NUCLEAR ENGINEERING

MASSACHUSETTS INSTITUTE
OF TECHNOLOGY

MODELS AND EVALUATION OF HUMAN-MACHINE SYSTEMS

by Marco Antonio Bayout Alvarenga
Massachusetts Institute of Technology
Department of Nuclear Engineering
Camridge, Massachusetts 02139 U.S.A.

MITNE-304
September 1993

MODELS AND EVALUATION
OF HUMAN-MACHINE SYSTEMS

by Marco Antonio Bayout Alvarenga
Massachusetts Institute of Technology
Department of Nuclear Engineering
Camridge, Massachusetts 02139 U.S.A.

MITNE-304
September 1993

Prepared for:

INTERNATIONAL ATOMIC ENERGY ASSOCIATION
Wagramerstrasse 5, P. O. Box 100
A-1400 Vienna, AUSTRIA

ACKNOWLEDGEMENTS

I would like to express my gratitude to the people at MIT who helped me in many ways in the completion of this report.

Particular thanks must go to Prof. David D. Lanning, my supervisor, who discussed a wide range of topics with me and introduced me to the academic work in the Nuclear Engineering Department (NED) related to the subject of Human-Machine Systems.

Many thanks to members of the NED faculty and staff who granted me interviews to discuss special topics: Prof. Michael Golay, Prof. Lawrence Lidsky, and Dr. John Bernard.

I must thank Prof. Thomas Sheridan of the Mechanical Engineering Department, an expert in the field of Human-Machine Systems. His discussions with Prof. Lanning and me are represented in Chapter 2.2.3.

I must also thank Prof. John Carroll of the Sloan School of Management for the discussions and material about the management/organization of nuclear power plants as well as cognitive models.

Many thanks to the Energy Laboratory staff where I was physically located, especially to Prof. Kent Hansen, S. Weiss, and their secretary Karen Luxton, who helped me in many administrative activities and office infrastructure.

Many thanks to Rachel Morton, who is responsible for the computational resources that allowed me to prepare the draft of this report.

Many thanks to Jack Schryver (ORNL), P. C. Cacciabue (JRC/CEC, Ispra, Italy), Tanabe (NUPEC), and Suniyama (JAERI), who sent me papers in the field of Human-Machine Systems and information about their institutions and who became interested in my report.

Finally, I must thank the IAEA and all its staff for the fellowship that made this research a reality.

CONTENTS

ABSTRACT

The field of human-machine systems and human-machine interfaces is very multidisciplinary. We have to navigate between the knowledge waves brought by several areas of the human learning: cognitive psychology, artificial intelligence, philosophy, linguistics, ergonomy, control systems engineering, neurophysiology, sociology, computer sciences, among others.

At the present moment, all these disciplines seek to be close each other to generate synergy. It is necessary to homogenize the different nomenclatures and to make that each one can benefit from the results and advances found in the other.

Accidents like TMI, Chernobyl, Challenger, Bhopal, and others demonstrated that the human beings shall deal with complex systems that are created by the technological evolution more carefully.

The great american writer Allan Bloom died recently wrote in his book 'The Closing of the American Mind' (1987) about the universities curriculum that are commonly separated in tight departments. This was a necessity of the industrial revolution that put emphasis in practical courses in order to graduate specialists in many fields.

However, due the great complexity of our technological world, we feel the necessity to integrate again those disciplines that one day were separated to make possible their fast development.

This Report is a modest trial to do this integration in a holistic way, trying to capture the best tendencies in those areas of the human learning mentioned in the first lines above. I expect that it can be useful to those professionals who, like me, would desire to build better human-machine systems in order to avoid those accidents also mentioned above.

Marco Antonio Bayout Alvarenga
M.Sc. of Nuclear Engineering

Present Address:

Comissão Nacional de Energia Nuclear
(National Commission of Nuclear Energy)
Departamento de Reatores (Reactor Department)
Rua General Severiano 90 sala 415
Rio de Janeiro - RJ - BRASIL
CEP 22.294-900
FAX: +55-21-295-6098 or
+55-21-239-5074
Electronic Mail: BAYOUT@BRLNCC.BITNET

1. INTRODUCTION: LEVELS OF HUMAN CENTERED DESIGN

The most important concept which we can learn from the automation is: no matter how people may be remote from a specific process control or may be supported by a sophisticated computer-based decision aids system, they are always ultimately responsible in some hierarchical organization level. Otherwise, we would have a world made only of machines. Rouse (1991) defined well this concept: "the design objectives should be to support humans to achieve the operational objectives for which they are responsible". This means that the design must always be human-centered (Bennett, 1993; Nelson, 1993). In other words, taking the example given by Rouse, "the purpose of a pilot is not to fly the airplane that takes people from A to B - instead, the purpose of the airplane is to support the pilot who is responsible for taking people from A to B." In the same way, the purpose of a nuclear power plant operators crew is not to operate the reactor - instead, the reactor is a means by which they can accomplish the purpose of the utility, that is to provide electrical energy with safety to the consumers. Consequently, there are two main objectives in a human-centered design: enhance human abilities and overcome human limitations.

We can find three approach levels of human centered-design. The first one emphasizes the interface level. This is the case of the Card, Moran, and Newell's approach which simulates the human-computer interaction, through a screen and a keyboard. The second one emphasizes the tasks to be executed, for example, in a nuclear power plant control room. The skill(S)-rules(R)-knowledge(K) based levels of the Rasmussen's framework represents this level. The third one considers the whole organization and its external and internal influences during the life-cycle of the design. In this chapter we will describe these levels, except the latter that will be discussed in the chapter 3.

1.1 CARD, MORAN, AND NEWELL'S APPROACH - MODEL HUMAN PROCESSOR (1983,1986)

This approach outlines the main components of the human information processing system: sensorial perception, cognition, and motor function. It is based in the psycho-physiological studies of the human behavior, which is constituted of stimulus-cognition-response, using the classification of the natural science. Reason (1990) considers this approach as a local theory and not a cognitive theory. In fact, it was used to model the temporal performance of expert skills in an interface between a user and a computer. It is not applicable to a qualitative aspects of the cognition such as those found in the manipulation of knowledge representations.

The Model Human Processor uses (Elkind, Card, et al.,1989): "a few parameters to characterize the architecture instead of detailed interacting mechanisms. The Model Human Processor has four memories (long-term memory, working memory, the visual store, and the auditory image store) and three processors (cognitive, perceptual, and motor). Each of these is characterized by parameters. For example, the visual image store decays exponentially with a decay constant of 200 milliseconds (msec.). Ranges are provided for all the parameters so that upper and lower bounds can be computed to take into account the approximate nature of the analysis and the state of knowledge in the literature. A set of accompanying laws of behavior (e.g., Fitt's law, Hick's law, Snell's law) augments predictions from first principles."

A general qualitative model of human performance like the above was provided by Wickens (1989,1991) who introduced a fourth component, attention, in his divided attention and resources theories. Based in the work of previous investigators, Wickens suggested a model of human information processing composed by the following structures:

a) sensory processing-stimuli receptors plus short-term sensory store (STST),
b) perceptual encoding,
c) decision making and response selection,
d) response execution,
e) feedback between response and stimuli,
f) attention resources,
g) memory (long-term memory and work memory).

The working memory exchanges information with the decision making and response selection structures. On the other hand, long-term memory provides learned information to the perceptual encoding.

1.2 RASMUSSEN'S FRAMEWORK (1986)

This framework gives attention to the work tasks to be executed and therefore emphasizes the cognitive characteristics of the human being. The framework is composed of three levels: skill-based behavior, actuated by the perceptual/motor systems and activated by time-space signals; rule-based behavior, related to the individual training with familiar work situations, represented by stored procedures rules and activated by signs; knowledge-based behavior, activated by symbols, related to the unfamiliar work situations without preconceived rules, when the individual has to use a creative reasoning to achieve the goals. In the last two levels (rules and knowledge) we have the following steps in a decision making: recognition or identification of the situation, association state/task or decision of a new task, selection of stored rules/procedures for the tasks or planning of the new task, respectively.

It is not difficult to relate this framework with the Wickens and Card models. In fact, we have the following associations:

WICKENS,CARD	RASMUSSEN
sensory processing (perception)	feature formation for the sensory input(S-L)

perceptual encoding (perception)	recognition(R-L)
	identification(K-L)

decision making (cognition)	association state/task(R-L) decision of task(K-L)
response selection (cognition)	stored rules for task(R-L) planning of task(K-L)
response execution (motor)	automatic sensor-motor pattern(S-L)

In the last years, many concepts from the parallel distributed processing have been arisen, the most important was the notion of a human memory organized as a parallel distributed processing system instead of a central processor. This system is composed of a set of specialized processors covering all aspects of mental function, without a control of a central processor. This lead to the Baar's concept of global work space (Reason, 1990) a kind of working memory where the specialized processors can interact each other.

After we have shown a general qualitative human model, we need theories to quantify that general model. Card's approach was described, but in view of the limitations of applicability (human-computer interface), we will discuss other alternatives in chap. 2.

2. ENGINEERING THE HUMAN-MACHINE SYSTEMS - ALLOCATING FUNCTIONS FOR DESIGN

2.1 GENERAL PRINCIPLES FOR ALLOCATING FUNCTIONS BETWEEN HUMAN AND MACHINES IN THE INITIAL DESIGN

Function allocation between human and machines constitutes the central problem in the human centered design and can only be done through the allocation-design-evaluation cycle until the final design has been achieved after several passes in that cycle. Then, an initial allocation is presupposed, followed by an initial design and evaluation through human performance workload indexes.

In the initial allocation we could use classical methodologies and principles found in the literature of ergonomics, which can be classified in three groups (Rouse, 1991).

In leftover allocation, the designer looks for automating every function that can be done by the technology state-of-art and the leftover is given to the humans.

In comparison allocation, each function is analyzed to fix skill requirements and performance criteria. By comparing human and machines abilities (see Meister, 1985, 1991, in case of comparison tables), the function are classified in four groups (IAEA, 1992):

a) functions which must be automated,
b) functions which are better automated,
c) functions which should be done by humans,
d) functions which should be shared.

To identify the functions, the Task Analysis methodology (see Meister) is used. Additionally, general criteria should be used for choosing the best performer.

FUNCTIONS WHICH MUST BE AUTOMATED
(skills in which machines are better performers)

a) rapid or long-term processing of large quantities of data,

b) tasks requiring high accuracy information (data processing or manipulation),

c) those requiring high repeatability,

d) those requiring rapid performance,

e) those where the consequences of error are severe,

f) those where errors can not readily be retrieved (corrected),

g) those which must be carried out in an unacceptable hostile environment.

FUNCTIONS WHICH ARE BETTER AUTOMATED

In this category, lie the functions that can be performed by humans but in view of certain task characteristics, are better performed by the machines. These characteristics are: lengthy, high consistency, high accuracy, risk involvement, and boredom/monotony.

FUNCTIONS WHICH SHOULD BE ASSIGNED TO HUMANS

Function which require heuristic, inferential and creative knowledge or flexibility in the actions, as in the case of accidents situation (knowledge-based behavior).

FUNCTIONS WHICH SHOULD BE SHARED BETWEEN MEN AND MACHINES

The leftover after the three categories above is found here. Nevertheless, some functions can be analyzed through the third group of allocation methodologies as follows.

Economic allocation

In this method, for each function that can be shared, we have to decide which is more economical of these two:

a) to select, train, and pay a person to perform the function, or
b) to design, to develop, and maintain equipment to perform the same function.

The IAEA(IAEA-TECDOC-668, 1992; Bastl et al., 1990) has stated some basic principles to help in this initial functions allocation. They are:

a) Human cognitive strengths should be fully exploited by the designer. There are some things that man does better than machines. The three disciplines of engineering, ergonomics and psychology must work in harmony to exploit these strengths.

b) Automation should be used to protect society from the fallibility and variability of humans. This requires a detailed analysis of the tasks which are proposed for man, the possible errors and the possible consequences. Areas of risk should be automated if this is practical, feasible and cost-effective.

c) Automation should start with the most prescriptive procedural functions first. Those manual functions that are memorized or performed in a prescriptive manner by detailed procedures should be automated whenever possible.

d) Automation should be used to reduce human cognitive overload. Humans can suffer from information overload and consequent mental overload. This can occur from high information rates, competing tasks or task complexity. Wherever the designer can predict this problem, or whenever operating experience demonstrates it to be so, automation should be used to relieve the human of that part of the function which causes the problem.

e) If possible, tasks which have been assigned to automation should not be returned to the man when the automation fails. In general, humans do not act effectively as a back-up to a machine. In most cases, the reason for using a machine is that a human capacity has been exceeded. Consequently, human back-up is unlikely to be appropriate. Machine performance is more consistent if not more available so humans make a poor substitute. Also, human capabilities grow stale with misuse. When a machine fails, to dump a load of tasks onto an unsuspecting operator is a prime example of poor design.

f) The correct process for balancing human and machine actions should become an institutionalized part of system design. The right balance will not emerge until there are processes in place and in common use by designers, operators, and management, which reflect the correct principles and embody proven practices.

g) The evaluation should include consideration of the professional motivation and psychological well-being of the operator.

2.2 EVALUATION OF THE HUMAN-MACHINE SYSTEMS: ESTIMATION OF PERFORMANCE AND WORKLOAD TO VERIFY THE FUNCTIONS ALLOCATION

Workload has two faces. If the workload is too high, humans become stressed and fatigued, with the consequent loss of performance. If the workload is too low, they become bored and distracted. Approaches to assessing workload are as follows (Rouse, 1991, 1990):

a) primary task performance - workload must be high when performance can not be sustained;
b) secondary task performance - workload on primary tasks must be high when performance on secondary task degrades;
c) physiological indices (e.g., eye pupil diameter) change to reflect high workload;
d) subjective reports - reported experiences of high workload are indicative of high workload.

For the design, we need predictive approaches, which request some kind of measurement. In this case, time is the central parameter for measuring, in view of the fact that workload is too high, when humans does not have enough time to do the tasks allocated to them. The aviation industry has many examples of this kind of approach.

2.2.1 APPROACHES TO WORKLOAD

The multiple resources theory as an approach to workload is due to Wickens (1989,1991). As we discussed earlier, Wickens sees the humans beings as information processors. The information resources are distributed among the perceptual, cognitive and motor processors as visual-verbal, visual-spatial, auditory-spatial, cognitive-verbal, response-manual, response-vocal channels. A predictive workload index algorithm (WINDEX) was developed by North (1989) adopting many assumptions of the multiple resources theory. WINDEX assigns resources demand levels (rated 1-5) to different channels or processing systems as a function of the task and the task characteristics. There is a conflict matrix with penalties for concurrence between two channels of information processing. Two tasks which have common processing channels, for example, will be highly penalized. The workload computation is achieved by multiplying that task demand vector by this matrix.

QUEUING THEORY (WLAM)

Elkind, Card, et al. (1989) proposed a Workload Analysis Model (WLAM) Structure, that combines the particular features of the PROCRU, HOS, INTEROPS, and WINDEX. After the workload index (WL) calculation, the value is compared to a "maximum workload" criterium (WL_m). If $WL<WL_m$, the next time point is calculated and WL is recompute. If $WL>WL_m$ (excessive workload), all tasks are checked about their priority levels. Those with low priority are placed in a queue, and the others are joined to the new tasks for next time point. Then we have again the competition between them. The highest priority task in the queue will enter the matrix if:

a) it has higher priority than tasks already in the queue, or
b) the computed workload with its inclusion does not exceed WL_m.

Of course, discrete tasks leave the queue after their completion.

Because of this, WLAM needs a time-line analysis chart with four vectors defined by the user for each task:

1. task priority,
2. a duration of time within which the task could be rescheduled,
3. estimated completion time for the discrete tasks,
4. demand level.

Another important concept arising from these time-sharing is the performance deterioration in view of the delay induced until the task reaches the head of the queue. If the working memory is involved, we can use the Card, Moran, and Newell's method (1983) to calculate the decay rate, as described in chapter 1.1.

In the case of monitoring and detection tasks, the percentage of resources allocated to the visual or auditory channels becomes a fundamental parameter to be used in the signal-to-noise ratio deviation, technique employed by PROCRU for calculating the resolution of visual and auditory inputs.

2.2.2 ANALYTICAL EVALUATION

2.2.2.1 MODELLING THE HUMAN-MACHINE INTERACTIONS - TYPES OF MODELS AND CONTROL PARADIGMS

According to the Rasmussen's framework (1986), the human performance models types can be classified as follows:

a) Knowledge-based behavior (AI/ES)

a.1) Psychological problem solving methods (AI)
a.2) Information flow models, production systems (AI)
a.3) GPS - General Problem Solver (AI)

b) Rule-based behavior

b.1) Decision theory (prescriptive-mathematical, descriptive-behavioral, explanatory-psychological)
b.2) Social judgment theory
b.3) Information integration theory
b.3) Attribution theory
b.5) Fuzzy set models (AI)
b.6) Production systems (AI)
b.7) Scripts (AI)

c) Skill-based behavior

sensorial perception (detection)

c.1) Signal detection theory
c.2) Estimation theory

motor function

c.3) Manual control models
c.4) Optimal control models

attention allocation

c.5) Sampling theory
c.6) Queuing theory

AI = artificial intelligence
ES = expert systems

Each representation has a human analogy (Rouse, 1991, 1980):

a) The ideal observer (estimation theory) assumes that humans deal with observed uncertainties in an optimal manner, subject to various behavioral constraints such as noisy perceptual processes and limited memory.

b) The servomechanisms (control theory) analogy assumes that humans are optimal feedback controllers subject to behavioral constraints that include noisy perceptual and motor processes, reaction time delays, and sluggish neuromotor responses.

c) The time-shared computer analogy (queuing theory) assumes that humans optimally sequence and perform tasks subject to constraints such as limited time, switching times, and perceptions of priorities. As we saw in the chapter 2.2.1, queuing theory can be used to predict workload, computer average task waiting times, average number waiting, and fraction of time busy.

d) The approximate reasoner analogy (fuzzy theory) assumes that humans are logical reasoning machines subject to constraints such as not having crisp knowledge of how things work, what connects to what, and which elements belong to different sets.

e) The knowledge-based system analogy (rule-based models) assumes that humans knowledge is encoded explicitly in verbal IF-THEN statements rather than implicitly in equations or routines of some sort. Behavioral constraints are characterized in terms of knowledge limitations.

f) The pattern-recognizer analogy (statistical models) assumes that people perform a direct mapping from displayed or perceived features to conclusions or actions, based on statistical relationships drawn from past experience. Statistical models includes neural network models.

Beyond the above models we need additionally models of working memory and cognitive architectures to integrate all of them. In the literature (see Card, Elkind, et al., 1989), 32 phenomena were identified and classified into: (1) the size and decay of verbal working memory, (2) contextual effects, (3) representations effects, (4) chunking, (5) skilled memory, (6) spatial working memory, and (7) phenomena related to long-term memory.

SIZE AND DECAY OF VERBAL WORKING MEMORY
(limits imposed by working memory on the processing of verbal information)

1. Short-term memory (STM) decay
2. Immediate memory span
3. Buffer span (or running span)
4. Effect of item type on span
5. Effect of word length
6. Temporal span
7. Articulation rate effect
8. Performance despite loading

9. Suffix effect

CONTEXT EFFECTS
(effects of earlier or later items in working memory on each other)

10. Recency effect
11. Primary effect
12. Release from proactive interference
13. Episodic memory

WORKING MEMORY REPRESENTATION
(the way in which items in working memory are actually coded or represented)

14. Phonological similarity effect
15. Unattended speech effect
16. Sequential output bias
17. Independence of item order information

CHUNKING
(Items in working memory comprise links to elements in long-term memory, rather than the elements themselves)

18. Chunking of recall
19. Between-chunk pauses
20. Opaqueness of chunks

SKILLED MEMORY
(few ways in which humans can optionally control process in working memory so as to improve recall)

21. Efficacy of rehearsal
22. Efficacy of mnemonics
23. Efficacy of elaboration

SPATIAL WORKING MEMORY

24. Multiple buffers
25. Spatial memory disruption
26. Spatial imagery interference

LONG-TERM MEMORY EFFECTS

27. Total time hypothesis
28. Elaborating versus maintenance rehearsal
29. Long-term recency effect
30. Simultaneous long-term recency effect
31. Learning despite impaired working memory
32. Weber's law time for discrimination.

Five main models cover the major effects above described:

a) Wangh and Norman (1965)
b) Atkinson and Shiffrin (1968)
c) Baddeley and Hitch (1974; Baddeley, 1986)
d) Anderson's ACT model (1983)
e) Schneider and Detweiler's connectionist/control model (1988)

These five models can be divided into two groups: those that are largely models of the working memory component itself (Wangh and Norman, Atkinson and Schiffrin, Baddeley and Hitch) and those in which the working memory model is part of a larger human cognitive architecture (Anderson's ACT and Schneider/ Detweiler). The second group of models is more computationally oriented than the first. Schneider and Detweiler's model (1987) has the most detailed computational coverage of working memory, but it is not yet part of a comprehensive cognitive architecture, which is the case of Anderson's ACT model that is more integrated with such architecture, but has only the lower coverage of phenomena.

Concerning to cognitive architectures (see Elkind et al., 1989), there are two main types: architectures that model human processing in terms of symbolic processing (symbolized architectures) and those that use some sort of subsymbolic processing, represented in graphs with weighted links (connectionist architectures). Between them are the hybrid architectures, like CAP2(Controlled Automatic Processing 2, Schneider and Oliver, 1991).

The most integrated of the symbolized architectures are ACT (Anderson, 1983) and SOAR (Rosenbloom, Laird, Newell, 1991; Newell, 1990). At the opposite extreme from integrated symbolized models, such ACT and SOAR, are models like the Model Human Processor (Card, Moran, and Newell, 1983) that use a few parameters to characterize the architecture instead of detailed interacting mechanisms. Between them, there is the Holland, Holyoak, Nisbett and Thagard (1986) theory of induction.

Connectionist models are attractive because they are more human brain neural net like (see McClelland and Rumelhart, 1986, PDP-Parallel Distributed Processing). In the present state-of-art, these models have been most successful at pattern recognition tasks.

Next, we will analyze each one of the representations in the Rasmussen's framework plus ACT (Adaptive Control of Thought), SOAR(States, Operators, and Results), and CAP2(Controlled Automatic Processing 2). The chapter will include a comparison of blackboard architectures.

CONTROL PARADIGMS (MOTOR FUNCTION AS A SKILL-BASED BEHAVIOR)

Basically, we have three types of control paradigms: manual control, supervisory control and collaborative control. In the manual control human being is merely a system component that produces outputs as function of the sense inputs. In the supervisory control, humans supervise an automated process, which is designed to perform directly the allocated tasks.· In the collaborative control, both humans and machines are supervisors, and the functions are dynamically allocated between them. It requires a complex operator support system together with a human machine interface; this will be discussed in chapter 2.2.3. From the point of view of Sheridan's supervisory control paradigm (Sheridan, 1992), which considers ten levels of automation, manual control would be the level one (humans does the whole job) and collaborative control would be the range between 4 and 6 (computer selects action to be approved or stopped by humans). Levels 2 and 3 (computer helps humans to supervise the process) would be supervisory control. Total automation will be 7 to 10 (computer does the whole job and then informs the humans).

Before analyzing the control models in detail, it's useful to point out that this kind of approach must not be seen as simple models of human motor, perceptual and cognitive activities, because they give important parameters for the evaluation these activities in other models more sofisticated.

Manual control models

Classical control theory - the human being is considered a servomechanisms trying to eliminate feedback errors in a closed-loop system (the Wiener's cybernetic point of view). The cross-over model (McRuer et al., 1965, in Stassen, 1989) is representative of this category and is based on the stability criterion of closed loop. These models help the system designer to judge if the control/handling characteristics are adequate in order to allow a well trained operator ("the servomechanism") to perform the tasks with a acceptable workload. This is more applicable to pilots than the NPP operators. Anyway, this model is particularly applicable to the manual control of single input/single output linear time invariant systems (Stassen, 1989; Allen, 1989; Rouse, 1980).

Optimal control model (OCM)

This theory considers the human being as optimal controller (Stassen, 1989; Allen, 1989; Levinson, 1989; Rouse, 1980). It means that a well-trained human operator is able to know the disturbances affecting the system, the human response capability, and the criteria which defines optimal control. The human limitations here are: processing time, inaccurate observation, inaccurate generation of system output, and limb dynamics. These limitations are modelled by means of a time delay, an observation noise, a motor noise, and a neuromuscular system, respectively. State equations model the system that the operator sees through a state estimation, represented by a Kalman-Bucy optimal filter. The system controlled is considered linear and the cost criteria are quadratic and the noises are white and Gaussian (Kleinman, Baron, and Levinson, 1971, see in Levinson, 1989). The model allows multi-variable control.

The most complete models of supervisory control (see in

Sheridan, 1992; Rouse, 1980; Stassen, 1989) are the observer controller decision model (Kok and Stassen, 1980) and PROCRU (Baron, Muralidharan, Lancraft, and Zacharias, 1980). The former is derived from the optimal control model, assuming that the prediction for time delay, the time delay itself and the neuromuscular system can be neglected for slowly responding processes. There is also a decision-making element to decide, on the basis of the estimated state, when to observe (Kalman filter) and when to make Kalman gain adjustments. Papenhuijzen and Stassen (1987, see in Sheridan, 1992) extended this model to include the use of the fuzzy set theory which represents better the operator knowledge in a linguistic form. PROCRU will be analyzed in the item 2.2.2.2.B.

SHERIDAN'S SUPERVISORY CONTROL PARADIGM

Sheridan's modelling should be complemented with the knowledge-based level of Rasmussen's framework. In this model, the control systems has an internal representation of the human supervisor or operator and has the capacity to predict human behavior. In such situation, the control system, that is integrated to the system, can advise the operator through operation support systems, or, in case of human error or failure, take the proper actions to bring the system to the normal operation. At this level, the control and operation support systems must work with knowledge bases and therefore, these systems can be considered knowledge based expert systems.

Later, we will see that the limitation systems at the KONVOI-KWU PWR plants work as a kind of operation support system between the rule- and the knowledge-based levels. Also, the new designs for French N4 PWR and OHI-3/4(PWR) and Kashiwasaki-Kariwa 6/7(BWR) in Japan provide examples of supervisory control.

A good human model must have sub-models for each one of the levels in the Rasmussen's framework. Many models work at the skill and rule based levels. On the other hand, control systems theory works well at the skill-level but not at the rules-level, where it needs help from cognitive techniques, one of the most common are the artificial intelligence IF-THEN production rules.

In case of accidents, however, the situation urges for a creative behavior, due the fact that the operators crew must face sometimes with non-anticipated accidents types and a multiple accidents sequences. This is work for the knowledge-based level that is more difficult to model. In the literature there are models which try to represent this knowledge through the same production rules seen in the rule-based level. But many authors consider this a simple way to reduce from one level to another.

Another concept to be given in the supervisory control is the difference between computer control and computer support. While the control system actuates in the lower level (skill level), in the other levels there is an interactive human-computer interface responsible for the high levels control area for the support of the operation crew. The question not totally solved is if there should be an interaction between the control systems and the support systems in all levels. This question will be discussed again in the chapters concerning the new design of control rooms.

Rasmussen observed that the supervisory control paradigm could be characterized by three different dimensions: functions of supervisory control, allocation of functions and attributes of trust (Rasmussen, 1990). But, first all, he extended the structure of the supervisory control to encompass the entire sociological-technical system. The structure was well applied to automated robot systems consisted of two interactions completely separated: human-computer and process-computer. Moray (1986, see Reason, 1990) defined those two interactions as TIS(Task-Interactive System) and HIS(Human Interactive System). This latter reduces the operator's workload but man can define goals without actually doing the tasks of control, which is attribution of the TIS. The only reason to keep the humans present in this structure is that they are important in case of emergencies when the knowledge-based reasoning is vital for the situation and the computers, as we already stressed, can not deal with the same efficiency in this level.

Rasmussen added other levels of interaction concerning the following control elements: operation and maintenance staff, technical management, executive management, economical and social environment, regulatory agencies and design team. As a consequence, the roles of supervisors and subordinates become more obscure. The operation of nuclear power plant is a dynamic process as well as its safety level. During the operation, the operators and the maintenance crew could note that the installation must suffer some design modifications in the hardware or in the procedures and even the personnel performance are affected by the training and management systems.

Other important questions which arises from this observation is if all these levels are prepared to realize the functions of the supervisory control described by Sheridan: planning, teaching, monitoring, intervention and learning. Monitoring is a perceptual-motor skill. Teaching and intervening are rule-based functions. Planning and learning are knowledge based functions.

Concerning the attribute of trust, we have: reliability, robustness, familiarity, understandability, explication of intention, usefulness, dependence.

At this point, it is useful to mention what Bainbridge(1987, see in Reason, 1990) called "the ironies of automation". First, the designer's errors (latent errors, Reason, 1990) contribute a lot for the accidents and the incidents. Second, they leave the operator "to do the tasks which the designer can not think how to automate".

There are other consequences of the automation. One is the operators can become de-skilled in view of the fact that they have very few opportunities for practicing in a highly automatized plant. So, when an emergency occurs, they can not have the required manual control skills to face the problem. The designers have provided support systems, including automatized procedures in screens, but, once more there is no guarantee that all the plants conditions are covered and the beyond design accidents will bring the operators to the same situation when they have to use their knowledge-base reasoning. Bainbridge said about this: "perhaps the final irony is that it is the most successful automated system, with rare need for manual intervention, which may need the greatest investment in operator training".

Reason explain this situation in other words:" human supervisory control was not conceived with humans in mind. It was a by-product of the microchip revolution...the active errors of stressed controllers are, in large part, the delayed effects of system design failures."

SENSORIAL PERCEPTION

Signal detection theory

"Given probability distributions of noise and signal plus noise, signal detection theory can lead to prediction of the probability of misses and false alarms in a detection task. The main difficulty seems to be in determining how the human's observations produce a particular value of likelihood ratio. The theory has more application in experimental psychophysics than in systems design" (Rasmussen, 1986).

Estimation theory

It is based in the basic Gai and Curry (1976, see Sheridan, 1992) theory that considers the human observer as an optimal Kalman filter (ideal observer). As we have seen, Kalman filters are used to estimate the system state in the optimal control. However, comparative experiments must be carried out to verify the performance in closed-loop versus open-loop.

ATTENTION ALLOCATION (STATISTICAL INFORMATION THEORY, STEIN, 1989)

Sampling theory

It is based on Nyquist's information sampling theorem, which states that the information from a source having spectral components with an upper limit frequency of w hertz can be completely represented by an observer who samples 2w times per second (Senders, 1964, see in Sheridan, 1992). Two limitations are apparent in this model: (1) correlation between displayed signals and (2) the interaction between control behavior and visual sampling.

