration of the ImagIn implementation on the experimental reactor SILOE of the CEA/Grenoble.
- identify a method which will allow us to build such an application on any nuclear installation in an industrial context.

## **2. TECHNICAL COMPONENTS**

An ImagIn application has three main technical components (fig.1) :

- the "Representation" component.
- the "Management" component.
- the "Interfaces" component.

### **2.1. The "Representation" component**

It consists in constructing a database that contains all the information about the real status of a plant at a given moment, still memorising its past history. It is the knowledge model of the plant.

This model has a generic frame, built on the semantic networks theory : the ImagIn Meta-Model (fig.2). The IIMM describes the types of objects of a plant that an ImagIn application can represent and manage. Its concerns materials, spaces, activities, procedures and regulations, staff organisation, language of the domain and documentation. So this very wide model allows us to describe the tangible reality of the installation, as well as the way to modify it, and the way to control it. It is implemented in an Object Oriented Data Base System.



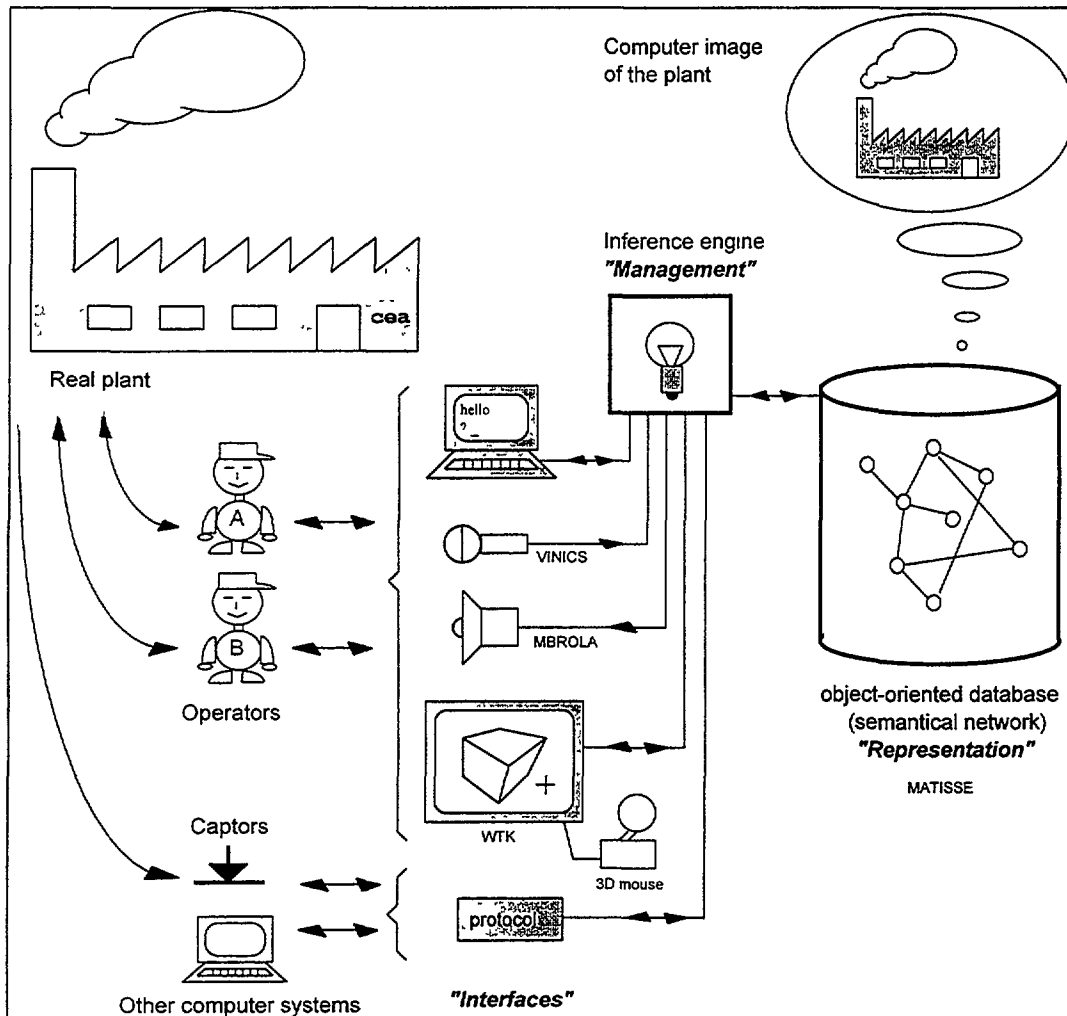


Figure 1. Overview of ImagIn system's components .

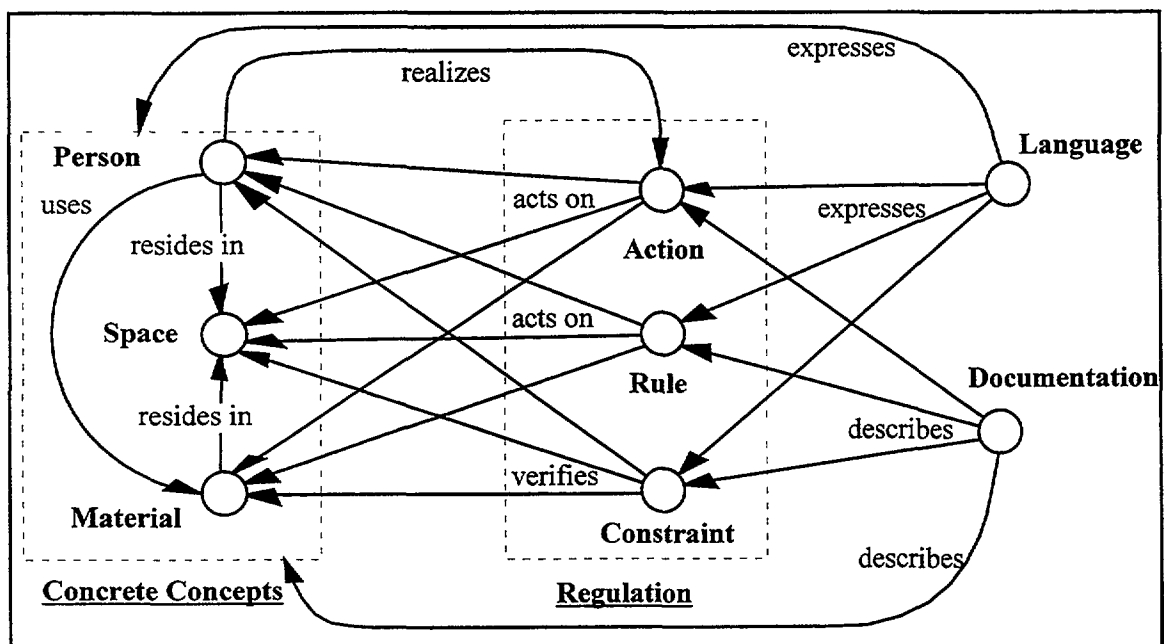


Figure 2. Simplified ImagIn Meta-Model (IIMM) .

The whole representation is based on information extracted from the documentation of the plant. To describe more precisely a given installation, an specialised Application Model is derived from the original Meta-Model by declining every concept into sub-families. This intermediate level of abstraction helps us reducing the « growing in size » effect, and allows us to stick specialised attributes on derived concepts (fig.3).

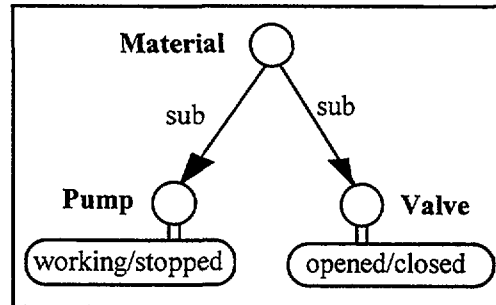


Figure 3. Application model .

The application model is then instantiated into final objets that describes the reality. In the following example (fig.4), a person P is localised in a space E and uses a valve V.

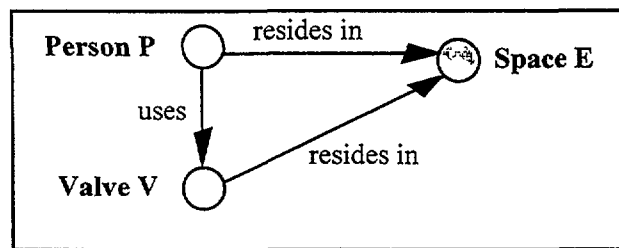


Figure 4. Example of representation .

A dating relation and attribute, and Modification objets are used to memorise completed operations and to provide a full tracability. On the following example (fig.5), a person P moves a pump O from a space E to a space F on date D.

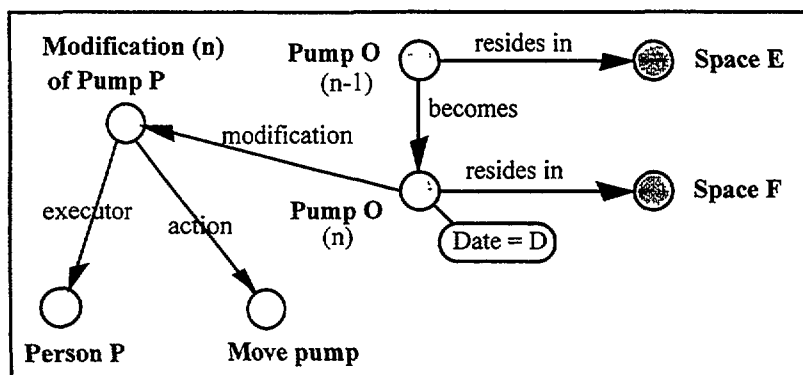


Figure 5. Example of dating .

## 2.2. The "Management" component

It consists in making the database evolve at the same time as the real plant while checking its inner coherence.

In the plant, every activity (maintenance, operation, handling, ...) has its own restricted point of view. For each point of view, there is an agent which is a computer process working on its specific knowledge database built on the same generic ImagIn meta-model. This agent can communicate with its dedicated human actors, involved in the same activity. All agents work independently at the same time and communicate with each other through a blackboard [ref.4] (fig.6).

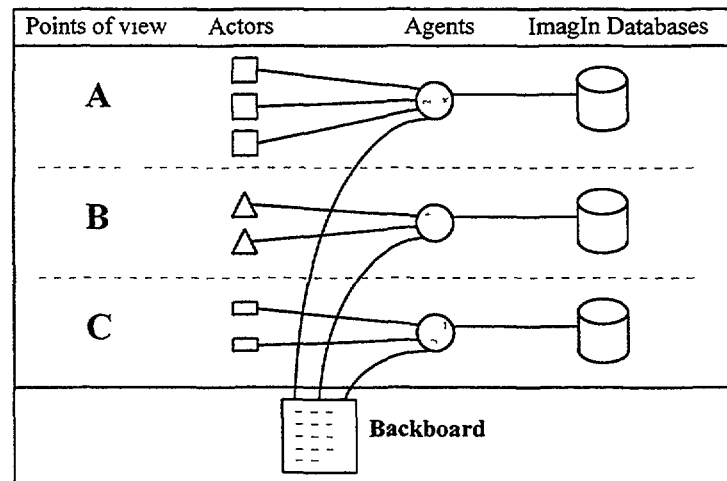


Figure 6. Communication between agents .





As soon as a human actor makes a modification on the plant, and tells it through an interface to his agent, this one reacts :

- it identifies the action and directly implied objects, trying to resolve any ambiguity (using the « Actions » part of the IIMM),
- it deduces any direct or indirect following modifications and updates its database (using the « Rules » part of the IIMM),
- it verifies the inner coherence of the database (using the « Constraints » part of the IIMM). In case of incoherence, it returns a warning message to the human actor who made the initial modification and to all its human actors concerned (according to their current work).
- it writes to the blackboard any modification recorded.

Simultaneously, any agent reads the blackboard and integrates any modification message it can understand. Then, as above, it verifies the coherence of the database and, in case of incoherence, informs all its human actors concerned, according to their current work.

