A Minimum Attention Control Center
for
Nuclear Power Plants

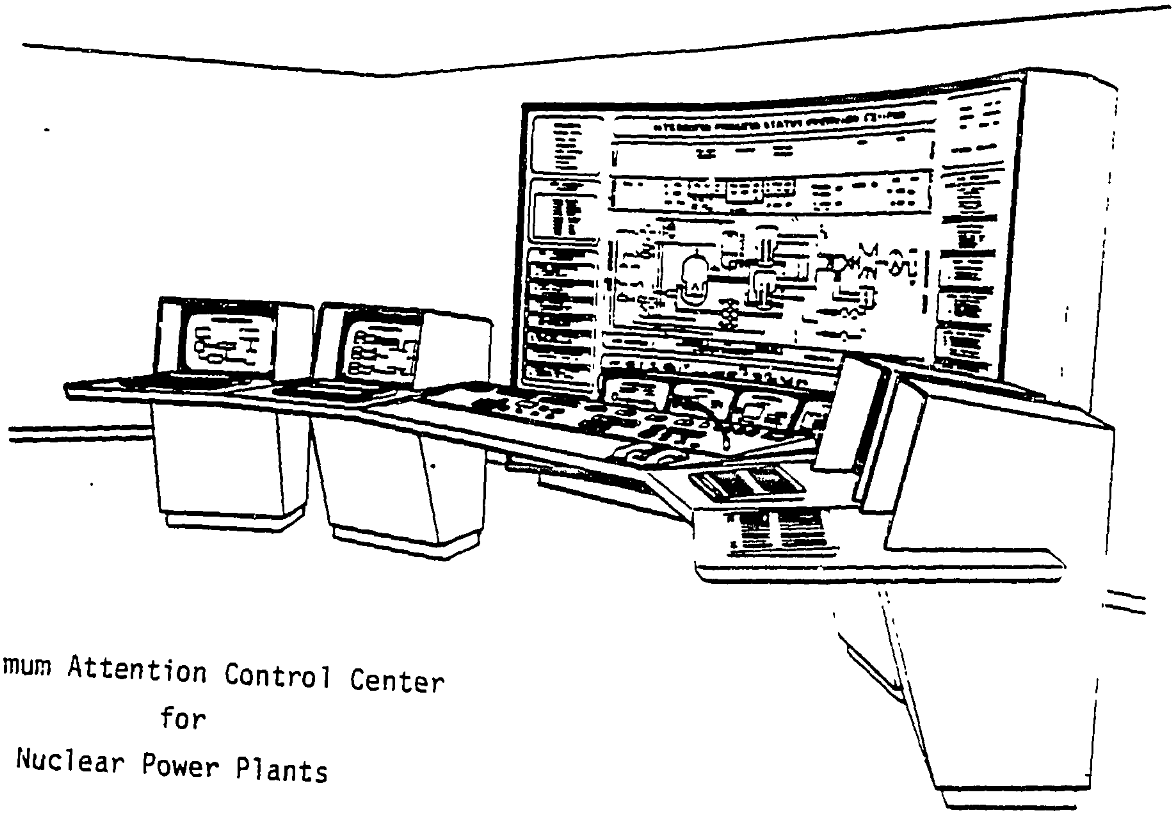
by

C. H. Meijer
Combustion Engineering, Inc.
Windsor, Connecticut, USA

Abstract

Control Centers for Nuclear Power Plants have characteristically been designed for maximum attention by the operating staffs of these plants. Consequently, the monitoring, control and diagnostics oriented cognitive activities by these staffs, were mostly "data-driven" in nature.

This paper addresses a control center concept, under development by Combustion Engineering, that promotes a more "information-driven" cognitive interaction process between the operator and the plant. The more "intelligent" and therefore less attentive nature of such interactive process utilizes computer implemented cognitive engineered algorithms. The underlying structure of these algorithms is based upon the Critical Function/Success Path monitoring principle. The paper highlights a typical implementation of the minimum attention concept for the handling of unfamiliar safety related events.



A Minimum Attention Control Center for Nuclear Power Plants

by

C. H. Meijer
Combustion Engineering, Inc.
Windsor, Connecticut, USA

Presented at the IAEA Specialists' Meeting on the use of Digital Computing Devices in Systems Important to Safety, Centre D'Etudes Nucleaires de Saclay, 28, 29, November, 1984.

Document No.: IPD-84-153

Abstract

Control Centers for Nuclear Power Plants have characteristically been designed for maximum attention by the operating staffs of these plants. Consequently, the monitoring, control and diagnostics oriented cognitive activities by these staffs, were mostly data-driven in nature.