Queuing theory

This theory considers tasks demands with Poisson or exponential distributions and queuing models of attention allocation postulated that humans optimize their performance according to a service strategy considering the arrival sequence and task priority. Queuing theory models have been used with success in the monitoring task modelling. Contributors for this were (Stein, 1989; Rouse, 1980): Carbonell (1966), Carbonell et al (1968), Senders and Posner (1976), Rouse (1977, 1978, 1979). Due the fact the queuing theory can be used in both perceptual and cognitive tasks, it is an approach normally found in the models. The theory has four insufficiencies pointed by Wickens: lacking of 1) parallel processing, 2) structural alteration effects (multi-tasks interference), 3) difficulty insensitivity, and 4) doesn't deal easily with tasks which can not be expressed in terms of time demand. It is important to consider also the resources models of human parallel (concurrent) processing that have been developed to account for these phenomena. As we have seen in the chapter 2.2.1, approach to workload, this can be done almost entirely by joining the WINDEX model with the queuing theory plus the characteristics of attention allocation as "observation noise" used by the optimal control model (see WYLAM).

RULE-BASED BEHAVIOR

Models of human judgement (Hammond, 1980)

In the rule-based behavior, signs are used to identify and recognize the system state. This process is not based in symbolic reasoning and must be based on empirical evidence (Rasmussen, 1986).

Decision theory (prescriptive) - Hammond, 1980

It is a mathematical model based on the expected utility theory. It deals with one person without full knowledge of the task situation and without feedback about the effect of decision (Rasmussen, 1986).

Behavioral decision theory (descriptive) - Hammond, 1980

It is based on the Bayesian probability theory. As in the latter theory, it treats the cognitive process of continuing probability and utility as "aggregation". This concept comes from the economic theory and doesn't have psychological basis (Rasmussen, 1986).

Psychological decision theory (explanatory) - Hammond, 1980

This theory uses probabilities but predicts when people replace the laws of statistics by heuristic. As the events operate from convenient signs, not defining attributes, the theory fails to develop valid statistical intuitions, because the events are normally not coded in terms of all factors that are crucial to the learning of statistical rules (Rasmussen, 1986).

Social judgement theory (Hammond, 1980)

The primary intention of the approach is not to explain, but to describe human judgement processes. The approach has been to assume that even though the person is not aware of the process , he will know the cues on which the process is based (Rasmussen, 1986). Experiments demonstrated that:

a) the judgment process tends to be very simple,
b) the process tends to be inconsistent (used rules vary much),
c) experts can differ considerably in the use of cues and weights,
d) people are not good to describe their judgements.

Information integration theory (Hammond, 1980)

The aim of the theory is to discover psychological laws that intervene between stimulus and response in quantitative terms of a "cognitive algebra" (Anderson, 1974; Rasmussen, 1986).

Attribution theory (Hammond, 1980)

"Attribution" can be considered a special case of inference or judgement. The theory is primarily concerned with inferences about causality, i.e., causal attributions (Rasmussen, 1986).

ARTIFICIAL INTELLIGENCE (AI)

AI models are even the best available tool for simulation of human information processing, not only for the design of intelligent support systems, but also for representing the human part in simulation of human-machine systems (Rasmussen, 1986).

AI provides models for intelligent systems,which may be either human or machine. A intelligent system is basically a structure composed by a knowledge representation as set of symbols and a reasoning mechanism using those symbols to hold and convey semantic knowledge (Sage, 1992).

Knowledge representation (Sage, 1992)

There five main representations and reasoning mechanisms: semantic networks, production systems, schemes, scripts and frames.

Production systems

"The basic idea behind a production system is that there exists a set, a production, or rules, in the form of various condition-action pairs, generally in the forms of IF-THEN combinations. Initially, these were exclusively explicit rules, although there is much current interest in incorporating fuzziness and imprecision introduction rule concepts for automated reasoning", through the fuzzy set theory (Sage, 1992).

Semantic networks

The knowledge is represented in terms of nodes, that represent objects, concepts or events, and links between the models to represent their interrelations. This allows a knowledge representations that is expressed in complex natural language. The size of the semantic network makes difficult its computational implementation. To solve this problem Minsky created the concept of frames (Sage, 1992).

Frames

It is a chunk of knowledge for representing a stereotyped situation. Although this theory attempts to break the knowledge in simple fragments, is still problematic its use in the computer because of the possible explosion of knowledge combination (Sage, 1992).

Schemes

The schema theory suggests that people have images or schemes that they use for comparison purposes (Sage, 1992). There are three problems in this theory (Anderson, 1983):

1) it blurs the procedural declarative distinction and leaves unexplained all the contrasts between procedural and declarative knowledge;

2) the units of knowledge tend to be too large. A production system having smaller units permits a richer possibility for recombination;

3) the size of schemata also makes it difficult to construct theories about their acquisition.

Scripts

"Like schemes and frames, script is a knowledge structure about a stereotypical sequence of frequently performed actions. They capture the action-event relations in situations that are so frequently encountered that the need for formal methods of problem solving seldom arises. They are self-contained knowledge chunks. As a consequence, it is difficult to transfer knowledge from one script to another. Also scripts may lack understanding" (Sage, 1992).

These expert systems or intelligent systems modelled as above only model human behavior at the rule-based level and lacks the ability to retreat to knowledge-based problem solving - it is only able to interpret in formation as signs . "Therefore, the systems fail abruptly when the environment changes and no longer conforms with the experiences behind the rules"(Rasmussen, 1986).

KNOWLEDGE-BASED PROBLEM-SOLVING MODELS

"The best model is still the General Problem Solver (GPS) from Newell/Simon (1972), based in verbal protocols"(Rasmussen, 1986). In 1983, Laird, Newell and Rosenbloom proposed a new model, SOAR (States, Operators, and Results), with a computational version in 1987. SOAR is a model which can deal with symbols and, therefore, is good candidate for future investigations.

COGNITIVE ARCHITECTURE AND SHORT-TERM MEMORY MODELS

As we stressed,the most attractive models here are: ACT, SOAR and CAP2.

CAP2(CONTROLLED AUTOMATIC PROCESSING 2)

Its framework (Schneider/Oliver, 1991; Schneider/Detweiler, 1987) is very close to the connectionist models. The model includes the associative and auto-associative models of J. A. Anderson's brain-state-in-a-box model (1983,1977). The model is a connectionist model (modules) with a control structure. The learning of the association and auto connection matrices between modules is done with a delta or Widrow-Hoff learning rule. The control structure can deal with the modules as a symbolic processor, resulting in a hybrid model (see in Levine, 1991).

ACT AND SOAR

ACT (J. R. Anderson, 1983) and SOAR (Newell, 1990) are the two main candidates for a unified cognitive theory, and therefore provide comprehensive cognitive architectures. These architectures are very related to the AI approaches because both use production systems. AI models have limitations because of the difficulty in representing the human intuition. The recent book on cognitive continuum models by Hammond et al. (1990) is a step to fill this gap.

Before comparing ACT and SOAR, we provide the following list of requirements for such architecture (Newell, 1989):

1. behave flexibly as a function of the environment,
2. exhibit adaptive (rational goal oriented) behavior,
3. operate in real time,
4. operate in a rich, complex, detailed environment:

a. perceive an immense amount of changing detail,
b. use vast amount of knowledge,
c. control a motor system of many degrees of freedom,

5. use symbols and abstraction,
6. use language, both natural and artificial,
7. learn from the environment and from experience,
8. acquire capabilities through development,
9. live autonomously within a social community,
10 exhibit self-awareness and a sense of self.

Beyond this, the architecture must have the following functions:

1. memory

a. contain structures that contain symbols tokens
b. independently modifiable at some grain size
c. sufficient memory

2. symbols

a. patterns that provide access to distal symbols structures
b. a symbol token in the occurrence of a pattern in a structure
c. sufficient symbols

3. operations

a. processes that take symbol structures as input and produce symbol structures as output
b. complete capacity of composing

4. interpretation

a. processes that take symbol structures as input and produce behavior by executing operations
b. complete interpretation capacity

5. interactions with external world

a. perceptual and motor interfaces
b. buffering and interrupts
c. real-time demands for action
d. continuous acquisition for knowledge

ACT (ADAPTIVE CONTROL OF THOUGHT) AND SOAR (STATE, OPERATORS, AND RESULTS)

Memory

ACT has three memories: (1) a declarative long-term memory (a semantic net of nodes with weighted links), (2) a procedural long-term memory (condition-action productions), and (3) a working memory. SOAR has two memories, a single long-term memory of productions and a working memory that contains a goal structure, information associated with the goals, preferences about what should be done, perceptual information, and motor commands. These differences are not so remarkable. First, ACT production corresponds to the SOAR problem-solving operators, as is used in AI. SOAR production operates as an associative memory. Second, ACT's production memory is realized as a network structure similar as a semantic net. The main effect is that activation governs the rate of matching of production in the same way that activation spreads through the declarative networks. Thus these two memories are not as distinct as it might seem (Newell, 1989).

Symbols

"Both ACT and SOAR starts with symbolic structures in working memory and determines that a production anywhere in the long-memory fire. The symbol tokens here are the combinations of working memory elements that match production conditions. Each productions left-hand side is a symbol. For SOAR is the only mechanism for distal access. For ACT, there is also a mechanism for distal access to its declarative memory, in fact a combination of two mechanisms. First, each token brought into working memory by firing a production (or by perception) makes contact with its corresponding node in the declarative semantic net. Second, spreading activation, then operates to provide access to associated nodes" (Newell, 1989).

Operations

For both ACT and SOAR, "the right-hand-side action becomes essentially just the operation of creating structures in working memory. In ACT and SOAR, storing information in long-term memory is separated from the act of computation in working memory. It is incorporated as learning new productions, called production compilation in ACT, and chunking in SOAR" (Newell, 1989).

Interpretation

"Interpretation is to be identified by finding where a system makes its behavior dependent on the symbolic structures in its long-term memory, in particular, on structures that it itself created earlier" (Newell, 1989).

In ACT, "elements in both long-term memories have strengths associated with them, and those in declarative long-term memory can have a level of activation associated with them. Working memory in the set of activated elements from declarative long-term memory (including goal structures) plus the set of action that create new structures in working memory. Activation spreads through declarative memory as a function of element strength. New productions can be created from the effects of previous activity that has made it to declarative long-term memory" (Elkind et al., 1989).

"In SOAR problem-solving operators are selected through a two-phase decision cycle. First, during the elaboration phase the long-term memory production memory is accessed repeatedly in parallel until quiescence. When all information possible has been accumulated, the decision procedure winnows the available preferences and makes the next decision, moving to the next cycle" (Newell, 1989).

Interaction with the external world

"ACT, as is typical of many theories of cognition, focuses on the central architecture. Perception and motor behavior are assumed to take place in additional processing system off stage. SOAR has the beginnings of a complete architecture, which embeds the central architecture within a structure for interacting with the external world" (Newell, 1989).

BLACKBOARD ARCHITECTURE (BBA, SEE ELGEMORE, 1988) AND PRODUCTION SYSTEM

"Certain aspects of the BBA have much in common with production systems. There is a blackboard, like working memory, that contains a wide range of relevant data, organized generally according to level. Numerous knowledge-sources, which are like productions, respond to data at one level and introduce data at another level. At any point in time the system must choose which source to apply, from a set of potentially relevant knowledge sources. This is the conflict-resolution problem. In BBA, this C-R decisions are made dynamically and intelligently by considering any relevant information. Various knowledge sources are responsible for evaluating the state of knowledge and deciding what should be done next. This flexibility causes a considerable computational cost. It allows for radical shift of attention when a new hypothesis seems promising. Hayes-Roth (1979) used this flexibility to plan low-level sequences of errands in the absence or in the violation of a high-level plan. This behavior was called "opportunistic". This causes problems, because skipping among its many plans and levels makes unrealistic demands in the working memory. In making distractibility the central purpose in a theory of cognitive control, they have lost the essential insight of the past theories, that human behavior acquires its organization through always being controlled by an organized structures of goals" (Anderson, 1983).

In the ACT theory there are five principles of conflict resolution: degree of match, production strength (application frequency), data refractoriness, specificity, goal-dominance (Anderson, 1983). "SOAR abandons the fixed conflict-resolution mechanisms and thus keeps itself free to move toward a closer approximation to the knowledge level. It does not, of course, abandon conflict resolution. The decision structure SOAR is the conflict-resolution mechanism. The impasses are the conflicts" (Newell, 1990). "It thus creates a sub-goal to resolve these impasses. The effect of deliberate sub-goals is achieved by SOAR by the combination of an operator, which is deliberately generated and selected, and an impasse that occurs if productions do not exist that implement the operator. The operator acts as the specification of a goal to be achieved for this sub-goal" (Newell, 1989).

2.2.2.2 REVIEW OF THE MODELS

The human performance models can be classified in two main groups: human reliability models and cognitive models.

2.2.2.2A HUMAN RELIABILITY ANALYSIS

HRA is defined as any method by which human reliability(HR) is estimated (Swain/Guttman, NUREG-1278, 1983). Fujita (1992) defines HR as the success probability of human activities of which failures are likely to give significant impact on the reliability of a human-machine system. The problem in the HRA is that it arises in function of the reliability engineering applied to the hardware systems. As a result, humans are considered as an additional hardware component. Therefore, HRA is only half human. It doesn't take into account the cognitive structure like in the Rasmussen's and Card's models.

The most successful HRA method until the early seventies was THERP(Technique for Human Error Rate Prediction) in which NUREG-1278 was based. After TMI in 1979, several HRA methods emerged:

a) Monte Carlo Simulation Technique, 1969;
b) TESEO (Tecnica Empirica Stima Errori Operatori- Empirical Technique to Estimate Operator's Errors), Bello/Colomberi, 1980;
c) APJ (Absolute Probability Judgment), Comer et al.,1984;
d) PC (Paired Comparisons), Hunns, 1982;
e) OATS (Operator Action Tree System), Wreathall, 1982;
f) CM (Confusion Matrix), Potash et al., 1981;
g) SLIM (Success Likelihood Index Method), Embrey et al.,1984
h) MAPPS (Maintenance Personnel Performance Simulation), Siegel et al., 1984;
i) ASEP (Accident Sequence Evaluation Program), Swain, 1987
j) HEART(Human Error Assessment and Reduction Technique), Williams, 1986;
k) HRMS (Human Reliability Manual System), Kirwan/Tamer,1989
l) IDA or STAHR (Influence Diagrams Approach), Philips et al., 1983;
m) SAIC TRC approach (Dougherty, 1987);
n) SAINT (Systems Analysis of Integrated Networks of Tasks, Siegel, 1974);
o) CREATE (Cognitive Reliability Analysis Method), Woods,1990

In the mid-eighties, the incorporation of HRA in the PSA (Probabilistic Safety Assessment) was done through the Systematic Human Action Reliability Procedure (SHARP). In order to introduce the concepts of a cognitive structures already mentioned, a fusion between the Rasmussen's S-R-K model and a Time Reliability Correlation (TRC) was realized providing a new method named HCR (Human Cognitive Analysis, Hannaman et al., 1984). SHARP uses either THERP or HCR to evaluate errors. A TRC was equally developed for improving the OAT method at that time (1984).

Although HCR has been the only trial to join quantitative aspects like human error probability with qualitative aspects such as the cognitive structures, Kantowitz and Fujita (1992) criticize this trial as premature. In fact, curve fitting technique found in correlations couldn't separate cognitive categories and this was identified by EPRI experiments which will be discussed in another chapter. Rasmussen, himself, is opposed to the tendency in quantifying his S-R-K model. A good review of the HRA methods can be found in Cacciabue (1988, 1992), in the IAEA-TECDOC-499 (1989), in Reason (1990), and in Kirwan (1993).

Barry Kirwan (1993) made a revision of the HRA techniques according to the following criteria:

1)the degree to which time appears to be dominant in the techniques as a predictor of human performance;

2)the overall convergence or divergence of the approaches in the way in which time is treated;

3)the degree to which the techniques appear to have theoretical validity in dealing with RS(response - straightforward or familiar and anticipated events) and RD(response-decision making or unfamiliar and non-anticipated events).

ROLE OF TIME

- Time is of low or at most moderate importance (APJ,PC,IPA).
- Time is moderately important but other PSF(Performance Shape Factors) can dominate (SLIM,CM,THERP,HEART,HRMS).
- Time dominates but is tempered significantly by other PSF (MAPPS,SAIC,SAINT).
- Time alone dominates (HCR,OATS,ASEP/THERP models)

Kirwan also presents a classification into 4 groups:

1) expert opinion based approaches (APJ,SLIM,PC,IDA)

2) experimental-data-based techniques: HEART

3) information process methods considering situations in depth (CM,OATS,THERP,SAINT,ASEP/CREATE)

4) information processing methods considering the Rasmussen's framework levels (HCR,SLIM,PC,HEART,HRMS,OATS-SLIM,GEMS).

The RS scenario can be quantified using a range of techniques, but with the RD scenarios this doesn't occur. Simple time-dominant approach (THERP/ASEP,MDM,OATS,HCR) is not suitable, because of the lack of other PSF. In the case of HCR, the difficulty is to decide if the scenarios is rule-based or knowledge-based behavior, as EPRI has already verified.

The PSF-based approach (HEART,HRMS,SLIM) which takes moderate of high account of time can be used to estimate performance. The non-PSF, expert based approach, can also model RD scenarios, depending on accurate timing estimator by judges (APJ,SLIM,PC,IDA). PC and SLIM depends on calibration. APJ could consider perseverance or delay in the operator reluctance or disbelief.

SAINT does not deal with RD scenarios. CM and HEART are techniques that can deal with misdiagnosis.

Kirwan suggests a combination of CM,PC,APJ,HEART:

- CM/PC for initial misdiagnosis and APJ for the misdiagnosis itself.
- HEART for thwarted diagnosis and finally APJ for completion of the diagnosis.

A study done in the IHF, Japan, reported by Hiei(1990), the following models were chosen after a careful evaluation: THERP, HCR, SLIM, STAHR, DeBDA.

CONCLUSIONS

HRA doesn't take into account the errors reasons and mechanisms. Because of this, it doesn't work as a human performance model to be used in human-machine systems design and evaluation. HRA can't be used also to give a quantitative characteristic to the qualitative models of the human cognition. The reason is that it's difficult to separate cognitive categories in a statistical fitting curve. HRA has only importance when integrated with PSA to give insight to the questions related to the accidents sequences involving human failures.

2.2.2.2B COGNITIVE MODELS

The cognitive models can be classified according to the sub-model in the Rasmussen's framework in which it is based. A good review of the Human Performance Models can be found in (Baron/Kruser, 1990). Optimal control approach was the basis for PROCRU. INTEROPS combines a tasks network (SAINT) with a qualitative reasoning programmed in LISP. Knowledge as ruled-based approach provides the basis for the cognitive science representations through artificial intelligence techniques. This is the case of GOMS, HUANG/SIU and CES models. Finally, there are models based in a global cognitive architecture. HOS is based in a psychological information processing model like Card/Wickens models in the chapter 1. COSIMO and A^3I are based in the BBAs. CAMEO is based in the multiple attention resources theory. All of them use production rules.

PROCRU (PROCEDURE-ORIENTED CREW MODEL)

Criticizing his own previous work, Baron (1984) comments on the OCM (Optimal Control Model): "...none of theses models considers any of the following: multiple tasks having different objectives; the detection of events not explicitly related to the system state variables; or multi-operators situations and the effects of communication among such variables. Perhaps the chief shortcoming of the models with respect to realistic supervision control tasks is that they do not include the procedural activities of the operators or the discrete tasks that are often part of such procedures".

Following Sheridan (1992): "to satisfy the above kinds of concerns, Baron et al. (1980) developed PROCRU (Procedure-Oriented Crew Model) for analyzing commercial aviation flight crew procedures for ILS(Instrument Land Systems) approach-to-landing. PROCRU incorporates both "by the book" procedures and more unconstrained monitoring and control activities. It models both continuous control and discrete procedural tasks which are triggered by controlled process state variables. The particular task chosen at any moment by the procedure selector is the one having the greatest expected payoff based on both mission priorities and perceived state as determined from both visual displays and auditory inputs from other crew members or from air traffic controllers(ATC). PROCRU models multiple crew members simultaneously".

"The state variables describing the aircraft are handled by the optimal control model, whereas verbal message from air traffic control or between crew members are handled by a rule based pattern recognition system. The output of the state estimation can either be used to drive S-B-B control actions or by means of pattern recognition to provide the left hand side of production rules for R-B-B." (Stassen, in McMillan, 1989).

"The system dynamics incorporated in PROCRU are non-linear, so the basic linear Kalman filter could not be used. However, inasmuch as most maneuvers in the terminal area are standardized, it is possible to make linear the vehicle trajectory about nominal segments. Then, a linear estimator can be designed to estimate the perturbations from these "nominal". The estimate of the total state is then the sum of the estimates of the perturbations state and of the nominal state" (Baron/Corker, 1989).

"Auditory messages are treated as priority interrupts, but they also may be missed if workload is high" (Sheridan, 1992). Workload analysis is done by computing the effects of attention sharing, modelled by an increase in the "nominal" noise/signal ratio. It means that

$$P_i=P_0\frac{1}{f_t}\frac{1}{f_s}\frac{1}{f_i}$$

where:
p_i=noise/signal ratio associated with the ith display,
p_0=noise/signal ratio associated with full attention to the display,
f_t=fraction of attention devoted to the control task as a whole,
f_s=fraction of attention devoted to the sub-task s,
f_i=fraction of attention devoted to the ith display in sub-tasks.

$$\sum f_s=1$$

$$\sum_i f_i=1$$

f_{tc} = workload index

"PROCRU has been successfully applied for flight control and landing approach planning. Efforts has been made to extend this model to process control, and in 1982 (Baron, et al.), a simulation model based on control theory has been proposed for simulation of the dynamic performance of a nuclear power plant [Baron,1988], including the operating staff. One important aspect of this approach is that human behavior at all three levels (skill- rule- and knowledge- based) as well as their interactions are considered in one integral model. It appears, however, at present to be difficulty to collect the explicit human performance data that are needed for implementation of the model.

This kind of integrated model has great importance for design of aviation and other vehicle systems because, in the decision and manual control tasks the operator forms one integrated task in direct coupling with system dynamics. The task of a pilot or driver is a direct space-time control of a moving physical object, the vehicle.

The sensorimotor level of the human information processing in this task serves for control signal processing, i.e., the output manual actions are continuous signals in the semiotic sense. For process plants of the present levels of automation the continuous control signal processing is however automated. This means that human output actions will typically be related to switching, and will be interpreted as stereotyped signs by the plant systems. This means that the human sensorimotor behavior will largely be used for an interface manipulation skill. For this, the time-space characteristics will have no direct relation to the basic system dynamics or the supervisory control tasks for which they in a way act as separating interface...models based on optimal control theory are only suited to represent the state identification of sensorimotor, behaviors and the featuring formation necessary to release and modify skilled patterns in case of manual control of well-structured dynamics systems, from which information is interpreted as signals. In less-structured situation when feature formation and state identification are based on recognition of information interpreted as signs, models of human judgement in terms of statistical representations are more suitable." (Rasmussen, 1986).

INTEROPS (INTEGRATED REACTOR/OPERATOR SYSTEM)

INTEROPS (Schryver, 1992, 1988, 1988) is a simulation model consisting of the link between ARIES-P and an operator simulator. ARIES-P means Advanced Reactor Interactive Engineering Simulation for PRISM, a modular liquid metal reactor design. Any reactor type can be used with that general operator simulator. The central part of the latter is SAINT, a network simulation language, with capabilities for both continuous and discrete events simulation. Because of SAINT does not have power to represent human cognitive activities which involve extensive symbolic manipulation of knowledge, this is provided by external models of expertise (qualitative models) developed in LISP language for fault diagnosis, situation assessment, decision making, and procedure generation. SAINT is responsible for normal planning, information-seeking, fault management, and scheduling/execution. Normal planning includes goal formation, subgoal planning, and normal procedure lock-up.

The information processing path through the task network follows this sequence: discrete monitoring, failure detection and interpretation, rate estimation, tend estimation and error detection, and situation assessment. Discrete monitoring generates an internal representation of the display variable which is unbiased and filtered through gamma-distributed noise to simulate perceptual error.

INTEROPS has the following cognitive features: dynamic monitoring strategy (structure and composition of the state variables queue together with the dynamic rules of modification); opportunistic monitoring (monitoring transition matrix $p(x_i/x_j)$ with the conditional probabilities x_i will be monitored next given that x_j was just monitored); forgetting (exponential decay of certainty in the working memory); evidence chunking (new fault diagnosis is only initiated following the arrival of a chunk); cognitive tunneling (probability of ignoring evidence, or reduction of the range of cue utilization, monotonically increased with a time pressure function or stress function, which exponentially increases with the diagnosis time); confirmation bias (processing diagnosis information in a biased fashion); hypothesize and test (to deal with confirmation bias tendency); means-ends analysis (search strategy for generating knowledge-based procedure); intentional error (errors associated with intention formation).

The INTEROPS model employs a time-shareable cognitive resource theory in terms of number of simultaneously active tasks, as well as the queue size, as an index of cognitive workload. As a cognitive architecture INTEROPS is more close to ACT, if we interpret SAINT tasks network as a declarative memory and the LISP knowledge base as a procedural memory. Both have a common working memory. Conflict resolutions are made by the means-ends analysis in the INTEROPS. Both models have decay of the short-memory. INTEROPS, however, has effects of monitoring, stress, error formation and workload calculation.

CES(COGNITIVE ENVIRONMENT SIMULATION)

CES (Woods, 1992) is a tool for simulating how people form intention to act in emergency operations in NPPs. This is to be used for another program named CREATE (Cognitive Reliability Assessment Technique). CES was developed using AI techniques and a problem-solving "shell" called EAGOL. As an AI system, CES contains a knowledge base and a inference engine. CES exhibits the following main features: a) process parameters monitoring; b) detection and diagnostics; c) response management (generate intention to take recovering actions).

GOMS(GOALS, OPERATORS, METHODS, AND SELECTION RULES)

In GOMS, the tasks are analyzed in terms of goals, operators, methods, and selection rules. Operators are actions that can be perform directly. Goals are actions that can be broken down further and often have alternative ways of being accomplished. Methods are procedures composed of goals and operators and simple control structures that can be used to achieve goals. Selection rules are rules for choosing among alternatives methods for accomplishing goals. The GOMS sort of analysis models the activities of settled skill in more or less routine environments (Elkind et al., 1989).

HUANG/SIU MODEL (MIT)

In the HUANG/SIU model (Ph. D. thesis, Huang, 1991), we can see the first trial to simulate a nuclear power plant control room crew. In this model, the SRO(senior reactor operator), the reactor operator(RO), and the ARO(auxiliary reactor operator) are simulated. Two parameters model the interpersonal relationship: self-confidence and one's confidence in another. The first is defined as the one's confidence in the one's capability of executing the tasks in one's responsibility area while the second is defined as the confidence in the other's capability of accomplishing the demanded task and his perception of other's trust worthiness. Messages rejection or acceptance are simulated by a sender's willingness model.

Each operator individual model processes the information in four stages: monitoring, situation assessment, planning, and execution. The inputs come from the other models: operators and plant modelling. The output could be an action or a message to the other operator. There are two memories: a knowledge base (long-term memory) and a short-term memory (working memory). In the knowledge base, three knowledge groups are stored: scripts for the responses to the plant changes, the production rules for fault diagnosis, and one's confidence in others (group characteristics). The short-term memory has capacity limit and the stored items decay with time.

In the monitoring stage, the plant parameters dynamic monitoring done by the operator are characterized by two features: parameters priority and filter threshold.

In the situation assessment stage, there are two kind of situation: familiar and unfamiliar. For the first one, rule-based responses are generated immediately. For the second one, there are four substages: in the concerns generation substage, tasks concerned to the situation are chosen. In the concerns merge substage, those concerns related to the same system or issues are mixed. All the concerns are allocated in a concerns list which is controlled by a queuing process. In the control activity substage, a process of diagnosis is initiated using the procedures rules stored in the knowledge base. More concerns could be generate in this substage. In the script selection substage, a script corresponding to a concern is selected.

The planning stage is composed by an actions list formed by the scripts generated. This list constitutes the second queuing process. All the actions and concerns compete each other according to their priorities.

The execution stage is characterized by three classes of actions: manipulation, monitoring, and messages exchange. These are the inputs for the next time step.

Three types of monitoring are identified: alarms, specific and general. Alarms and specific monitoring are assumed always successful. The general monitoring occurred only when the operator has no task to do. This monitoring is characterized by priorities and filter thresholds. The initial priorities increase if the parameters were or has been monitored. The operator will monitor only the parameters with the priorities higher than the filter threshold, which depends on the stress level. The stress has three components: burden stress(BS), frustration stress(FS), and irritation stress(IS). BS depends on the number of items in the short-term memory. FS depends on the time spent until the diagnostic conclusion is achieved. IS is proportional to the message tone difference between sender and receiver. The tone is proportional to the stress level. The filter threshold is a linear function of the stress level.

HOS(HUMAN OPERATOR SIMULATOR)

HOS is constituted by three programs: HOPROC(Human Operator Procedures), HOM(Human Operator Model), and HODAC(Human Operator Data analyzer and Collator). HOPROC is an English-like language used to define user-tasks, crew -station layouts, hardware and software specifications, etc. HODAC provides the outputs such as time lines, link analyses, procedures analyses, anatomy loadings, etc. HOS is composed by submodels described below (Baron/Kruser, 1990).

Long term memory retrieval

It is constituted by learned procedures and the types and location of display and control devices.

Attention and recall of current task responsibilities

The attention submodel, when accessed, computes a Figure of Merit(FOM) for each active procedure and selects the one with the highest FOM.

Statement processing

It uses its rules and algorithms to determine the next micro-action to invoke in its attempt to satisfy the overall goal of the HOPROC statements.

Information estimation

Depending on the current situation and the type of information needed, it may invoke short-term memory recall, information absorption, or information calculation to obtain needed estimates.

Short-term memory retrieval

Computes the probability of recall for a previously estimated value or state as well as the need for physical manipulation of controls or displays (movement time).

Information absorption

Corresponds to the perception of information from external sources such as displays and controls.

Information calculation

Possibility in obtaining information by calculating through equations.

Anatomy movement

This submodel determines the part(s) of the anatomy that must move in order to access a display or control, and which is desired anatomy part is currently busy.

Decision making

Uses the decision rules in the format IF(assertion) THEN(consequences).

Accessing relevant portions of procedures

It contains a function that makes it possible to bypass portions of procedures that have become irrelevant to the current situation.

Although is a complete system, HOS doesn't have an internal model of the operator able to deal with rapidly changing complex systems or knowledge-based behavior. HOS includes each human-machine interaction at the components level. But there is no interaction between these components. Such details of a complete system are useful only for evaluation of control/display design and layout.