An important point is that ImagIn must be as much as possible a preventive tool rather than a corrective one. That is why it works on a « intention/permission/action » basis : the actor declares his intention, waits for a permission, and then realises the action. But as ImagIn should just be an adviser, the actor should be the only one able to take the final decision (fig.7). These features raise

an important theoretical problem : the introduction of « possible » or pending actions (in a multi-user environment). This problem is quite similar with a more general time problem : we are working on the possibility to declare *a priori* a action planned in the future, and to declare *a posteriori* an action realised in the past.

actor	intention of action			
ImagIn	verification in every point of view $\Leftrightarrow$ consistency of the action ?			
⌚ delay...				
ImagIn	permission		action denied	
⌚ delay...				
actor	action 	cancel... 	action !  ( $\Leftrightarrow$ warnings)	no action 

**Figure 7.** The « intention/permission/action » cycle .

### 2.3. The "Interfaces" component

Two original interfaces have been developed : a bi-directional vocal interface and a 3D interface.

#### 2.3.1. The vocal interface

The input of the vocal interface is supplied by a continuous speech recognition system developed using the VINICS system of the CRIN/Nancy/France [ref.5,6]. This system is speaker-dependant and needs a learning stage. It is based on a new approach to phoneme-based continuous speech recognition, in which a time function of the plausibility of observing each phoneme is given. To improve the recognition, it also uses a phonetical grammar that describes the language of the domain. One of its advantage for industrial applications is that it can work in a noisy environment.

The grammar needed by the system is built using the « Language » part of the IIMM. As we are using one grammar per point of view, the recognition bandwidth is shortened and results should satisfied our requirements. As an example, VINICS average results are better than 98% success, on a word basis. Its only drawback for the moment is the calculation time (about 30 seconds), but we demonstrated at least that such a system is feasible, and we think it would be possible to use it efficiently in 10 years.

The output of the vocal interface is supplied by a speech synthesis software, called MBROLA and developed by TCTS/University of Mons/Belgium [ref.7]. This synthesiser can generate various intonations : this can be used to express different levels of urgency. It also permits a feedback in case of misunderstanding in the recognition step. Current work of TCTS is based on prosody (automatic intonation generation).

But both systems only convert analog voice signal to ASCII sentences : we developed natural language understanding and synthesis systems to change an ASCII sentence into an ImagIn understandable action and vice-versa.

### 2.3.2. The 3D interface

A virtual reality interface provides a 3D realistic but synoptical image of the plant, in which a user can navigate with a 3D input device in order to consult from a terminal the status of any parts of the plant (fig.8). On such a display, results of any action can be followed in real-time.

This interface is implemented with the World Tool Kit library [ref.8]. This library can support virtual reality devices. The background of the image displayed on the screen is built up using the « Space » part of the ImagIn model and will show buildings, rooms, doors, ground and stairs. Movable objects are issued from the « Material » part of the model and can be selected in the 3D view using the 3D pointer.

This interface can also be used as a simulator and various menus are provided to select actions to execute on objects selected in the 3D view.

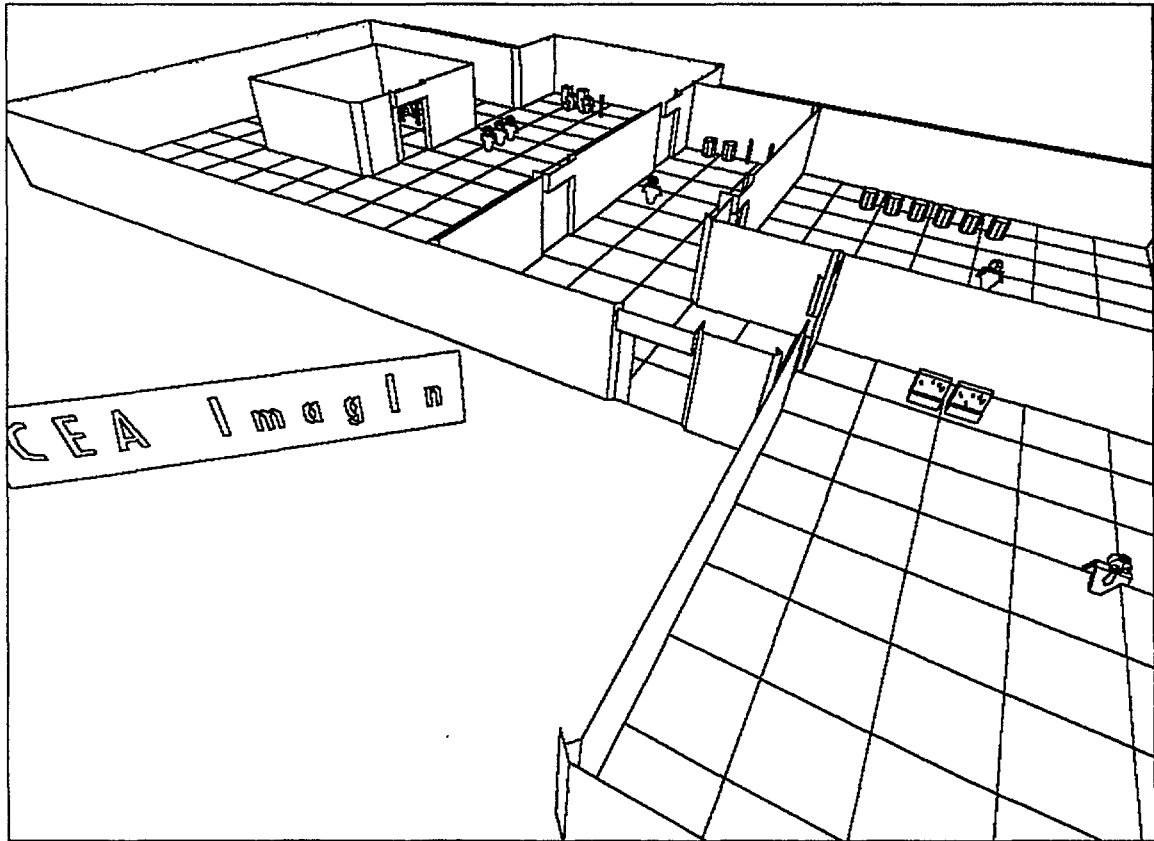


Figure 8. 3D overview of an installation .

## 3. CURRENT WORK

A laboratory application called ImaLab has already been developed, for purpose of tests and demonstrations. It represents a simple fictitious installation and demonstrates all the features of ImagIn using several possible scenarios, without having to manage the whole mass of information attached to a real nuclear installation.

The main goal of the ImagIn project is now to build up a prototype application on the experimental nuclear reactor SILOE located at CEA Nuclear Research Center of Grenoble. This application should be installed on the site at the very beginning of 1997. During this first real-sized experience, we will learn how to built a large ImagIn database, and write down the ImagIn Method.

## REFERENCES

- [1] « Evolution of the future plants operation for a better safety », P. Malvache / B. Papin, International topical meeting on advanced reactor safety - ARS' 94, Pittsburgh, PA.
- [2] « Real et virtual installation : the ImagIn project », P. Malvache / S. Tamisier, 2nd International Conference on Interface to real and virtual worlds, Montpellier, France, March 1993.
- [3] « Interactive plant management with real-time conformity checking : the ImagIn Project », D. Haubensack / P. Malvache / P. Valleix, July 1995, HCI Tokyo.
- [4] « Distributed Artificial Intelligence » (vol. 2), L. Gasser / M.N. Huhns, Research notes in artificial intelligence, Pitman, London.
- [5] « Principles and applications of VINICS continuous speech recognition system », Y. Gong / J.P. Haton, Advanced Speech Applications : European Research on Speech Technology, Springer Verlag, Berlin, September 1994.
- [6] « Stochastic trajectory modelling for speech recognition », Y. Gong / J.P. Haton, Adelaide, Australia, April 1994.
- [7] « The MBROLA Project : towards a set of high-quality speech synthesizers free of use for non-commercial purposes », T. Dutoit / V. Pagel / N. Pierret / F. Bataille / O. Van Der Vrecken, ICSLP'96, Philadelphia.
- [8] World Tool Kit by Sense8 Corp., 4000 Bridgeway #101, Sausalito CA 94965, USA.



**USE OF COMPUTER AIDS INCLUDING EXPERT SYSTEMS  
TO ENHANCE DIAGNOSIS OF NPP SAFETY STATUS  
AND OPERATOR RESPONSE**  
*VDU displays in accidents — Interact*

P. HUMBLE, D. WELBOURNE  
NNC,  
Booths Hall, Knutsford, Cheshire,  
United Kingdom

**Abstract**

This report describes NNC development of a demonstration concept called *Interact* of Visual Display Unit (VDU) displays, integrating on-screen control of plant actions. Most plant vendors now propose on-screen control and it is being included on some plants. The integration of Station Operating Instructions (SOI) into the VDU presentation of plants is being developed rapidly. With on-screen control, SOIs can be displayed with control targets able to initiate plant control, directly as called for in the SOIs.

*Interact* displays information and control options, using a cursor to simulate on-screen display and plant control. The displays show a method which integrates soft control and SOI information into a single unified presentation. They simulate the SOI for an accident, on-screen, with simulated inserted plant values.

The *Interact* displays were developed using 'Toolbook' (ref 1). The basic concept is a rolling succession of simple displays, responding directly to operator actions. Many simple displays are used, with simple choice and control operations. This is preferred to systems using fewer, more complex displays with complex operations and menu choices.

Selection initially gives an overview of the sequence to be followed. Entry to the sequence gives the right hand half screen showing the detailed operating instruction. The left hand half screen shows specific information for the operating instruction shown. The operator can select 'yes' or 'no' against the decision criteria of the instruction, using the information on the left half screen. If not satisfied with the decision, it can be changed. It is then confirmed by selection of 'continue', which gives the display of the next operation.

For control operations, the instruction shows the plant items and the action needed. The operator then selects the plant items required. The information display on plant state is made to follow the action, but with a random number bias for failure. 'Continue' rolls the display to the next operation. Colour and text show the changes and show which soft buttons can be used at each stage.

Feasibility of the process has been shown, although extensive work would be needed to implement the SOIs in the way suggested. Recommendations are given in the paper for a full development of some ideas produced during the work.

The work was partly funded by the European Union, DGXII, under the fission safety programme.

## 1. Introduction

The use of soft control on-screen for control of nuclear power plant is not yet established. Most plant vendors now propose it and it is being included for the EDF Chooz B plant. The integration of Station Operating Instructions (SOI) into the VDU display systems of plants is being developed rapidly. With soft screen control, SOIs can be displayed with control targets able to initiate plant control, directly in the way called for in the SOIs. The targets can call up sequences of plant or multiple operations of several plant items to achieve an operating goal.

The NNC work on *Interact* investigated display concepts which include the human factors consideration of a separate report giving full recommendations for VDU use. The development was at the level of feasibility and of presentation aspects, with simulated on-line capacity only.

The principal terms used are:

‘VDU’ refers to the visual display unit itself,

‘VDU display’ refers to the information shown on a VDU, where a distinction is needed.

‘Soft control’ and ‘soft button’ refer to plant control action or display action initiated or controlled by on-screen target areas for mouse click or touch action.

## 2. Objectives

The NNC work aimed to develop display recommendations and soft control display designs for accident management. These aimed to take full account of the information and control needed for a real plant, and the human factors and other recommendations of the separate study on VDU use. The work is based on and builds from the Sizewell B VDU display designs and SOIs, prepared by NNC for Nuclear Electric.

The initial aim of the work was to make recommendations on VDU display design, taking into account the use of touch screen soft control, and any experience of other SOI display methods. This is available within NNC as a detailed set of recommendations.

The second aim was to produce a conceptual design of the method of display of SOIs which integrates soft control and SOI information into a single unified presentation to the operators.