This paper addresses a control center concept, under development by Combustion Engineering, that promotes a more knowledge-driven cognitive interaction process between the operator and the plant. The more "intelligent" and therefore less attentive nature of such interactive process utilizes computer implemented cognitive engineered algorithms. The underlying structure of these algorithms is based upon the Critical Function/Success Path monitoring principle. The paper highlights a typical implementation of the minimum attention concept for the handling of unfamiliar safety related events.

LEGAL NOTICE

This document was prepared as an account of work performed by Combustion Engineering, Inc. Neither Combustion Engineering nor any person acting on its behalf:

A. Makes any warranty or representation, express or implied including the warrenties of fitness for a particular purpose or mechantability, with respect to the accuracy, completeness or usefulness of the information contained in this document, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method or process disclosed in this report.

A Minimum Attention Control Center
for
Nuclear Power Plants

by

C. H. Meijer
Combustion Engineering, Inc.
Windsor, Connecticut, USA

INTRODUCTION AND SUMMARY

The control centers of conventional PWRs and BWRs in the US, have traditionally been designed for mostly manual operation of these plants. This manual operation was supported by automated plant safety shutdown systems, and by control rooms characterized by multiple control panels utilizing an extravagant mixture of indicators, recorders, annunciators, hand-operated controls, etc. To maintain control of such plants, the operating staffs must continuously perceive a multitude of plant symptoms, and process these in cognitive algorithms to obtain the knowledge needed for understanding of the status of the plant, and to take the necessary decisions for control actions, if so required. The cognitive algorithms utilized during this mostly "data-driven", maximum attention interactive process with the plant, included cognitive algorithms based on education, training and experience, and represented the cognitive elements normally associated with human intelligence such as reasoning, and the acquisition and representation of knowledge.

Considering the growing complexity of nuclear power plants in general, and the resulting complexity of the human cognitive process to monitor, control and diagnose these plants, it seems not surprising that the nuclear community has sought for means to support this process. Initially this support included carefully documented procedures detailing every step from cold shutdown to full power operation, post-trip actions, procedures for emergency operations, refueling, maintenance, etc. Later, as the awareness of the human cognitive process increased and especially the psychological and the physiological effects on this process during adverse plant situations, additional support was provided in terms of better human engineering of the control panels[1,2], and systems that provided information, e.g. the recent SPDS developments[3]. As a result, the cognitive process of an operating staff became more "information-driven" in nature, in many cases promoting a less complex and less attentive, and therefore more reliable cognitive process in itself.

Realizing that information implies in essence a random collection of data rather than an orderly synthesis of data into an awareness of understanding or knowledge, Combustion Engineering (C-E) embarked subsequently on the development of "intelligent" information systems. The Critical Function Monitoring System (CFMS)[4], described in some detail in this paper, is such a system. The CFMS promotes a more "knowledge-driven" cognitive process by means of sophisticated computer-based knowledge-yielding cognitive algorithms which closely emulate those of an operating staff when performing a task during a specific plant situation.

Further realizing that a higher degree of knowledge-driven cognizance is closely related to a lesser degree of attention and consequently higher human reliability, CE started the development of a minimum attention control center for nuclear power plants during the early 1980's. The development is based on the hypothesis, that to maintain any technological environment in a safe and efficient state, the human interaction with that environment can be accomplished best, if the environment is being viewed as an intelligent entity interacting with the human by itself. The resulting mutual interaction, within the boundaries of the environment, can be considered natural, and rational, if the basic criteria for the interaction between two intelligent agents can be adhered to (see Table 1).

TABLE 1

Some Basic Criteria for a Natural (and rational) Interaction (or communication) between Intelligent Agents

- o Must have a common purpose or goal (easier interpretation of messages).
- o Must have a shared understanding (or models) of the domain and the interactive agents themselves.
- o Must utilize an underlying cognitive concept or structure.
- o Must allow for expectation-driven processing of common knowledge (understanding of incomplete messages).
- o Must allow for predictive analysis of anticipated actions before execution.
- o Must be able to explain conclusions and actions.
- o Must be conducted using a common language.
- o Must allow for gaining of new knowledge (learning).