COSIMO(COGNITIVE SIMULATION MODEL)

COSIMO (Cacciabue et al., 1988, 1990, 1992) has two fundamental components: a limitless knowledge base(KB), containing both declarative and procedural knowledge structures and a limited, serial working memory(WM).

The KB is structured in frames or schemata which represent the operator knowledge about the plant in the form of geometrical structures (connections, locations, states of components), process representations (variables behaviors, causal relations, functional landmarks and thresholds), and control sequences (actions, tasks, procedures and respective effects).

Two main types of frames are distinguished. The first one, called knowledge-frames, describes only the process and the structure of the system in terms of general physical and engineering principles, as well as rules of thumb. The second one, called rule-frames, encompass predefined plans of actions for different situations.

External cues coming from the environmental data enter into WM, making the KB be explored through two mechanisms: similarity matching(SM) and frequency gambling(FG). SM generates frames, which are candidates to represent the current situation. FG solves possible conflict between these candidates in favor of the more frequent one encountered in the past. The product of these two criteria is called CIF(Currently Instantiated Frame), which is given to WM for confirmation and execution.

These structures are implemented in a blackboard architecture, which is composed by three parts: 1. blackboard itself with its internal structure, 2. the agents or knowledge sources/specialists and 3. the controller, governing the agents actions. The blackboard structure consists of different hierarchical levels of abstraction corresponding to the structured-objects that may be dealt by the model.

Agents are specialized inference mechanisms that work in specific levels of the BB blackboard. The controllers governs the agents actions through a control cycle. In this cycle, new tasks are added to the list of tasks in an agenda and the controller selects one of them to be executed. The latter generates new objects which together with the incoming objects modify the agenda of tasks.

The controller can be designed using a BBA. So, we have to distinguish two different BBs: the domain-BB(DBB) and a control-BB(CBB). The levels of the CBB are: problem, strategy, focus, policy, agenda and task. The agents of the CBB are: put-problem-on-BB, stop-problem, start-strategy, update-strategy, initiate-focus, update-focus.

The levels of the DBB are: environment cues, signal, sign, perceived cues, set of hypothesis, CIF, action. The agents of the DBB are: Get-environment (external cues are associated with objects in the environment level), decoder, cognitive filter (relevance of the cue to the situation), semantic interpreter (the translation is performed by means of fuzzy matching between semantic and numerical expressions), similarity matcher, frequency gambling and executer.

The CIF is implemented through a structure called FUGOS(Fuzzy Goal Oriented Script). FUGOS has top goal, subgoals and subtasks arranged in a tree structure. A goal is an element of the network at any level. An act is a goal in the last level of the network, i.e., an elementary action. A task is the sequence of acts to perform a goal at any level. Each goal is characterized by the following parameters: degree of priority(GDP), degree of membership(GDM), degree of satisfaction(GDS), GDC (degree of certainty).

Errors mechanisms are generated through mistakes (defects in the formulation of the strategy in KB), lapses (memory failures during the execution of the task), slips (imperfections of attention monitoring). Slips are modeled by a stress function and a decay of attention with the time. Lapses are generated as a function of a stress function.

The architecture of COSIMO is based in the fallible machine as well as in the GEMS(Generic Error-Modelling System) framework, both from Reason(1990). In the GEMS, we have slips and mistakes in the S-L behavior due the inattention and overattention, mistakes in the R-L behavior due to misapplication of good rules and application of bad rules, and mistakes on the K-L based behavior.

In the fallible machine, we have WM and KB. WM is divided in FWM(focal WM) and PWM(peripheral WM). PWM corresponds to the part of the WM in COSIMO which receives the environment cues. FWM corresponds to the part of the WM in COSIMO, where CIF is stored. Similarity-matching (SM) and frequency-gambling (FG) are retrieval mechanisms of the FWM. Reason also created the concepts of HLDM (High Level Decision Making) for diagnosis and planning and LLDM(Low Level Decision Making) for execution, optimization and error detection. SM and FM activities are HLDM, while CIF is LLDM.

A^3I(ARMY-NASA AIR CREW/AIRCRAFT INTEGRATION)

The major product of the A^3I program is the development of a prototype human factors/computer-aided engineering(HF/CAE) system called MIDAS(Man-Machine Integration Design and Analysis System). MIDAS is composed by three parts: user interface, simulation system, interactive crew station design tools. The user interface receives three kind of inputs:

1) Operator characteristics (physical and cognitive),

2) Mission (flight profiles, way points, behavior of scenario objects, operator activities from mission plan, equipment-specific activities),

3) Crew station design (cockpit equipment functionality, 3D cockpit geometry, 2D representation of display/controls, cockpit equipment layout).

The simulation system generates as output the following mission and operator performance measures:

1) Activity traces
2) Task load timeliness
3) Resource conflicts
4) Information flow
5) Analysis results

The interactive crew station design tools generates visibility and legibility analysis among others. As general outputs, the program gives a visualization of the simulated mission: operator activities and equipment states.

The central part of the MIDAS is the Mission Simulation System(MSS). MSS has two parts: a world model (vehicle and environment) and a Symbolic Operator Model(SOM).

SOM is divided in the following parts:

1) Perception/attention vision
2) UWR(Updatable World Representation)
3) Motor
4) SOM queues
5) Task Loading Models(TLM)
6) Scheduler

UWR is composed by: mission goal decomposer, decision by rules, decision by algorithm, demons/daemons, activity, and equipment. The declarative structure is a semantic net. Information is subject to differential temporal decay to represent a forgetting function. The GEST(Generic Expert System Tool) provides the inference engine for rule-based decision making. The decision algorithms are: weighted additive algorithm, equal weighted additive algorithm, lexicographical algorithm, satisfying conjunctive algorithm, majority of conforming dimensions algorithm.

There are five som queues: current-activities, working goals, pending activities, scheduled activities.

The scheduler has a goal decomposer (GD) that decomposes the mission goals into activities that can be scheduled. The Z-scheduler generates a total order of activities based on temporal constraints (after, during, overlaps, start-at, start-by, end-at, end-by) and resources constraints from TLM. The Z-scheduler use a BBA provided by GEST.

TLM is an operator task loading model based on current research in multiple resources theory, scaling, workload, and perception(see WLAM, in chapter 2.2.1).

CAMEO(COGNITIVE AND ACTION MODELING OF AN ERRING OPERATOR)- FUJITA ET AL., 1993

CAMEO is based in the Wickens multiple attention resources theory and his framework described in the chapter 1 with the perception, cognitive, motor, and attention substages. The second concept in CAMEO is the task-switching. There are three modes of tasks environments: dual-task, background task, and task interrupt. There are also two strategies for the task switching: temporal and opportunistic.

In the dual task model, two tasks (primary and secondary) are being attended at one time; background tasks are handed over to someone; a task interrupt occurs as a result of intrusion of an additional task.

The temporal task-switching strategy causes a task interrupt by the following factors: functional importance of intrusion and personal trait (divergent versus convergent).

The opportunistic task-switching strategy determines which task must follow a task just completed. The sequence of tasks is influenced by the following factors: functional constraints among tasks, personalized task processing methods or policy, outcome of proceeding tasks, and change of problem space.

The decision making(DM) is composed by four task modules: vigilance of cue signals (DM-V), diagnosis(DM-D), response selection (DM-RS), and confirmatory evaluation (DM-CE).

There are two types of knowledge stored in the long-term memory used to carry out the tasks: rules and normative knowledge.

When the attention resources are not enough to cover the necessities of the Wickens framework stages, error-inducing methods become operational. In the perception stage, stored information could not be updated and less salient incoming signals receive no attention.

In the cognitive stage, familiar but inappropriate strategies or rules could be activated, leading to an erroneous conclusion. In the same manner, in the motor stage, unappropriated actions could be selected or conditional actions steps could be omitted.

COMPARING SOAR WITH OTHER MODELS

In the state-of-art of the cognitive architectures, it is necessary to carry out a specific research project to choose the most appropriate among them for a determined application. Nevertheless, Allen Newell assumed in his last work that the cognitive science is ready for a unified theory (Newell, 1993, 1990). He claimed for SOAR(States, Operators, and Results) this role, although he also pointed out other candidates: ACT(Adaptive Control of Thought), the theory of induction from Holland et al., and MHP(Model of Human Processing). In this list, connectionist and hybrid models such as PDP(Parallel Distributed Processing) and CAP2(Controlled Automatic Processing 2) don't appear. It seems that Newell considered these models only a way to adapt some cognitive concepts to the available computer technology. In the Newell's point of view, human information processing is entirely symbolic, although he didn't mention any artificial intelligence technique like BBA(Blackboard Architecture).

To compare SOAR with other architectures, the discussion will be concentrated in the cognitive and attention stages, because the perception and motor stages are interfaces with the external world and can be treated outside of the central processing. Consequently, the focus will be on the cognitive control, memory, and attention allocation.

There are five types of cognitive control: production systems, agenda, blackboard, procedural attachment, and means-ends analysis (Stillings, 1987). In the case of production systems, there is a three-phase control cycle: matching, conflict resolution, and action. In the agenda schema, the tasks are ordered and placed in an agenda, according to their priorities, recencies, importances, and restingnesses. In the BBAs, the knowledge sources are used as a generalization of the rules of production, dividing the problem-solving responsibilities among these sources. This kind of approach is very flexible, but the exchange of information between sources can be difficult, limiting the creativity. Beside this, the working memory(WM) can be subjected to high demands due to the opportunistic search executed by this kind of control, which is unrealistic when compared to the human memory. Because of these critics, there is a doubt if the BBA is a good representation of the human cognition, especially when applied to the knowledge level of the Rasmussen's framework. The procedural attachment uses frames to obtain a specific procedure for the problem. The means-ends analysis is used by the Newell's GPS(General Problem Solver). It creates a way of decomposing the problem into subproblems, which can be solved easily. This general approach can fail when applied for a domain-specific knowledge.

Each one of these control types uses one or more knowledge representation techniques, such as semantic nets, frames (different aspects of a stereotypical item), scripts (sequence of events of a stereotypical knowledge), rule-based representations, and logic-based representations. Scripts and frames are similar to the shortcuts in the Rasmussen's framework, representing stereotypical behavior.

A review of the HPMs(Human Performance Models), shows the following use of the above techniques:

PROCRU - production rules, scripts (procedures), and agenda
COSIMO - frames, procedural attachment, scripts (procedures), and BBA
HOS - production rules/production systems
CES - production rules/production systems
GOMS - production rules/production systems
CAMEO - normative knowledge (scripts=procedures, frames)

production rules, agenda
A^3I - daemons/demons, scripts, semantic nets, frames and BBA
HUANG/SIU - production rules, scripts (procedures), and agenda
INTEROPS - frames (qualitative models), scripts (procedures), agenda, and means-ends analysis
SOAR - production rules, elaboration and decision
ACT - semantic nets, production rules/production systems

SOAR uses a generalization of the production rules, programmed in OPS5: recognition-based productions stored in the long-term memory(LTM) using objects and attributes in short-term memory(STM). Through this, it deals with three kinds of knowledge: procedural (like in production rules), episodic (like in scripts and frames), and declarative or semantic (like in semantic nets and logic-based representations). An important characteristic of SOAR is that the episodic knowledge can be used as procedural knowledge as well as for recalling and recognition of familiar tasks as in scripts, frames, shortcuts, and knowledge sources. This means that SOAR doesn't need a fixed cognitive control like in BBA and procedural attachment. SOAR doesn't have a conflict resolution, instead the control cycle is done through elaboration in parallel (access long-term memory until quiescence) and decision. However, impasses can arise when none of the possible states in the problem space are acceptable. The impasses are resolved by generating subgoals, procedure that reminds in part the schema adopted by GPS. There are four types of impasses: tie impasse (none of the alternatives are preferred to any of the others), no-change impasse (no choice available), reject impasse (the only preference may be rejecting one of decisions already made), conflict impasse (the same operators have opposite preferences for different production rules).

The decision procedure is achieved by examining the context stack, consisting of sets formed by goals, problem-spaces, states, and operators, called elements (object-attribute-value triples). Every cognitive task is represented by a problem-space. A problem-space search generates new states applying operators to an initial state until achieving a desired state. Operators are chosen according to the following decisions concepts: acceptable, reject, better/worse, best/worst, and indifferent.

To understand the attention allocation in SOAR, we must look how it works as a total cognitive system. Besides the goals stack in the working memory and cognitive productions(C) in the LTM, SOAR has a perceptual system(P) and a motor system(M). P-system elements are stored in LTM as encoding productions(E). Motor actions are produced through decoding productions(D). These productions have the same structure as C-productions, but they don't have decisions cycle, running to quiescence, or impasses. To manage the perceptual system, there is an attention operator(A) which works as a channel selector, establishing a bridge between the E-productions and the P-system.

The last characteristics to be analyzed are the memory phenomena, important to model the perception errors, forgetting, and task deletions. These phenomena are related to the residence time of the WM elements. This is tied to the duration of the problem-space activity. Other problem-spaces may run in simultaneously, forcing the WM changes be very rapid with each new production cycle. If an element of the WM is not being attended, it could be removed (replaced) for being outside of the central system. If the attention is shifted back to that element, it could be recovered if it is still there.

There are many controversies about the SOAR as an Unified Theory of Cognition. The volume 59(1993) of the Artificial Intelligence Journal provides a good review of these controversies, mainly through the commentaries of Marvin Minsky (Media Lab and co-founder of the MIT AI Lab), who compares SOAR with his SOM(Society of Mind); Arbib, who compares SOAR with connectionist theories, schemas, and Chomsky's competence theory; Michael Fehling, who compares SOAR with other cognitive architectures like BBAs, as well as Chomsky's competence theory; and Barbara Hayes-Roth (creator of the BBAs). Rosembloom and Laird, Newell's colleagues in the SOAR development, provided responses to these commentaries in the same volume of the AI journal.

CONCLUSIONS (HPSM-HUMAN PERFORMANCE SIMULATION MODEL - A PROPOSAL)

A HPSM must have the following structures:

a) Perception submodel
b) Cognitive architecture and control
c) Motor submodel
d) Attention allocation submodel
e) Crew model
f) Errors generation

Perception submodel

The three important perception types are: visual, auditive, and tactile. Vision is the most important perception in some models such as PROCRU, A^3I, and HOS, due the fact that these three models were conceived for using in the aviation industry. For NPPs(Nuclear Power Plants) control room, visual movement in 3D is not used for the system state estimation like in the aircraft. Instead, we need static models for instruments displays or, in the modern designs, computer screens and mimic screens. These models must simulate the sensory memory, the pattern recognition (objects and speech) and the perceptual knowledge representation. HOS and A^3I models give emphasis in the spatial perception and the display of spatial information. In the NPPs, the time-space characteristics of the sensorial human behavior doesn't have a direct relation with the systems dynamics and can be treated separately from the model, as a human-computer interface performance. In other words, the manual control in NPPs are more related to signs instead of signals. So, we need only a submodel for signals knowledge representation in terms of signs in the sensory memory, i.e., perception is reduced to monitoring task. Now, we are going to observe how NPPs-HP models do that (CES and GOMS are excluded):

a) INTEROPS - dynamic monitoring strategy (priorities) and
opportunistic monitoring (Markov chains)
b) HUANG/SIU - parameter/message filter threshold and priorities
c) COSIMO - cognitive filter (salience function)
d) CAMEO - salience function

In particular, the HUANG/SIU model identifies three types of monitoring: a) alarm monitoring, b) specific monitoring (by shift supervisor request), and c) general monitoring. The a) and b) types are considered always successful. For the third one is applied the stress dependent filter threshold and the priorities concept.

The optimal condition could be achieved if the filter threshold is combined with the cognitive filter, in view of the necessity in joining the parameter salience for the task and the operator stress in the monitoring activity.

Crew model

Only provided by the HUANG/SIU model.

Motor submodel

The human motor behavior has the same characteristics as the human sensory behavior. So, it could be treated equally as in the perception submodel. The difference is that the feedback effects of the motor activities are taken into account by the changes occurred in the system parameters being monitored.

Attention allocation submodel

This model must manage the attention resources between the perceptual, cognitive and motor channels.

Only the CAMEO, PROCRU, and A^3I models treat this question under a comprehensive view. For the last two models, due the fact that the attention allocation is critical in the aircraft cockpit designs.

For the NPPs, cognitive tasks are the main concerns in the INTEROPS, COSIMO and HUNG/SIU models. Below, the approaches for this problem are shown for each one.

PROCRU - observation noise/signal rate
A^3I - WLAM (WINDEX+queuing theory) - see Elkind, et al., 1989
INTEROPS - queuing theory and priorities of the tasks
COSIMO - CBB (not totally implemented), deal with problem strategy
and strategy focuses
HUANG/SIU - priorities for the tasks
CAMEO - multiple resources with an attention allocation theory.

The better theory is clearly the WLAM methodology.

Cognitive Architecture and Control

The mentioned HPMs use the following architectures:

PROCRU - HIPF, procedural attachment, and production rules
INTEROPS - HIPF, means-ends analysis, hypothesis and test, evidence chunking(procedural attachment) and agenda
COSIMO - BBA and procedural attachment (CIF)
HUANG/SIU - HIPF and agenda
A^3I - BBA, procedural attachment(demons/daemons),production rules, and agenda
HOS - HIPF(Human Information Processing framework), production rules
CES - production system
GOMS - production system
CAMEO - HIPF, procedural attachment, and agenda.

The tendency is in the use of a HIPF. However, it is necessary a cognitive architecture that can deal with the knowledge-based behavior. There are four options. The first is A^3I that tries to solve this problem by using the decision-by-algorithms method. The second approach is SOAR, described in a recent book by A. Newell (1990), who claims for his theory as the only one which can deal with the knowledge level (see comments of Newell about cognitive architectures structures, 1989, 1990). The third one is the INTEROPS approach, which uses the qualitative reasoning about the plant physical processes in the LISP language. The fourth one is the CES modeling of the operator intention in emergency situations.

None of these approaches seems to be satisfactory. Decision algorithms are restrict to the field of a specific application. The qualitative reasoning generates ambiguities not totally solved by any method (see chapter 2.2.3). The creative capacity in the knowledge-based level is related mainly to the learning capability. The mechanism of learning new rules in SOAR is called chunking (see chapter 2.2.2.1). However, neurophysiology studies seem to point out that the human brain has a hierarchy of structures, at least in two main levels.

One is a programmable, sequential processor that operates consciously to the human. It has a rather limited capacity and speed, and its main task is to take care of the data handling in unique conditions calling improvisations, rational deductions, and symbolic reasoning. It functions as a high-level coordinator or controller of the second part, the main data processor.

The main processor has many features of a distributed, parallel-processing analog computer with high processing capacity. It functions mainly subconsciously to the human.... (Rasmussen, 1986).

Johnson-Laird (1988) is of same opinion: ....different levels of representation: high-level explicit symbols and low-level distributed symbolic patterns...the low level processes implement the high-level rules.

Another problem that is managed with difficulty by the productions systems, like SOAR and ACT, is the capacity in treating uncertainty and fuzziness. The most critical problem is that of human categorization.

Instead of forming a property list for a category, we store 'a best example' of the category (or possibly a few best examples). The system....classifies the new example as an example of the category in the nearest - neighbor sense...(J. A. Anderson, Foreword, in Kosko, 1992).

This is an induction mechanism and in the Induction Theory (Holland et al., 1986), classifier systems allow a broad range of inductive mechanisms from rules strength adjustments to analogies. Many of these mechanisms can be controlled by inferential rules. The new rule discovery procedure in a classifier system is the genetic algorithm that manages the uncertainty of the search space, reducing uncertainty during the problem solving. It requires the use of test outcomes (samples) to estimate regularities in the search space as well as their distribution. The focus is on subspaces and the contained elements instead of paths and their ultimate destinations or goals (Booker, 1990).

In the same way, connectionist architecture cab modify their connections strengths through the use of fuzzy sets theory (Kosko, 1992) to treat adequately the problem of categorization. This suggests the use of fuzzy production rules (Reason, 1990) instead of chunking or classifier systems to discover new rules suitable to a new situation.

A third question is concerned to a hierarchy of goals that govern the cognitive architecture. Frames of fuzzy rules can trigger scripts through daemons/demons according to a hierarchy of goals. If the fuzziness of the situation is such that any goal is not identified, thus it is necessary to apply a specific plan. While frames is due to the work of Minsky(1985), The theory of Goals, Scripts, and Plans was developed by Schank and Abelson (Schank and Riesbeck, 1981; Schank and Abelson, 1977). To understand the one's goals, it's necessary to use comprehension in natural language. The Conceptual Dependency Theory(CDT) (Schank and Riesbeck, 1981; Schank and Abelson, 1977), using semantic nets and coupled with Goals, Plans, and Scripts is still the best tool to heal with natural language.

All of these knowledge atoms (Smolensky, 1986, see in Levine, 1991) - goals, frames, and scripts, are examples of schemata (schema in singular), a neuropsychologist notion introduced by Bartlett in 1932 (see Reason, 1990). To deal with schemata in the connectionist approaches, harmony theory was used (Smolensky, in Rumelhart et al., 1986). There are, however, additional types of subsymbolic knowledge representation for the schemata. The most interesting are the FCM(Fuzzy Cognitive Maps) and the ART(Adaptive Resonance Theory) (see in Kosko, 1992; Levine, 1991).

In the case of BBAs, we must compare the COSIMO, and A^3I approaches. The table 1 is autoexplanatory.

Generation of errors

Memory effects

The most important effects to be considered in the memory are the size and decay of the working memory. INTEROPS, HUANG/SIU, and A^3I provide a treatment for these effects.

Errors treatment and stressors

The errors can be classified in: slips, lapses and mistakes. Below are the approach given to the human errors in each model.

	COSIMO	A^3I
DBB-KS	-get-environment -decoder -cognitive filter -semantic interpreter(similarity matching and frequency gambling) -executer	-mission goal decomposer -rules -algorithms -demons -activity -equipment
DBB-KL	-environment cues -signal -sign -received cues -set of hypothesis -CIF (Current Instant. Frame) -actions	SOM queues: -current activity -working goals -pending activity -scheduled activity -signals
CBB-KS	-put-problem -stop-problem -start-strategy -update-strategy -initiate focus -update-focus	-after -during -overlap -start-up -start-by -end-at -end-by
CBB-KL	-problem -strategy -focus -policy -agenda -task	-perception -UWR -motor -TLM -scheduler

TABLE 1 - BBAs COMPARISON

PROCRU - high noise/signal ratio inducing loss of information
COSIMO - slips (perceptual errors), lapses (tasks deletion)
HOS - none
CES - none (to be integrated with CREATE, a program for human reliability)
INTEROPS - slips (perceptual errors, forgetting), lapses due a time pressure (tasks switching and deletion)
HUANG/SIU - slips (perceptual errors, forgetting), lapses due to stress(tasks deletion)
A^3I - forgetting
GOMS - none
CAMEO - errors inducing mechanisms that depend on the attention resources

To get better results we have to combine COSIMO and HUANG/SIU perceptual errors for slips and INTEROPS and HUANG/SIU for lapses. HUNG/SIU, A^3I and INTEROPS use the same approach for the forgetting errors. Also the parameters measuring attention resources must be used to induce errors like in CAMEO.

SUMMARY

1. Cognitive architecture and control - HIPF(combination of INTEROPS, COSIMO, CAMEO, and HUANG/FU structures) + fuzzy rules + NLP(Natural Language Processing) + implementation as low level cognition with meural networks and fuzzy logic
2. Attention allocation - A^3I
3. Crew model - HUANG/SIU
4. Perception, memory and errors - HUANG/SIU modified by INTEROPS time pressure function and COSIMO cue salience function, and attention resources level in CAMEO.

2.2.3 CRITERIA FOR THE FUNCTIONS DYNAMICALLY ALLOCATED - APPLICATION OF THE ANALYTICAL TOOLS FOR THE EVALUATION OF THE OPERATOR SUPPORT SYSTEMS AND ITS HUMAN-MACHINE INTERFACE

As we saw in the chapter 2.2.2.1, Supervisory Control Mode was proposed for guiding the design of human-machine systems that have a long delay time between input and system response. In this control paradigm, the operators has the function of monitoring the system, detecting, diagnosing, and correcting the failures in the system performance. However, this creates new design questions (Eggleston, 1987): 1) How will the system maintain operator alertness over a designated, watch period? 2) How will signal malfunctions and their causes be communicated to the supervisor? 3) How should the human be brought back into the control loop in case of an emergency?

We could add to this list the following: 4) How could the operators be still skilled to deal with such emergency after a long period of supervising time?, 5) How could the operators be trained to deal with non-anticipated accidents in such emergency?

Clearly, the Supervisor Control Mode can not be used in an unfamiliar situation, in which the system control is outside from its design limits. In this case, a cooperation between the humans and the machine becomes necessary for making correct operation decisions. This carries us to a new conception: the collaborative control mode(CCM), where an adequate interface must be designed to give the proper information support for both humans and machine. To construct such interface, it is necessary two more items: 1) mental models, that represent the system as seen by the operators, and 2) an architecture that synthesize the entire system consisting of humans, machine, and interface (Eggleston, 1987; Kneer/Schryver, 1989).

An architecture for an intelligent interface like above was proposed by Rouse, Geddes, and Curry, in 1987 (Rouse, 1991), to be implemented in the McDonnell-Douglas F/A-18 fighter aircraft cockpit. It is presented as a framework to be used either as a conceptual design or in a specific design, and is outlined in the figures 1/2, for application in nuclear power plants.

The architecture emphasizes the characteristic of being designed entirely as software, as should be in case of a human centered design. The hardware is external and is represented by the process control system(PCS) and its controllers/actuators, the sensors signals processing and the analog/digital interface, and the human-machine interface in the operator's console or CRTs, that substitute the instrumentation panels used in the past.

The states of the world(see chapter 3), system, and operators are defined in the table 2. Particularly, the system state is provided by a (DSS)Decision Support System, similar to the DASS and COSS, which were designed after TMI. The difference here is that the DSS actuates not only as a system safety parameters status display (SPDS) but it provides operation guide to the process control system(PCS), the operators and the intelligent interface (figure 2).

The (IMA)Interface Manager (figure 3) receives messages and requests (M/R) from the PCS and the functions allocator(FAL). The IMA manages these information in order to utilize optimally the human-machine interface according to the available input/output channels resources in the operator cognitive model (OCM), as well as taking into account the information priorities.

The priorities are determined by the relevance of the current situation. The OCM gives priorities to the M/R, according to the hierarchical representation of goals, plans, scripts, and actions of the operators (Schank, 1981, 1977). The PCS gives priorities to the M/R, according to the operators awareness about specific parts of the plant current situation, that are not included in the OCM.

Scheduling is a standard problem in this case, because the operators don't share time in the same speed as the computers do.

After prioritization and scheduling, the IMA selects the modality and the format of the information channels according to the available resources. Modality selection uses the multiple resources theory described in the chapter 2.2.1 for attention allocation. The choices for the channels modality can be visual-spatial, visual-verbal, auditory-spatial, auditory-verbal. Formatting must be chosen in terms of aggregation and abstraction space (Rasmussen, 1986). Different display windows could represent the same information in this space.

However, to avoid frequent changes between information channels, which could confuse the operators, it is necessary to define default modalities and formats for different types of M/R. Deviations should be only permitted if certain conditions are met, and in this case the operators should be informed about the reasons for this.

The error monitor(EMO), figure 4, is one of the most important parts in the collaborative control model. Its function is to avoid that operator's inappropriate action has disastrous consequences for the plant. However, EMO should not limit the operators' capacity for creative thinking in unfamiliar situations of accidents and correcting themselves(see for items a) and b) from the IAEA basic principles, chapter 2.1).

So, EMO must first feedback information in order to provide elements to the operators in the detection and corrective actions for a wrong operation behavior. Second, depending on the situation seriousness, the EM should recommend to the FAL that control be allocated to the automatic system in the PCS, in order to avoid damages to the plant and the world environment.

Nevertheless, there are accidents characterized by unfamiliar situations. In these situations the EM could not know if the automation is possible, but even in this case, the EM would determine if what the operators are doing are consistent with the goals and plans that they are following to bring the plant to a normal condition. These goals and plans must be consistent with the procedures synthesized in the DSS.

There are basically two types of errors: omission and commission errors. Omissions are due to the attention failures(slips) and memory failures(lapses), as in monitoring and procedures tasks. Commission errors (mistakes) are due to the misapplication of good rules or to the application of bad rules (Reason, 1990; Rasmussen, 1986).

Besides this kind of identification, the EMO might verify the coherence of the operators' actions with the current goals, plans, and scripts (Schank, 1981, 1977), which is provided by the operator cognitive model. Rouse identified three types of problems in doing this. First, it is necessary a substantial knowledge engineering. Second, it is necessary feedbacks inside the error monitor to help in identifying errors that are consequences of previous errors, as in the case of choosing an inappropriate procedure, generating additional erroneous actions. Third, errors of commission depend heavily on degree of the system structure. Since errors of commission represent operators intention that go outside of the procedures domain, they can be irrelevant, depending on the situation.

The error classification as slips, lapses, and mistakes must be communicated to the operators before they can accept it as an erroneous behavior, because mistakes can mean misunderstanding.

Excessive workload is responsible for the generation of the errors for an operator well-trained and in good physical and psychological conditions. The FAL must avoid workload, allocating tasks between automatic control systems and operators according to the attention resources (see chapter 2.1, item d) of the IAEA basic principles).

It is possible that in some situations a consequence model becomes necessary to evaluate correctly an error recovery. Expert systems in Probabilistic Risk Assessment(PRA) could be useful for this.

Misclassification is another problem that should be solved in order to permit that operators have free to use innovative actions in a beyond design basis accident or non-anticipated situation. Again, similar in the case of mistakes, the error monitor must first advise the operator about the detected errors and recommend corrective actions, to be confirmed by the crew.

There are three basic types of errors recovery: monitoring, feedback (as in case of mistakes), and automatic control. In the latter, the recovery depends on the feasibility of the control, because some functions must be always automated, others never automated, and there are functions that can be performed by both humans and computers (see chapter 2.1). In the automatic control mode, the misclassification of errors should be avoided.

In conclusion, in some situations, the recovery corrective actions must be approved by the operators. In other situations, the automatic control system will actuate, unless the operators stop it. The treatment of errors will be showed in the chapter 2.2.5.

The FAL, figure 5, is the second most important part of this collaborative control model(CCM). The basic philosophy behind FAL is keep the operator with the maximum degree of control, unless the attention resources allocation be overloaded or the abilities to do the tasks don't be enough.

First, a queue of tasks with priorities is determined according to the operational situation. Additions or deletions to this set are done by the EMO and the PCS.