The final aim was to produce demonstration VDU designs and prototypes for use in a severe accident. They present the operator with information needed and allow on-screen operator selection of actions and groups of action to be taken on plant. They simulate the post-trip SOI for an accident, on-screen, with simulated values from plant. The VDU designs include mouse cursor areas to simulate touch-screen areas, for display navigation and plant control.

No attempt has been made to produce real-time software suitable for use with the soft screen controls of a real plant. No attempt has been made to produce software able to



interact with any existing on-site control and indication computer system. The *Interact* displays, considered as a knowledge base, are fixed in content during the design stage. This is intended as the method of achieving a licensable design concept, since a deterministic behaviour will then result.

### **3. Critical Safety Function monitoring**

CSF monitoring is an essential part of the operations performed by the operator in assessing severe accidents. The CSFs used are, in hierarchical order:

1. Subcriticality
2. Core cooling
3. Heat sink
4. Integrity
5. Containment
6. Inventory.

For CSF monitoring of the reference PWR, key measurements are checked for normal and abnormal conditions. Three levels of challenge are defined. These are off-normal, severe and extreme challenge. Off-normal requires action for that CSF, provided no other CSF has a more severe challenge.

The value in the normal range implies that there is no challenge to the CSF, and no action is needed from the operators. The value in the off-normal range may allow the event-specific SOI to continue to be followed, since the limit is within the design basis fault for which normal SOIs are defined. If the range of the variables is outside this, the operations supervisor can choose to re-diagnose the fault and adopt an alternative event-based SOI or an alternative strategy. The upper limit of the off-normal ranges require transfer to specific SOIs for restoration of CSF, by priority of challenge.

If a severe or extreme challenge is involved, then action to control the CSF must be taken, unless a CSF higher in the hierarchy is also severely or extremely challenged.

The operating concept followed enhances the diversity of approach, and thereby minimizes the risk of mind-set conditions. The initial CSF monitoring after a reactor trip is symptom-based and done by the supervisor, or an assistant operator under the instruction of the supervisor. This monitoring is done in parallel with the reactor unit operator actions, which follow event based procedures. These procedures support and monitor the automatic trip and ESF actions taken following trip or safety injection (SI).

An NNC input to the work was the program 'Navigate', developed to allow simulated operation of the reference PWR displays on a PC. It allowed the integrated presentation of the displays in a relatively realistic manner. The displays and their readability, clarity and usefulness were assessed. The displays used for accident management and CSF monitoring were identified. The SOIs were used for this. These displays generally are based on the detailed process plant designs. They are mostly plant review and system displays with a few operator task-based displays, and in general are not directly related to the tasks defined in the Station Operating Instructions (SOIs).

In the development reported here, the displays are defined from the operator's tasks, rather than from a plant review basis. Each operator task and the information identified for checking or decision making is then placed on the appropriate VDU display page. This display page directly defines the SOI decision or control blocks required. The display pages then link one to another in the sequence of the tasks required. The demonstration system and concepts are called *Interact*.

#### **4. Software used**

The aim was to use a standard PC for the *Interact* demonstration work. The Toolbook package (ref 1) was assessed for use for the development of the demonstration displays. It includes all the features needed. Keyboard control after cursor selection of a signal allows insertion of new values. The only special requirements are for a Windows 3.1 environment with super VGA. The *Interact* displays were therefore developed using 'Toolbook'.

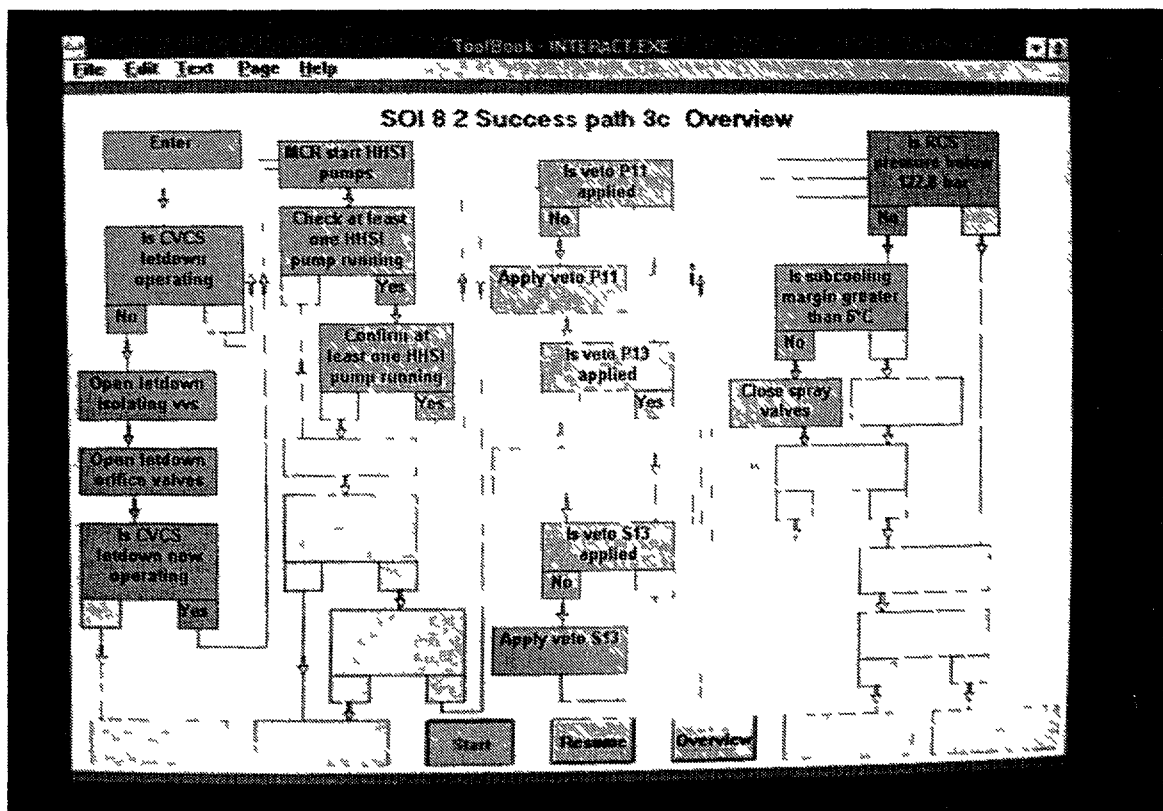
#### **5. Basic concept**

The basic concept of *Interact* is a rolling succession of simple displays, which respond directly to the operator actions. The operator is in control of all display choices and all action demands at all times, without any automatic presentation of new displays. Many simple displays are used, with simple choice and control operations. The operations aim to be simple and self-explanatory. This is preferred to fewer, more complex displays which could require complex operations and menu choice processes.

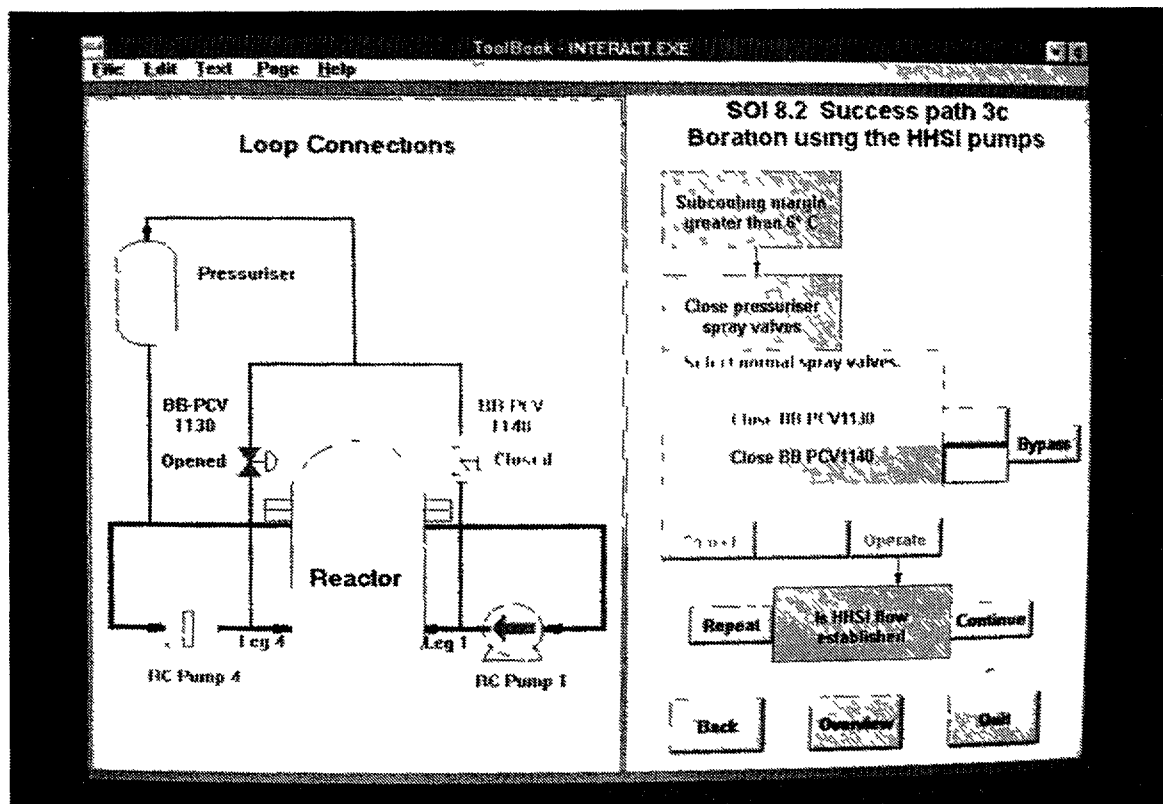
Selection of a group of operations initially gives a whole screen overview of the sequence to be followed (see figures 1, 3). Entry to the sequence gives the right hand half screen showing the detailed operating instruction. The left hand half screen shows specific information needed for monitoring the conditions referenced by the operating instruction (see figure 4). The displays thus show each instruction and the direct information to support the instruction. The instruction identifies the operator check and decision or the control operation required, and the information presented is specifically that needed for the instruction. The information half screen gives options to display alternative data sources, if the preferred signals have failed. On completion of the step the operator proceeds to the next step, described earlier as a rolling progression.

For information checks and decisions, the instruction shows the check required (see figure 4). The operator can select 'yes' or 'no' against the decision criteria of the instruction, using the information on the left half screen. A 'yes' is always downwards and corresponds to a lesser challenge, with 'no' upwards. If not satisfied with the decision, it can be changed. It is then confirmed by selection of 'continue', which gives the display of the next operation.

The displays provide monitoring to determine whether a challenge to a CSF exists and the level of criticality of that challenge. This is done through the CSF status trees, using defined thresholds for each key parameter measured. Some systems automate this process and this would clearly be simple, but for use in accidents the monitored signals could have failed. Therefore the display process was not automated and each decision was explicit, with choice of alternative parameters given for each decision. The explicit decisions also illustrate the concepts in a wider context than accident management alone.