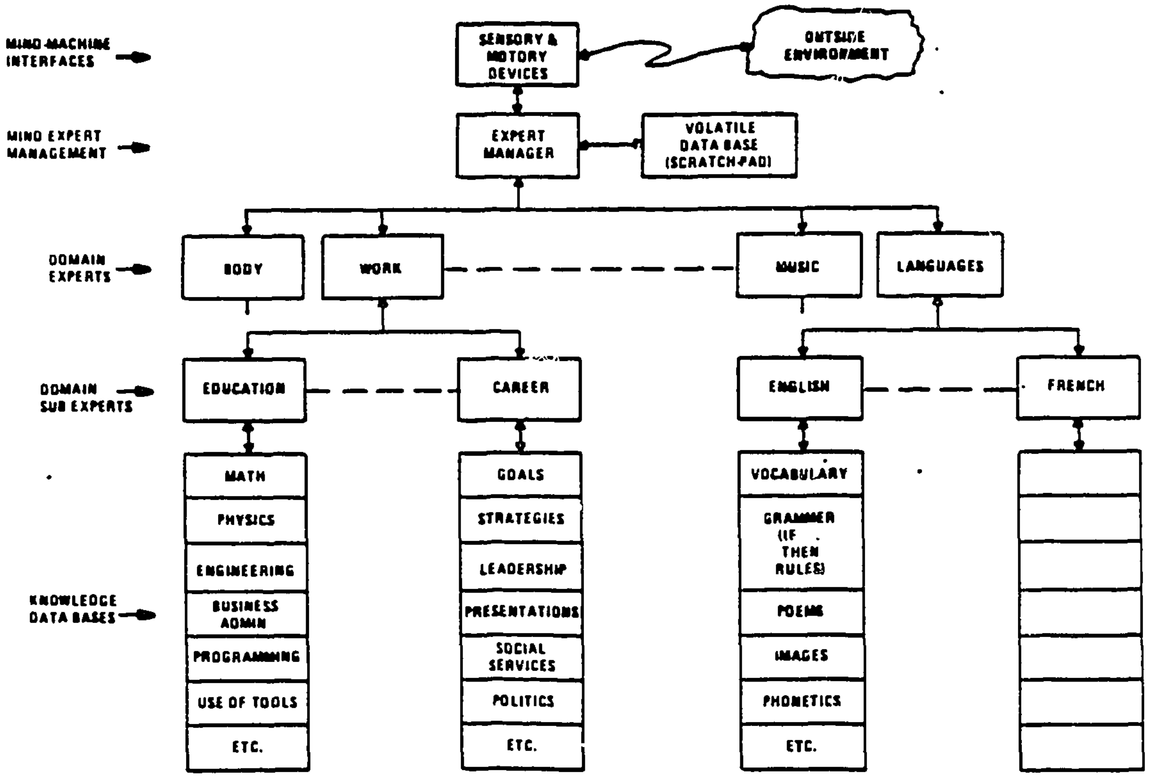


Figure 1. The Human Expert System?

As can be observed from Table 1, the criteria identified largely coincide with those groundrules generally adopted by those practicing the development of artificial intelligence (AI) based natural language processing (NLP) techniques[5].

In addition to the criteria listed in Table 1, an interaction process between two intelligent agents might further be improved if the framework and utilization of the knowledge-base of each of the agents is (or appears) simular. Several AI practitioners believe that the human knowledge base (expert system) is structured like a hierarchical society of experts[6] cooperating with each other, vertically as well as horizontally within the hierarchy, like in an ideal corporation (see Figure 1).

Further, due to the natural limitations of the human data processing capabilities[7], humans have a tendency to think in terms of multiple knowledge-based hierarchies, with the maximum number of levels within each of the hierarchies probably being not more than seven plus or minus two, or three to four levels for most of us.

With a limited number of levels within each hierarchy and the human mind rarely accessing more than one hierarchy at a given time, a structure of the knowledge base of a technological intelligent agent, that is or appears to be simular to that of the human interacting with this agent, seems the appropriate approach. As will be seen from the further text in this paper, the knowledge base of the minimum attention control center is largely constructed like the human expert system. Subsequently, the representative medium of this knowledge base is through a visualization of this knowledge base, in terms of a selectable multi-hierarchy color graphics display system with a maximum of four display levels within each of the hierarchies.