The tasks need to be specified with a time-line analysis chart defined by four vectors (see chapter 2.2.1):

1) Task priority,
2) A duration of time within the task could be rescheduled,
3) Estimated completion time for the discrete tasks,
4) Demand level.

Besides this, the tasks receive a primary allocation (see 2.1):

1) Human only (H)
2) Computer only (C)

3) Both (H/C)

Tasks designated as (H) are allocated to the operators. Tasks designated as (C) are allocated to the computers. Tasks designated as (H/C) are allocated to the operators, unless a impossibility arises due to:

1) An operator's preference to allocate the function to the computer,
2) The operator doesn't have enough attention resources or abilities to do the task,
3) The operator is unaware of the task.

In case of an impossibility, the FAL must inform the operators. If the performance of the operator becomes degraded along the time, in a specific task previously allocated, the FAL will try first advice the operator about the situation. If the task performance continues to be degraded, the task will be allocated to the automatic control system.

This reallocation philosophy depends on the speed of the performance changes. Abrupt changes require immediately automation. Another important point is the coherence with the IAEA basic principles, item e) (see chapter 2.1). The reallocation must be done in the human-computer direction and NEVER in computer-human direction.

The figure 6 shows the operator cognitive model(OGM). It is composed by three submodels: intent model, resources model, and performance model.

The intent model is composed by two modules: script applier and plan inferencer (Schank, 1981, 1977), each one with its own knowledge base. The script applier updates the active scripts according to the operators' actions. Unresolved actions are passed to the plan inferencer that tries to find the plans which are coherent with the active goals and the unresolved operators' actions. If the plans are found, the script associated with them become active. If not, unresolved actions are passed to the error monitor. The outputs of the intent model are: activities, awareness, intentions and decoded motor actions. It includes a list of active goals, plans, and scripts.

The resources model is the same as WLAM described in the chapter 2.2.1. The human performance model can be implemented using a combination of the cognitive architecture characteristics recommended in the chapter 2.2.2.2B.

The system state is provided by a decision support system (DSS), which is coupled with a simulator faster than real time (Kalman filters could be used here, see Gofuku, 1989, 1988) to estimate and predict the system state parameters (SSP).

DSS receives the plant validated signals, and together with SSPs, provide a diagnostic of the plant operational status, using the Rasmussen's diagnostic sequence technique and his search modes (topographic, symptomatic, and hypothesis and test) (Rasmussen, 1986). According to this status, it activates a set of goals, plans, and scripts (procedures). In case of non-anticipated situations, it triggers a "Problem Solver" program that initiates a diagnostic search strategy which can be one of the above (Rasmussen, 1986). In chapter 2.2.4 we will see the experiences in validating such approach.

The hardware parts of the system are concentrated in the PCS and the HMI. PCS with its controllers are designed using digital control models. Among these, we find the intelligent control based in the artificial intelligence and fuzzy logic (see Bernard, 1989, 1991, 1992, 1993). In the chapter 2.4, we will describe the M.I.T. research in this field. Fuzzy logic is not totally accepted in some countries like USA, although it has nowadays a fast development in Japan. HMI can be designed using a combination of techniques (see Downton, 1991) like HPM (see chapter 1) and GOMS (see chapter 2.2.2.2B), and an ecological approach (Vicente/Rasmussen, 1993; Rasmussen/Vicente, 1992; Fujita , 1993; Sage, 1992). In chapter 2.3, the Software Engineering will allow treat this and the problems related such as real-time, validation, and design process will be discussed.

As we can observe, all the software in the CCM is knowledge-based, and can be considered as an expert system. How is the most adequate knowledge representation and reasoning mechanism (inference engine) for each structure of the CCM?

This question should be answered by two disciplines that complement each other: cognitive psychology (Stillings, 1987) and artificial intelligence (Firebaugh, 1988; Winston, 1992). The cognitive psychology provides two types of knowledge representation: declarative (propositions and mental images) and procedural. Propositional knowledge can be represented by semantic networks, scripts, frames, and schemes. Procedural knowledge can be represented by production systems. In contrast with the heuristic reasoning of humans beings, IA uses also representation based in logic (Bratko, 1990). Three types of logical reasoning are recognized by the cognitive psychology: deduction, induction, and abduction. Within the reasoning problem, the IA brings the questions of search and control in the problem space. There are two types of search, blind and heuristic, and five types of control (production systems, blackboard, agenda, procedural attachment, and means-ends analysis). Blackboard systems, for example, combine several control strategies such as scheduling like in agendas, focus of attention like in production systems, and reasoning about actions (rules). Nowadays, the model-based deep reasoning arises as an alternative (Bobrow, 1985; Widman, et al., 1989; Amsterdam, 1993; Faltings/Struss, 1992; Dobrzeniecki/Lidsky, 1989). The control knowledge are sometimes referred as a meta-knowledge (Coyne, 1990).

Using the language of the Systems Theory applied to the knowledge representations, we can distinguish between representations of the system structures and its behavior. The structure is related to the concepts of decomposition (objects or components), taxonomy (objects variants or classes, properties, and instances), and coupling (relation between objects) - see

Zhang/Zeigler, 1989.

For the structures, the representation could be the declarative knowledge (or propositional): objects and relations as semantic networks, objects and properties as frames or semantic networks, instances and classes as semantic networks, frames, or rules (Coyne, 1990).

The behavior could be represented by empirical relations between the objects, which can be declarative (graphical or statistical) or procedural knowledge. The latter can be rule-based or model-based knowledge. The model can be continuous (differential equations or qualitative physics) or discrete (event, activity, process or tasks) - see Zhang/Zeigler, 1989.

The most part of the expert systems in the nuclear area were developed with procedural knowledge based in rules (Bernard/Washio, 1989; IAEA-TECDOC-542, 1990). Three deficiencies can be found in this approach: 1) the rules do not have usually a close relation to the physical phenomena they are representing; 2) the rules do not take into account the dynamic behavior of the systems and, therefore, the temporal history of the system variables and parameters; 3) the rules usually do not take into account the abstraction hierarchy in the different levels of the system structures (Bernard, 1992; Lind, 1982; Bizantz/Vicente, 1993). With these deficiencies, it is impossible to construct a reliable knowledge base, mainly for the DSS, a critical part of the CCM, in view of its responsibility to diagnose the system state. The right option for this should be an object-oriented programming using a procedural representation based in physical models, in different levels of abstraction and aggregation. Two different systems, however, could exist in the DSS. One based in production systems for normal and anticipated accidents; another one based in qualitative models for beyond design basis accidents.

Anyway, a combination of the representations and reasoning techniques mentioned above, to be used in a specific application like in the nuclear power plants, is one of the main challenge for the designers (Bernard, 1992).

The world state in the CCM concerns the external world modeling in different levels, not only in the organization & management of the plant operation aspects but also in the influences generated by the economical and political/sociological environment. This can be considered the second major challenge.

In spite of the difficulties, these two challenges must be overcome if we desire to improve the safety of the new nuclear power plants.

The OCM was discussed in the chapter 2.2.2, and the EMO as well the IMA will be discussed with more details in the chapter 2.2.5 and 2.3, respectively. The PCS, controllers, and signals processing will be treated in the chapter 2.4. Thus, the structures of the DSS and the FAL will be more detailed in the following lines.

DSS(DECISION SUPPORT SYSTEM)

The DSS has to provide the following information to the rest of the CCM:

a) dynamic state in terms of estimation and prediction of the system state variables (quantitative analysis);
b) operational modes and failures status of the subsystems (qualitative analysis);
c) information about the upcoming and current operational phases and their applicable procedures.

The item a) will be covered by simulator which works faster than real-time because of the prediction characteristic necessary for the system. Kalman Filters are still the best way to reduce the number of calculations in a simulation through the estimation techniques. These filters can be preadjusted using a best estimated computer code (Gofuku et al., 1989).

For covering the item b), it is necessary a hierarchical structure of functions and systems components in different levels of abstraction, as well as a diagnostic search technique through this structure.

Rasmussen (1986) identified three steps or activities until achieving the actual system state, each one generating a state of knowledge resulting from the information processing: activation and alert state, observation and set of observation, identification and system state. The first step lies in the skill-based level and constitutes the decision phase. The other two constitutes the knowledge-based analysis state phase (a system state qualitative estimation). A shortcut between observation and the system state (a stereotyped process) can sometimes bypass the identification stage. The item c) must be divided into three phases: 1) knowledge-based consequences analysis (a qualitative prediction for the system state), 2) knowledge-based planning, 3) actions execution. The first step is accomplished by two steps: 1) Interpretation generating ambiguous situations and 2) evaluation by the performance criteria (safety and production goals), generating ultimate goal to solve the ambiguities. Then, the interpretation process will continue to process the information in order to generate a target state for the system. The second and third phases involve three more steps: 1) tasks definition and tasks set, 2) procedures formulation and procedures set, and 3) procedures execution (Rasmussen, 1986).

However, there are many shortcuts between the many steps connecting the information activities processing of the state and consequences analysis phases with the knowledge state of the planning phase. These connections constitute the rule-based level. They are called stereotypical behavior or processes: 1) activation of a task interruption, 2) observation causing perception in terms of tasks and procedures to be done, 3) identification in terms of target state, tasks, and procedures, 4) interpretation in terms of tasks. There are also shortcuts among the knowledge states between system states analysis phase and the planning phase. They are called associate leaps: 1) system state/task association and 2) set of observation/task association. In the skill-based level, a shortcut between activation and execution is found (Rasmussen, 1986).

Coming back to the item b), the abstraction hierarchy and the identification or diagnosis problems will be discussed. The abstraction hierarchy levels can be identified as following (Rasmussen, 1986): 1) functional purposes, 2) abstract functions, 3) generalized functions, 4) physical functions, 5) physical form.

The level of physical form

It refers to the physical description and configuration of the system and its parts.

The level of physical function

Functional description of the systems and its parts.

The level of generalized function

Functional description of the system without linking with its parts.

The level of abstract function

Overall function of a system represented by a generalized causal network, in terms of mass, energy, and information flow.

The level of system purpose

Purpose of the system means the intended function effect of the system upon its environment.

The MFM(Multilevel Flow Model) is an example of this process of hierarchization in levels of abstraction (Lind, 1982; Sassen/Jaspers, 1992).

Rasmussen (1986) identified also three types of diagnostic search strategies: 1) symptomatic, 2) topographic, and 3) hypothesis and test. The topographic search is performed by a good/bad mapping of the system through the abstraction hierarchy levels.

This kind of search is adequate for normal operation, because it is based in mental models derived from the design for the normal operation.

The symptomatic search is based in the information content of observation to obtain identification of system state, instead of the location of the information source. The search is done by matching the observed state of the system to a prestored set of reference standard states or generated by an on-line simulator (hypothesis and test search). Hypothesis can be triggered by an uncertain or fuzzy topographic search. Symptomatic search can be used in anticipated disturbances which are well known in the design. In case of nonanticipated disturbances (unfamiliar situation or beyond design basis accident) the hypothesis and test search must be used. This kind of search uses a qualitative reasoning in terms of causal relations among objects and components, as well as states and events, instead of relations among variables.

The knowledge representation in the DSS can be accomplished using the abstraction hierarchical level:

Level of physical form

Physical objects and physical properties as semantic networks or frames;
instances and classes of physical objects as frames or semantic nets or production rules;
physical objects and causal relations as semantic networks and facts (events, symptoms, and states);

Level of physical function

Physical objects and functional properties as semantic networks or states frames.

Level of generalized function

Nonphysical objects (variables) and deterministic relations as semantic networks and facts (differential equations).

Level of abstract function

Nonphysical objects (flow of mass, energy and information) as a semantic network of causal relationships.

Level of system purposes

Nonphysical objects and external causal relations as semantic networks and facts (goals, plans, scripts or procedures).

Semantic networks can be considered the most basic level of knowledge representation. Semantic networks can be hierarchized and then converted to decision trees or decision tables which themselves can be transformed in production rules (Carnico, 1989). Causal and deterministic relations are behavior representations based in models. Properties, instances, classes are structures representation. Facts can be classified in both types: physical (structures), nonphysical (behavior) based in discrete models.

The uncertainties in the knowledge could be represented by the following techniques: 1) fuzzy sets, 2) Bayesian statistics, 3) nonmonotonic logic, 4) certainty factors, 5) truth maintenance reasoning, to be incorporated within production rules.

Production systems are controlled by a basic three-part cycle: 1) matching, 2) conflict resolution, and 3) action. The cycle can be implemented by two manners: forward chaining (FC) and backward chaining (BC). In FC scheme the movement is toward the conclusions direction in the physical form level. In BC, is to the goals direction in the level of system purpose. It is necessary to achieve first a goal and they find the diagnostic conclusion in the lowest level. All the knowledge representation have priorities which are used to compose an agenda. To make more easy the manipulation of the knowledge, the most of the production rules can be organized as frames and scripts, which also provides a mean to represent, the stereotypical behavior. The individual uncertainties in the production rules can be joined to give the global uncertainty of the whole frame. The diagnostic system can skip to a more appropriate frame in case of doubt about the reliability of a certain frame. If more information is needed, the frame will activate a procedural attachment or demon/daemon. These characteristics are useful in case of hypothesis and test type diagnosis. Demons are useful also to activate special procedures called scripts which involves sequence of events, with goals and plans, like in the operational procedures at a nuclear power station.

MBD(MODEL-BASED DIAGNOSIS)

Felkel (1990) defines the role of MBD as follows: "The real question is not qualitative or quantitative models but to what extent (in view of information goal) they must be both quantitative and qualitative".

In this research at GRS(Gesselschaft für Reaktor Sicherheit mBH - Reactor Safety Commission) he looks for expert systems that satisfy several of the following requirements:

1) quantitative process description
2) qualitative process description
3) integration of both to be used simultaneously
4) real time aspects
5) time dependency aspects.

To describe the quantitative and qualitative processes, it is necessary a MFM(Multilevel Flow Model, Lind, 1982; Stassen & Jaspers, 1992) and a structure of hierarchization and abstraction-aggregation levels (Rasmussen, 1986; Iwasaki, 1992).

At the top of this structure, there is the functional purpose level, that is characterized by two ultimate goals: electricity production and safety (prevent leakage of radioactive material) goals. Examples of structures for these goals can be found in Stassen/Jaspers(1992), Itoh et al.(1993), and Monta et al.(1992).

The next level is related to the abstract functions, which are the energy and mass balance maintenance that follows the goals. This is represented by the MFM.

The levels (generalized functions-GF, physical functions-PF, and physical forms or components-PC) correspond to object classes as defined by Robinson(1989):

1) physical-system classes(GF), such as flow loop and heat transport networks,
2) basic physics classes(PF), such as heat sources, heat sinks, and material properties,
3) plant-components classes(PC), such as pumps, pipes, and valves and their functions.

To apply object-oriented techniques, it is necessary to define objects from the categories 2) and 3), which correspond to objects in class 1). Robinson defined the following objects for each class:

1) Physical systems:

   a) thermal-network
   b) hydraulic-loop
   c) hydraulic-network

2) Basic Physics:

   a) thermal-node(fluid-node or slab-node)
   b) reservoir
   c) heat-source
   d) flow-source
   e) transport delay

3) Plant Components:
   Fuel-pin
   Kinetics
   MIMO-controller
   Mixing-plenum
   SISO-controller
   Pipe
   Pump
   Tank (steam-generator, pressurizer)
   Valve (check-valve, flow-control-valve)
   and others.

A heat exchanger can be constructed from fluid-node and slab-node objects.

The thermal-network objects, for example, can be represented by the following equation:

$$\frac{dT}{dt}=A(t)+\underline{f}(t)\text{, } where$$

T(t) represents the vector of temperatures, A(t) is a time varying coefficient matrix, and f(t) a forcing function. These form the instances variables of the objects.

In the same way, the hydraulic-loop can be represented by:

$$a\rho\frac{dQ}{dt}=\sum_i F_{Bi}(Q)\text{, where}$$

a=geometrical parameter,
F_{Bi}=force term, the instances variables of the objects.

The instances variables depend, of course, of the object type in the plant components.

Some trials have been made to develop solutions of these equations in real-time or faster than real-time. One of these is PRISM(Power Reactor Inherently Safe Module) simulator (IWGFR/71, IAEA, 1989). Another one is the PRISM(Pressurizer Reactor Interacting Simulator Model) real-time simulator at the MIT for PWR-Type Multimodular Power Plant. One that is particularly interesting because of its estimation and prediction capabilities is TOKRAC (Gofuku et al., 1986, 1988, 1989). To achieve the objective of real-time characteristics, TOKRAC uses Kalman Filter to estimate unobserved variables and parameters by the plant sensors. This estimation is done in a faster-than-real-time calculation. Then a real time track of the simulation is done with the observed and estimated parameters and variables being the initial input of the program. Actually, TOKRAC estimates pressurizer surge line, flow-rate, steam generators break size, brake flow specific enthalpy, heat transfer rate, and flow rate. However, it does not have a secondary model, an asymmetric calculation with several loops, or a prediction for the future situation of the system.

The main concern is the use of Kalman Filters to estimate variables (reducing the calculation time) and to predict the system state. It can be used also for detection as an option to the production rules.

"Kalman Filters technique is a linear minimum mean-squared errors estimator of state variables using a linear system model and measurements" (Gofuku, 1988). A model can be represented by the following state and measurement equation in discrete form (Aström/Wittenmark, 1984):

$$x(kh+h)=\Phi x(kh)+\Gamma u(kh)+v(kh)$$

$$y(kh)=Cx(kh)+e(kh)$$

where v and e are discrete-time Gaussian white-noise processes with zero mean and the covariances are:

$$Ev(kh)\,v^T(kh)=R_1$$

$$Ev(kh)\,e^{T}(kh)=R_{12}$$

$$Ee(kh)\,e^{T}(kh)=R_{2}$$

Assuming $R_{12}=0$, the predictor will be

$$\hat{x}(k+1/k)=\Phi\hat{x}(k/k-1)+\Gamma u(k)+K(k)\,[y(k)-C\hat{x}(k/k-1)]$$

$$K(k)=\Phi P(k)\,C^{T}(R_{2}+CP(k)\,C^{T})^{-1}$$

$$P(k+1)=\Phi P(k)\,\Phi^{T}+R_{1}-\Phi P(k)\,C^{T}(R_{2}+CP(k)\,C^{T})^{-1}CP(k)\,\Phi^{T}$$

As an estimator, the Kalman Filter will be

$$\hat{x}(k+1/k+1)=\Phi\hat{x}(k/k)+\Gamma u(k)+K(k+1)\,[y(k+1)-C(\Phi\hat{x}(k/k)+\Gamma u(k))]$$

$$K(k)=P(k/k-1)\,C^{T}[R_{2}+CP(k/k-1)\,C^{T}]^{-1}$$

$$P(k/k-1)=\Phi P(k-1/k-1)\,\Phi^{T}+R_{1}$$

$$P(k/k)=P(k/k-1)-K(k)\,CP(k/k-1)$$

$$P(k/k)=P(k/k-1)-K(k)\,CP(k/k-1)$$

$$P(0/0)=R_{0}$$

As a detector or system identification, Kalman Filters can be used to estimate the parameter theta for a specific state of the system in the loss function derived from the principle of least squares:

$$J(\Theta)=\sum_{k=1}^{N}\lambda^{N-K}[y(k)-\Theta\varphi(k)]^{2}$$

where

$$\Theta(k+1)=\Theta(k)$$

$$y(k)=\varphi(k)\Theta(k)\ (k)+e(k)$$

and y(k) is the expected state and phi(k) is the measured state.

Once the system state was identified, estimated and the variables tendency were predicted, it is necessary a qualitative reasoning to evaluate the operational state of the subsystems and their modes of failures.

Dobrzeniecki and Lidsky (1989) classified the model-based analysis in five levels:

1) the physical systems that are to be represented,
2) mathematical models like TOKRAC,
3) qualitative simulations,
4) object-oriented models with constraints,
5) heuristic analysis.

At the top level, the methods employed in AI are found. Two of them are the most used: rule-based systems and frame-based systems. As said early, the first one is not adequate for large scale systems as in nuclear power plants. The second is more oriented to objects and can be combined with the diagnostic searches described by Rasmussen (1986). A good example of this is found in Fujita(1991). A plant abnormality model (PAM) is constructed as a mapping of the hierarchic abstraction-aggregation structure in the MFM, already described. The PAM contains objects that are knowledge sources or frames. In the abstraction functions level there are alarms frames corresponding to the safety functions abnormalities. These frames trigger other frames in the lower levels of the hierarchy. For situations not covered by alarms, there are the symptoms frames which are triggered by qualitative reasoning. All possible causes, however, are placed in a queue and analyzed for confirmation by a verification frame until the symptoms disappear. Finally, if the confirmation is done, there are guidance frames that are used to select the required operational procedure. The guidance frames have start conditions and completion conditions. The alarms frames are similar to the topographic search, while the symptoms frames are similar to the symptomatic and hypothesis-test searches. When a procedure is started, several tasks are scheduled to be executed. Procedures in this case are the same as scripts.

Below the heuristic analysis comes the Dobrzeniecki and Lidsky approach that uses satisfaction of the constraints through the hierarchic levels of the model structured in objects networks, a concept close to the frames technique. As the symptom frames could be triggered by qualitative reasoning in case of knowledge-based behavior, it is necessary some kind of qualitative simulation. With the help of the prediction evaluation in the mathematical models, it becomes more easy the qualitative analysis, in view of the fact that the variables signal direction can be known. With the help of the qualitative reasoning the consistency of the causal-effects between variables can be verified (Galperin/Evrard, 1991; Forbus and Falkenheimer, 1992).

The first methods of qualitative reasoning appeared in 1984(Bobrow, 1985). One of these was conceived by de Kleer and Brown(1985) who called it naïve physics (also, qualitative process theory, qualitative physics, common sense knowledge or mechanistic mental models), although these methods are, in fact, a qualitative calculus or qualitative differential equations based on confluences (of derivatives). Forbus called it QPT(Qualitative Process Theory, 1985,1992). Kuipers called it common sense reasoning about causality, qualitative simulation(QSIM), or causal reasoning (Kuipers, 1985; Crawford, Farqhas, Kuipers, 1992; see also Amsterdam, 1993). Widman/Loparo (1989) made a revision of the state-of-art in this field. D'Ambrosio(1989) extended the mathematics of QPT. Widman (1989) used a semiquantitative method like the constraints created by Kuipers for the differential equations. These constraints can be used to predict the system behavior. Oyeleye/Kramer (1989) introduced causal and non-causal in the qualitative modeling based on confluences. A revision of the methods used in qualitative analysis can be found in Fouché/Kuipers(1992).

Recently, Nigam/Bhastar (1992,1988) have developed a qualitative analysis using dimensional analysis (DA). With this tool they were successful in analyzing all the sequence in the TMI accident. Considering this method is very fast, it suggests that DA could be a possible tool for qualitative reasoning. Another attractive possibility is the fuzzy qualitative simulation (Shen/Leitch, 1992; and Kitamura et al., 1989). In this method, the constraints (qualitative variables) referred by Dobrzeniecki/Lidsky, are considered fuzzy numbers set. Another one is MIDAS (Model Interactive Display Analysis System) developed by Oyeleye/Kramer (1989) and based in the ESDG(Extended Sign Directive Group), an evolution of the confluences method.

Particularly, the fuzzy qualitative simulation appears to be a powerful tool, in view of its rigorous mathematical support to the uncertainties treatment in the variables, beside the TMS(Truth Maintenance Systems, de Kleer, 1986) and the Dempster-Stafer probability theory (Takahashi et al., 1989) for the uncertainties in the knowledge-base (inconsistences and imperfections). As suggested by Kosko(1993), neural networks(NN) could be the "eyes" of this fuzzy system. Neural networks are adequate for "learning" the knowledge of the system and can provide a plausible hypothesis set for the system state utilizing the signals of the sensors. NN also could be used for the signal validations itself. We will discuss more about these techniques in the chapter 2.4(MIT and ORNL).

REAL-TIME AND TEMPORAL REASONING

As it said in the chapter 2.1 time is the critical parameter for workload evaluation. During the work under time pressure, operators can commit several types of errors. Time has a psychological influence in humans and many operation phenomena related to it were described by Decortis/de Keyser(1988) and Decortis/Cacciabue(1988). The description of a dynamic system is a difficult problem in any field of the science or engineering. Trials to take into account time into the expert systems, including qualitative reasoning, can be find in Gonzalez(1993) and Van Brek(1992). As the OOPs(Object-Oriented Programming) are the most suitable systems for the diagnosis process in NPPs, their methods will be adapted in this analysis.

In object-oriented design, there are two ways of expressing the temporal characteristics: state transition diagrams and timing diagrams. In the book of Grady Booch(1991), considered a standard reference by the object-oriented programmers, the following text gives an idea of the OOPs approach:

"Each class (of objects) may have a state transition diagram associated with it that indicates how the time ordering of external events can affect the state of an instance of the class. A single object diagram represents a snapshot in time of an otherwise transitory event or configuration of objects; thus, we may use a timing diagram in conjunction with each object diagram to show the time ordering of messages as they are sent and evaluated. In some circumstances, structured English or a reasonably expressive PDL(Program Description Language) are appropriate substitutes for timing diagrams. Additionally, either timing diagrams or a PDL can be used to document the dynamic semantics of how process are scheduled in a process diagram".

The example given by Bernard(1992) shows how the problem of time ordering is critical for a correct diagnosis:

1) High pressure in a PWR pressurizer followed by a low pressure alarm can indicate that the PORV relief valve stayed open; but
2) Low pressure alarm followed by a high pressure alarm should indicate that the heaters actuated and stayed in operation.

Functions-oriented diagnostic rules like above lead to a conflict in the reasoning. In the object-oriented diagnostic rules, each object (heater or relief valve) would have a state transition diagram or timing diagram linked to it, and the time ordering can be evaluated to show how external events or messages can influence the object state.

FINAL CONCLUSIONS ABOUT DYNAMIC FUNCTIONS ALLOCATIONS

Dynamic functions allocation depends heavily on a reliable Decision Support System (DSS) and an Operator Cognitive Model(OCM). The Error Monitor(EMO) can be considered an OCM appendix because it uses the information that the human performance model generates for the operators' state. The role of the PCS(Process Control System) is: 1) to detect abrupt and very unsafe (system protection) changes in the system which are not suitable for the operators to manage; 2) to monitor safety parameters and inform the operators; 3) to detect tasks to which the operators are not aware and inform them; 3) to control the system in higher levels of the abstraction hierarchy (limitation systems) instead of controlling in lower levels (that is the task of the subsystems controllers using fixed setpoints - chapter 2.4). The EMO (chapter 2.2.5) and the PCS (chapter 2.4) are responsible for adding and removing tasks from the input queue in the Functions Allocator(FAL). This queue works with tasks priorities that are determined by the relevance of the situation. This latter can only be accomplished with an adequate system state diagnosis coming from the DSS and a world state information (systems dynamics - chapter 3). The evaluation of this system state in order to find the target system state is a task for the PCS. The FAL implements the allocation of the required actions for the tasks according to the operators' resources (given by the resources model in the OCM) and the system necessities. However, this allocation is always human centered unless resources lack, human errors, and very unsafe or abrupt changes are involved. The diagnostic (purpose="why level"), evaluation ("what level"), and implementation ("how level") phases correspond to the three levels of abstraction to be considered for a control task (Rasmussen, 1986). These three levels can move along the levels of abstraction during a dynamic work situation. The FAL will take over the actions for the automatic control system in case of a task deterioration. This is judged according to the task time line (see Wickens Theory in chapter 2.2.1). All the open tasks are due a matching between the tasks contained in the system state and the tasks identified by the intent model in the OCM and stored in the operators' state data. Messages and requests coming from the PCS and FAL are managed in the Interface Manager(IMA) and given to the operators crew through a human-machine interface(HMI). This is commented in the chapter 2.3.

The intent model in the OCM could use the scripts theory (Schank, 1981, 1977) as a knowledge representation and a linguistic reasoning. The Conceptual Dependency Theory(CDT) (Schank, 1981, 1977) is an adequate approach for treating symbolic knowledge within operational procedures which work like the scripts in the Schank theory, with goals and plans. The CDT has a Script Applier Model (SAM) and a Plan Applier Model(PAM). The PAM is useful in case of an unfamiliar situation in which there is no script(procedure) pre-established and the system has to infer what is the operators' plan according to the system goals. This is a problem solving in AI and the GPS(General Problem Solver) of Allen Newell was the first trial to treat it. Newell moved his research to SOAR(States, Operators, and Results) as an UTC(Unified Theory of Cognition). GPS used the means-ends analysis type reasoning while SOAR is based in preference between operators to be applied in the initial state to achieve the goal state. CDT uses a plan inferencer while SOAR uses subgoals generation as a creative behavior. The human performance model works as a task agenda with priorities and time line charts. It uses the resources model and the time pressure effects to evaluate the performance of the tasks execution, that can be monitoring involving perception, or actions involving motor activities, or both at the same time. It is an open question if the SOAR would generate errors mechanisms. In case of unfamiliar but anticipated situation, the SAM can use Minsky's frames to trigger the scripts(procedures). This is a procedural attachment control and the triggers are called Demons or Daemons. SOAR doesn't use frames but preferences between operators. Frames contain groups of production rules to deal with stereotyped situations (rule-based behavior).

The knowledge representation in the operators' long-term memory will consist of frames of production rules, scripts, and goals. This representation must follow, however, a hierarchy of abstraction levels. In these levels, operators' mental models about the system are represented. These mental models are causal (also qualitative or common sense) representations of the several system objects and their cause-effect relations, associated events, states, and classes instances. Semantic nets are the most basic representation for this objects network. They can be transformed in frames.

This is a contrast against the deterministic (also quantitative, numeric) models that are based in formal relations between the physical variables provided by the physics laws and the differential equations.

Deterministic models are used by the designers in the higher level control decisions. These involve interpretation of the consequences of the current system state evaluated with performance criteria in order to find a target state that is suitable for the situation. In normal operation, these steps are bypassed by the operators using stereotyped behavior. In the lower-level control, the actions are performed by the individual subsystems controllers.

However, in an unfamiliar and nonanticipated situation the operators have to go through the entire hierarchy of abstraction to select the right level at which the control should start. Higher levels of abstraction means higher priorities and also high-level behavior(knowledge based level). The operators have to judge the consequences of the disturbance to find priorities (purpose and abstraction functions), the counteractions (generalized and physical functions) and the root-causes (physical functions and forms) to find the resources and means for actions (procedures selection). The root-causes diagnosis can be done through a topographic search. Symptomatic search are used for anticipated accidents (frames!). The frames will use fuzzy production rules that can trigger a topographic search when the uncertainties of the rules are such that they are no more longer valid (Reason, 1990; Hunt/Rouse, 1984). The topographic search will be done in the topologic net of the system objects comparing the system state to a model of normal operation. Combination of causal(human) and deterministic(computer) should be used in this model to obtain a coherence between the two analysis and solve ambiguities. Also for the consequences analysis of the disturbance this combination will be necessary.