### Figure 1



### Figure 2

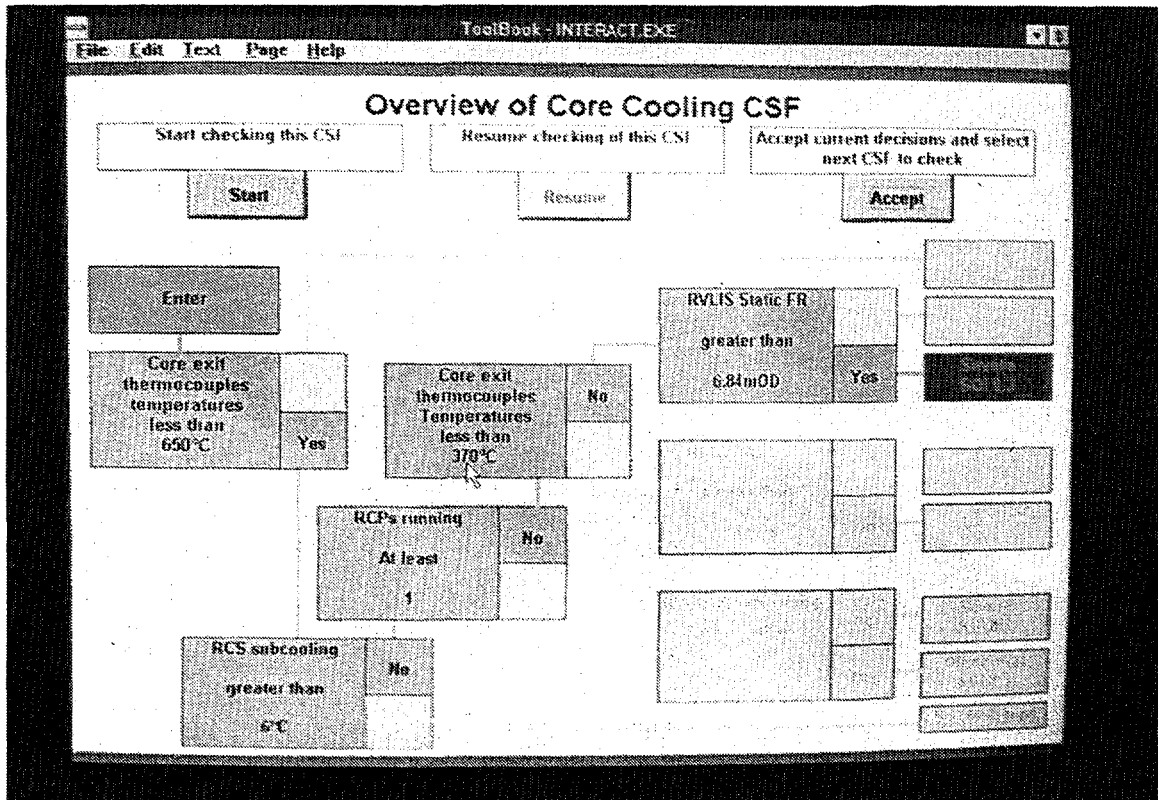


Figure 3

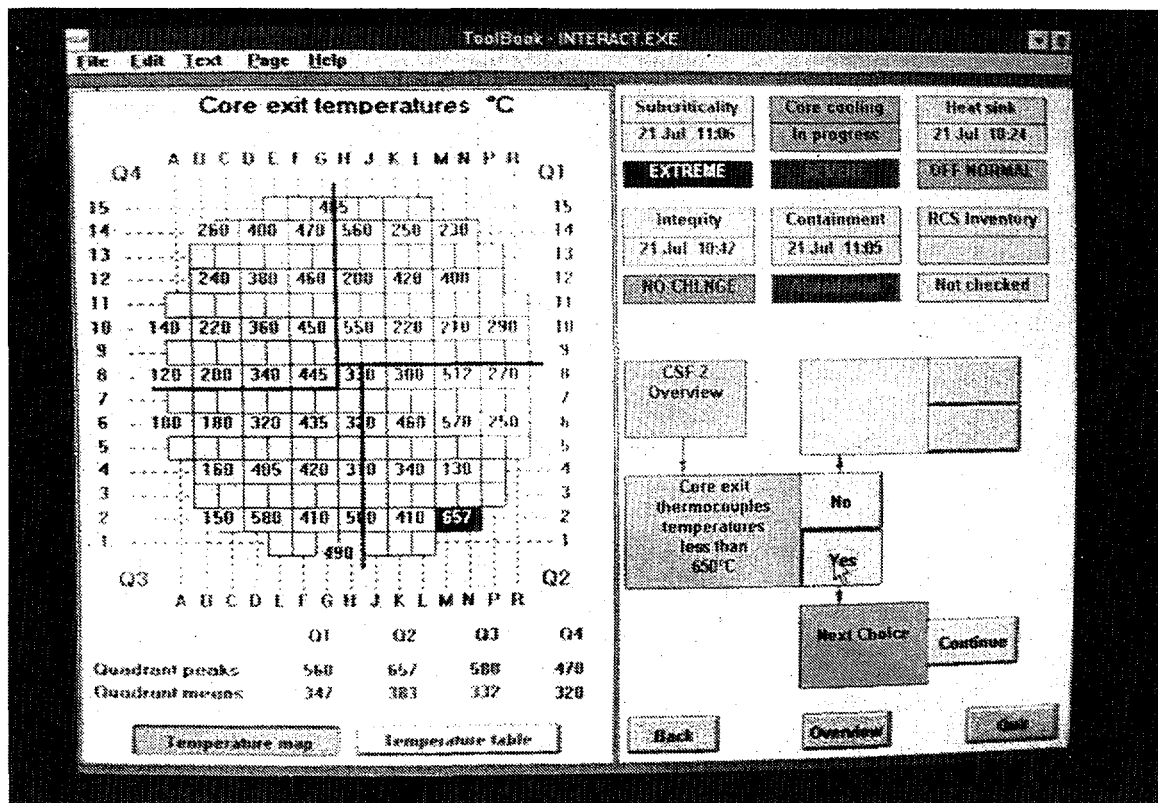


Figure 4

For control operations, the instruction shows the plant items and the start, open or other action which is needed (see figure 2). The operator can then select the plant items required or change the selection. The 'select' soft button toggles, to select or deselect each item. An 'enable' then an 'operate' action is then required. On this confirmation, the operator has the option to continue, if the action was successful. 'Repeat' allows the action to be attempted again. The display layout is standard. The support information display on plant state is made to follow the action, but with a random number bias for failure. 'Continue' makes the display roll forward for the next operation. Colour and text show the changes and show which soft buttons can be used at each stage.

A skeleton display scheme for CSF monitoring was produced first, on paper. The detailed specific measurements and states called for in the SOIs were found. The instructions were reduced to the simplest basic logic operations of checks against criteria and instructions to change plant state. Specific problems were met of ambiguity and lack of failure paths for some operations defined in the SOIs, but were generally resolved by reference to the writers of the SOI. Some simplifications of operations were included, since the display design aim was to show principles, rather than to overcome every SOI problem.

The displays for progression through the CSF for the primary signals were identified and entered to Toolbook, and a prototype display sequence produced successfully for initial review. Human factors experts provided comments, which were then included in the developed version of *Interact*.

The internal NNC design recommendations for VDUs were used in defining the *Interact* displays. The primary and alternative CSF monitoring signals for use if the primary measurement has failed or is not valid were identified. Additional displays were produced for the alternative signals. Calculations of averages of redundant signals were added where appropriate. Uniformity of colour presentation for within or outside each limit was included.

The detailed SOI actions for extreme, severe, and off-normal challenge to CSF1 were investigated, with consideration of the operator actions and control activities undertaken for any challenge. These sequences of actions are termed 'success paths', which reduce reactivity by various methods in the case chosen. An overview display of all CSF1 success paths was defined. The initial success paths involve checks that the automatic protection has operated and manual reinforcement of those actions. Due to the very extensive operations involved, these paths were not simulated, since the intention was to show the principles, not the full detail.

A single success path to reduce the CSF challenge was implemented as displays (see fig 1). This involved operator action to attempt to reduce flux (RCS boration using HHSI pumps, success path 3c). The set of displays needed were identified as illustrative of the accident management operations and show the principles suitably.

## **5.1 Development of display concepts**

Concepts which were considered in the development described above included:

- (i) A representation of the plant for each CSF, with detailed zoom or display switching into the selected CSF chosen for the study, or the actions selected. This approach

was rejected, after study of the plant and CSF displays, which are almost totally abstract and are not suited to a single plant mimic with zoom.

- (ii) A rolling display of the SOI information, included as windows on plant background displays. This was used, as the basis of the SOI presentation aspect, and partly for the plant state information.
- (iii) A representation of the plant at detailed level, with navigation through it and presentation of the SOIs as a selectable half-screen window with the plant. This was selected as the most flexible approach, together with the rolling display concept.
- (iv) Representation of the plant in an abstract manner, with the emphasis on the SOI information, assuming use of the previously designed displays on another screen or a window. The decisions taken at each step of the SOI are generally based on single redundant parameters and new displays were produced for them.
- (v) Soft control targets for initiation of plant actions called for in the SOIs, both for single actions and in groups or sequences. Although the project timescale did not permit this to be achieved completely, sufficient work was done to illustrate the feasibility of this approach.

The approach chosen was a split screen, as described above, adopting features of several of the initial ideas.

## **5.2. Display design development**

The initial development showed various features only partly foreseen or not anticipated at all. These included:

- (i) The need for a 'back' control on most displays to show the last display again;
- (ii) The need for an exit and resume facility, to leave the detailed logic and to show the full logic and stage reached. Resume returns to the checks and actions at the point reached;
- (iii) The VDU ability to show many parameters was normally not relevant, and only few parameters, as directly needed for a decision or operation were needed for each step. This allowed greatly improved clarity of information display compared to the reference displays of Navigate;
- (iv) The need to show path options and path followed, and the situations diagnosed. This was well shown by colour fill with legend where ambiguity from colour alone could result.

These features were included.

## **5.3 Recommendations arising**

Relevant recommendations for on-line operator instruction displays are:

- (i) Use an automated tool for generating and transforming the SOI to formally structured text;
- (ii) Use a split screen, with one half for instructions, one half for support information;
- (iii) Limit the on-line SOI information to two or three steps at most;
- (iv) Provide on-line support information on only one or two parameters or use limited mimics, as needed for the SOI step selected;
- (v) Provide a page back or last screen target;
- (vi) Provide colour enhanced and written text to trace the path followed in the logic and the status of each check;
- (vii) Provide an exit and resume facility, or a facility to check the logic path progress while still following the detailed path.

The literature recommends that there should be only one method of presenting each procedure component, and that action statements should not be embedded in notes and cautions. The need to keep a record of the place reached within a procedure and the need for decisions to be clearly worded is also quoted. The nature of *Interact* enforces these requirements.

Different consideration apply to the information which can be provided to support staff in a Technical Support Centre, where far more detailed information can be digested, and far more complex displays used.

## 6. Implementation

The *Interact* concepts were successfully implemented and then developed for CSF monitoring and for operations to meet challenges. The following describes various options considered and used.

The use of two or more displays on one screen as windows displays, which are usual for installed systems, was considered initially. Although the Windows environment used for the software would have allowed this, it was decided not to implement this as being application-specific and outside the illustration of principles needed for the work.

A background display, for zoom, display switching and sub-navigation targets to access information was considered unnecessary. An overview display of the CSF groups with their current state and last checked time, and an overview display of the success paths provides centre points for the demonstration. The navigation process through the demonstration is recorded dynamically on these displays, and the CSF information repeated in summary at the head of the detailed CSF displays.

Touch targets were simulated by use of a mouse. The soft control instruction on plant control displays alter the plant states shown, but with a random number used to cause action failure. The display changes as simulated plant states changes, but no further simulation is included.

The information displays show a dummy of the plant state and plant measurements and dummy the plant responses to control actions of the operator. Initial design showed that the discrimination needed for decisions was generally best seen from histogram displays of the measurements, with options for alternative signals.

The ability to change information display values was added, using cursor and keyboard. This is possible on first display of a value, with re-selection of the display giving update. Some displays needed simple mimics showing valve or pump status with limited flow paths and some digital values. Suitable displays were developed. An interface to D-Base was used for a core plan display of fuel channel outlet temperatures, and could be extended.

A random number generator is used with a bias to simulate the potential failure of instruments, resulting in a fault display for the signal. State displays similarly have a random number bias. Plant actions taken have a random number bias to failure to act.

The use of tick boxes on information displays was tried, to allow the operator to record any decisions on failed signals and retain that record while reviewing other data sources. This would allow recording of the situation where the preferred information signals are not valid and alternative sources must be used in a accident. In tests this appeared not needed, since defective instruments would be directly shown in any case. It was therefore not included.

A simple validation test was defined and used to check for errors and inconsistencies in the operation, and to confirm the software was correct at each change.