Considering some of the criteria identified in Table 1, the common goal is to maintain a safe and efficient operation of the nuclear power plant. The underlying cognitive concept or structure chosen, is the Critical Function concept, which has been described in some detail in this paper. This concept is also described in the context of its effect on the emergency operating procedures in US nuclear plants. The shared understanding, knowledge, or model of the domain, is in this case a nuclear plant visualized by a permanent integrated process status overview display,supported by a three-level color graphics multi-hierarchy display system. Each display hierarchy embedded in the display system can be selected for display, one at the time, on the three visual display units (VDU). Each display hierarchy contains the knowledge base related to only one specific aspect of the overall plant. For example, individual display hierarchies can be selected for a post-trip accident monitoring situation, or a load-following monitoring and control condition, or a signal data validation requirement, or a plant protection system monitoring requirement, etc. The integrated process status overview display, although dynamic in nature, remains permanently displayed, to assure that the common model of the knowledge base is not removed from the interaction process. This seems good human engineering, because during human communication a common visualized model of the knowledge of a domain, often greatly enhances such communication. The overview display and supporting display hierarchies are driven by knowledge-based algorithms which directly process the (dynamic) data content of the plant signal data-base. The algorithms of individual display hierarchies also contain the necessary elements for expectation-driven processing, predictive analysis and explanatory functions. The paper concludes with a brief description of the intelligent workstation of the minimum attention control center itself.

THE CRITICAL FUNCTION CONCEPT

As discussed above, a natural and rational interaction between intelligent agents must have an underlying cognitive concept or structure. The concept chosen for CE's minimum attention control center is the Critical Function concept.

Although addressed in detail elsewhere,[8] it currently becomes more clear that in any environment where perturbed behavior of man or machine can lead to undesirable situations, the concept of "Critical Functions" may be a good basis for control of that environment. In this context, a critical function is generally considered as a function that <u>must</u> be accomplished by means of a group of actions (or successpaths) undertaken to reach a chosen goal or target. If the critical function is not accomplished, reaching of the goal or target will be highly unlikely.

In a technological environment such as a nuclear power plant, a critical function can be Safety, Availability, Operation, Efficiency, Maintenance, Security, Radiological, etc., related.

Some self-explanatory examples of limited sets of critical functions are given in Tables 2 and 3 for an educational and an aircraft type environment respectively.

TABLE 2

SOME TYPICAL CRITICAL FUNCTIONS FOR HOW TO GET A DEGREE

NO.	CRITICAL FUNCTION	PURPOSE/SUCCESSPATH
1	Finance Control	Review Financial Situation and Secure Fees for Courses, Books, etc.
2	Time Control	Review Personal Time Schedules and Select Time Windows for School and Study
3	Transportation Control	Secure Transportation by Car, Bus, Train, etc., into the Direction of School
4	Knowledge Control	Select Right School, Courses and Materials, Filter Out Unrelated or Superfluous Information, etc.
5	Cognition Control	Disciuline Your Cognitive Process to the Professor's Standards
6	Health Control	Avoid Physiological and Psychological Deterrents
7	Behavior Control	Be Nice to Professor and Others

As can be concluded from Table 2, if one of the critical functions shown is not met, it is highly unlikely that the goal of obtaining a degree will ever be reached.

The first five critical safety functions in Table 3 must be accomplished to maintain the safety of the aircraft and could be labelled as "anti-crash" critical functions. Numbers 6 and 7 are the critical functions mainly to protect the health and safety of the crew and passengers, although these functions could indirectly also be considered as anti-crash functions.

The critical functions for a Nuclear Power Plant in terms of its operational safety have been highlighted in Table 4.

76

Table 3

SOME TYPICAL CRITICAL FUNCTIONS TO KEEP AN AIRCRAFT FLYING

NO.	CRITICAL FUNCTION	PURPOSE/SUCCESSPATH
1	Lift Control	Keep the Aircraft Flying by Control of Airspeed, Airfoil, Attitude etc.
2	Stress Control	Maintain Integrity of Airframe to Keep Aircraft in Flyable Condition by Limiting G-Loads
3	Power Control	Assure and Control Fuel Supply to Engine to Maintain Required RPM
4	Flightpath Control	Maintain Aircraft on Controllable Flightpath Through Coordinated Positioning of Control Surfaces Such as Rudder, Ailerons, Elevators etc.
5	Altitude Control	Keep Aircraft From Unplanned Ground Contact by Airspeed or Power Control
6	Cabin Environmental Control	Prevent Exposure of Crew and Passengers to Unhealthy Environments by Maintaining Cabin Isolation and Appropriate Temperature, Pressure and Oxygen Control
7	Aircraft Environmental Control	Avoid Adverse Flying Conditions Such as in Thunderstorms, Turbulences etc by Stick/Throttle Control to Limit Stress on Aircraft and Maintain Welfare of Crew and Passengers