The DSS being an important part in the system, responsible for giving the system state to the operators, must use the same mental models as the humans and must use real-time simulators to complement the causal reasoning.

As there is more relationship between causal reasoning and the system faults, the programming must be object-oriented(OOPs), in view of such causal reasoning are based on objects, states, and events. This mental model has many similarities with semantic nets in the script theory but also with the elements (objects, states, goals, and operators) in SOAR.

There are many common sense models and reasoning. They can be classified according to the following level of hierarchy: space, time, quantities and measurements, physics, minds, and society models. For the application in discussion here, it's necessary only to take into account the time quantities/measurements, and physics models. Mind and Society models will be seen in the chapter 3. Space models deal with movements and in a process control for NPP, it is not so important as in transportation systems, for example.

Temporal logic (Van Beek, 1992; Gonzalez,1993; Davis, 1990) has been considered in the last years as a method to think in terms of time. It is useful when combined with object-oriented programming and model-based simulation. Quantities and measurements are linked by qualitative differential equations(QDE) which can be simulated by QSIM(Qualitative Simulation; Kuipers, 1986, 1992) or by the confluences methods (de Kleer, 1985; Oyeleye/Kramer, 1985,1989). However, QDE must be constructed from the physics phenomena which are more close to the objects-oriented structure. This carries us to the physics models (also called naïve physics or models based in first principles) or Qualitative Process Theory (QPT) (Forbus, 1985). Two approaches are considered in the development of such physics models: QPE(Qualitative Process Engine; Forbus, 1990) and QPC(Qualitative Process Compiler, Kuipers, 1986, 1995). QPE is based on an ATMS(Assumption-based Truth Maintenance System; de Kleer, 1992) whereas QPC is built in a frame-based knowledge representation and, therefore, more suitable for an object-oriented approach. However, common-sense reasoning should handle incompleteness of knowledge (Gryzmala-Busse, 1991; Graham/Jones, 1988) which only could be treated in a nonmonotonic logic(NML). The most popular NML have been the ATMS from de Kleer, although there are other techniques such as modal logic, autoepistemic logic, default logic, circumscription and plausible reasoning (Gryzmala-Busse, 1991).

Common-sense reasoning should also handle variables uncertainties, in view of the QDEs. The methods to treat this can be classified as follows (Gryzmala-Busse, 1991): 1)one-valued quantitative approach, i.e., Bayes' statistics, belief networks with genetic algorithms (Rojas/Kramer, 1993) and certainty factors; 2)two-valued quantitative approaches (Dempster-Shafer Theory); 3) Set-valued quantitative approaches(fuzzy set theory).

In the technical literature we found two important methods: 1) one using TMS and Dempster-Shafer probabilities theory (Takahashi, Kitamura, Sugiyama, 1989); 2) another one using fuzzy logic (Kitamura, Buba, Takahashi, Sugiyama, Washio, 1989; Shen/Leitch, 1992).

The integration of qualitative and quantitative reasoning is done by verifying the consistence of the qualitative versus numeric results. Forbus (SIMGEN, 1992), Kuipers (1986), and Galperin (1991) give examples of this integration.

The best model to be chosen is still an open question. Zeigler (1989) observes that the Oyeleye/Kramer method didn't solve all the ambiguities problems in the causal reasoning. Causality is also a great problem concerning to the concept itself (Iwasaki/Simon, 1986; de Kleer/Brown, 1986; Iwasaki/Simon, 1986).

Zeigler uses the concepts of endomorphism and intelligent agents. These concepts arise when an object has models of other objects. So, the object can be modelled several times into the system. Zeigler makes use only of numeric models. However, as objects have similarities with frames, it is possible that someone might create fuzzy objects (Graham/Jones, 1988) triggering qualitative models to be used in a complementary way. Object-oriented approach as used by Zeigler and logic rules with non-monotonic reasoning are two complementary techniques for knowledge representation (Evrard, 1993). Considering that OOPs are adequate to take into account uncertainties levels for the system, causality could be evaluated by the propagation of constraints through the levels.

2.2.4 EXPERIMENTAL EVALUATIONS - USE OF SIMULATORS TO COLLECT DATA FOR THE FUNCTIONS ALLOCATION

2.2.4.1 JAPAN

The IODA(Integrated Operator Decision Aid) system for BWRs is a known experience with experimental evaluations of man-machine systems (Fukutomi et al., 1992). IODA is composed of three subsystems: a standby system management system(SSMS), a disturbance analysis system(DAS), and a post-trip operational guidance (PTOG). SSMS, a fault-tree analyzer, assists the operator in the plant setup and in the overall maintenance and management of plant safety functions. DAS detects a disturbance involving multiple failures, diagnoses the cause, identifies plant conditions, predicts the propagation of the event, plans recovery actions and provides guidance for selected operational procedures. The objective of DAS is to minimize the occurrence of anomalies and investigate their impact. PTOG minimizes the consequence of an event providing operational guidance based in safety critical functions preservation. IODA was conceived to help the operators in their making decisions steps according to the Rasmussen's framework. To make more easy the tests results, Fukutomi reduced those steps into five: detection of the anomaly (detection, observation, collection of data, and identification of the system state), interpretation of the situation (interpretation, alternatives evaluation, decision on a course of action), selection of the target state, planning of a strategy, procedure execution. Applying cognitive tasks analysis, Fukutomi's group identified that the operators' weaknesses are concentrated in the planning and execution of procedures, and the identification and interpretation of situations. The errors mechanisms more frequent are errors of discrimination among disturbances (mistakes- misapplication of good rules) and incorrect memory recall (slips) in the procedure planning. Omission errors were more frequent in anomalous situations (stress?!). The man-machine interface of the IODA system is based in CRT touch-screens, voice announcement, and alarms systems. The CRT displays have three hierarchy levels and use the abstraction concept. The experiments were conducted in a real-time full scope simulator of 1100 MWe BWR, using nine experienced operating crews. Each crew was composed of 4 persons - a shift supervisor, a main panel operator, and a BOP panel operator. The movements and communications in the control room were recorded using audio and video equipments. Using these records plus several IODA logs a tasks time-line table was constructed. This table together with an activities check list formed a decision making process diagram which was evaluated adding data from the operators' answer to questionnaires and interviews. The experiments were executed with and without IODA systems aid for the same set of transients. The evaluation showed that IODA can help .the operator in the decision making, avoiding unnecessary trips, and slips(forgotten items) in the operational procedures during a mitigation of an anomaly. These conclusions were done after comparing time-line charts of operational activities with and without IODA system aid. This shows that full-scope simulators and operators' mental models of the decision making as in the Rasmussen's framework are necessaries items in the experimental verification of man-machine systems.

COGNITIVE TASK ANALYSIS

The cognitive task analysis were done using the data collected in two full-scope simulators in the BTC(BWR Operator Training Center) in Japan, one for 800 MWe BWR and the other for a 1110 MWe BWR (Yoshimura et al., 1992). Once more, the Rasmussen's framework for the cognitive task analysis has the central role in the methodology (Rasmussen, 1986). The latter is composed of four stages: 1) information processing tasks, 2) knowledge states obtained from the results of information processing, 3) mental images corresponding to the knowledge states and its movement in the problem space consisting of two dimensions of hierarchy: the levels of abstraction and the whole decomposition in physical parts, and 4) information processing task control mechanisms. From the envelopes of trajectories for searching in the problem space, the type of necessity for information can be established for each level of hierarchy.

BEHAVIOR UNDER STRESS

Another group of experiences were made in the BTC to evaluate the requirements of a human-machine system to support operators under stress during an unfamiliar accident situation (Ujita, 1992). The following prerequisites were identified in this case: 1) to fit the information timing to the operator cognitive process, 2) to indicate the information in the operator's attention points according to the situation, 3) to control the information according to the operator psychological state. The experimental results demonstrated that: 1) the correct phase in the cognitive process can be estimated by the elapsed time, plant situation, and verbal protocol analyses. In the CCM (chapter 2.2.3) it means time-line charts in the multiple resources theory, system states, and operator intent evaluation through the scripts theory; 2) the attention points of the operator can be determined on the hierarchic functional model, based on eye movements and verbal protocol analysis; 3) the psychological state (workload and stress) can be estimated by the physiological information such as brain waves and heart beats rate measurements. In the chapter 2.2.3 the WINDEX approach was suggested.

Particularly, the CRIEPI (Central Research Institute of Electric Power Industry) in Japan has developed the THURMOS, a human performance monitoring system (Inoue et al., 1990). THURMOS monitors several physiological parameters: electrocardiogram information, skin resistance level and reflection, respiration curve, body movement, posture, and visual behavior. The objective is to investigate the effectiveness of automation in reducing the operator workload and stresses, as well as the understanding of the errors physiologic mechanisms, contributing for the human error reduction.

In the BTC, a research through questionnaires (Susuki, 1991) revealed that the operators accept well the automation in tasks very monotonous, but not so well for the automation of different operation in a short period (mismatch between machine performance and human performance is the reason). This shows the necessity of a human-centered design. The operators must decide the possible tasks to be allocated to them, and which are more adequate to the present situation. However, in case of stressing situation, the IODA experiments demonstrated that the operators feel that the system is a helpful tool to their decisions.

Other area of importance for evaluating the stress and workload is the maintenance activities. A laboratory simulation of maintenance activity was created in the Battele Human Affairs Research Center (Kantowitz, 1988). Kantowitz uses the Wickens/Card model of the human information processing and selects measures that are adequate for a specific maintenance task (Kantowitz, 1992).

2.2.4.2 FRANCE

This topic will be touched in the chapter 2.4.1.

2.2.4.3 USA

The EPRI conducted a series of experiments to measure operator crew reliability (ORE-Operator Reliability Experiments). Six american utilities plus EdF and TPC(Taiwan Power Corporation) participated in the ORE. The HCR method was used, but the experiments demonstrated its inaccuracy (Singh/Spurgin, 1990).

The ORE project has 4 objectives (Moieni, Spurgin, Spurgin, 1993):

1) develop a simulator data collection methodology - OPERAS (Operator Reliability Assessment System) written in EXCEL and C in a WINDOWS environment;

2)develop a data reduction and analysis methodology;

3)validate the HCR correlation, or modify it, if necessary;

4)provide insights/inputs for HRA and PRA/IPE studies.

The dependency of the crew's response time on the procedure logic led to the development of a modified version of the HCR. A study about these response times using data of six simulators established criteria to support revision of a design. These criteria will be implemented for the revision of the ANS-58.8 standard, now in process..

2.2.5 THE TREATMENT OF HUMAN ERRORS IN HUMAN-MACHINE SYSTEMS EVALUATION MODELS

A range of 70 to 90% of all accidents in the transportation systems and process plants systems are due to human errors. Instead of considering humans as a component (like in the probabilistic approach) it is more adequate in the human-machine systems(HMS) the causal approach. As pointed in the chapter 2.2.2.2A, the HRA is important in risk analysis integrated to the PRA. In the HMS, the main concern is the cause and the compensation of the error instead of counting them.

In the EMO described in the chapter 2.2.3, three phases were established: identification, classification, and remediation. The identification of the errors involves the external models of malfunction during some step of the human information processing (detection of anomalies; identification of the system state; decision selection for the goals, targets states, and tasks; actions performance in terms of operational sequence, execution, and communication). These models take into account omission of specified acts or commission of erroneous/extraneous acts. The OCM, through the operators' state data, provides the information necessary for the EMO in the identification of errors. These data contain all the goals, plans, and scripts opened by the operators, and all the tasks/actions in progress and that are coherent with them. Acts not explained in this way are considered commission errors. Omission errors are identified during the verification of the task sequence. Feedback to the identification phase helps in finding a common cause error, as in case of choosing an inadequate procedure to the system situation.

The second phase (errors classification) involves the identification of the errors mechanisms, its causes and contributing factors, as well as the consequences analyses.

Reason(1990) classified the errors mechanisms in slips, lapses, and mistakes. He distinguished also between unintended actions (slips and lapses) and indented actions (mistakes and violations), both being types of unsafe acts (or active failures).

He observed that every system has latent failures (design and management/organizational failures). The latent failures combined with the active failures diminish the defence-in-depth of the system against local triggers (atypical conditions or intrinsic defects) which are responsible for the accident initiation. While the latent failures pertain to the world state, the EMO has to preclude the occurrence of active failures. Violations of operational procedures and technical specifications are the most obvious failures that the system can avoid if it was designed with humans in mind. Slips and lapses are committed in the skill-based level. They can be grouped in errors of inattention (omitted checks) or over-attention. The most common errors of inattention are the double-capture slips: "I had decided to cut down my sugar consumption and wanted to have my corn flakes without it. But next morning, however, I sprinkled sugar on my cereal, just as I always do." Next we have omissions(lapses) associated with interruptions ("I picked up my coat to go out when the phone rang. I answered it and then went out of the front door without my coat"). Reduced intentionality are normally slips. These include detached intention ("I indented to close the window as it was cold. I closed the cupboard door instead"), environment capture ("I went into my bedroom intending to fetch a book. I took off my rings, looked in the mirror and came out again - without the book") and multiple sidesteps ("I indented to go to the cupboard under the stairs to turn off the immersion heater. I dried my hands to turn off the switch, but went to the larder instead. After that, I wandered into the living room, looked at the table, went back to the kitchen, and then I remembered my original intention"). Sometimes these errors occurs as lapses (states instead actions): the what-am-I-doing-here or the I-should-be-doing-something-but-I-can't-remember-what. Perceptual confusions or slips involves recognition schemata in off-repeated tasks ("I indented to pick up the milk bottle, but actually reached out for the squash bottle"). Finally we have interference errors (blends and spoonerisms). Example of blend of speech and action: "I had just finished talking on the phone when my secretary ushered in some visitors. I got up from behind the desk and walked to greet them with my hand outstretched saying 'Smith speaking'". Example of a behavioral spoonerism ("In a hurried effort to finish the house work and have a bath, I put the plants meant for the lounge in the bedroom and my underwear in the lounge window"). Over-attention can occur as omissions, repetitions and reversals of action. An example of reversal is: "I got the correct fare out my purse to give to the bus conductor. A few moments later I put the coins back into the purse before the conductor had come to collect them".

Mistakes can only occur in the rule or knowledge-based levels. RB mistakes arise from the misapplication of good rules or from the application of bad rules. Example of the first type are: first exceptions (<u>the strong-but-now-wrong rule</u>), a kind of stereotyped behavior. Bad rules can have deficiencies in the problem encoding or in the action component of the "problem-solving". So, there are wrong rules, inelegant rules, and inadvisable rules.

In the Chernobyl accident the operators followed a wrong rule when they were testing the ECCS pumps in a low power level condition: "IF (there is more water flowing through the core) THEN (the reactor will have a greater safety margin, and hence there will be less risk of requiring ECCS cooling, which would be unavailable)". In a low power level with a positive reactivity coefficient, the required action was the opposite.

Mistakes at the knowledge-based level arise due a several mechanisms: selectivity (attention given to the wrong features), conscious work spare limitations, out of sight-of the mind characteristic, confirmation bias for the hypothesis, overconfidence in the one's knowledge, the "check-off" illusion, illusory correlation, halo effects, problems with causality (oversimplification), problems with complexity.

The causes and contributing factors for these errors mechanisms described in the last paragraphs come from four general classes of factors: inherent human limitations, inherent system limitations, contributing conditions, and contributing events (Rouse, 1991).

Inherent human limitations encompass the knowledge about the system, natural skills from the person, and general attitudes concerning the life situations.

Inherent system limitations include the design limitations and the level of simulator fidelity, compared to the systems actual behavior.

Contributing conditions encompass the physiological and psychological stressors including the excessive workload (see chapter 2.2.1). This latter can be evaluated from the resources submodel together with the human performance submodel in the OCM.

Finally, the errors must be classified according to their consequences to the system. Nowadays, it is possible to find expert systems in PRA that have the capability to give the risk associated to a specific action on line to the operators. The program EXPRESS (Ancelin, 1990 - Electricité de France) is an example for that.

The last phase of the EMO is the error remediation, that can be done in three levels: advice for monitoring, feedback of information, and automatic control. The task of classifying correctly the error is critical for remediation. A misclassification could generate a situation more dangerous than the initial condition.

As slips and lapses are unintended actions, they are easily handled and detected by the system. Mistakes and violations are indented actions, however, and the systems must feedback this information (with proposals of compensatory actions) to the operators to be accepted by the crew before the automatic action. Of course, EMO should recommend immediately an automatic control to the FAL in case of high risk of disastrous consequences for the plant.

2.3 OPERATOR SUPPORT SYSTEMS - SOFTWARE VALIDATION AND USE OF CASE (COMPUTER AIDED SOFTWARE ENGINEERING)

THE DESIGN PROCESS

The following activities are necessaries in the design of large software systems as those found in the expert systems for the nuclear area:

1. architectural design
2. abstract specification
3. interface design
4. component design
5. data structure design
6. algorithm design

The process above is repeated for each subsystem in a top-down approach within a hierarchic tree of subproblems. In an object-oriented programming, however, the top-down approach is not useful because each object is a design framework itself.

There are two basic design strategies: functional design and object-oriented design. As already seen in the chapter 2.2.3, the latter is more adequate for DSSs in the NPPs. Both use usually structured methods as design methodology and can be implemented as sequential or concurrent programs. With fast processors, there is no necessity in most cases to use parallel programming (Sommerville, 1992).

In the last years, several tools were developed to design software and they constitute the term used to designated such automated support, i.e., CASE(Computer-Aided Software Engineering). CASE tools are classified into a two-dimensional matrix, constructed by the ortogonal directions:

1. activity-oriented - specification, design, implementation, verification and validation;

2. function-oriented:

test data generation tools
modelling and simulation tools
program transformation tools

interactive debugging systems
program analysis tools
language processing tools
method support tools
user interface management systems
data dictionary tools
diagram editing tools
prototyping tools
configuration management tools
document preparation tools
planning and estimating tools.

This list is not exhaustive and the tools must be integrated in a CASE environment structure. The latter is composed by the tools set, an operating system, an user interface, and an object management system(OMS). CASE tools interact each other through several types of software objects. OMS has the function of managing these objects and their relations. Object-oriented databases are generalizations of OMSs and should be exploited in CASE environments as this technology matures. There are three types of integration which should be taken into account during the software development: data integration, user interface integration, and activity integration (Sommerville, 1992).

EID (Ecological Interface Design)
(Rasmussen/Vicente, 1989; Vicente/Rasmussen, 1992)

One of the most important part in the HMS software design is the MMI. The interface can be considered as a part of the control system. A good controller must possess a model of the system to be controlled as well as its constraints which are derived from the systems purposes, the physical phenomena involved and the environment constraints. As a form to represent the constraints, Rasmussen purpose an abstraction hierarchy. For describing process control system, he identified 5 levels of constraints: functional purpose, abstract function, generalized function, physical function, and physical form. This abstraction hierarchy is important to choose the complexity level in which the information shall be given to the operators.

Additionally, this information should be presented in a way that is compatible with the human cognitive and perceptual characteristics. These characteristics are represented in the Rasmussen's framework consisting of knowledge, rules, and skill levels. As the first part of the problem is related to the environment and the second one is related to human beings, the interface attending these two necessities is called ecological.

Constraints are special relationships between system variables that are known in the design process. Occurring a fault in the system these constraints will change. The task of diagnosing a fault consists in determining the breaking of one or more constraints governing the system in normal situations. To do that is necessary the verification of all variables involved with a particular constraint. So, the interface must inform the operators a set of constraints that are relevant to the system goal. The variables values deviations found by the constraints breaking can be used either for diagnosis or for control, although the control allocation should be done according to the principles in the chapter 2.2.3. Other important characteristic of the abstraction hierarchy is that it is goal-oriented. This allows a problem-solving search starting in higher levels of goals and ending in the lower levels of subsystems of interest within the subtrees of the hierarchy (forward search).

Rasmussen identifies three basis kinds of events for a human-machine systems:

1. familiar or routine events in the skill-level behavior;
2. unfamiliar, but anticipated events in the rule-level behavior;
3. unfamiliar and unanticipated events in the knowledge-level behavior.

Although the human beings tend to rely upon on the lower levels, the task demands could require higher levels of cognition. Thus, the obvious conclusion is that the interface should not use levels above the required levels, but should support the operators in all three levels. Rasmussen formulated consequently their principles for the EIDs:

1) SBB (Skill-based behavior)

"To support interaction via time-space signals, the operator should be able to act directly on the display, and the structure of the displayed information should be isomorphic to the part-whole structure of movements".

2) RBB (rule-based behavior)

"Provide a consistent one-to-one mapping between the work domain constraints and the cues or signs provided by the interface".

3) KBB (knowledge-based behavior)

"Represent the work domain in the form of an abstraction hierarchy to serve as an externalized mental model that will support knowledge-based problem solving".

In the paper of Leo Gugerty(1993), other models are presented for the design of human-machine interface. They are compared within the seven stages of the cycle of human-machine interaction activities (Norman, 1986): perception, interpretation, evaluation, goals, intention, action specification, execution. They are equivalent to the Rasmussen's framework information processing activities: activation, observation, identification, interpretation, evaluation, task definition, action specification, and execution.

Two models (GOMS and OFM) emphasize the three last stages (goals translated into actions) although both cover the whole process information. The other two emphasize the display perception and interpretation(ANET and Tullis). Particularly, GOMS has been mentioned in the chapter 2.2.2.2B.

"GOMS models are applicable to routine cognitive skills. They focus on 'how to do it' (or procedural knowledge), as opposed to factual (or declarative) knowledge...The form basic elements of GOMS models are goals, operators, methods, and selection rules. GOMS models are hierarchical. The assumption is that at the highest level, peoples' behavior on a routine task can be described by a hierarchy of goals and subgoals...the number of production-system cycles required for a task can predict the task performance time... the number of productions can also predict learning time...the number of statements in working memory during the production system operation (working memory load) may be able to predict the number of errors users make". (Gugerty, 1993).

As representants of the ANETS and Tullis models, the MHP of Card et al. can be mentioned (see chapter 1.1). As emergent models, Gugerty lists SOAR(Newell, 1990) that is an architecture for PUMS(Programmable User Models), and hybrid models from Kintsch, combining ACT, GOMS and connectionist models.

EXPERT SYSTEMS VERIFICATION AND VALIDATION(V&V)

The definition of verification and validation are as follows (Naser, 1989):

"Verification is the review of the requirements to see that the right problem is being solved and then the review of the design to see that it meets the requirements."

"Validation is the operational test and evaluation of the integrated hardware and software system to determine compliance with the functional, performance, and interface requirements".

There are two types of V&V testing (static techniques and dynamic tests) and two types of testing (statistical and for searching of defects). Static techniques don't require the program execution opposite to the tests which do. Statistical tests are used to determine the software reliability against selected inputs. Defects testing are useful to reveal the presence of defects in the system. This kind of test deals with the process to locate and correct the defects (Sommerville, 1993).

The EPRI classifies the expert systems in 6 types (EPRI-NP-5978, 1988; Naser, 1989):

1) Monotonic reasoning, factorable search spaces, and finite in size and concept
2) First type, including uncertainty handling
3) First type, but the knowledge is elicited

4) Third type, including uncertainty handling
5) Non-monotonic reasoning, large unfactorable or infinite search spaces, multiple knowledge bases with possibly conflicting sets of heuristic, learning capabilities or other features
6) Fifth type, including uncertainty.

Some parts of the expert systems are conventional software and so conventional verification and validation are applied. These are the implementation hardware, the expert system shell (including the inference engine, the knowledge representation scheme, the control options, and the utilities), the customized user interface, and special methods. Consequently, the verification and validation must be concentrated in the knowledge base (Naser, 1989).

The problems found in the knowledge base are classified in four groups (EPRI, 1988): inaccuracy, logic inconsistence, logic incompleteness, functional incompleteness. Particularly in the logic inconsistences and incompleteness, there are basically 8 types of errors:

1. redundant rules
2. conflicting rules
3. subsumed rules
4. circular rules
5. unnecessary IF conditions
6. dead-end rules
7. missing rules
8. unreachable rules

Examples of these errors can be found in Gonzalez (1993) and EPRI(1988). It should be noted that an object-oriented programming would become more easy the task of the V&V, because in such approach the objects hierarchy is a natural environment for testing and also the reduction in the programming effort is considerable in terms of the coupling between objects.

SOFTWARE QUALITY ASSURANCE AND STANDARDS

The NUREG/CR-4640 (1987) is a handbook of software quality assurance techniques applicable to the nuclear industry. It establishes a software life cycle whose activities are:

1. requirements specifications
2. functional specification
3. detailed software design
4. coding and software generation
5. testing, installation, and commissioning
6. transfer of responsibility
7. operation maintenance
8. project management

In this handbook there is a list of tools to develop software that can be considered CASE tools. Matras(1993) did a recent revision of the criteria used for hardware and software in NPPs. In the top level is the IEEE Std. 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Station". This norm requires the use of ASME-NQA-1 for a Quality Assurance Program and ASME-NQA-2a part 2.7-1990 for "Quality Assurance Requirements of Computers Software for Nuclear Facility Applications". Matras shows also the relation between the 18 criteria of a quality assurance program and the software life cycle phases (requirements, design, implementation, installation, operation/use/maintenance). Verification and validation must be done during the entire cycle and the IEEE Std 1012-1986 "IEEE Standard for Software Verification and Validation Plans" is referred. The adaptation of these concepts to the expert systems types 1,2,3,4 is shown in Naser(1989) and EPRI(1988). For the software design management process model the Boehms' spiral model (EPRI, 1988; Sommerville, 1992) is adopted.

SOME PRACTICAL EXAMPLES

A good example of software design and V&V is the PPS(Primary Protection System) for Sizewell B PWR in the UK(Hunns/Wainwright, 1993, 1991). The IEC 880 Standard Software for computers in the safety systems of nuclear power stations was used. The static analysis was done using the tool MALPAS(Malvern Program Suite) in three stages:

1) syntax(control flow, data use, information flow)
2) semantic analysis (describes the outputs mathematically in terms of the inputs).
3) compliance analysis (verifies the code against a mathematical representation of the specification).

An important characteristic of this project is the task of the "Source to Code Comparator" to check that the executable code installed in the PROMS(Programmable Memories) matches the source code using MALPAS semantic and compliance analysis. The dynamic test was composed of transients data of the 11 potential faults. 50.000 tests were carried. The design took 200 man-years and V&V by the designer 50 man-years. The MALPAS analysis took 80 man-years and the dynamic testing 15 man-years. The code has 100.000 lines and uses 100.000 lines data. The BCS(British Computer Society) suggested statistical testing, indication of adherence to IEC 880 and certification of Nuclear Electric and all subcontractors to ISO9001.

EPRI(1988) gives two examples of expert systems V&V. The first one is EOP Tracking System (Expert System type 1). The open procedures were documented in IF-THEN format and compared to the knowledge base one-by-one (static verification). The validation consisted of integrated dynamic tests using data of transients, and full scope simulator tests with the operators participation. The second one is REALM, an emergency management program, combining rules and object-oriented programming. The V&V was made for each REALM subsystem using tests for each one of the 8 errors described previously for the knowledge bases.

2.4 EXAMPLES OF FINAL DESIGNS - NUCLEAR POWER PLANTS CONTROL ROOMS

2.4.1 N4 - CHOOZ FRENCH DESIGN (PEYROUTON/PIRUS, 1993)

The N4 series of 1400 MW PWRs will start operation in the end of 1995 on the site of Chooz. This N4 series will use a computerized main control room(MCR), having the following features:

1) similar operation under normal, incident, or accident conditions, to avoid confusing the operators;
2) centralized managing of large flow of data, synthesizing the relevant information for an adequate alarm processing and an efficient diagnosis aid;
3) intelligent control and monitoring;
4) integration of maintenance and operation actions;
5) automatic periodic testing;
6) possibility of changing plant data without stopping operation.

The I&C system of the N4 series has four levels:

level 0 - actuators and sensors
level 1 - protection equipment and logic/analog controllers (automatic control and protection system)
level 2 - control room with the KIC(computerized system) and manual conventional systems (mimic, auxiliary panel and emergency shutdown panel)
level 3 - KAD and KDS (maintenance and site computer-aided system); KDT and KGD (I&C data configuration computer).

In the level 1, there are two systems:

a) CO3 system, supplied by FRAMATOME/MERLIN GERIN, composed by three subsystems:

1)the nuclear instrumentation system
2)the control rod control system(SPIN).

The signal in the SPIN are processed in the DAPU (Data Acquisition and Processing Units) and are transmitted via local networks made of fiber optic transmission.

b)P20 CONTROBLOC, controlling the rest of the plant, developed by CEGELEC. It was connected to the level 2 computer system. Because of the hardware complexity and software developments problems, the P20 was abandoned, causing a delay of 4 or 6 years in the project. The P20 was substituted by two systems:

1)The CS3, developed by MERLIN GERIN and FRAMATOME for the control of some auxiliary systems, necessaries to maintain the safety critical functions;

2)The CONTRONICE system (HARTMANN&BRAUN) for the control system (except the main turbine) and the signals interchange between the level 1 and 2.

In the level 2, there are two systems:

1)KIC(Operating Computerized System)
2)Operating Conventional Devices, using conventional technology as backup to the computer based system, including a mural mimic connected to the level 1.

The KIC system is composed by hardware, software, and interface.

HARDWARE

13 computers interconnected by a dual local area network(LAN). It collects data from 155 programmable logic controllers(PLCs) and uses VAX 4000-300 and VAX stations.

SOFTWARE

Designed by SEMA GROUP, written in ADA, uses Digital's VMS operating system, ISO-based network, X-WINDOWS graphical operating formats, and object-oriented real-time data base.

MAN-MACHINE INTERFACE

There are 4 operators workstations (for 2 units), each one with 3 graphical CRT screens for operating display format, procedures, and historical data presentation; 4 alarms CRT lumped in two screens; 3 touch-sensitive screens for configurable menus (1 for commands reports, 1 for display calls, 1 for commands); 1 track ball to select objects on screen; and 2 functional keyboards (1 for control and 1 for alarms). Each station works only reading the operator card identification.

In the level 3, there are integrated tools, technical management and maintenance functions, to produce and validate all I&C data.

The qualification and validation is being executed according to the IEC880 standard methodology. The facilities for validation are the following:

1)level 1 facility - 5 islands for the 10 CONTRONIC E cubicles,
2)level 2 facilities - a KIC full scope simulator.

The on-line procedures were designed by a group of nine future operators and consumed 10 man-years. There are 300 procedures images for normal situations, 100 for incidental situations, and 300 accidents.