## **7 Possible developments and conclusions**

Successful displays were produced, but some developments, and some features could be added, as follows:

- (i) The use of the control displays showed that the option to open and to close valves, or start and stop pumps should be included, with the preferred action for the operation indicated.
- (ii) The SOI logic showed the potential need for functions to count operation attempts or cyclic loops and provide warnings, and for subroutine structures.
- (iii) The potential for inclusion of automatic determination of CSF challenge level on the preferred instruments exists. This was not adopted, for the reason given that the instruments may have been destroyed by an accident.
- (iv) Time did not allow checks with operators of the concepts, and these should be made.
- (v) The detailed process of transfer of SOIs to a computer display process is valuable of itself for identification of problems of ambiguity and incomplete definition of operations.



The *Interact* system aimed to complement other systems investigated during the work, and not to overlap. It aimed to provide a demonstration display suite only, to show the ideas of a rolling interactive display used for direct plant control. It aimed to include the human factors recommendations on VDUs identified in NNC. It aimed to show many simple displays rather than few detailed displays, and aimed to keep the operator actions to control the displays very simple and self-evident. No other systems considered have included plant control or the human factors aspect fully.

Although it is clear that extensive work would be needed to implement the SOIs in the way suggested, feasibility has been shown. The advantages of an almost self-explanatory system which presents only few decision requests on each screen have been shown.

The system has potential for development as

- a training aid for operators;
- a method of rigorous checking of SOIs as they are developed;
- a method for feasibility testing of on-screen control;
- an off-line method of presenting SOIs, using on-line data via data links;
- for full scale development of on-screen control.

### Reference

- [1] Toolbook 3.0. Asymetrix Corporation, 110-110th Ave. N.E., Suite 700, Bellvue, WA 98004, USA. Asymetrix Sales, USA 800-448-6543, fax 206-637-1504

# **INTEGRATED APPROACH TO KNOWLEDGE ACQUISITION AND SAFETY MANAGEMENT OF COMPLEX PLANTS WITH EMPHASIS ON HUMAN FACTORS**

K.T. KOSMOWSKI

Technical University of Gdańsk,  
Gdańsk, Poland

## **Abstract**

In this paper an integrated approach to the knowledge acquisition and safety management of complex industrial plants is proposed and outlined. The plant is considered within a man-technology-environment (MTE) system. The knowledge acquisition is aimed at the consequent reliability evaluation of human factor and probabilistic modeling of the plant. Properly structured initial knowledge is updated in life-time of the plant. The data and knowledge concerning the topology of safety related systems and their functions are created in a graphical CAD system and are object oriented. Safety oriented monitoring of the plant includes abnormal situations due to external and internal disturbances, failures of hardware/software components and failures of human factor. The operation and safety related evidence is accumulated in special data bases. Data/knowledge bases are designed in such a way to support effectively the reliability and safety management of the plant.

## **1. Introduction**

Potentially hazardous systems such as nuclear power or chemical plants are designed and operated according to national regulations and safety standards. However, due to complexity of the plant design and many interactions within the system: 'man'-'technology'-'environment' (MTE), the disturbances and abnormal situations, some of stochastic nature, occur during the plant operation. Frequencies and consequences of potential abnormal/emergency situations depend on the nature of the MTE system and the safety features of the plant. The reliability characteristics of its components change in time. Therefore, the permanent safety assessment and management are required starting from the conceptual design stage of the plant to its decommissioning.

The influence of so called human factor on the safety of complex industrial systems, nuclear power plants (NPPs) and hazardous chemical installations in particular, is widely recognized. Human-system or simply human interactions (HIs) is the term that describes all interfaces between humans and the system (Moieni et al. 1994). Errors committed by man managing, operating and maintaining these systems are often most significant causes of accidents and risk associated with their operation (Dougherty & Fragola 1988).

On the other hand the state of the art of the human reliability methodology and available at present methods/techniques for probabilistic assessment of human failures indicate that this methodology is not mature. It was confirmed by results of some experimental research, aimed at validation of the human reliability analysis (HRA) models, more frequently used in engineering practice. Another problem is associated with the fact that the human reliability assessments are profoundly dependent on expert judgment. Results of HRA benchmark exercises, summarized e.g. in (Poucet 1988), have shown that the human error probability (HEP) and assessed frequency of some accident situations for specified plant, obtained by different groups of HRA experts, can reach discrepancy as high as orders of magnitude.

HRA in the context of the probabilistic safety analysis (PSA) is an attempt to model HIs and predict the impact of such interactions on the reliability and safety of plants. When a system is complex with a large number of human interactions, in various phases of the plant normal operations or abnormal conditions, then HRA becomes an extremely important part of PSA for realistic assessment of plant safety (Moieni et al. 1994).

Therefore, considerable research efforts have been undertaken at some research institutions and regulatory bodies to improve the methodology, verify models and propose approaches standardizing HRA performed within PSA studies (IAEA 1992). It is very important for obtaining correct quantitative results, used often in engineering practice for the reliability management and safety related decision making. For accomplishing these objectives a tendency of growing interest in computer aided PSA and HRA is observed, especially in employing the expert system technology. In this paper an integrated approach to the knowledge acquisition and safety management of complex industrial plants is proposed and outlined.

## **2. Knowledge acquisition as modeling of the plant with emphasis on the human factor**

### **2.1. Features of a software system for computer aided PSA**

There is a growing interest to design supporting computer programming tools for managing more effectively the complexity of PSA and HRA and to reduce subjectivity of assessments, as these analyses should be adequately documented for future scrutinizing and modifying when new evidence will be available ("living" PSA). Lately this interest has been focused on employing the expert system technology (Wang & Modarres 1990, Poucet 1990, IAEA 1990, Kosmowski et al. 1994). The knowledge based systems (expert systems) are developed to imitate the knowledge of the domain experts and are designed to use various information sources including external data and expertise (IAEA 1990).

A prototype expert system REPSA1ES (*Reliability Evaluation and Probabilistic Safety Analysis-level 1-Expert System*) has been designed (Kosmowski et al. 1994). This system consists of a CAD system for graphical representation various diagrams, various data bases, a shell for building expert system and a coordinating module, all integrated in the programming environment of MS Windows 3.1. This knowledge based system has some interesting features, e.g. the user friendly interface with extensive graphical support using several CAD modules to represent the topological information and functional-logical knowledge. It enables effective data/knowledge acquisition as well as the iterative logical and probabilistic modeling of complex safety related systems.

### **2.2. Human reliability analysis (HRA) in the context of PSA**

The HRA is often performed according to the SHARP procedure (Hannaman & Spurgin 1984). Introducing the human failure events into the structures of the fault and event trees is performed at present in REPSA1ES by the user. There is a general guidance to perform these tasks. Since the effects of slips during plan-directed activities usually do not propagate unassisted by other failures beyond the component(s) affected, they can be incorporated into the fault tree models. Mistakes, which are most significant in event-driven activities, because of their propagative potential, are to be incorporated best at the top of the fault trees or in the event trees. Recovery events are tacked on the end of the dominant accident sequences for which they apply and may not be formally included in the event or fault trees (they can be left as adjoints to cut-sets). In this way, the classification effort supports the integration effort (Dougherty & Fragola 1988).

After the selection of appropriate HRA method the assessment of HEP is carried out according to determined procedure with regard to attributes of the situation analyzed. Thus,

the system provides a computerized framework to perform HRA, calculate HEPs and document analyses. However, depending on the method selected more or less external expertise from the domain expert is required to provide the description of the situation of interest and some factors influencing human performance.

In the current version of this system a prototype version of simplified THERP technique, based on ASEP-HRAP approach, is available and tested. The evaluation of HEP is initiated when the human failure event is placed into the fault tree. Then some attributes of such event are determined in dialogue with the user according to the procedure available in the HRA module. At the end of the session the value of HEP is calculated and placed of the human reliability data base (HRDB), related to given PSA project.

In the HRA/PSA screening process only more important and probable human failure events are taken into account for further analysis (Hannaman & Spurgin 1984). Obtained HEPs are to be stored in a project human reliability data base (Kosmowski et al. 1994). Some data bases have been designed, related to specific HRA methods, to store values of attributes for the situations analyzed. Thus, the human reliability modeling process is documented.

### **2.3. Levels of details of computer aided PSA/HRA**

Three levels of effort to carry out balanced PSA and HRA have been distinguished: I, II and III which correspond to the PSA and HRA basic methodological issues (methods applied, details of modeling and the contribution of experts required) and relevant scopes of the computer aided analyses (Kosmowski et al. 1993, 1994). The development of the software system with an open architecture has been scheduled for gradual and balanced realization of the research and designing works with regard to resources available.

At present the designing works are concentrated on selected methods of the scope II and III, namely: the THERP technique with graphical representation of the human reliability analysis event trees (HRAET) and a computerized version of modified SLIM technique. The situation specific HRAET enables representing possible paths of human actions and failures including errors and recovery potential. Obtained structure is then assessed based on the procedure and probabilistic data available within THERP.

## **3. Challenges associated with integrated approach to safety management of complex plants**

### **3.1.A general concept of the knowledge acquisition and safety management**

A general concept of an integrated approach to the safety management of the man-technology-environment (MTE) system is presented in Fig. 1. Safety monitoring of the plant includes abnormal situations due to external and internal disturbances, failures of hardware and software components and failures of human factor. The operation and safety related evidence is accumulated in special data bases. Several knowledge bases are conceptually designed in such a way to support effectively the reliability and safety management of the plant. Properly structured initial knowledge is updated in life-time of the plant to include changes of technical specifications or operation conditions.

A knowledge based 'living' Probabilistic Safety Analysis (PSA) and Human Reliability Analysis (HRA) is assumed to be a methodological basis for knowledge acquisition and safety management. The modeling process and analyses are performed based on a graphical and symbolic object-oriented representation of the plant. It includes the topology of systems (P&IDs), the hierarchical description of safety functions, directed graphs for defining relations between the states of functional objects and process variables, logical models (success trees, fault/event trees, HRA trees). The construction of logical structures (fault and event trees) can

be partly automated based on topological/logical information. These structures are then quantitatively assessed using special calculation modules.

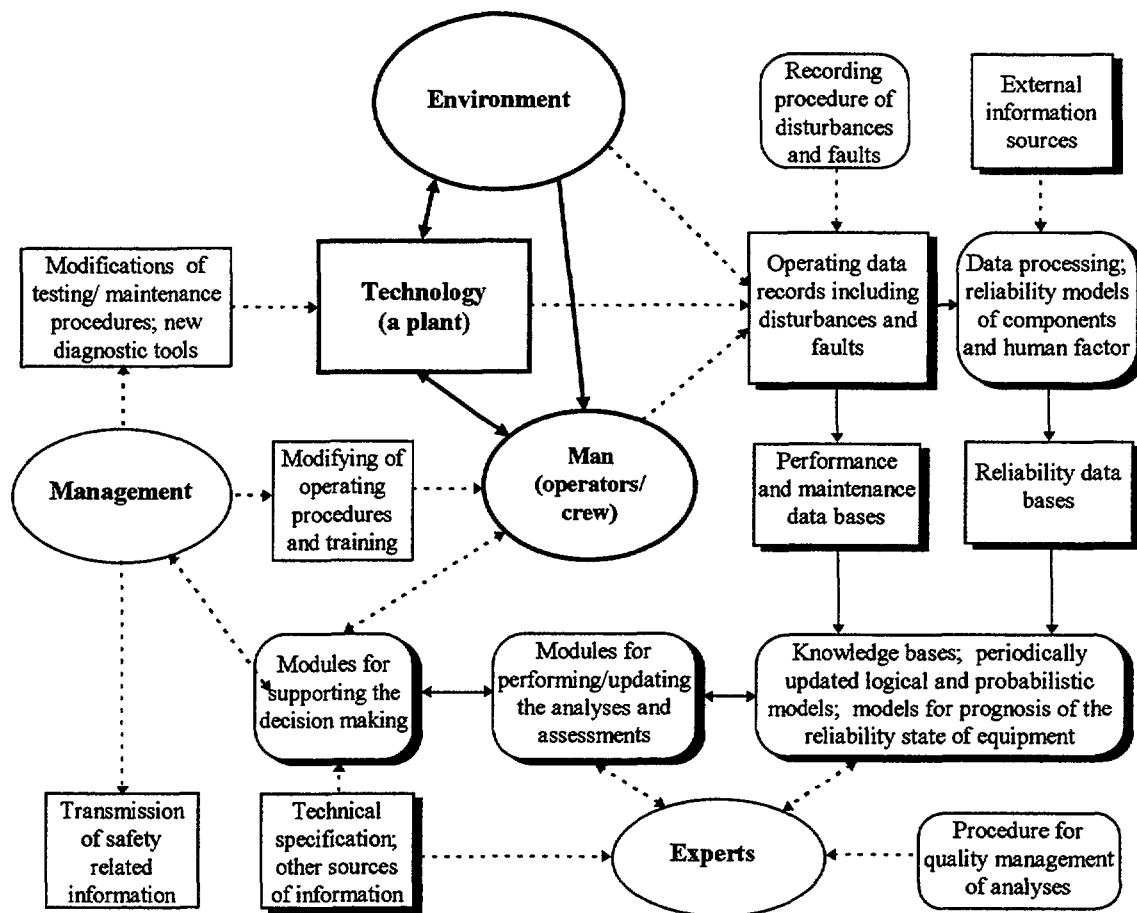


Fig. 1. Schematic illustration of general concept of an integrated approach to the safety management of the man - technology - environment (MTE) system