Table 4

TYPICAL CRITICAL SAFETY FUNCTIONS FOR A NUCLEAR POWER PLANT

NO.	CRITICAL FUNCTION	PURPOSE/SUCCESSPATH
1	Reactivity Control	Limit Core Heat Production to What is Required
2	Reactor Coolant System Inventory Control	Maintain a Coolant Heat Transfer Medium Around Core
3	Reactor Coolant System Pressure Control	Maintain the Appropriate Heat Transfer Properties of the Coolant
4	Reactor Core Heat Removal	Transfer Heat from Core to a Coolant
5	Reactor Coolant System Heat Removal	Transfer Heat from the Core Coolant to Heat Sink
6	Containment Pressure/Temperature Control	Maintain Containment in Proper State to Prevent Damage and Radiation Releases
7	Containment Isolation	Maintain Radioactive Material Within the Containment

The first five critical safety functions as shown in Table 4 could be regarded as anti-core melt critical functions, numbers 6 and 7 as the critical functions to protect the health and safety of the public.

As can be observed from Table 4, the accomplishment of each critical function must be performed at all times by automatic or by human action(s) or a combinations of both, to maintain a chosen target state of the plant. This is of particular importance during the occurrence of an unfamiliar or adverse event as correctly identified by Fortney[9], Goodstein and Rasmussen[10], and others. The actions to be taken to acccomplish the Critical Functions are commonly identified as Primary and Alternate Successpaths.

A simple representation of human cognitive process utilizing the concept of Critical Functions is shown in figure 2.

Most human cognitive processes, although often performed unconsciously, seem like that shown in Figure 2, and being part of a normal rational behavior. If the goal is to make a bicycle trip, it is obviously irrational to pump up the tires of the automobile if the bicycle tires need pumping up, correct bicycle tire pressure being one of the critical functions to be accomplished for any bicycle trip. It is therefore also quite normal to assume that an operator in a nuclear power plant thinks along the same process as shown in Figure 2, to solve any situation, normal or abnormal. A generic type cognitive process for such operator can then be illustrated as in Figure 3.

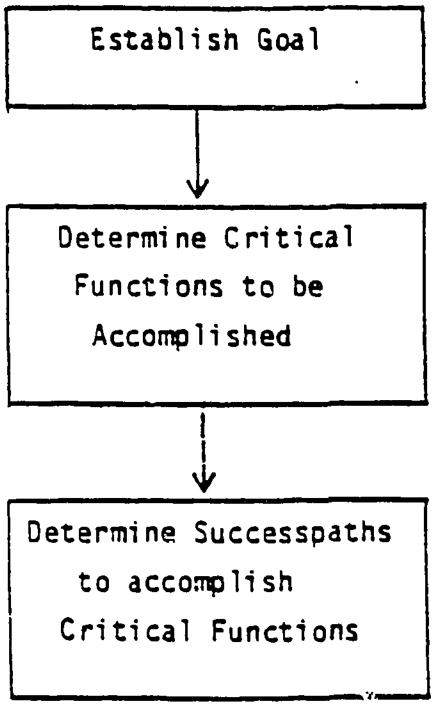

Establish Goal
Determine Critical Functions to be Accomplished
Determine Successpaths to accomplish Critical Functions

Figure 2
Basic Human Cognitive Process to reach an established goal utilizing the concept of Critical Functions.