The KIC system works in different steps: control step, test step, and information step, and others. When a workstation is being used for control, the other is used only for monitoring. The KIC needs only a supervisor and an operator to control the plant. The computer never has the final control of the plant. All the operation are presented on the screen, under request of the operators, and only they can validate an operation command. When the operator enter into conflict with the KIC system, the information is presented to the operators, who has the final word. Therefore, there is no dynamic allocations and the design is strictly centered in humans.

When a chosen operation route is not possible or available, by the operators' request, the reason for the interlock is presented with the technical data about the system or component. It means that the diagnostic system gives the plant state, including components status, without explaining the causal effects. Abrupt changes are managed by the protection systems and the system keeps the operators informed about the evolution of the plant parameters through displays, alarms and advises for corrective actions. There is no evidence of mental models in the system or attention resources control, but there are reported experimental tests occurred in 1989, with satisfactory results (Bozec et al., 1990).

2.4.2 OHI-3/4 (PWR) AND KASHIWASAKI-KARIWA 6/7 (BWR) JAPANESE DESIGN

COSS(COMPUTERIZED OPERATOR SUPPORT SYSTEM)

The first reaction from Japan against the consequences of TMI-2 accident in the human-machine systems design was the 5-year COSS project(1980-1984), under the sponsorship of the Japanese Ministry of International Trade and Industry(MITI), involving six private companies: Hitachi Ltd, Mitsubishi Heavy Industries, Mitsubishi Electric Corporation, Mitsubishi Atomic Power Industries, Inc., Toshiba Corporation, and Nippon Atomic Industry Group Co. Ltda, responsible for the Nuclear Steam Supply System(NSSS) in Japan for BWRs (Toshiba and Hitachi) and PWRs (Mitsubishi). The functional subsystems of the COSS were developed as an Integrated Operator Decision Aid System(IODA) (Fukutomi et al, 1992). The IODA system is composed of three parts:

1. a standby systems management system(SSMS);
2. a disturbance analysis system(DAS) for monitoring the plant status and diagnosing a disturbance;
3. a post trip operational guidance(PTOG) system for providing symptom-based operational guidance during the plant abnormalities after a reactor scram.

The SSMS has three main functions: standby state monitoring and management, technical specifications management, and surveillance test management. The first function uses a fault-tree analysis(FTA). The DAS detects earlier failures in the plant and is based on a plant diagnosis model(PDM) which was prepared with the utilization of the FTA and FMEA(Mode and Effects Analysis) based in eight top events (seven main scram causal events plus partial power operation). DAS provides operation with appropriated guidance to the operators to avoid an unnecessary trip.

The PTOG selects the proper operational procedure based in the compilation of critical safety functions. It has four tasks: 1) diagnoses abnormal system functions, 2) decides on an operational goal by considering the main plant safety-related parameters, 3) selects an appropriate system to be used in maintaining the safety functions, 4) determines and presents the operational procedure PTOG diagnosis, equipment and plant subsystems failures, and process parameters deviations. This uses cause-and-effects relationships and is based in production rules.

The IODA system was experimentally evaluated (see chapter 2.2.4) with a full scope simulator and several crews of experienced operators.

MMS(MAN-MACHINE SYSTEMS FOR NUCLEAR POWER PLANTS)

After the COSS project completion the same group of companies agreed in a new 8-year(1984-1991) project to develop an advanced operator support system by applying artificial intelligence(AI) techniques and multimedia communication technology. While COSS is to be used in the rule-based level of the Rasmussen's framework, MMS is designed to be used in the knowledge-based level. In this level, scenarios beyond design basis accident, with and without scram, excluding severe core damage, will be covered.

To accomplish this, the Rasmussen's levels of hierarchy described in the chapter 2.2.3 were adopted as well as the multilevel flow modeling(MFM) for the abstract function level. This level determines the operational objectives according to the purpose level and the generalized function affected. The knowledge base was called ALKB(Abstract Level Knowledge Base). The symptom-based operational procedures for counteracting are constructed in the physical level (function or form) and a new knowledge base called PLKB(Physical Level Knowledge Base) is needed. These two bases constitute the INCAMS(Incident and Accident Management System). To implement them, a flexible and hybrid knowledge representation was used: frame base system for ALKB with object oriented program for PLKB. The LISP language was adopted (Monta et al., 1988).

INCAMS uses a topographic diagnostic search and the operator information processing as given by Rasmussen in the chapter 2.2.3 (Monta et al., 1990):

- detection of plant anomalies
- identification of plant status
- interpretation and planning of
- operational goal
- planning of operational strategy
- synthesis of operational procedures

The abnormal situation detector verifies the performance indices for energy and mass flow functions, constructed with the plant process parameters. The plant status module identifies the origin of the deterioration following the multilevel flow model hierarchy. It computes failure certainties for the flow functions. The operational goal selector chooses alternative operational goals according to the flow functions. The lowest failed flow function has the higher priority in the same hierarchy level. An operational goal is selected among the following: continuation of the current operation, decreasing of the current power level, achievement and maintenance of cold shutdown, and keeping the primary containment integrity.

The operational strategy planner selects an operational strategy that achieves the selected operational goal under the current plant status. It plans from top(whole) to bottom(part) level of the MFM, selecting proper goals and their associated actions. If the action are not adequate at the time, a recursive algorithm is used to choose an alternative action starting from the upper level. The planner applies production rules and forward chaining. This approach usually does not work in real time, because in each inference cycle, the memory elements have to be retracted from the working memory. To avoid this, the planner uses an assumption based truth maintenance system(ATMS, de Kleer, 1986).

The operational procedures synthesizer establishes the physical alignment of components and systems to achieve the operational strategy, taking into account failures and unavailabilities. To avoid conflict between operational procedures, the ATMS is used again (Hattori et al., 1991; Kato, 1991).

The INCAMS is called Cognitive Model based Advisor (Monta et al., 1993) or MPS(Machine Problem Solver) (Monta et al., 1990; Itoh et al., 1993). It plays the role of the DSS in the chapter 2.2.3.

THE ROBUST AUTOMATIC SEQUENCE CONTROLLER

The MMS project is based in three basic design criteria: an ecological interface, support of the operator's direct perception and analytical reasoning, a machine problem solver, support of the operator's cognitive resources and a robust automatic sequence controllers (Itoh et al., 1993; Monta et al, 1993).

The ABWR in Japan will be a totally automated plant. The scope of automation is as follows: the plant startup and shutdown activities, post-plant trip operation activities, surveillance tests emergency procedures and load follow-up (control rod system) (Iwaki, 1990; Utena, 1990; Nakamura, 1992). For example, the knowledge representation for the ABWR startup is given in Sekimizu et al., 1992. A production rules system programmed in PROLOG was utilized.

However, the operators has to supervise the computer decision makings and, in case of accidents, they have to take over the actions from the automatic control system. To make these computer decisions transparent to the operators, the robust controllers have a configuration based in knowledge engineering. It is composed by the following parts: knowledge base, plant data base, operational procedure synthesizer, and a system controller.

The knowledge base contains knowledge about plant design (designer intentions), system operation, and sub-loop controllers. The dynamic operational procedure synthesizer uses this knowledge base and the plant data base coming from the sensors. It triggers the subloop controllers, under the supervision of the system controller, which compares the current plant status (including the subloop controllers status and its logic) with the knowledge base, detecting anomalies and normal deviations in the plant. The system controller put constraints in the plant operation caused by anomalies, as well as give the compensation strategies for them, which will be additional requirements for the operational procedure synthesizer.

The system controller plays the role of the PCS in the chapter 2.2.3. There is no direct dynamic allocation between humans and machines. However, Monta et al.(1988) postulate that if the computer decision making is an emulation of the operators' cognitive process, it is more easy for the humans to understand the operational situations and make interruptions in the automatic control to take over the appropriate actions. So, in case of nonanticipated accidents, the risk of humans errors and inappropriate actions of the automatic control system will be largely reduced.

ECOLOGICAL MAN-MACHINE INTERFACE

The MMS project adopted the EID(Ecological Interface Design) principles of Rasmussen and Vicente mentioned in the chapter 2.3 (Itoh et al., 1993; Monta et al., 1993). This ecological interface is composed basically in three parts: information presentation manager, navigator, and dialogue manager. The navigator allows the operators to go through the abstraction-aggregation space with the help of a menu and a mouse to choose the best level. The display of information is based on the MFM and in the levels of abstraction. For the MFM, a Rankine cycle display is used.

The dialogue manager is composed by three subparts: a voice recognition system, an input processor for push buttons and touch sensitive screens, and a query understanding system. It needs two knowledge bases: one for natural language processing and other for smooth dialogue control. The information presentation manager contains two functions: information presentation function and information edition function. The first one controls the quantity and the form (visual, auditive) of presentation for the information, according to the operators' cognitive capacity. The second one decides the priorities of the information to be presented, according to the operators' request history and the plant states. It alerts also the operation about a difference between their focus of attention and that required by the plant state (Kato et al., 1990; Monta et al., 1988).

The function above were described for the IMA in the chapter 2.2.3. There is no information about how is evaluated the operators' attention allocation in the MMS. In the chapter 2.2.3, the Wickens' multiple resources theory was mentioned. However, there is an Operator Cognitive Model called CAMEO, which is being developed and this model uses the Wickens theory.

More complex is the task of the information editing function. In the chapter 2.2.3, this function was given to the intent model and the Script Theory was suggested. Also here nothing is said about how MMS will perform this task. A step beyond this will be to allow the robust automatic sequence controller take over the actions if the information editing function detects an operator error after successive advises. This would be a true dynamic task allocation. Nevertheless, it would depend on a human performance model and an error monitor like in the chapter 2.2.3. For example, the CAMEO (Fujita et al., 1993) program has an error modeling based in the attention resources allocation.

VALIDATION AND VERIFICATION(V&V) OF THE MMS

Yoshimura et al.(1992) discuss several aspects of the man-machine interface, some of them were mentioned in the chapter 2.3 and 2.2.4. The V&V methods in Japan are summarized in the guideline JEAG-4609. It is recognized, however, the necessity for further requirements and the CASE tools are identified to play this role. Nevertheless, this implies that the nuclear industry must develop CASE tools to be applied in specific applications.

Concerning to the experimental evaluation, the japanese industry is following the same procedure, exemplified in the chapter 2.2.4. A demonstration of MMS is provided by Kato et al. (1991) with a generator-tube-rupture accident. Monta et al. (1993) mention a validation test in course using a BWR full-scope simulator and six crews of operators.

NEW CONTROL ROOMS IN JAPAN

BOILING WATER REACTORS

Iwaki (1993,1990) provides a history of the three generations of control rooms in the TEPCO(Tokyo Electric Power Company, Inc.). The first generation incorporated the TMI recommendations and included the following modifications:

- color coding of important instruments and switches
- rearrangement of switches in accordance with actual process flow
- importance classification of alarms
- installation of a cathode ray tube (CRT) display terminal at the operations supervisor's desk.

Details of these modifications can be observed in the IAEA-TECDOC-565.

The second generation was introduced in the early 1980's and had the following design features:

- a control panel configuration consisting of three operator interface panels: a main control panel and two auxiliary control panels,
- seven CRTs on the main control panel as the primary means of monitoring plant conditions,
- automation in some plant startup and shutdown operations, such as the warming of turbine at a programmed rate at the changeover of reactor feedwater pumps,
- operational guidance messages displayed on a CRT to support manual operators during plant startup and surveillance tests.

The IAEA-TECDOC-565 shows details of the control rooms in Fukushima-Daini 3 and 4 as examples of this second generation.

The third generation type, Kashiwasaki-Kariwa 6 and 7(ABWR), was entitled (Ross, 1993) A-PODIA(Advanced Plant Operation by Displayed Information and Automation). A-PODIA integrates digital control systems, optical data transmission systems, process computers, and man-machine interface.

The design criteria of the A-PODIA are the following(Iwaki, 1993 and 1990; Tai et al., 1991):

- an operator shall be able to perform all of the primary monitoring and control functions, over the full range of the plant operational modes, from seated position;
- operator's control and monitoring actions after scram should be minimized;
- information related to the safety shall be presented in such a manner that it may be used, in common, by the entire operating crew.

These design criteria arise from the experimental evidence that the peak in the operators' workload occurs immediately after a scram, due a several routine operations to bring the plant to safe condition, which causes stress. Also, in the earlier designs, the operators had to walk very often in front of the panels to perform their tasks and sharing the information orally with the crew members, which increased the occurrences of human errors.

The A-PODIA has three main functions: monitoring function, automation function, and alarm function. The monitoring function is preformed by a Compact Main Control Console with 7 CRTs and 12 Flat Display Panels and a Large Display Panel.

The Flat Display Panels are used only for safety system. All the displays on the main panel have touch sensitive screens.

The Large Display Panel has three parts: wide screen, mimic display panel, and the alarm display. The wide screen monitors the whole plant parameters. The mimic panel is made of hardwired devices and monitors the safety systems even in case of failures of the process computer and its driven CRTs. The alarms display panel is made of hardwired devices.

The alarm function is divided between the alarm display panel (plant level) and the system level alarms (main console) plus the equipment level alarms (CRTs).

The automation function was conceived to extend the automation to the following activities:

- control rod operations
- sequential automatic operation of each auxiliary system
- surveillance test operation
- auxiliary equipment operation after reactor scram

The automation function in the A-PODIA has several main characteristics:

1) There are several breakpoints in the start-up and shutdown operation in order to allow a confirmation of the approximate plant conditions by the operators;

2) The process computer is designed to have high reliability through the use of redundant CPUs(Central Processing Units) and power sources. It is installed on a seismically isolated floor to prevent a simultaneous plant trip and computer failure during an earthquake.

3) There are three hierarchical levels of control. In the plant supervisory control level the operators supervise the automatic control through the automatic console. In the system control level, the process computer controls automatically the start-up and shutdown operations. The operators set the operation mode through master switches (hardwired to avoid errors with touch screens). In the equipment control level, the process computer triggers the microprocessor-based controllers. The operators can control each equipment or subsystem individually through touch screens switches in the main console. In case of failures of the process computer the operators can use hard switches in the main console.

Iwaki (1993) doesn't believe that AI based expert systems are enough to obtain operators confidence. He thinks that an extended operator training program together with a control room that allow operators to have the operation initiatives are complementary activities. In fact, this is the point of view of the human-centered design already exposed.

PRESSURIZED WATER REACTOR

Japan has 39 NPPs (1991) with a capacity of 31 GW, including 18 PWRs. While Toshiba and KEPC are applying the MMS results in the BWRs, Mitsubishi and Kansai Electric Power are doing the same for the PWRs. Saito(1993) identifies four generations of PWRs control rooms in Japan. The first generation was imported overseas and they consisted of hardwired technologies. The second generation incorporated the japanese human factors studies (human engineering or ergonomy) and the Cathode Ray Tubes(CRTs) to display information. The third generation is represented by the NPPs OHI-3 and 4 (Takashima, 1991; Saito/Tani, 1990; Nitta et al., 1990).

These plants started operation in 1991 (december) and use extensively digital control systems to automate the following functions:

- RCS start-up and cooldown
- Main turbine/generator start-up (roll-up, on-grid and load up)
- main turbine turning
- feedwater pump turbine start-up
- high pressure turbine steam extraction for acting in high pressure heaters

Breakpoints in the operation are used as in the BWRs. The CRTs are the main mean for displaying information and use of three colors alarms systems with prioritization was installed. The digital control is based on INTEL 80286 processor and has a 100% of redundancy. With the failures of both microprocessors (main and backup) the control systems switches automatically to manual operation.

The fourth generation will be based in the MMS project. One operator will control the whole plant through a main console of 5 meters with 4 CRTs and two FDPs (eletroluminescence flat display panels) and LDP (large display panel) with 100 inches. Two CRTs are for monitoring, two for control and monitoring, and two for backup of safety and non-safety systems. In front of each one, there are six FDPs touch screens. The operators are monitored by a supervisor which has a 3 meter panel with two CRTs (and two FDPs with touch screens) only for monitoring.

The DPAS(Dynamic Priorities Alarm Systems) deals with three colors of priorities which are fixed with three kinds of rules: mode rules, cause-consequence rules, and importance rules. There is no alarms suppressed. A KBOSS(Knowledge-based Operator Support System) based in the MMS project is being considered for the next PWRs control rooms.

Dynamic validation tests were conducted using a full-scope simulator for OHI 3 and 4 and several operators crews. The results demonstrated the feasibility of such control room with adjustments to be done in the display manipulations sequence and in the reduction of some red alarms. Concerning to the KBOSS, the acceptation vary significantly among the operators.

The system seems to be more useful for the supervisors, but the operators received well the diagnostic and functions guidance (Fujita, 1993). Fujita sees the use of advanced information technologies and artificial intelligence with caution. He says that a clear design criteria to allow computerize only something that surpasses the operators' cognitive abilities is lacking. Also, he believes that mere use of these technologies doesn't achieve a match with such human cognitive characteristics. This is related to the abilities in modeling these human cognitive features, which was discussed in chapter 2.2.2.2B. Nevertheless, Fujita's group has a project to develop such model with CAMEO (see chapter above). An evaluation with THERP showed that 25-30% of the operators workload were reduced comparing with the third generation control rooms, reducing therefore the possibility of human errors (Saito, 1993).

The KBOSS in PWRs use a different approach from the MMS in BWRs for diagnosis. Instead of using MFM performance indices, a symptom-based diagnosis system within a hypothesis-and-test framework was used. Each failure is identified by a verification frame. These frames are triggered externally by alarms frames and symptom frames (anomalous symptoms not covered by alarms) and internally by higher and lower levels verification frames. These levels are the hierarchy levels in the Rasmussen's framework. The verification frames contain verification conditions for the hypothesis-and-test search and once confirmed, operational procedures are triggered by guidance frames in the last slot of the verification frame. The system was programmed in LISP and was called Plant Abnormalities Hierarchy Model (Fujita et al., 1991; Monta et al., 1990).

THE PROJECT OF AN AUTONOMOUS NUCLEAR POWER PLANT IN JAPAN

Nakamura and Hiei(1992) as well as Kurashige and Hiei(1990) give an overview of the research in man-machine systems for NPPs in Japan. There is a long-term project to construct a fully automated nuclear power plant by 2005. This project started in 1987 and involves 5 governmental research organizations under the coordination of STA(Science and Technology Agency): Power Development and Nuclear Fuels Corporation(PNC), Japan Atomic Energy Research Institute(JAERI), Institute of Physical and Chemical Research Institute(IPCR), Eletrotechnical Laboratory(ETL) and Ship Research Institute(SRI).

Each organization has its own research line: development of robot technologies(IPCR), development of human acts simulation technologies(JAERI), development of environment recognition technology(ETL), development of technologies for knowledge base systems(PNC), and the technology development for man-machine interface(SRI) (Tanabe, 1992).

PNC defined three levels of autonomous plant:

1) fully automated operation plant supervised by the operators and maintained by humans;
2) autonomous plant which is operated without humans but yet maintained by them;
3) autonomous plant whose operation and maintenance are unmanned.

The autonomous plant in the third level will be composed of the following subsystems (Miki/Tanayama, 1989):

1) general judgment system (manages the interface between the other subsystems)
2) diagnosis system
3) state estimation/evaluation system
4) state prediction system

5) query-answer system
6) operation system
7) robot system for maintenance
8) local artificial intelligence control systems

This list is in a hierarchical structure. All these subsystems have knowledge-bases and inference engines. They are, therefore, expert systems and based in the AI(Artificial Intelligence) techniques.

The knowledge base will have the following characteristics:

1) use of the operator thought model (using the Rasmussen's decisions making model),
2) use of deep knowledge, model-based, as a complement of the production rules IF-THEN,
3) clear structures of knowledge (mental model) using the Rasmussen's abstraction hierarchy levels and qualitative reasoning,
4) acquisition of knowledge with learning, verification of knowledge, and man-machine interface (initial acquisition),

The inference engine will use high-level reasoning with:

a) hypothesis-based reasoning (the hypothesis will be verified by the use of deep knowledge),
b) analogical reasoning.

This system will use a PROLOG machine and depends heavily on the definition of a deep knowledge model of the reasoning methods in machines and operators.

Support function for maintenance work planning in the control rooms can be found in Monta(1990) and Kato et al. (1991), as a part of the MMS project. This work planning process consists of four steps:

1) initial scheduling, considering personal limitations,
2) checking for interference between tasks and plant operations as well as interference among tasks,
3) searching for a method to resolve interference and editing the tasks procedures,
4) adjusting the time schedule to create an optimal one, which has no interference.

ARTIFICIAL INTELLIGENCE IN JAPAN

Concerning to the AI research to accomplish the goals of an autonomous plant, Rubinger(1988) gives the scope of AI research in Japan. The main institutions for the nuclear area (that are mentioned) are: CRIEPI, ETL, HITACHI, ICOT, Universities of Tokyo, Tohoku, and Kyoto, MITSUBISHI, PNC, and TOSHIBA. As already seen, HITACHI, TOSHIBA, AND MITSUBISHI, are involved in the MMS project. PNC and ETL were involved directly with the autonomous NPP development. CRIEPI in collaboration with JAERI and NUPEC have a research program in Human Factors that will be described in the next item. ICOT is developing the Fifth Generation Computers which also will described in a separate item.

Particularly, PNC, Toshiba, and the University of Tokyo are largely involved with the development of knowledge bases and inference engines. Toshiba has developed an ATMS(Assumption based Truth Maintenance System) - based knowledge verification system for diagnostic applications (Tanaka, 1991). This system called KNOV(Knowledge Verification System) has been implemented in Extended Self-Contained PROLOG(ESP) on the Personal Sequential Inference Machine (PSI-II) developed by ICOT.

The University of Tokyo and Tohoku are leading centers in the development of causal (or deep) reasoning. Kitamura et al. from U. Tohoku (1989) describe a knowledge acquisition method for diagnosis of nuclear power plant by qualitative simulation with fuzzy logic. Takahashi et al. from U. of Tokyo(1989) describe a diagnosis system based in TMS(Truth Maintenance System) and in the Dempster-Schafer probability theory. Rubinger(1988) describes the same research as the latter going on the U. of Tokyo.

The U. of Tokyo and Mitsubishi are developing new digital control strategies for NPP based on a simple control logic of comparison between the available time (the time for the error signal to disappear) and the required time (the time for the time derivative to match that of the target trend).

The U. of Kyoto developed a simulator faster than real time, TOKRAK, based on Kalman Filters (Gokuku/Wakabayashi et al., 1989, 1988). It combines plant signals with estimated and predicted parameters by the Kalman Filters, that are not measured.

HUMAN FACTORS RESEARCH

The CRIEPI(Central Research Institute of Electric Power Industry) established the Human Factors Research Center in 1987. The Nuclear Power Engineering Corporation(NUPEC) established the IHF in 1987. The JAERI(Japan Atomic Energy Research Institute) established its Human Factors Research Laboratory in 1989. All these initiatives were incentives of the MITI(Ministry of Trade and Industry) after Chernobyl accident in 1986, as the same way that COSS and MMS projects were started by the MITI after TMI in 1979. The research program is given in Isoda(1993) and in the letters received by Alvarenga from the NUPEC and JAERI directors (S.Takashima and F. Tanabe, respectively).

The CRIEPI subjects are:

- analysis and assessment of human error during operations and maintenance (Takashima/Furuta, 1992),
- reduction of maintenance personnel errors and inefficiencies modeling of human behavior
- methods for monitoring behavior of operating and maintenance personnel - THURMOS (Inoue et al., 1990)
- operator education system,

- data bases (Kameda/Kabetani, 1990)

The NUPEC subjects are:

- human behavior and its modeling - CAMEO(Fujita, 1993)
- development of human reliability evaluation methods (Hiei, 1991)
- establishment of human reliability data base
- general subjects (human-machine role allocation, human sense and motivation, cognitive psychology)
- NPP human characteristics experiments programs

The JAERI subjects are:

- man-machine system evaluation (Tanabe, 1993; Vicente/Tanabe, 1993; Yamaguchi, 1992; Tanabe, 1992)
- Human Reliability analysis
- Human Cognitive behavior.

ICOT

The fifth generation computer sponsored by MITI was reevaluated (Crevier, 1993; McNeil/Freiberger, 1993). At first, this computer would deal only with numerical and symbolic data using PROLOG. The japanese recognized the necessity to introduce semantics data using fuzzy logic instead of probabilities. This new machine will be hybrid, both binary and fuzzy. Also, beyond the two main parts, processor and memory, it will have a data base. This is connected with the neuroanatomy. The left brain is analytical and deductive and uses symbols for mathematics and language. The right brain is synthetical and intuitive and uses fuzzy knowledge.

Minsky (MIT) criticizes the use of the PROLOG in this machine (Crevier, 1993). This critic comes from the fact that humans beings don't use formal logic in their reasoning. They prefer to use frames and scripts as discussed in chapter 2.2.3. LISP is the language more used in USA. However, ICOT has incorporated in the PROLOG an object-oriented feature.

Fuzzy logic is being used largely in the control systems and equipments in Japan (Kosko, 1993), although its use in nuclear power plants is still an interrogation mark. Nevertheless, Laboratory for International Fuzzy Engineering Research(LIFE) was established in Japan in March 15, 1989.

A step beyond this is the combination between fuzzy systems and neural networks. Fuzzy neural systems can improve learned fuzzy rules and deal with new situations not predicted in the rules.

MITI has launched its Sixth Generation project, combining neural networks and conventional AI but not fuzzy logic. It is expected that this will be also reviewed.

2.4.3 DARLINGHTON 4 CANADIAN DESIGN AND THE CANDU 3

The Darlinghton 4 canadian plant is the most recent design of the AECL-CANDU series. This installation has many conventional characteristics of hardwired technologies, although it uses digital control and CRTs (18 per unit). There are four CRTs complementing the alarms panel (two for turbine-generator/feedwater systems, 1 for the reactor, and 1 for heat transport), four CRTs as data display divided in the same way as the alarms, and 10 CRTs for safety systems (including one for the emergency injection system test). Two additional CRTs are used for testing two shutdown systems. There is a SPDS system and EOPs on-line as well as 2000 color hierarchized graphics and the input are via keyboard and light-pen (IAEA-TECDOC-565).

There are three generation of control rooms for the CANDUs (Olmstead et al., 1990):

1st generation - conventional panel (hardwired) and intuitive human factors design;
2nd generation - integration of CRTs and keyboards with the control panels; application of ergonomic principles mainly in the layout panels;

3th generation - use of distributed control systems and information technologies.

CANDU 6 is an example of the 2nd generation. Its characteristics are:

- dark panel concept (light signals only in case of operators' action request)
- fifteen minutes rule - automation of safety function during 15 minutes following an accident.
- automation: process control, shutdown, refueling, and some tests considered boring
- nonintrusive manual tests
- control panel layout (mimics)
- reduced panel congestion (alarms and displays)
- alarms management
- use of anthropometrics.

The third generation is largely based in CRTs. Darlinghton-4 is an example.

The fourth generation (CANDU-3) will make use extensively of local networks (LAN) and will be based in a formal design process called Human Factors Engineering Program Plan (HFEPP). The design methodology follows the standard exposed in the Norms IEEE-1023 and IEC-964 (Malcom et al., 1993). The Rasmussen's decision making framework is being used, as in the case of alarms systems (Davey/Guo, 1993), to define levels of automation (Lupton et al., 1990). To establish the foundation for allocating control functions between humans and machines, a FDM (Functional Design Methodology) was proposed, consisting in the following steps (Lupton, 1990):

1) function analysis

2) function information analysis
3) function allocation
4) peer review
5) preliminary man-machine interface
6) preliminary analysis
7) formal design review
8) requirements hand-over

For the function allocation (initial), the two-dimensional decision space proposed by Pulliam & Price in 1983 will be used (Malcolm et al., 1993).

2.4.4 KWU - KONVOI GERMAN TYPE

The KWU-Konvoi series plants combine the conventional hardwired panels with the use of CRTs (maximum of 32). There is a limitation system between the control system and the protection system. Its function is not allow the safety parameters achieving their operation limits. Working in the range of operation not permitted to the control system, the limitation system will actuate in the control systems bring any safety parameter to its normal operation range. The system will actuate automatically taking over the actions from the operators differently from the canadian, french, and japanese cases.

In case of accidents, there is an automation of the safety systems by the limitation systems during 30 minutes, longer than the 15 min. in Canada or the 10 min. in Japan.

The automatic functions are:

1) protection systems
2) control systems
3) heat removal
4) limitation systems.

The manual functions remains as:

1) plant startup and shutdown (through video display)
2) beyond design basis accident handling (expert systems in emergency procedures)
3) recurrent tests (computer aided)
4) transfer of data (computer aided)
5) optimization of the operation.

The plant is also designed to meet all safety requirements for a period of 10 hours after loss of the control room without any operation action.

The Process Information System(PRINS) is composed basically of two systems:

PRISMA(Process Information System for Monitoring Alarms) - alarm reduction,

PRISCA(Process Information System Computer Aided) - process and variables monitor, with calculation and process displays.

Only for the PRISCA and PRINS systems, a man-machine interface is provided with keyboards and a tracking ball. The system has event-oriented procedures and diagnostic approach based in 30 accidents scenario and 20 operational malfunctions.

There are also function-oriented procedures based in critical safety functions according to the IAEA guidelines (Roth-Seefried, 1992). However, these procedures don't have a strict procedural format, because the system isn't able to diagnose each component and subsystem in the plant, as in the case of the MPS(Machine Problem Solver) in the japanese ABWR. After 30 minutes, the operator have to judge how to combine the two types of procedures. In case of beyond design basis accidents, there are special procedures for mitigating the consequences of the event.

Although the limitation systems will minimize the initial conditions of an event to mitigate the consequences of an anticipated and familiar accidents, nothing can be said about the case of nonanticipated and unfamiliar accidents. In this latter, the action of an operator is necessary since the first second of the accident.

In other words, the limitation system is a good system for the rule-based level but not for the knowledge-based level of the Rasmussen's framework. Also, it is necessary to combine the events-based procedures and the safety-function-oriented procedures in symptoms-based procedures, because it's not possible to conceive all the events in accidents situations.

2.4.5 80+ COMBUSTION ENGINEERING DESIGN

The 80+ system from the ABB-Combustion Engineering Nuclear Power(ABB-CENP) will the first advanced PWR to receive final design approval and design certification from the NRC, under the new regulation process, 10CFR52, scheduled for november 1993.

The design is a joint effort between ABB-CENP, Duke Power Company, and the EPRI, under the ALWR program. The 80+ system is not totally based in CRTs and keyboards, because the intention is to make a transition between conventional control rooms and the next generation, according to the demand of new plants in the market for 1993 to 1997. Therefore, the system 80+ introduces CRTs; keyboards; touch screens; reduction, prioritization, and colorful presentation for the alarms; better use of ergonomy to minimize operators movement and miscommunication; SPDS-based EOPs (Emergency Operation Procedures) and a big board display (6X8 feet) called IPSO(Integrated Process Status Overview) (Transactions of the ANS, 1992). The data communication are based in fiber optic transmission.