Different modules are proposed to enable 'intelligent' reprocessing of information for given purpose, e.g. to support decisions concerning a testing strategy for safety systems, to evaluate safety-related limitations of the plant operation due to partial failures. Several diagnosis support modules are conceptually designed to be in accordance with the symptom oriented-operating procedures but with possibilities to support the operators in diagnosing of multiple failures and evaluating the recovery paths. Psychological aspects of human interactions within complex plant during abnormal situations have been also considered.

The concept of a software system IKASM (Integrated Knowledge Acquisition and Safety Management) have been developed and its basic modules specified (Kosmowski 1996). Some of them are modifications of modules of mentioned above expert system REPSAIES. It was assumed that the knowledge acquisition and reprocessing of information within IKASM will be performed according to a procedure of quality management which includes issues of uncertainty representation and treating (Kosmowski 1996).

### 3.2. Recording of failures and analyzing their causes

To improve the performance of the plant it is important to reduce the hardware, software and human induced faults. It can be done effectively if the situation context and possible causes of a failure/ fault will be recognized. A data recording system and a software system should

support the analyst to answer “what”, “how” and “why” questions. In the case of human faults “what” happened, corresponds to the initial conditions, the circumstances and consequences. “How” it happened, corresponds to the source of the error in the task, and “why” it happened to the failure mechanism. Mechanisms of failures can be divided into ergonomics, environment, documentation, communication, training, organization and personal factors. Most promising way to design such software system is to use the expert system technology (Ives 1991).

Identification of causes of human errors can be also valuable for programming of operator training through the development of intelligent computer-assisted instruction systems (Furuhashi et al. 1995).

### **3.3. Adapting/developing HRA methods for knowledge based supporting computer tools**

Theory of human reliability is not yet well established and there are expressed opinions about the necessity to develop the next generation of human reliability models (Dougherty 1993, Lydell 1992). Human reliability can be considered as a more general problem of human factors in complex organizations (Llory 1992). The HRA modeling approaches which now emerge fall into four categories: procedural, temporal, influential and contextual (Dougherty 1993). New HRA approaches should be based more than in existing techniques on psychological aspects of human error (Reason 1990). Some HRA approaches are evolving in the direction of the cognitive simulation environments using the artificial intelligence (AI) methods (Woods et al. 1990). Cognitive modeling is considered to be a fundamental issue for human reliability analysis (Cacciabue 1992).

It has been indicted (Dougherty 1993) that the analysis should remain a fundamental part of the human reliability assessment by examining cases of cognitive problems. The relevant methods should include four major efforts: (1) Identify the goal matrix for the situation and any possible goal conflicts, (2) Develop a functional chronology of the situation including time matrix of the actions and decisions to be made, personnel links and the impact of distributed decision making, (3) Perform a cognitive task analysis, and (4) Perform knowledge acquisition (interview of operators, make simulations and walk-downs). On that basis the quantification, using e.g. SLIM technique, will have substantial justification and the results obtained will be translatable to useful insight for further risk management.

### **3.4. Using the logical/probabilistic models for supporting diagnosis and safety related decision making**

Fig. 2 shows relationship of the diagnosis and decision support modules for transients, abnormal and emergency situations. There are several proposals to design these modules using success trees, heuristic approaches using rule based expert systems, and neural networks (Kim et al. 1990). Bottom middle and right supporting modules in Fig. 2 are designed with regard to knowledge acquired during the logical and probabilistic modeling of the plant. The bottom right decision support module for abnormal/critical and emergency situations is presented in some details in Fig. 3.

The emergency operating procedures (EOPs) used in nuclear power plants are symptom oriented (Kang et al. 1994, Yang et al. 1994). It was assumed that in an early phase of an emergency situation the operators will follow steps of selected EOP, but then they start the identification process of possible causes of current situation which can be supported by a module A (Fig. 3). In the case of a redundant system the possible cases of its total fault are identified in inferring process on a set of rules in the form

$$IF S_i \text{ and } S_j \dots THEN F_i$$

where  $S_1, S_2, \dots$  are symptoms related to a minimal cut set (MCS) and  $F_i$  represents a set of components (failure events) of  $i$ -th MCS. Such rules are developed based on a fault tree constructed for given system (Schwarzblatt 1996). A modified approach to the construction of fault trees have been developed with a special treatment of symptoms assigned to gates and basic events. Because the number of rules considered in inferring process can be large a method has been developed to reduce the searching space using a measure of frequency of symptoms evaluated with regard to the reliability importance of components (basic events).

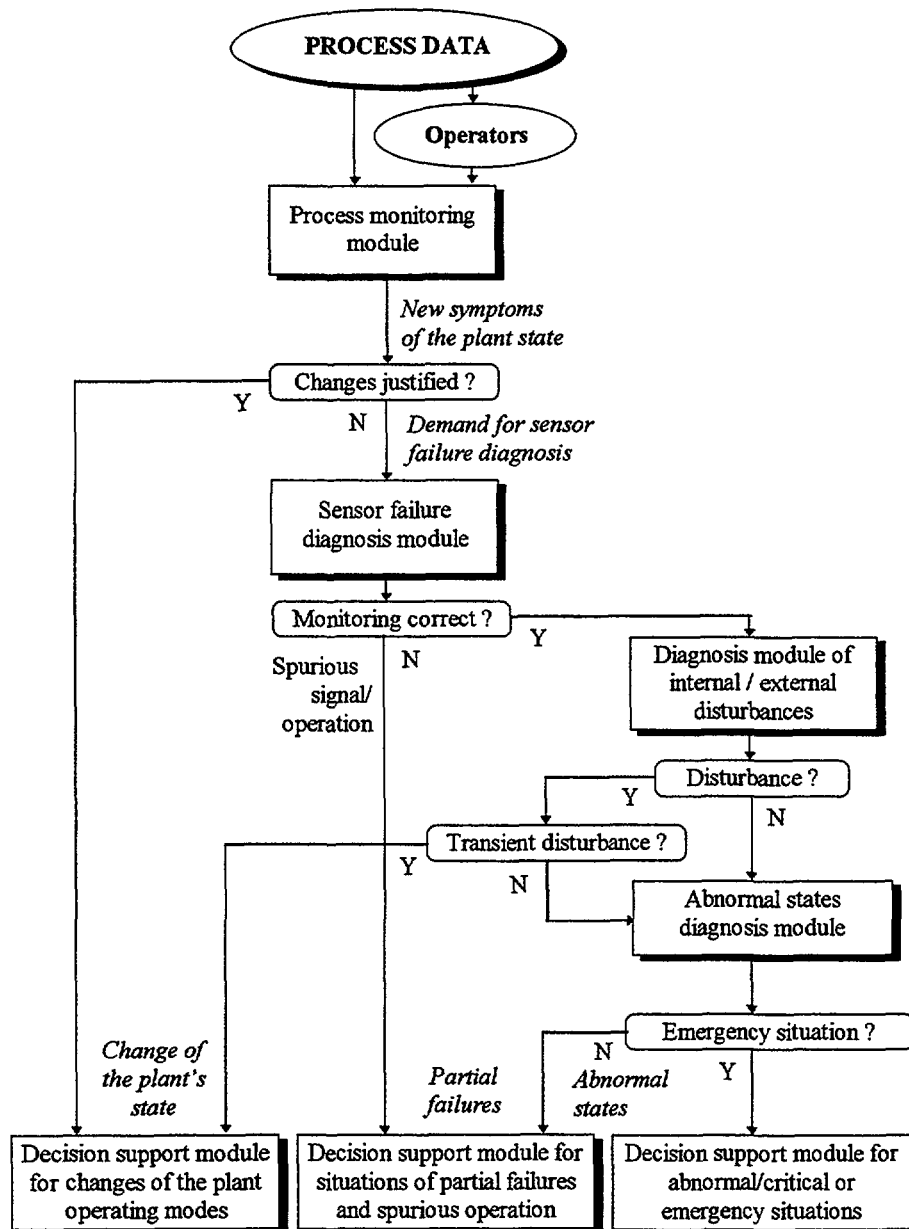


Fig. 2. Relationship of diagnosis and decision support modules for transients, abnormal and emergency situations

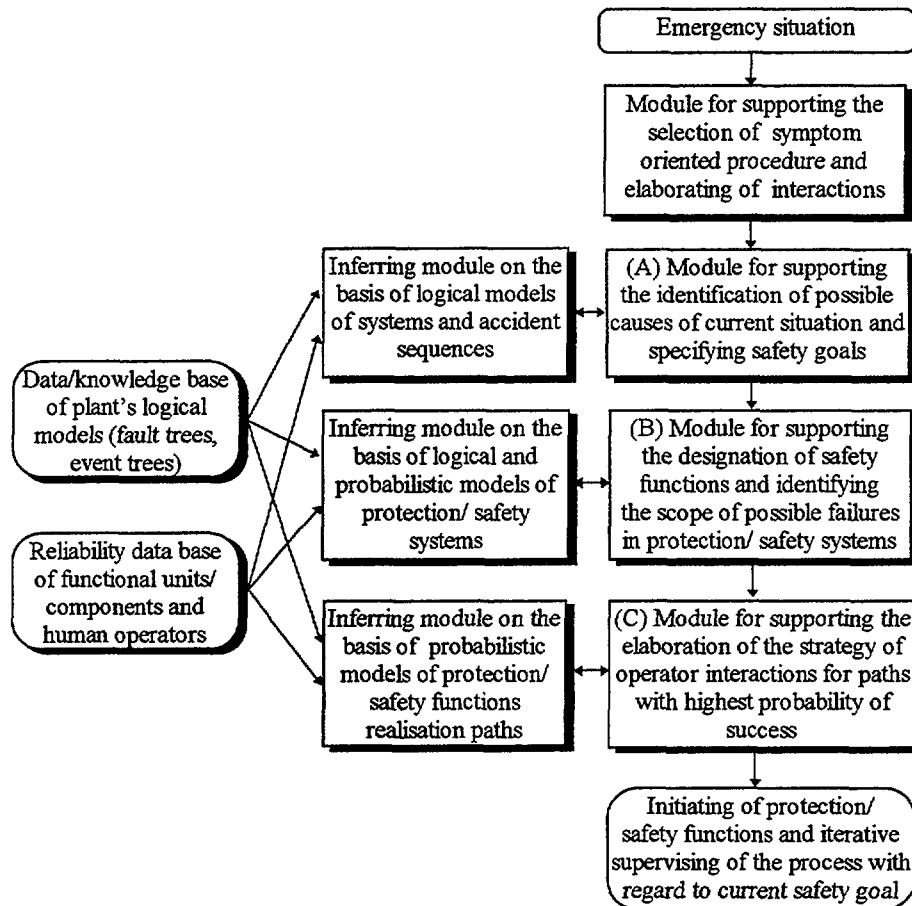


Fig. 3. A proposal to use of object oriented logical and probabilistic models of the plant for supporting the diagnosis and decision making in emergency situations

### 3.5. Quality aspects of logical/probabilistic modeling

There is an increasing interest to apply the probabilistic safety analysis and human reliability analysis not only in nuclear industry to support the reliability and safety related decision making. There are, however, problems of quality of analyses (Rouhiainen 1993) making the results obtained questionable for safety related decision making. There are several important sources of uncertainties:

- defining and decomposing of systems to be analyzed,
- scope and assumed level of details of analyses,
- uncertainties in the statistical data and models available,
- modeling the topological, functional and statistical dependencies,
- modeling the human factor reliability,
- subjectivity of expert judgment (Mosleh et al. 1988),
- issues related to quality control and management of safety analysis.