2.4.6 ALWR WESTINGHOUSE DESIGN (AP-600)

The AP-600 is in the final design approval by NRC (Transactions of the ANS, 1993). Its man-machine system will be implement with digital computers technology. The design process will use the methodology exposed by Rasmussen(1986). The Rasmussen's operation decision making model modified by Woods will be adopted. The methodology was called FBTA(Function Based Task Analysis). Inside the FBTA there is an initial function allocations between man and machines. This initial allocation is not yet defined, although the methodology described by the IAEA group (Jenkinson, 1990) is being taking into account (Carrera et al., 1991; Carrera et al., 1993).

2.4.7 FAST BREEDER REACTOR DESIGN IN THE USA

Under the sponsorship of the US Department of Energy(DOE), the research on advanced controls for advanced reactors is concentrated at the Oak Ridge National Laboratory(ORNL) in the Advanced Controls Program, at the EBR-II (Experimental Breeder Reactor) by the Argonne National Laboratory(ANL), and at the GE Nuclear Energy(General Electric) in the design of the Power Reactor Inherently Safe Module(PRISM) reactor.

Other programs of interest are the EPRI(Electric Power Research Institute) research in control and instrumentation as well as NASA(National Aeronautics and Space Agency) research in expert systems and neural networks.

The US nuclear energy must employ automation to compete with alternative energy sources, absorbing the experience in other US industries - steel, automotive, aviation, electronic, defense, and food processing (White et al., 1989). The advanced characteristics of automation will be incorporated in the future advanced liquid metal reactors (LMRs).

These reactors will have features that will allow improved reliability, low operating costs, simple operation, and reduced challenges to the active or passive safety features:

1)fault-tolerant design, multiplexed fiber optic with noise reduction and cables reduction(improved reliability);

2)reduction by 100 people in the operating staff, $4 million per plant year(low operating costs);

3)PRISM concept(GE) and intelligent support systems and interface for the operators(simple operation);

4)fault-tolerance, improved diagnostics and graphical display techniques(reduced challenges).

The EBR-II will serve as a tests platform for the design above.

The transition from the analog control systems to the complete automation under human supervision with digital control will be done in 4 phases.

The first phase has been already started with the replacement of analog controllers by digital controllers, performing a PID control, in some plants.

The level 2 consists in the automation of some operation routines like start-up, shutdown, load changes, emergency response procedures, and refueling, using expert systems and graphical interfaces. The control strategies are a combination of hierarchical, optimal, linear, and robust techniques. The EBR-II is in this phase.

The level 3 will consist of full automation of all hierarchical levels of control with an intelligent adaptive supervisory control systems interacting with the operators through an intelligent interface. It will use sensors able to validate their own signals and robust, nonlinear fault-tolerant process controllers. These controllers will be able to reconfigure the control logic to meet the operational objectives selected by the supervisory control system. The maintenance planning will be automated, tracking the operational experience of all plant systems and components stored in an automated data base as well as the operation historic data.

The control system will have a human performance modeling to allow a optimal allocation of functions decision between humans and computers, in a human centered design, in order to keep the operators motivated and well-informed. This is the central idea behind a collaborative control system described in the chapter 2.2.3. This level is the main goal in the PRISM design by GE(General Electric).

The level 4 will foresee a total automation of the plant, not only in the systems but also in the maintenance and management services. The control system will utilize not only the local plant information but a network contained operational experiences data from others US plants and abroad. Intelligent robots will make the maintenance and security surveillance job. It's expected that this level will not be achieved in the USA for many years, although in Japan a similar project is scheduled by the year 2005.

ARGONNE NATIONAL LABORATORY

The ANL research is concentrated in the following areas(White et al., 1989):

a) human-machines systems reliability sensors signals validation
b) graphics, real-time communication and diagnostics
c) networking and distributed control local intelligence
d) plant testing of passive safety features
e) fault tolerance
f) faster than real time simulation

The reliability of the system is being issued in two ways:

1) tolerance against individual controllers failures or human errors;
2) fault tolerance of computer hardware and software.

The sensors validation is being studied by the use of several techniques, including an System State Analyzer(SSA), a Sequential Probability Ratio Test(SPRT), Analytic Redundancy, Kalman Filters, and so on. ANL is also following the ideas of Beltracchi, Rasmussen, and Vicente for constructing a real-time graphical displays that are thermodynamic models of the plant.

The data transmission in real-time is being provided by an Ethernet system in optical fibers that collect plant data from the Data Acquisition System(DAS) at one-second intervals. Two techniques of diagnostic are being considered: one uses pattern recognition statistical techniques and the other uses fuzzy logic for real-time applications. Faster-than-real time simulator with prediction capacity are being constructed to run in the CRAY supercomputers.

ORNL(OAK RIDGE NATIONAL LABORATORY)

The advanced control systems need an integration of several emerging technologies such as control theory, software engineering, artificial intelligence, and human-machine systems.

The ORNL established four kinds of activities to achieve their integration:

-demonstration of advanced control system designs that would meet the goals described earlier;

-establishment of a design environment that allows designers to formulate and test various control strategies;

-testing and validation of advanced control system designs by simulation;

-guidance in control software and hardware specification and implementation.

DESIGNS DEMONSTRATIONS

The EBR-II in Idaho, the FFTF(Fast Flux Test Facility) in Washington, the research reactors in ORNL and in other national laboratories will be utilized for these demonstrations:

-demonstration of a digital control for feedwater systems.
-demonstration of hierarchized supervisory control system
-automated start-up, fault-tolerant

DESIGN ENVIRONMENT

-intelligent control analysis and design workstations

-strategies for advanced control (adaptive, model-based digital control)

The use of process models will provide not only an estimate of the complete state vector but mainly the generation of the feedback signal. It is necessary a model that can deal with both, continuous and discontinuous variables type systems. ORNL intends to combine state-based and object-based control logic.

HUMAN-MACHINE INTEGRATION R&D

The model INTEROPS will be used to simulate the human-machine interaction in order to specify design criteria in the design preliminary phase. The final design will be tested and evaluated with a full scope real-time simulator and experienced operators.

TESTING AND VALIDATION BY SIMULATORS

Methods are being developed to test and validate the plant process simulator and controller hardware (firmware - software programmed in PROMs) according with the american standards(ANSI,IEEE,NRC Regulatory Guides, etc.).

CONTROL SOFTWARE AND HARDWARE R&D

CASE tools are being developed to provide software quality according to the american standards, especially IEEE, ANSI, NRC and DoD-2167a. Higher-order languages (C or ADA) and fourth- and fifth-generation tools(4GL and 5GL) will be used.

AUTOMATED START-UP OF THE EBR-II

This system has great similarity with the CCM in the chapter 2.2.3. It has a DSS that gives a strategy to validate the information necessary to judge if the control strategy used by the control system or the operator is correct. Several control techniques are being tested:

-non-linear reconstructive
-adaptive
-linear-quadratic-gaussian(LQQ)
-LQG with LTR(loop-transfer-recovery)
-PID(proportional-integral-derivative)
-closed-loop nonlinear control
-fuzzy logic control

To model the DSS, a structured state-transition and data transformation technique was proposed. It will be integrated in a object-oriented programming in the future designs. This integrated tool can be already found in the book of Schlaer and Mellor(1992). To describe the time-oriented behavior of discrete states three tools will be constructed to store the data associated with their state transformation:

DFD(Data Flow Diagram)
STD(State-Transition Diagram)
ERD(Entity-Relationship Diagram)

The STDs are implemented in IF-THEN rules and the states define breakpoints in the automation, as in the Japanese ABWRS.

SUPERVISORY CONTROL

The supervisory control has a structure similar to the CCM in the chapter 2.2.3. The plant state vector is provided for the operators, the subsystems controllers, and the system supervisory controller. The operators exchange information with the supervisory controller through an intelligent interface and send a proposed control vector. The subsystems controllers send also a set of proposed control vectors. The supervisory controller selects a control vector according to the system state. It is implemented in OPS5(production system) running under LUCID LISP on a SUN4 computer. The graphical interface programmed with the object-oriented graphical package DVTOOLS and runs in SUN3.

The simulators are written in the Advanced Continuous Simulation Language(ACSL) and run on a SUN3 computer. For discrete event simulations, ORNL is developing a design environment on a LMI LISP machine using FLAVORS object-oriented language and a Macintosh-II based Texas Instruments Explorer (SUN workstation is planned for the future). The methodology was described in chapter 2.2.3. Robinson (Robinson, 1989; Robinson/Otaduy, 1988) uses the commands:

FLAVORS	**CLIPS** (see item 2.4.9 MIT)	
defflavor setf	defclass definstances	to define class of objects and instances
defmethod	defgeneric/ defmethod	to define operations to be executed in the objects
send	defmessage-handler	to send messages to the objects to execute some operation

HUMAN-MACHINE SYSTEMS

In the Kneer/Robinson paper(1989), they pointed out two important conclusions about human-machine systems. One of these came from Thomas Sheridan(MIT):

"Communication at the human-machine (human-computer) interface has two principal functions: communication of the human operator's intent to the machine and communication of the machine's state to the humans". (see intent model and IMA in the chapter 2.2.3).

The other is one of final conclusions in the paper:

"What is evident from this work is that efforts associated with dynamic allocation of tasks and functions are critical to advances in the development of intelligent computer-based operator associates". (see chapter 2.2.3 about CCM and dynamic allocation).

To simulate the human-machine interaction an object-oriented qualitative simulation (QS) of human mental models was developed (Schryver, 1992). This QS model will be incorporated in INTEROPS (see chapter 2.2.2.2B) to simulate the knowledge-based behavior of human beings. The qualitative simulation is based in the confluences method (de Kleer/Brown, 1985). Schryver discusses the Iwasaki/Simon (1986) critic about causality in the deKleer's method, although he keeps the mythical causality inside the model. He recognizes some deficiencies in this approach as well as the lack of a hierarchical model (and a topographical search), and an abstraction versus aggregation space, concepts discussed in the chapter 2.2.3. These deficiencies are to be implemented in future developments.

The QS model was implemented in Common LISP/FLAVORS on a VMS-based VAX machine. The "defmethod" command was used to implement the SOLVE-CONFLUENCE method. The control of the constraints propagation is done by the PROPAGATE method that triggers other methods to execute state transitions, trip criteria, feedback control, inputs, etc. The UPDATE method controls the messages between objects.

MAN-MACHINE INTERFACE

A methodology for the initial design of the new EBR-II interface is being developed utilizing the GOMS technique (see chapter 2.3).

SOFTWARE V&V

Uhrig (ORNL) emphasizes the necessity of CASE tools development to automate the software process. In the USA, the code cost is $60 to $100 per line of validated code. A code like in Sizewell B (chapter 2.3) protection system, having 200 thousand lines, will cost $20 million. The Japanese experience with CASE has shown a reduction factor of 15 in the costs (Uhrig, 1989). He mentions a CASE facility called Advanced Control Test Operation(ACTO) being developed in the ORNL.

ROBOTICS

Uhrig(1989) mentions a DOE program in Robotics research, called Nuclear Energy University Program in Robotics for Advanced Reactors. It involves ORNL and 4 Universities (Florida, Michigan, Tennessee, and Texas).

USE OF NEURAL NETWORKS FOR DIAGNOSIS AND SIGNALS VALIDATION

Bartlett and Uhrig (1992) describe a method to train a neural network for diagnosis using the SOSLA (Self-Optimizing Stochastic Learning Algorithm), with 27 plant variables at 0.5 s. intervals for at least 250 s. They used the simulator data from 8 main accidents for the Watts Bar Nuclear Power Station.

Upadhyaya and Eryurek (1992) used the backpropagation algorithm (BPN) to train a neural network for signals validation using EBR-II sensors data in different levels of power. This is an alternative method compared to the classical pattern recognition techniques (discriminants and autoregressive models) tested in the EBR-II (Upadhyaya et al., 1989).

In the paper of Uhrig (1993) about use of neural networks in the analysis of complex systems, he describes the research going on the ORNL and U. of Tennessee, including the work mentioned above. Particularly, a hybrid system for transient identification, combining neural networks and a rule-based expert systems using fuzzy logic is described. A pre-learned neural network (with the same 8 transients from the Watts Bar Nuclear Power Station) provides the membership function for the fuzzy logic based system. This approach is the same suggested later as a research theme for the MIT. Uhrig mentions genetic algorithms (GAs) in the introduction of his paper, which demonstrates the same vision already referred in the use of GAs to optimize the choice of neural networks parameters or fuzzy sets membership functions.

The Electric Power Research Institute(EPRI) is emphasizing two research areas: nonlinear dynamics and neural networks. EPRI is supporting some investigations concerning the neural networks (1993, Wildberger):

-an expert system to assist the designer of a neural network,

-the use of genetic algorithms to evolve a superior network for a given application,

-the design of neural networks with hierarchical structures that are related to the known structure of the application, and

-combining neural networks with fuzzy sets to the advantage of both technologies.

The research of genetic synthesis of neural networks is being developed at the Honeywell Sensor and System Development Center and "this simulates a form of natural selection in which the parameters and structure of the neural network, as well as its weights are optimized in accordance with some prescribed 'fitness function'" (Wildberger, 1993).

The research in intelligent computer-aided engineering is being developed in the U. of Nevada, Las Vegas, combining neural networks, fuzzy logic, and genetic algorithms.

The research in hierarchically structured neural networks is being developed at the U. of Maryland and the main goal is to design a neural network to reflect prior knowledge about the structure of the physical systems, through a hierarchical decomposition of the set of inputs to be used as training data.

"The inputs are clustered hierarchically into successive subsets of related inputs, based on those inputs that refer to one small portion of the physical system, one constraint, or a single interval. The neural network is then designed out of hierarchically connected small subnets mimicking the structure of the invent data. Each layer of subnets feeds its output into subnets at a higher level that represent a greater aggregation of the physical input data." (Wildberger, 1993).

"If the behavior of the system to be modeled is understood in, at least, a general of approximate way, then the design can begin with a qualitative model and neural networks used to quantify it. The hierarchically structured neural networks described above are one way to approach this. Another way is to structure the qualitative model in terms of 'fuzzy sets', and then use neural networks to define and structure the contents of each set. In this case the networks can serve both as 'fuzzifiers' to place input data in the appropriate set or sets, and as 'defuzzifiers' to produce specific numbers from the output sets constructed or selected by the 'fuzzy logic' of the underlying causal model". (Wildberger, 1993).

This latter approach is similar to the one described later in the chapter about the researches suggestion for the MIT.

2.4.8 HALDEN PROJECT

The Halden Project is a joint effort of US, Japan, and 8 European countries to develop an advanced control room. The Halden design group identified the following weaknesses in the current man-machine interface and their solutions (Haugset et al., 1992, 1990):

1) lack of process information - use of advanced display features and COSS(Computerized Operators Support Systems);

2) overflow of information - prioritization of alarms;

3) one sensor/one instrument technique - integration of separate pieces of information;

4) wrong or inconsistence information - signal validation;

5) poor presentation of information - CRTs based graphical information;

6) lacking support in diagnosis of problems - diagnosis systems;

7) lacking support in planning of actions - tools based on faster than real-time simulations and expert systems;

8) errors in implementing control actions - computerized procedure systems.

Taking the Rasmussen's operator decision making model as a base, the problems above can be classified as:

1)<u>status identification</u> (detection, observation, and identification): problems 1,2,3,4,5,6,
2)<u>action planning</u> (evaluate, define task, and select actions): problem 7,
3)<u>action implementation</u>: problem 8.

For each problem, the Halden designers developed a specific system:

Problems	SYSTEMS
1	EFD,CFMS
2	HALO
3	GRAPHICAL DISPLAYS
4	SIGNAL VALIDATION
5	12 GRAPHICAL DISPLAYS
6	DISKET,DPP
7	SCORPIO,PS,SPMS
8	COPMA

The EFD(Early Fault Detection) is an alarm system for detecting disturbances. EFD acts as a complement to HALO. The EFD will trigger the DDP system. The CFMS(Critical Function Monitoring System) detects deviations in the critical safety functions, informing the system when it is approaching its limit, and the operator when it is violated. The former is important to distinguish severe disturbances from less important ones.

The HALO(Handling of Alarms using Logic) managing the alarms, suppressing the unnecessary alarms and prioritizing them.

The DISKET is a knowledge-based systems developed at JAERI(Japan Atomic Energy Research Institute) that generates hypothesis for the causes of the alarms.

DDP is composed of DD and DP. The DD(Detailed Diagnosis) uses knowledge-based techniques to identify the failed components. The DP(Detailed Prognostic) is a model-based system that predicts the process behavior following the disturbance detected in EFD and diagnosed by DD.

The SPMS(Success Path Monitoring System) suggests action plans to the operator when a critical function is violated or its limit is being approached. It uses alternatives displays and the information from DD and DP.

The PS(Procedure Selector) identifies the relevant procedure when a disturbance is diagnosed. COPMA is a system that presents to the operator a procedure, step-by-step on screen.

An intelligent co-ordinator(IC) supervises and controls the information flow among the COSSs described above. The set of IC and the COSSs constitute the ISACS(Integrated Surveillance and Control System) concept. The ISACS hardware in the Halden Man-Machine Laboratory(HAMMLAB) is constituted by 12 computers, using ETHERNET Local Area Network(LAN). IC was developed with the expert system shell G2. The database was implemented with SYBASE and the user interface management system PICASSO-2 controls the MMI display and dialogue.

The "cockpit control room" (Førdestrommen/Haugset, 1991) of the ISACS has 4 keyboards, a voice output device, a bell for the HALO alarm system, and 13 screen (12 color graphic CTRs, one in black/white) divided as follows:

1)four displays for overview information: HALO overview, state identification, action planning and implementation, and Rankine cycle;

2)HALO list, alarms screen displaying the alarms as text strings;

3)four identical NORS(full-scale PWR simulator) process I&C stations, for operating the plant, with tracking ball;

4)COPMA, workstation for computerized procedures with mouse;

5)the two stations COMBI/COSS and COMBI/COSS with keyboards and tracking balls, which are six different COSSs(CFMS, SPMS, DISKET, EFD, DPDF) integrated. COMBI means combined information.

The evaluation of ISACS-1 started in 1991 with three different methods (Folleso et al., 1993; Haugset et al., 1993):

1)guideline evaluation (results showed some inconsistences of coding remedies, and slow response time for display of information);

2)GOMS analysis (not finished); preliminary results indicated reduction in the workload;

3)using expert operators (well accepted by the crew).

The DISKET system was evaluated in the NOKIA research simulator (NORS) experimental control room(full-scope). The results showed that DISKET improved the quality of diagnoses (Endestad, 1993). However, in situations when DISKET is vague or imprecise, it might impair the operators performance.

The OECD Halden Reactor Project has started a new research program called CAMS(Computerized Accident Management System) to develop an object-oriented simulator based in Kalman filters to estimate and predict system parameters (Bjørlo et al., 1993).

2.4.9 MASSACHUSETTS INSTITUTE OF TECHNOLOGY RESEARCH REACTOR EXPERIENCE

John Bernard (MIT) made a revision (1993) of the challenges in the application of intelligent systems to nuclear plant instrumentation and control. He shows the evolution of the control system design through the following design classification:

method	improvement
1. proportional-integral-derivative	automated operation
2. transfer functions	theoretical determination of gains and stability (single output)
3. state-space methods	selection of response characteristics (feedback of all variables)
4. optimal control	satisfaction of performance indices
5. feedforward control	control of non-linear trajectories(robotics) -real time
6. computer-torque method	trajectory tracking (robotics)-real time
7. expert systems and intelligent control	real-time diagnosis and autonomous operation

Methods 2 and 3 are linearized system models while 5-7 are non-linear system models. Method 4 can be implemented in both ways. Analog equipment can implement PID controls and linearized models. Digital computer can implement both, linear and nonlinear models.

The nuclear area has utilized digital techniques merely substituting analog equipment by the digital units without using the full potential of this technology. Also the nonlinear methods have been ignored. But, as Bernard stressed in his paper, with the intelligent control this will not happen because this technology is the base to solve the problems arising from unfamiliar and nonanticipated events. Furthermore, there are also a tremendous costs savings with digital control.

The MIT started its research in digital control through a joint effort with the Charles Draper Laboratory(CSDL) in 1980. After the demonstration of techniques for signal validation and instrument fault detection, the MIT-CSDL Non-Linear Digital

Controller(NLDC) was developed and licensed in april 1985 by the NRC. The NLDC uses reactivity constraints to determine a change in the present control signal in order to avoid an overshoot in the some future time. The NLDC has a function of verifying the design of each other control being tested and will intervene in case of unsafe condition. In the NLDC two kinds of equations were used: a standard dynamic equation (without and with prompt terms) and a alternate form of the dynamic period equation.

At the same time, a fuzzy logic controller was tested (Bernard et al., 1986; Bernard, 1986). In 1986, a cooperation between MIT and Sandia National Laboratories(SNL) was started for the study of control strategies for a reactor-powered spacecraft. This resulted in the MIT-SNL Period Generated Minimum Time Control Laws for rapid maneuvering of reactor power, an approach related to the computed-torque method for trajectory tracking in robotics (Bernard, 1989). Later, a cooperation between MIT and ORNL resulted in the PMSIM(PWR - type Multimodular Plant Simulation Program) (MITNRL-049, Kim et al., 1993). The PMSIM was based in the experience of the other simulator developed in the MIT: PRISM(Pressurized Reactor Interacting Simulator Model) (MIT-NRL-041).

Faster than-real-time simulators are important for the next step in the control systems research in the MIT. They are an alternative option to the expert systems based in rules. As already pointed in the chapter 2.2.3 and 2.3, rules based systems contains several deficiencies: lack of a hierarchization structures, little relation to the physical laws, incompleteness, lack of temporal reasoning, difficult V&V.

Bernard(1992) discusses several problems to be solved for the acceptance of intelligent decision support systems like the CCM (chapter 2.2.3) and the continuation of the research in the MIT. To construct such systems, not using the traditional expert systems, a model-based approach is necessary. This requires a faster-than-real time simulators, which represents a tremendous task because it must involves the whole plant and its all possible states, although some studies has been done in the MIT to understand the complexities of the systems and its relationships with the diagnostic problem (Golay, 1988, 1988, 1989).

One solution proposed was the use of qualitative differential equations instead of quantitative differential equations. As seen in the chapter 2.2.3., still remains ambiguities in such approach that can only be solved with an integration between qualitative and quantitative results. This was already propposed by some authors (see chapter 2.2.3). The solution for that was already mentioned in the chapter 2.2.3: an object-oriented programming, where the systems constraints will be represented by the relation between objects, an approach followed by two researchers in the MIT-NED (Dobrzniecki/Lidsky, 1989), in contrast with the qualitative simulation research in the MIT Chemical Engineering Department (Oyeleye/Kramer, 1988 and 1989). The MIT AI Lab. is also following this latter method.

Two additional questions are important here, the cognitive model and the intelligent interface. The MIT has an on-going research to improve the former methodology of Huang/Siu described in the chapter 2.2.2.2B, where there is a revision of several cognitive models.

Concerning to man-machine interfaces, the MIT was successful in constructing some predictive displays that show to the operators in its research reactor, the consequences of their actions (Bernard, 1992).

SYMBOLISM X CONNECTIONISM

As in the cognitive models, intelligent support systems have two extreme approaches: one, symbolic(artificial intelligence) and the other connectionist (fuzzy logic and neural networks). There is, however, a link between these two extremes. The production rules are the link. In the fuzzy systems, fuzzy rules will be used instead of rules with certainty factors. In the production systems, the rules are fired without a methodology to order them along the time. In fuzzy systems, the rules are fired at the same time. A structure for this is the FAM(Fuzzy Associative Memory) (Kosko, 1992 and 1993). Fuzzy systems work with a theory of the possibilities instead of a theory of probabilities in order to deal with uncertainties. Zadeh claims that the Theory of Probabilities is not enough to represent all the systems uncertainties (Grzymala/Busse, 1991). Besides these uncertainties, the system has to deal with knowledge incompleteness. Which we need is a system that could learn and generate its own fuzzy rules. This can be achieved through another Kosko's suggestion, the Adaptive Fuzzy Systems(AFS).

In the AFSs, a neural network learns the training data and generate FAM rules. An Adaptive Vector Quantizers(AVQ) like the Differential Competitive Learning (DCL) is used to recover the bank of FAM rules (Kosko, 1992).

The possibilities of this system are such that we can use the AFS after a certain level of training to work alone without supervision. The system will deal with situations not included in the training data. This characteristic sounds very similar to that we need in the case of unfamiliar and nonanticipated events in nuclear power plants. In other words, the AFS is a system that could work in the knowledge-based level of the Rasmussen's framework.

But we have other problem. It is the different levels of hierarchization. This can be solved with other structure suggested by Kosko: the Fuzzy Cognitive Maps(FCMs). A FCM is a network of causal (constraints) relationships. The nodes of the network are cognitive elements (neurons or other neural networks). For the operators' activities in the NPPs they represent the operators' mental models and their human information processing. Each node can represent an object (abstract or concrete) in the levels of hierarchization (MFM or the physical network of components and systems) or the information processing activities. According to the fuzziness of the rules, we can simulate the stereotyped behavior in the Rasmussen's framework or go to the knowledge based level to identify a goal for the new situation.

The structure in terms of objects would make more easy the V&V compared with the production systems based expert systems. At first, we had production rules, then frames, scripts, and semantic nets. A generalization of these concepts is found in objects. Similarly, like fuzzy frames, we can construct fuzzy objects using FCMs. In terms of an object-oriented paradigm, we could have the following parallel:

objects (knowledge sources, frames)	sub-FCMs
attributes (frames slots)	fuzzy rules
relationships(messages)	fuzzy rules
states	nodes
events(causes,operators)	fuzzy rules
actions(scripts, production rules,procedures, goals,plans,tasks,control)	fuzzy rules
system of objects (semantic nets)	FCMs
state models	sub-FCMs

Thus FCMs will be used from the highest level (operation goals) until the lowest level (components and subsystems status). The causal relationships between the attributes or variables (fuzzy sets) of the objects (sub-FCMs) or between objects are defined by fuzzy rules. The control actions are also defined by fuzzy rules generating events that equally fuzzy rules. The causal relationships (constraints) can be learned by the system through a Differential Hebbian Learning(DHL) if we think the FCMs as neural nets and the fuzzy causal edges as synapses of the neural nets.

Artificial Intelligence is not contrary to the fuzzy neural networks as seen by many authors, but they are complementary. AI is a bridge between our higher levels of cognition, governed by goals, plans, operators and preferences (like in SOAR or in the Theory of Scripts) and the actuation in physical plane (the objects structured in networks). Rasmussen (1986), for example, gives a framework for the human processing system in which a conscious processor (symbolic, sequential) controls a subconscious processor (analog, parallel). Newell has a similar approach when he compares SOAR with connectionist models(1990). Nevertheless, some neurologists could not accept this model for the human brain.

Edelman(1992) has the opinion that a neuronal net model for the human brain doesn't differ much from the actual computers (serial or parallel) based in the Turing's machine. In the latter the brain (or the computer) is seen like an information processor which transforms the inputs into outputs. If the inputs were stored in a tape, the true Turing's machine would need an infinite tape (Penrose, 1989). Neural networks are basically symmetrical matrices like connections, following Edelman. He claims that the learning of the neural nets are not selectional, and that the "responses (not the values) of connectionist systems are specified in advance and are imposed on the system by a human operator...". However, there is another option for the neural networks to learn the data from the training. It's based on the genetic algorithms (GAs, Holland et al., 1986). In this case, GAs are used to select the parameters or weights of the neural nets. GAs could also be used to select memberships functions in fuzzy sets.

From above, we must conclude that it's necessary a hybrid model for the human cognition that can be used in a human-machine systems. In the chapter 2.2.2.2B we saw many models of cognitive architecture as well as several partial models based in production systems or their generalizations in terms of frames or knowledge sources (BBAs). The cognitive architectures were divided in three extremes: production systems (ACT and SOAR), connectionism(PDP), and empirical models(MHP). Between HPS and ACT/SOAR we found the intuitive models (Holland et al., 1986). There are several hybrid models in the middle of these three extremes. The best known is CAP2, based in the Schneider/Detweiler model for the working memory (WM), covering almost all the WM aspects.

A model like CAP2, combining SOAR, the Holland's genetic algorithm, the empiric evidences of MHP, and the fuzzy neural nets structures would approximate better of the human cognitive model in our brains. In fact, the efforts conducted in the ICOT (the 5th and 6th generations of computers) as well as in the LIFE(Laboratory for International Fuzzy Engineering), in Japan, would carry us to new machines suitable to solve the actual problems of HMS and the CCM.

RESEARCHES PROPOSALS FOR THE MIT

The MIT has developed PRISM, a real-time simulator for PWRs. The outputs of PRISM could be read and analyzed to get an autonomous diagnosis of the generated accidents. A good theme to be investigated is a performance comparison between the fuzzy rules generated by the training of a neural network with an AVQ(Adaptive Vector Quantization) algorithm (Kosko, 1992) and the qualitative explanation rules generated by qualitative equations transformed into production rules (Yoshimura et al., 1992). For the latter, it is necessary a knowledge based systems shell. This author used the CLIPS shell to read the data from PRISM. CLIPS has a language similar to LISP and the production rules can be constructed with 'defrules' and 'deffacts' commands. Following Gonzalez(1993):

"CLIPS stands for C Language Implementation Production System. Developed by the Artificial Intelligence Section of the Johnson Space Center of NASA, CLIPS is a forward chaining rule-based system based on the pattern matching algorithm (the Reti algorithm) developed for the OPS-5 system. The system provides high portability, low cost, and high degree of integration with external programs."

This version includes a CLIPS object-oriented language(COOL). A better object-oriented program is NEXTSTEP (available in the NED-MIT), which has multimedia interface. In this case, it is necessary to reprogram PRISM in an object-oriented approach. This would be a natural step to go further and construct a neural network of objects in levels of hierarchy.

3. OPERATORS TRAINING SYSTEMS AND INFLUENCE OF ORGANIZATION & MANAGEMENT IN THE PERSONNEL PERFORMANCE

The problem of the human error is not merely technical in the scope of the relationships between humans and machines. As in the chapter 2.2.3, a world state is linked to the DSS in the CCM scheme. Many problems that arise in a control rooms have their origin outside the plant. Reason described an accident as a combination of latent failures and active failures (chapter 2.2.5). These latent failures come from the management and organization activities in the utility that operates the nuclear power plant as well as socii-political-economical constraints in the environment. This constitutes the world state for the operators crew in the control room.