To manage the quality of safety analyses the standardization concept is needed (Rouhiainen 1993). The safety analysis always includes subjective decisions. However, systematic tools for integrating quality management in the planning and execution of the safety analysis are needed to standardize the practice and to limit individual variations. A promising direction is to develop tools and perform the computer aided analyses, e.g. based on the expert system technology. Quality of such software systems would be accepted by regulatory bodies and users if a proper verification and validation (V&V) procedure were carried out with regard to standardization requirements.



#### 4. Concluding remarks

So called human factor significantly influences the reliability and safety of complex plants and, therefore, should be adequately included and quantified in the overall probabilistic assessments. It is crucial for assuring a high quality of results to be used for safety related decision making. The human reliability analysis is significantly dependent on expert opinions.

To facilitate the HRA and PSA studies the use of the expert system technology is proposed, although designing the software system based on this technology requires considerable effort. According to current practice in performing PSA and HRA three scopes of studies have been distinguished. The design effort is now concentrated on the scope I and II of this software system. The process of PSA and HRA in such knowledge based software system will be documented to enable scrutinizing and auditing of results. Employing the expert system technology would be an important step in standardizing of relevant analyses.

The quality of the human reliability analyses can be improved by selection of the appropriate method for the case considered to include if possible psychological aspects of human actions and errors. The human reliability analysis should be not aimed only at obtaining quantitative results. No less important are qualitative results of analyses which should be considered for improving the man-machine interactions to minimize possibilities to commit errors or to limit their consequences.

Additional research effort is required to include following topics:

- the event driven simulation of the plant and human cognitive performance, including intention failures (Woods et al. 1990), aimed at qualitative and quantitative modeling of the human factor,
- an advanced framework for representing and treating of imprecision and uncertainties in PSA and HRA at different levels of the model hierarchy of the complex plant,
- methods for combining quantitative information from various sources of different quality (credibility) including experts,
- the quantitative evaluation of accident scenarios under uncertainties with regard to different kinds of dependencies (topological, functional and statistical),
- integrated treating of human, organization and management factors in safety analyses.

Artificial intelligence methods, and the expert system technology in particular, offer a promising platform to deal more systematically with some challenging issues of PSA and HRA. However, the development of advanced PSA/HRA methods and related software tools will require a considerable research and design effort. The verification and validation procedures must be also developed related to the quality management procedures.

#### References

- Cacciabue, P.C. 1992. Cognitive modelling: A fundamental issue for human reliability assessment methodology?, *Reliability Engineering and System Safety*, Vol. 38, pp. 91-97.
- Dougherty, E.M., J.R. Fragola 1988. *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. A Wiley-Interscience Publication, John Wiley & Sons Inc., New York.
- Dougherty, Ed 1993. Context and human reliability analysis. *Reliability Engineering and System Safety*, Vol. 41, pp. 25-47.
- Furuhashi Y., Furuta K., Kondo Sh. 1995. Identification of causes of human errors in support of the development of intelligent computer-assisted instruction systems for plant operator training. *Reliability Engineering and System Safety*, Vol. 47, pp. 75-84.
- Hannaman, G.W., A.J. Spurgin 1984. *Systematic Human Action Reliability Procedures (SHARP)*. EPRI NP-3583, Research Project 2170-3.

- Humphreys, P. (ed.) 1988. Human Reliability Assessor Guide. Safety and Reliability Directorate, UK, RTS 88/95Q.
- IAEA 1990 (International Atomic Energy Agency). Use of Expert Systems in Nuclear Safety. IAEA-TECDOC-542, Vienna.
- IAEA 1991 (International Atomic Energy Agency). Case study on the use of PSA methods: Human reliability analysis. TECDOC-592, IAEA, Vienna, April 1991.
- IAEA 1992 (International Atomic Energy Agency). Procedure for Conducting Human Reliability Analysis in Probabilistic Safety Assessment (a draft report).
- Ives G. 1991. Developing expert system to analyze human performance in NPP events. Journal of ENS (European Nuclear Society), Nuclear Europe Worldscan 11-12.
- Kang K.S., Chang H.S., Chang S.H. 1994. Developed of the advanced procedure for emergency operation using task allocation and synthesis of PRA results. Reliability Engineering and System Safety, Vol. 45, pp. 249-259.
- Kim I.S., Modares M., Hunt R.N.M. 1990. A model -based approach to on-line process disturbance management: the models. Reliability Engineering and System Safety, Vol. 28, 1990, pp. 265-305.
- Kosmowski, K.T., K. Duzinkiewicz 1993. An integrated approach in probabilistic modelling of hazardous technological systems with emphasis on human factor. Proceedings of ICOSSAR'93 - the 6th International Conference on Structural Safety and Reliability, Innsbruck, Austria, 9-13 August 1993. A.A. Balkema/Rotterdam/Brookfield/1994, Vol.3, pp. 1889-1896.
- Kosmowski, K.T., K. Duzinkiewicz, M. Jackowiak, J. Szcześniak 1994. Representation of topological and functional-logical knowledge in an expert system for probabilistic safety analysis. IAEA-TECDOC-796, p.123-136.
- Kosmowski, K.T., G. Degen, J. Mertens, B. Reer 1994. Development of Advanced Methods and Related Software for Human Reliability Evaluation within Probabilistic Safety Analyses. Berichte des Forschungszentrum Jülich; 2928. June 1994.
- Kosmowski K. T. 1995. Issues of the human reliability analysis in the context of probabilistic studies, International Journal of Occupational Safety and Ergonomics, Vol. 1, No. 3.
- Kosmowski K T.. 1996. Integrated approach to probabilistic modeling and safety analysis of man-machine systems (in Polish). VI Safety Conference. Kiekrz 10-13.06.1996, pp. 97-104.
- Llory M.A. 1992. Human reliability and human factors in complex organizations: epistemological and critical analysis - Practical avenues to action. Reliability Engineering and System Safety, Vol. 38, pp. 109-117.
- Lydell, B.O.Y. 1992. Human reliability methodology. A discussion of the state of the art. Reliability Engineering and System Safety, Vol. 36, pp. 15-21.
- Moieni, P., A.J. Spurgin, A. Singh 1994. Advances in human reliability analysis methodology. Part I: Frameworks, models and Data. Reliability Engineering and System Safety, Vol. 44, pp.27-55.
- Moieni, P., A.J. Spurgin, A. Singh 1994. Advances in human reliability analysis methodology. Part II: PC-based HRA software. Reliability Engineering and System Safety, Vol. 44, pp.57-66.
- Mosleh, A., V.M. Bier, G. Apostolakis 1988. A Critique of current practice for the use of expert opinions in probabilistic risk assessment. Reliability Engineering and System Safety, Vol. 20, pp. 63-85.
- Poucet, A. 1988. Survey of methods used to assess human reliability in human factors reliability benchmark exercise. Reliability Engineering and System Safety, Vol. 22, pp. 257-268.
- Poucet, A. 1990. STARS: knowledge based tools for safety and reliability analysis. Reliability Engineering and System Safety, Vol. 30, pp. 379-397.

- Reason, J. 1990. Human Error. Cambridge University Press.
- Rouhiainen, V.: Importance of the quality management of safety analysis. Reliability Engineering and System Safety, 1993, Vol. 40, pp. 5-16.
- Schwarzblat M., Arellano J., Mendoza P.R., Smith J.E. 1996. The use of probabilistic safety analysis assessment results for the development of diagnostic and alarm processing expert systems, in: Development of safety related expert systems. International Atomic Energy Agency, IAEA-TECDOC-856, Vienna, pp. 59-66.
- Wang, J., M. Modarres 1990. REX: An intelligent decision and analysis aid for reliability and risk studies. Reliability Engineering and System Safety, Vol. 30, pp. 195-218.
- Woods, D.D., H.E. Pople, E.M. Roth 1990. The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability. Westinghouse Science and Technology Center. Pittsburgh, USA. NUREG/CR-5213, Vol. 1.
- Yang J.-E., Jeong K.-S., Park Ch.K. 1994. Development of an emergency operation supporting system for nuclear power plants. Reliability Engineering and System Safety, Vol. 43, pp. 281-287.

# MODEL PROTOTYPE OF INFORMATION SUPPORT SYSTEM FOR OPERATOR APPROACHES AND REALIZATION



XA9847290

O.B. SAMOILOV, V.A. GALUSHKIN, V.V. DRUMOV,  
A.V. KURACHENKOV, S.L. SHASHKIN, V.M. MORDVINCEV  
OKB Mechanical Engineering,  
Nizhny Novgorod, Russian Federation

## Abstract

In connection with the appearance in a structure of the national regulatory documentation on safety of the requirement about availability of information support systems, the works on development of such system are necessary for making a decision of a question on start-up each NPP. It was developed a model - prototype of the system for Voronezh AST (VAST). Main principles of this model are described in the present report. Besides, similar works on other types of NPPs are carried out.

## Introduction

The necessity of development of the information support system was determined for VAST by the appearance of the appropriate requirement in the national regulatory documentation on safety. According to this documentation, the system should provide the control, analysis and forecast of condition, output of the recommendations on RP (reactor plant) control and check of the operators actions. The recommendations for system engineering were also given by IAEA-commission, carried out an examination of Gorky AST. The commission has paid attention of the AST - developers to necessity of the assistance to the operator in identification of modes with deviations from normal modes of operation and in emergency modes.

The system should realize a determined volume of functions from the moment of start-up of RP, as well as other monitoring and control systems. Therefore, at its development a problem to define a base set of functions for providing of system start-up readiness was put. It was assumed, that the system will be improved during the system operation in accordance with development of technology of information support for operator.

During the work it was used an information on modern work in this sphere, an IAEA - documentation and other sources. The experts of various fields of knowledge, operational staff of NPPs participated in work .

Principle of a system work is the following: on attributes formed by system it identifies a situation from the determined list; informs the operator about its name, list of situation identification attributes and recommendations, appropriated to this situation. The main method of situation identification is a modeling of algorithms of the operators logic activity at the decision of such problem. At a present stage unequivocal algorithms are used only, the attempt of modeling of heuristic thinking is not made.

## The main approaches

As far as the system should assist the operator to identify a situation quickly and correctly in a conditions, especially in complex, at a significant flow of the information, the information is presented by the system should be carefully selected. Its contents and the form of representation should not require additional time from for operator to current situation, on the contrary, it should reduce a time of making the correct decisions.

The work on this system has shown, that it should be in a certain measure separated from a main information system, which, first of all, forms and presents the operator a complete volume of the primary information from object. It is expedient, in first, for allocation of a part, which is directly connected with problems of operator's participation in safety providing ( it is an element of " safety panels").

In second, in accordance with perfection of knowledge in the field of recognition of images, in accordance with purchase of this system operation experience there are inevitable updatings of algorithms, attributes and list of situations, textual and graphic messages and etc. Such updatings should not mention the main information computing system, and, accordingly, should not lead to a reactor shutdown during a time of loading and debugging of the updated software. In this connection it is accepted, that the system should be local one and should consume the information from main information-computing system, to exclude duplication of sources of the primary information.

The considered system has some differences from usual diagnostic systems of the NPP's equipment. This system make logic procedures of recognition of situations, which are required only operative control interferences on the level of RP (reactor plant) as a whole, to prevent an emergency situation or to provide the good safety (to duplicate protection actions when failures of automatic control systems take place, beforehand to reduce capacity for prevention actions of emergency protection and etc.). The situations, when immediate control actions are not required, are subjected to the detailed analysis by usual diagnostic systems, first of all, to define fault elements for the further taking out of operation, repair, replacement and etc.. Search of primary cause of violation, a primary fault element of equipment is not a main task for the considered system. The purpose of the system is to help operator to remove the reactor plant in safe condition. The depth of cause's search of dangerous condition is defined, first of all, by the opportunity of identification of such mode.

The logic procedures of determination of dangerous situations are performed by automatic emergency control systems, including protection system, but they usually start to act at the last stages of situation development. There are situations at early stages of development of deviations, when it is exists an opportunity to prevent remove the normal situation to emergency and situations with postulated failures in protection system, should be analized in considered system. That is why, number of identified situations is essentially more for this system, than only for protection system and other automatic emergency control systems.

In accordance with its purpose, the system defines a situation only from the list determined beforehand on given attributes, having processed them on certain algorithm. At the development of such list a careful selection and improvement of identified situations, attributes and algorithms are performed. The main attention is paid to the absence of crossing of the arrays of input parameters values with different elements of the situation list. At detection of crossings there are took measures to loading values of additional input parameters. At absence of such opportunity the list of identified condition is revised in the direction of integration ( in borders, appropriate to a system designated purpose ). In this case the operator get either situation type in a more common kind, or recommendations on additional analysis of a condition.

So, at growth of temperatures of a coolant in one loop it is identified deterioration of heat removal in it, at growth of temperatures in three loops there are required additional data on reactor's capacity.

In situations with loss of integrity it is possible, that there are no additional sensors for detection of which system leaks. In this case the system can inform, for example, that there is loss of the primary coolant circuit integrity and it should perform an additional analysis - to find the system having leakage and to perform control actions in accordance with appropriate to this

case instructions. Such message, at least, will organize the operator in a situation, will reduce a degree of indefiniteness. The text of appropriate instruction can be called on a display.

Research have shown, that the system should give the operator the name of a situation, list of attributes, on which identification was made and package of the information, appropriate the situation. The package should include the recommendation for control and / or recommendations for the additional analysis of the situation, as well as can include the messages with the forecast of development of a situation in absence of control actions, in particular. The structure of the recommendations should not include recommendations, the fulfilment of which can reduce the safety.

The priority function of a system is an identification of design basis accidents and accidents beyond the design basis, especially seldom met, at which operator has difficulties with identification and fast making of the correct decisions on control (including stress).

Below on a degree of importance there are situations with deviations and abnormalities, when opportune control actions of the operator make possible to prevent operation of automatic protection, including the reactor shutdown.

The reseaches have shown an opportunity and expediency to add the system with some service functions - for example, information support of long-term, monotonous processes; instruction support; logging of the information, if the fulfilment of such functions is not provided by the main information system.

### **The realization of a model - prototype**

The realized model - prototype of a system has the appropriate software, set of operating and data presentation algorithms, depending on the type of reactor plant.

Structurally the system is executed as two interconnected personal computers (PC). The model of a system includes a third PC, which simulate processes in RP and output a data about its condition.

In the list of identified situations are an unauthorized extraction of reactivity control rods, reduction or termination of a heat removal from RP and loss of the primary circuit integrity - first of all, at postulated failures in protection systems. The algorithms of the system operation include elements of algorithms, processing in protection system and taking into account probable failures in these systems, as well as algorithms of search of deviations from normal operation conditions. Besides, some algorithms of the operator's work on identification of condition of reactor plant and systems, on making control decisions are used.

The system performs processing of the information on parameters, received from the main information system. In the model this information flow is simulated by the third computer. On receiving of parameter's values the system compares it with diagnostic setpoints, fixes change of an equipment condition. Thus the attributes of situation, fixed by system, are formed. Further the system performs a comparison of an attribute's set of a current condition with attributes, being present in the base of knowledge and reveals an availability of defined situation (situations).

For the fixing of situations with a movement of control rods, in particular, time of continuous moving is registered and, if it is exceeds a time, required for any normal mode, the name of event with the recommendations to act on EP-4 (emergency protection - аварийная защита - прим. пер.) ( prohibition to move upwards ) and on a key of choice of operation mode of control rods set is formed. At failure of a heat removal automatic regulation system there are fixed deviations of parameters and formed a complex of attributes. Using this attributes the system forms the message about regulators failure and necessity of transfer to remote control or

switching on a reserve channel. If in this or similar situation the emergency signal was generated, but when certain time was over and there was no information of protection rods falling, the system had to form the information for the display presentation. This information should contain an information about current situation with failure of protection the recommendations to the operator for removal of power supply voltage from control rod drives by additional means and etc.

For the textual information presentation to the operator the special form is stipulated (see figure 1). The textual information is presented automatically.

ТЕКУЩЕЕ ВРЕМЯ ЧАС. МИН. СЕК. 00 : 21 : 50		<b>СОВЕТЧИК ОПЕРАТОРА</b> <b>ВАСТ</b>		ДАТА ЧИСЛО МЕСЯЦ ГОД 15 04 1985	
РЕЖИМ СТАТИКА				БУФЕР СООБЩЕНИЙ 3 2 1	
<p>3. ИЗВЛЕЧЕНИЕ РО № 6 СУЗ БОЛЕЕ 20 СЕКУНД</p> <p>ИЗР № 6 &gt; 0      5.175      РАУБ=ИСПРАВ.      ИСПРАВ.</p> <p>ВРЕМЯ(СЕК) &gt; 20      30.000</p> <p>1. ПРОИЗВЕСТИ РУЧНОЙ ВВОД В ДЕЙСТВИЕ АЛГОРИТМА АЗ-4</p> <p>2. ПЕРЕВЕСТИ СВ/СТР В ПОЛОЖЕНИЕ "0"</p> <p>3. В СЛУЧАЕ ПРОДОЛЖЕНИЯ САМОХОДА РО СУЗ НАЖАТЬ КНОПКУ АЗ-1</p>					
СОВЕТ	ПОДДЕРЖКА	КОНТРОЛЬ	ДАТЧИКИ	ЖУРНАЛ	ВЫХОД

Fig. 1. The textual message of a system at unauthorized moving of control rods.

Simultaneously the system forms the graphic information on a condition of reactor, work of its equipment with representation on other display. Mimic schemes presented the main safety parameters - as in the kind of numerical values near the place of measure, as in the kind of the curves of parameters changes for a certain period are used. Also histograms, which present the ratio of current values of parameters to required ones by the static characteristics are used.

The main mimic schemes are functionally oriented at situation's type. For example, scheme related to reactors and heat removal circuits for a situation with of heat removal violation is shown on the figure 2.

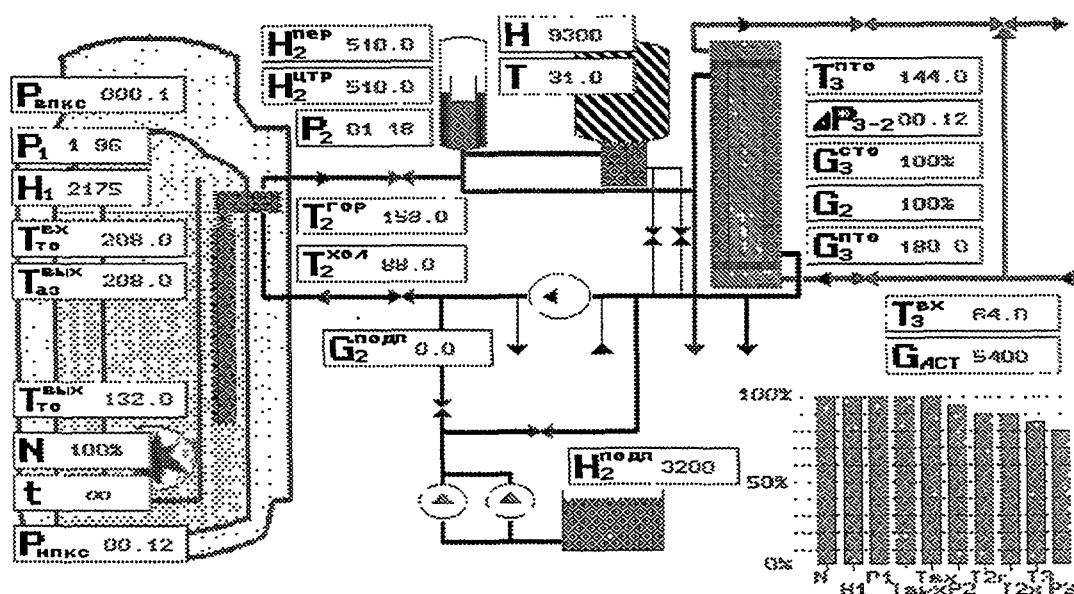


Fig. 2. Mimic scheme, oriented on heat removal situation.

The system provides an operator's help in management of long-term modes of normal operation, which require determined sequence of actions, for example, during reactor start-up.

At occurrence of a incident the information on displays, concerning the current normal process, automatically disappear, and the appropriate emergency textual and graphic information appears on displays, other data can be called by the operator after it.

Contents of the problems and the ways of their decision, degree of improvement are corresponded to the stages of development of different reactor plants and are oriented to system installation, which begins to operate from the moment of NPP comissioning. The problems arising at development are connected with the modeling of the operator's activity; with minimization of additional sensors for the system ( for excluding of imposing of attributes of various situations ), with achievement of high stability of data transmitting systems, with improvement of interaction of software and etc.. Fulfilled work have allowed to get a decision of required problems in a real time scale (within the limits of one updating cycle of the information in information computing system). At the current time it is achieved a degree of readiness, which appropriate to the stage of system implementation related to a certain information computing system at the determined reactor plant.

The experience received to present time shows an opportunity of the solving of arising problems on the base of above-mentioned approaches, as well as an opportunity of further improvement of a system with more complete use of modern achievements in the field of development of the information support systems for the operator and in the field of the theory of image's recognition.

The results of the work provide an opportunity of adaptation of a system to any reactor plant. In particular, the local system of this type can be connected to existing being present information systems at operating NPPs, that allow to increase their safety and to provide a fulfilment of the normative documents requirements related to the information support system.



## CONTRIBUTORS TO DRAFTING AND REVIEW

Aynsley, M.	Intelligent Automation Division, United Kingdom
Bugby, C.	Salford University Business Services, United Kingdom
Chu, C.K.	The CAKE Consortium, United Kingdom
Chudin, A.	Department of Nuclear Reactors, Russian Federation
Dawson, G.	GENSYM, United Kingdom
Drumov, V.	OKB Mechanical Engineering, Russian Federation
Dusic, M.	International Atomic Energy Agency
Ellidge, T.	British Nuclear Fuels plc, United Kingdom
Fandrich, J.	Siemens AG, Germany
Hanski, E.O.T.	Teollisuuden Voima Oy, Finland
Harrop, G.	BNFL, United Kingdom
Haubsensack, D.	CEA/DER/DER/SSAE, France
Irving, A.	Scottish Nuclear Ltd, United Kingdom
Kosmowski, K.T.	Technical University of Gdansk, Poland
Lamb, N.	BNFL International Group, United Kingdom
Tasset, D.	Institute of Protection and Nuclear Safety, France
Turkcan, E.	ECN, Netherlands
Welbourne, D.	Booths Hall, United Kingdom

### **Consultants Meeting**

Vienna, Austria, 27 June–1 July 1994

### **Specialists Meeting**

Manchester, UK, 15–19 July 1996