Embrey (1991) shows the importance of bringing organization factors to the fore of human error management. A survey conducted by the Institute of Nuclear Power Operations(INPO) has indicated a contribution of 51% to the events arising from human performance problems:

1. human performance problems - 51%
2. design deficiencies - 32%
3. manufacturing - 7%
4. external - 5%
5. other - 5%

If we think that many problems in the items 2 and 3 are in fact due to human failures, then the item will achieve a worth of 70%. The IAEA statistics show that this is the case.

Among human performance problems the following distribution is found(INPO):

1. deficient procedure or documentation - 45%
2. lack of training or knowledge - 18%
3. failure to follow procedures - 16%
4. deficient planning or scheduling - 10%
5. miscommunication - 6%
6. deficient supervision - 3%
7. policy problems - 2%

All these items pertains to the field of management & organization, including training systems. Llory and Larchier-Boulanger(1988) observe that there are three levels of analysis to study human factors:

1st level - the human interacting alone with the machine
2nd level - group's level: problems arising from the interaction between groups (communication)
3rd level - organization level: psycho sociology of organization and business enterprises.

As a background level, there are the cultural aspects of each organization, group, or human being. In 1987, a consortium of Japanese utilities in collaboration with US engineers and scientists started a research program called CRES(Control Room Evaluation System) to study the human deficiencies associated with the group's level, taking into account cultural differences (Fujita et al., 1993).

In this program PSFs(Performance Shaping Factors) have been identified, using the operators participating in three training courses:

1)normal retraining course
2)advanced retraining course
3)educational opportunity course

The training simulator was a replica of the Takahama Unit-3 control room (840 Mwe PWR) operated by the KEPC.

The PSFs were classified in categories:

1) cognitive ability
2) personality
3) background stress and stress coping measures
4) leader behavior
5) background experience
6) group interactions measures.

The results has demonstrated that:

1) the training system and the personality characteristic of an individual have a great impact in his or her performance,

2) the human behavior in the USA is characterized by an individualism while in Japan by a collectivism; this explains why the japanese workers communicate with themselves more than their colleagues in USA;

3) previous research in anthropology and cross-cultural psychology shows that there are more differences within groups than between cultural groups.

A recent paper (Isoda, 1993) described the phenomena of technology transfer between two cultures, USA and Japan. The conclusion from this observation is that a third culture can be created, a result of the miscegenation of the cultures (Fujita, 1993). Echizen and Taniguchi (1993), for example, discuss the social forces behind the japanese style of management and the reason why the Deming's Total Quality Control worked in Japan and didn't work in USA, although its origin was in the latter.

In the USA, the NRC Program of Human Factors established 7 items of research:

1) personnel performance measurement (protocol, data, and NCR/LER reports evaluation),
2) organization & management evaluation (modelling and performances indexes),
3) personnel subsystems (training, qualifications, and licensing examinations),
4) human-system interface (human engineering* and procedures),
5) reliability assessment (HRA/PRA integration).

* Human Engineering:

1) local control station
2) hierarchized annunciator systems
3) advanced I&C (use of artificial intelligence and expert systems)
4) evaluation the impact of the automation in the human system interface - cognitive models)
5) computer classification
6) expert systems verification and validation
7) Halden Project

The INPO is helping the NRC with the subject in the items 1 to 5. The man-machine studies are spread over the national laboratories and the EPRI. Particularly, in the item 7, there is a research at the BNL(Brookheaven National Laboratory) supported by NRC to include the organizational factors in the PSA. In recent paper (Haber et al., 1993) BNL and UCB(U. of California at Berkeley) reported a joint field research in NPPs outage management. At the same time, UCLA(U. of California in Los Angeles) is developing the Word Process Analysis Model(WPAM) methodology to include organizational factors (OF) in PSA (Apostolakis et al., 1993), through OF event trees and the Reason's models for human errors classification and accidents causation (Reason, 1990). Also, the U. of Maryland, at College Park, is developing similar assessment, using a diamond tree with organizational hierarchy, a structured top-down success-oriented tree that describes a NPP and its operation(Modarres et al., 1992).

At the MIT Center for Energy and Environmental Policy Research, the MIT International Program for Enhanced Nuclear Power Plant Safety was developed. Three main research topics are (Progress Report, 1993):

1) Use of PSA to planning outage scheduling for a NPP, under supervision of Prof. Norman C. Rasmussen;

2) The science of management of nuclear power plants program, directed by Prof. John S. Carroll from the MIT Sloan School of Management;

3) Analysis of Social Political Factors in NPPs, conducting by Prof. Kent Hansen (Energy Lab. Director) and Tatsujiro Suzuki (visiting scientist).

The main research projects in the Program of Science and Management are:

1) Plant selection by performance history
2) Organizational Pathways in Outage Planning and Scheduling
3) Mental models and organizational learning
4) Relationship between NRC and plants management
5) Total Quality Management
6) Transfer of best practices between utilities.

All the research items are in progress. Concerning to the Analysis of Social/Politics Factors, two researches were started:

Phase I(1991-1992) - Development of a PIP(Policy Influence Path) for Nuclear Power Plant (Suzuki/Yamaoka, 1992, 1993).

Phase II(1992-1993) - Analysis based on SPDM(Social/Political Dynamic Model) for Nuclear Power Plant, using the software package called STELLA-II of Systems Dynamics (Eubanks, 1993).

Phase III(1993 and beyond) - Decision Analysis Tools for Nuclear Safety).

This tool could be the base for a description of the World State in the CCS (chapter 2.2.3). In the Appendix of this report an alternative systems dynamics formulation will be discussed,i.e., the FCMs(Fuzzy Cognitive Models). FCMs could also be used for the diagnostic system (a part of the DSS in the chapter 2.2.3). These FCMs are modelled with Neural Networks and the Hebbian Learning Law.

The human-centered design become the main focus of my discussion in this Report. The use of more and more technologic sophistication shall help us to construct machines and interfaces that can give us the power of controlling our environment with safety and economical adequacy, without wastefulness and pollution. In order to make the machines useful in this way they have to reflect the human mental models to be acceptable and understandable human beings, otherwise a mismatch could cause errors of both parts, and a disastrous consequence in the environment.

An autonomous nuclear power plant like the japanese and the ORNL projects (see chapter 2.4) is not a distant aim, although we can not forecast when it will happen. Efforts in the field of the Artificial Intelligence seem to point that we must bring to it the contributions in other areas.

The ICOT project in Japan and its successor, the sixth generation computer, are important entrepreneurs that will form the base for future developments. The creation of the LIFE(Laboratory International of Fuzzy Engineering) and the neural computation studies in Japan will dictate the next projects.

In the USA, these subjects are more polarized with the classical artificial intelligence(AI) in the east coast (MIT AI Lab) and the Fuzzy Neural Network in west coast (Californian Universities). Between them, we found hybrid models like CAP2 (chapter 2.2.2.2B). In the Europe, there is the ESPIRIT project.

Two disciplines are very important to integrate AI, Fuzzy Logic and Neural Networks: cognitive psychology and neurophysiology. The first one giving the concepts of high level cognition (symbolic) accomplished the goals of the AI. The second one to establish the hierarchized structures under which the neural networks will execute the AI processes as low level cognition (subsymbolic).

The most advanced design of human-machine systems in developing for the nuclear area is the MMS project in Japan. This project is based entirely in the classical AI techniques emulating characteristics of the human cognition with the Rasmussen's framework for the human information processing. The knowledge-based level is then treated symbolically aided by numerical simulations. This combination of qualitative and quantitative results in a hierarchical structure is able to deal with most of the situations of operation. However, the adaptive characteristic of such systems, necessaries to the creative capacity in unfamiliar events, can be better simulated with the use of neural networks and fuzzy rules structured in that way.

This can be seen as the great challenge for the next years.

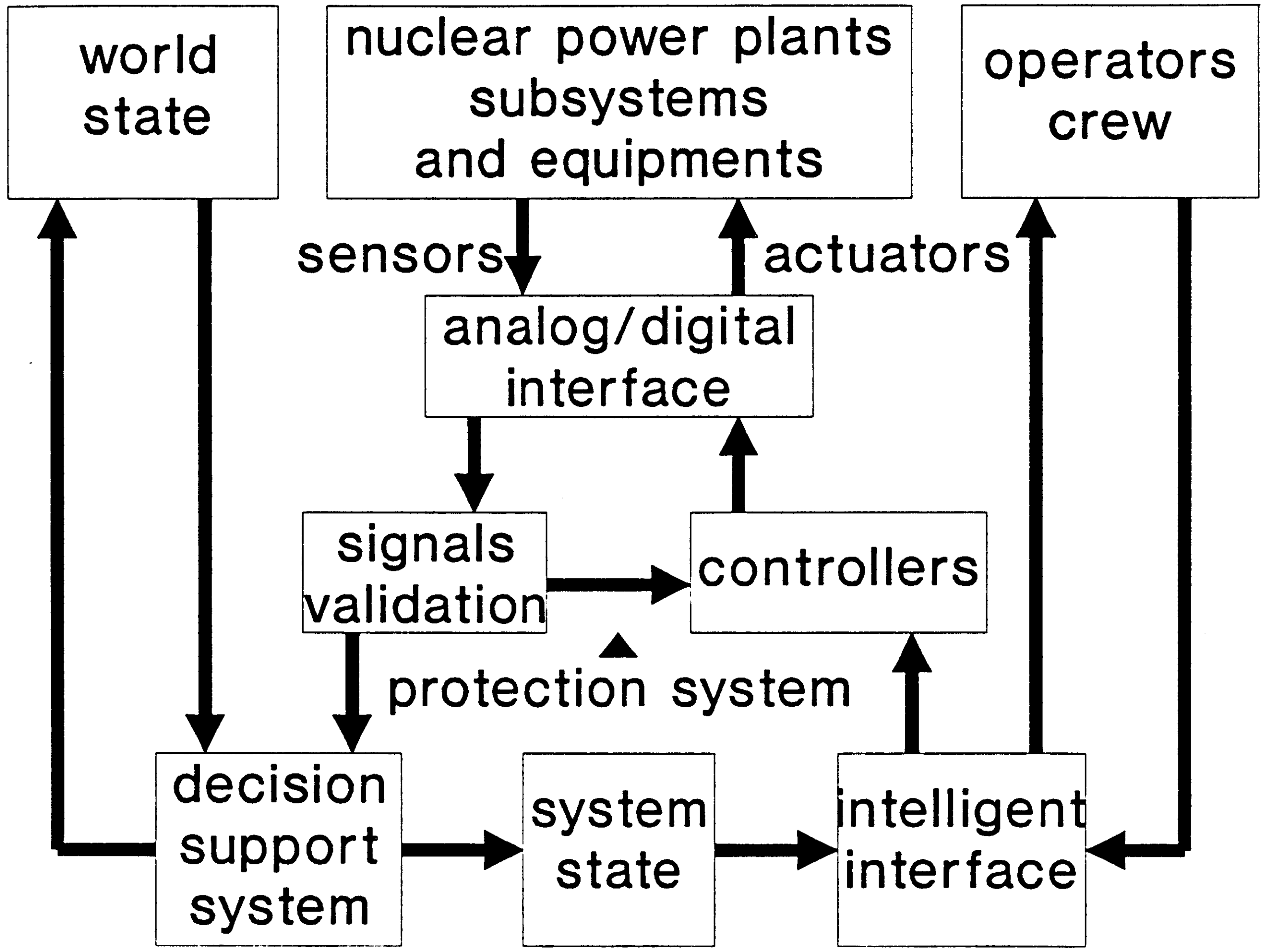

Fig. 1 - Collaborative Control Model for Nuclear Power Plants

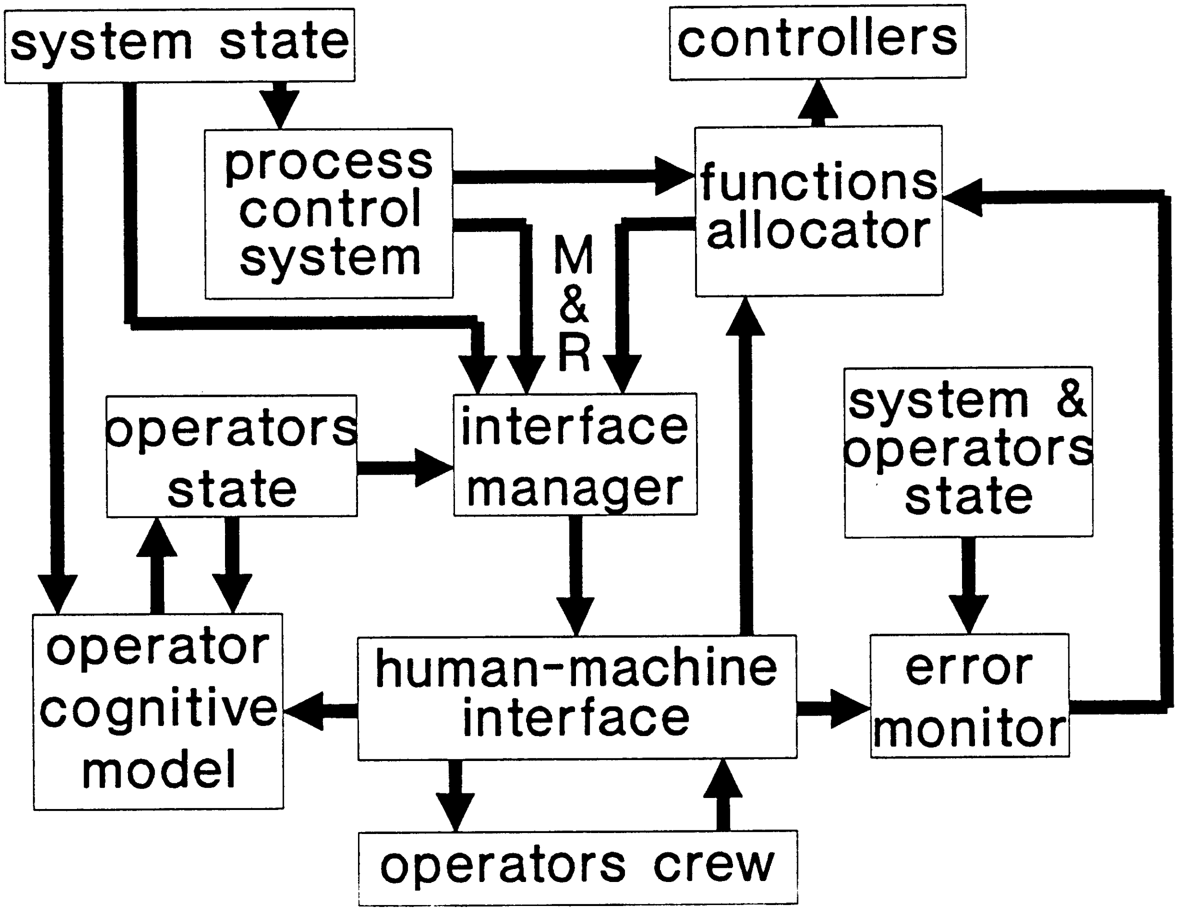

Fig.2 - Intelligent Interface

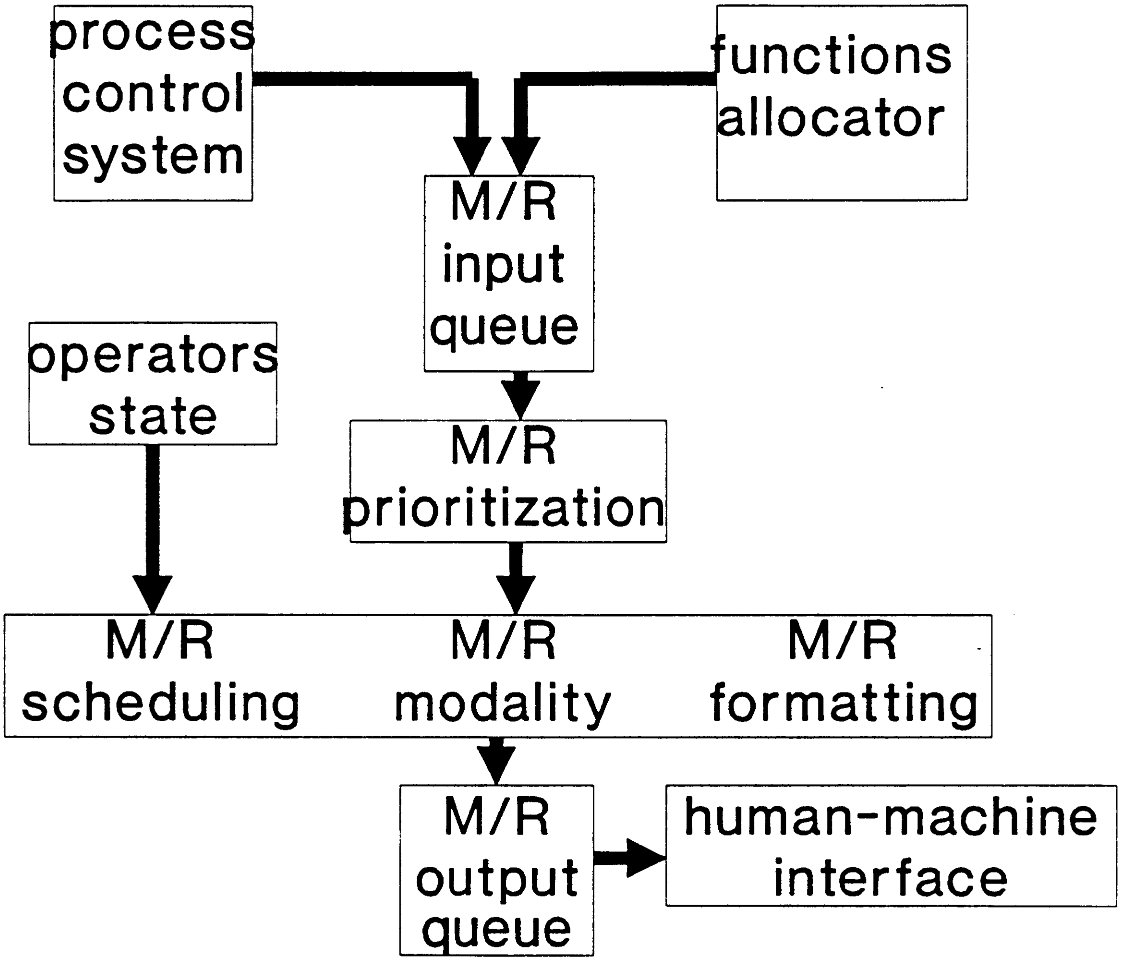

Fig.3 - Interface Manager

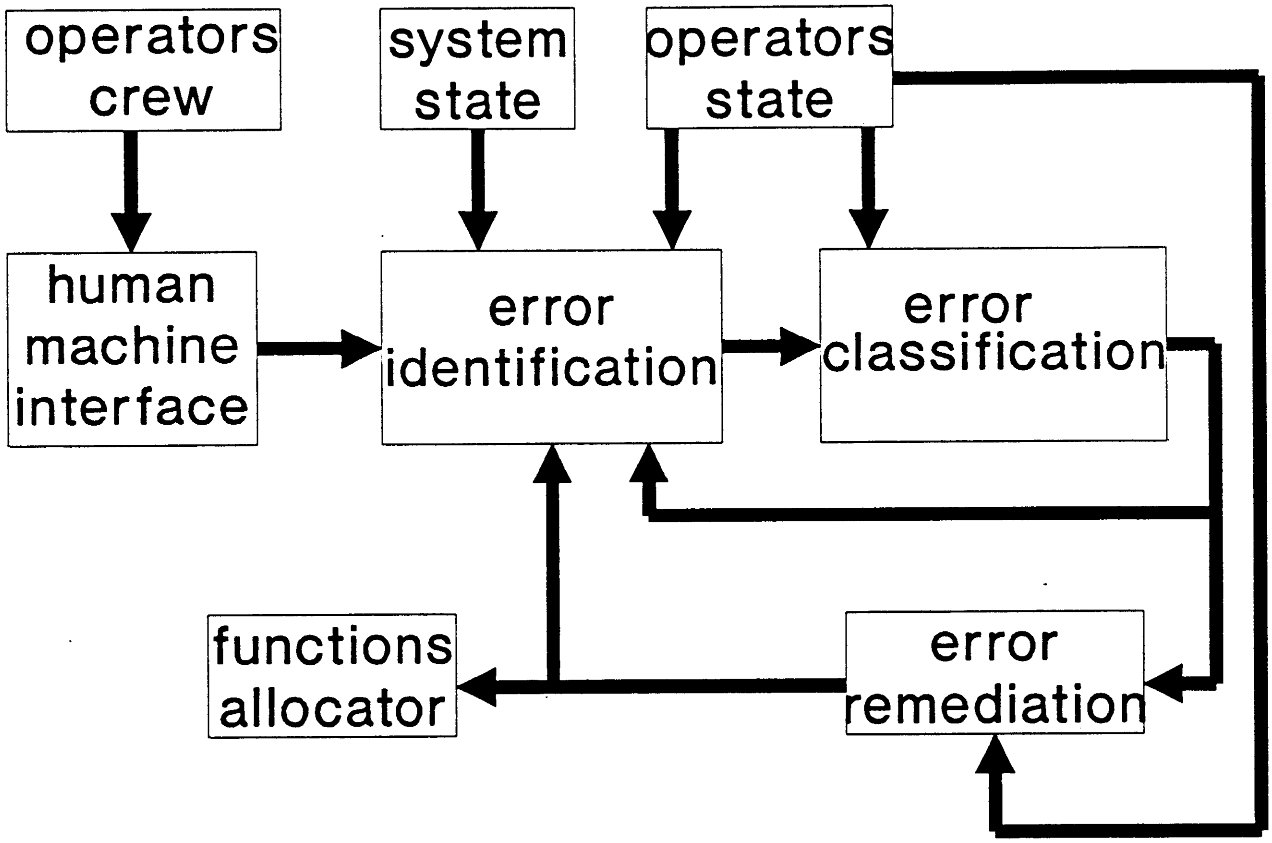

Fig. 4 - Error Monitor

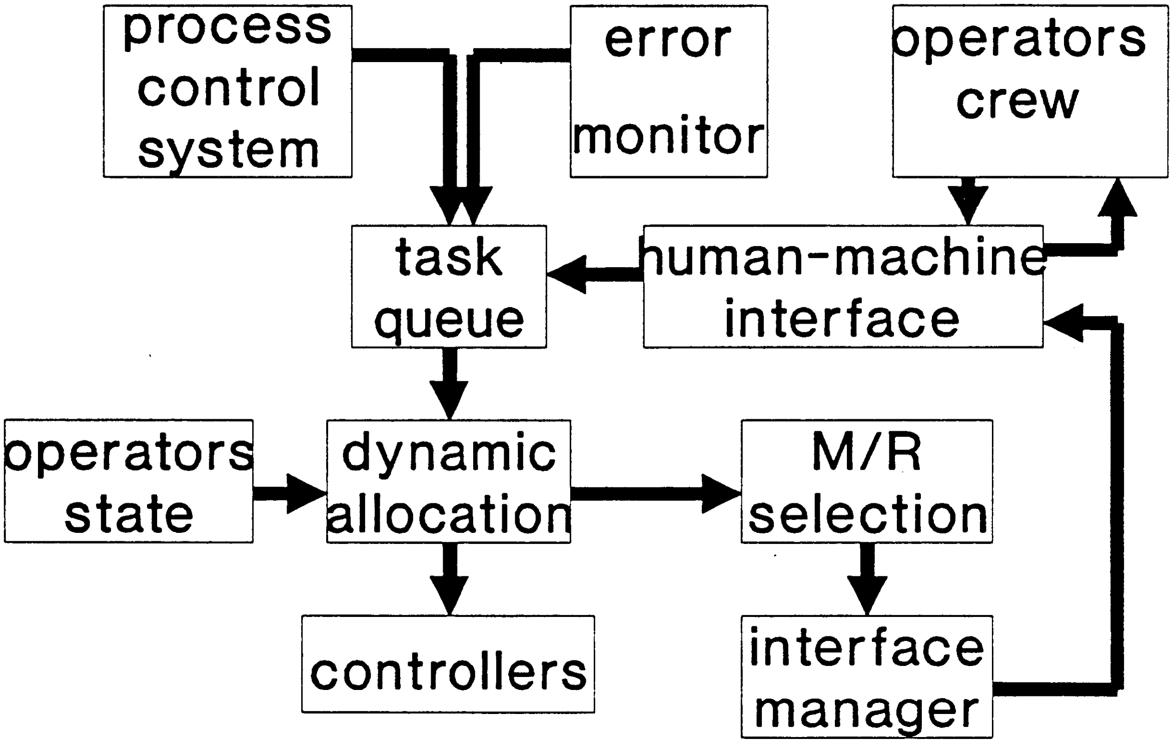

Fig. 5 - Functions Allocator

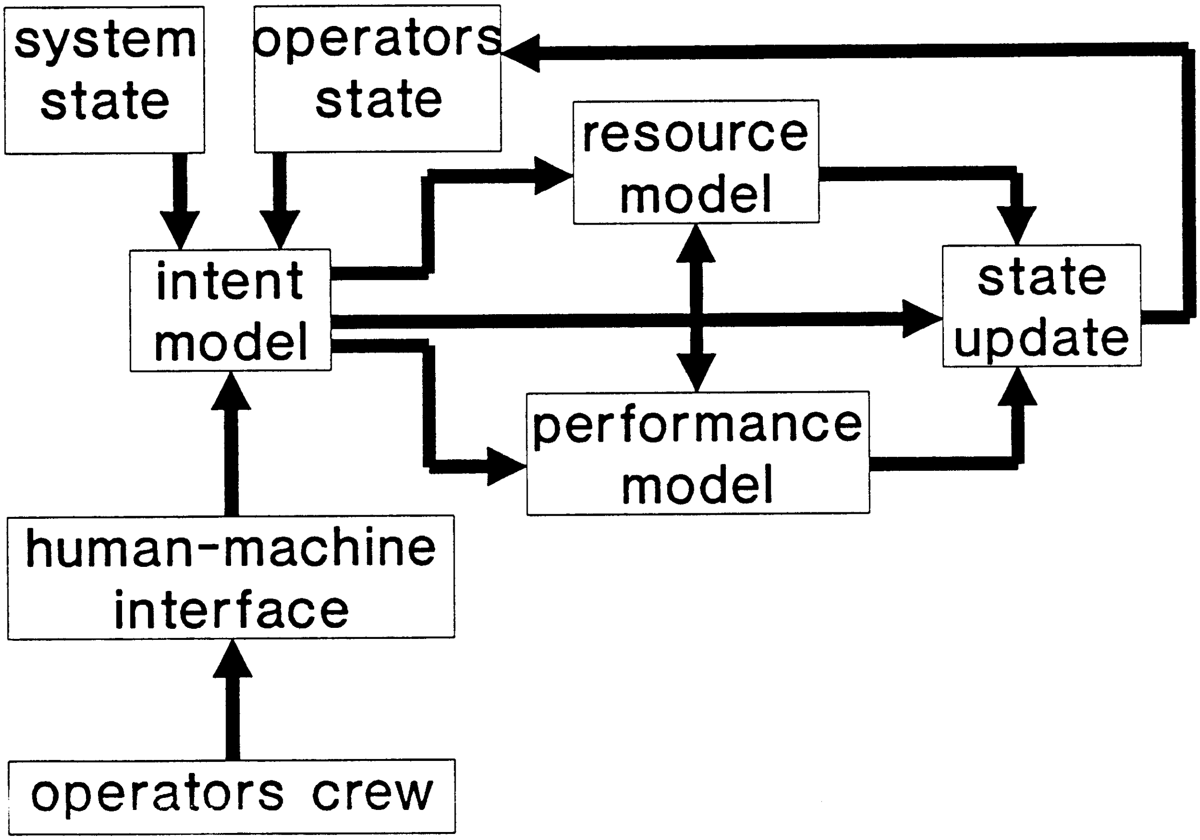

Fig.6 - Operators Cognitive Model

system state

dynamic state
modes and failures status of subsystems
information on current and upcoming
operational phases and applicable procedures

operators state

activities (according to the intentions)
awareness (of tasks requirements)
intentions (goals and plans)
resources (attention allocation)
performance (errors mechanisms)

Table 1 - System and Operators States

FUZZY COGNITIVE MAPS(FCMs) FOR DIAGNOSIS

A FCM is a neural network composed by fields of neurons:

1) input field F_X containing n neurons, and
2) output field F_Y containing p neurons.

The neural system samples or "experience" m vector associations during m time intervals $(\mathbf{X}_k,\mathbf{Y}_k)$. These associations constitute a function $f:R^n\text{->}R^p$. The overall neural network behaves as an adaptive filter (Kosko, 1992). The vector components x_i and y_i are activation time functions of the ith neuron in F_X and the jth neuron in F_Y. They are governed by first-order differential equations, that are stochastic in principle:

$$\frac{\delta\vec{X}}{\delta t}=\vec{g}(F_X,F_Y)\ ;\ \frac{\delta\vec{Y}}{\delta t}=\vec{h}(F_X,F_Y)$$

In fuzzy neural networks, the function f maps fuzzy sets into fuzzy sets(Fuzzy Association Memory):

$f\ :\ I^nXI^p\ ,\ I^n=[0,1]^n\ ,\ I^p=[0,1]^p$

$\mathbf{X}(t)=\{x_1(t),\ldots,x_n(t)\}\ ,\ \mathbf{Y}(t)=\{y_1(t),\ldots,y_n(t)\}$

where **X** and **Y** are multivaluated set or fuzzy set, defined by the membership functions m_A and m_B:

$m_A\colon X\text{ -> }[0,1]^n \qquad m_B\colon Y\text{ -> }[0,1]^p$

The neurons are activated by signal functions:

$\mathbf{S}(\mathbf{X}(t))=(S_1^X(x_1(t),\ldots,S_n^X(x_n(t)))$

$\mathbf{S}(\mathbf{Y}(t))=(S_1^Y(y_1(t),\ldots,S_p^Y(y_n(t)))$

In the diagnosis with causal relationships between neurons, the threshold signal function is more adequate:

$$S(x^{k+1})=\begin{cases}1 & \text{if}\quad x^{k+1}>x^k\\ 0 & \text{if}\quad x^{k+1}=x^k\\ -1 & \text{if}\quad x^{k+1}<x^k\end{cases}$$

where k denotes the time interval.

Each neuron is linked to another neuron through synapses. These synapses form two connection matrices:

$N : F_X \rightarrow F_Y$ forward projection

$M : F_Y \rightarrow F_X$ backward projection

If F_X and F_Y have the same topological structures, then:

$M = N^T$ and $N = M^T$

therefore the networks are bidirectional or BAM(Bidirectional Associative Memory).

In the additive activation models the differential equations become:

$$\dot{x}_i = -A_i x_i + \sum_{j=1}^{p} S_j(y_j)\, n_{ij} + I_i$$

n