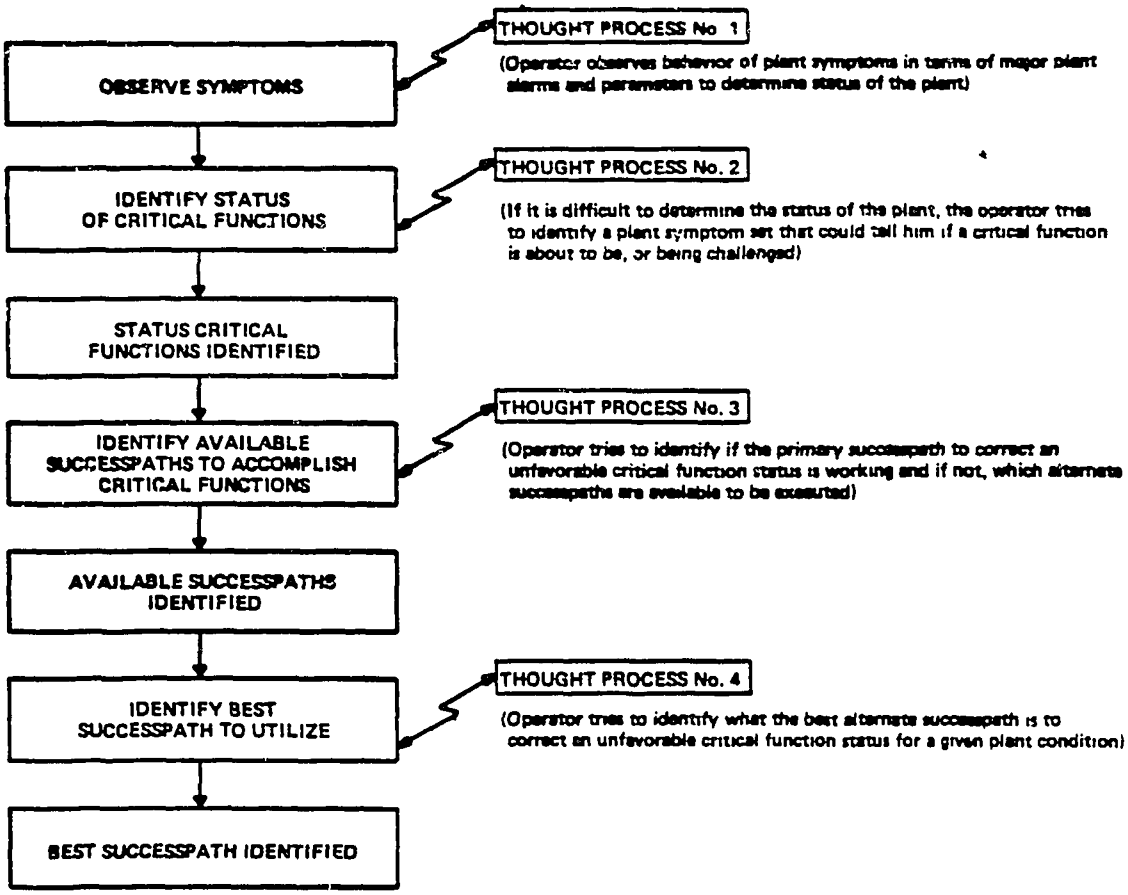

OBSERVE SYMPTOMS
IDENTIFY STATUS OF CRITICAL FUNCTIONS
STATUS CRITICAL FUNCTIONS IDENTIFIED
IDENTIFY AVAILABLE SUCCESSPATHS TO ACCOMPLISH CRITICAL FUNCTIONS
AVAILABLE SUCCESSPATHS IDENTIFIED
IDENTIFY BEST SUCCESSPATH TO UTILIZE
BEST SUCCESSPATH IDENTIFIED
THOUGHT PROCESS No 1
(Operator observes behavior of plant symptoms in terms of major plant alarms and parameters to determine status of the plant)
THOUGHT PROCESS No. 2
(If it is difficult to determine the status of the plant, the operator tries to identify a plant symptom set that could tell him if a critical function is about to be, or being challenged)
THOUGHT PROCESS No. 3
(Operator tries to identify if the primary successpath to correct an unfavorable critical function status is working and if not, which alternate successpaths are available to be executed)
THOUGHT PROCESS No. 4
(Operator tries to identify what the best alternate successpath is to correct an unfavorable critical function status for a given plant condition)

Figure 3: TYPICAL COGNITIVE PROCESS OF NUCLEAR POWER PLANT OPERATOR UTILIZING CONCEPT OF CRITICAL FUNCTIONS

Whatever the established goal is, changing plant mode, tackling an event, responding to a security violation, etc., it seems that, although also often unconsciously, an operator thinks like all of us, in terms of accomplishing a selected number of critical functions by carrying out the best selected successpath(s) to reach his goal. As a matter of fact, the rationality of human interaction could in many cases substantially benefit from an underlying common structure or concept, such as the critical function concept. And if this is true for humans, then it seems also true for those cases where a human must intereact with a machine or a process, such as a nuclear power plant.

One could therefore conclude, that a better "cognitive coupling" between interacting intelligent agents can be obtained if the elements by themselves are critical function based. In the case of a nuclear power plant, Combustion Engineering decided to develop the Emergency Procedure Guidelines (EPGs) and the Critical Function Monitoring System (CFMS) as critical function based operational tools to improve the interaction between the operator and his plant. The EPGs, developed in cooperation with the CE PWR Owners group, provide the operator with a post-trip functionally oriented recovery approach, in addition to the more event oriented or optimal recovery approach. The concept of the EPGs is described in the next chapter.

EMERGENCY PROCEDURE GUIDELINES

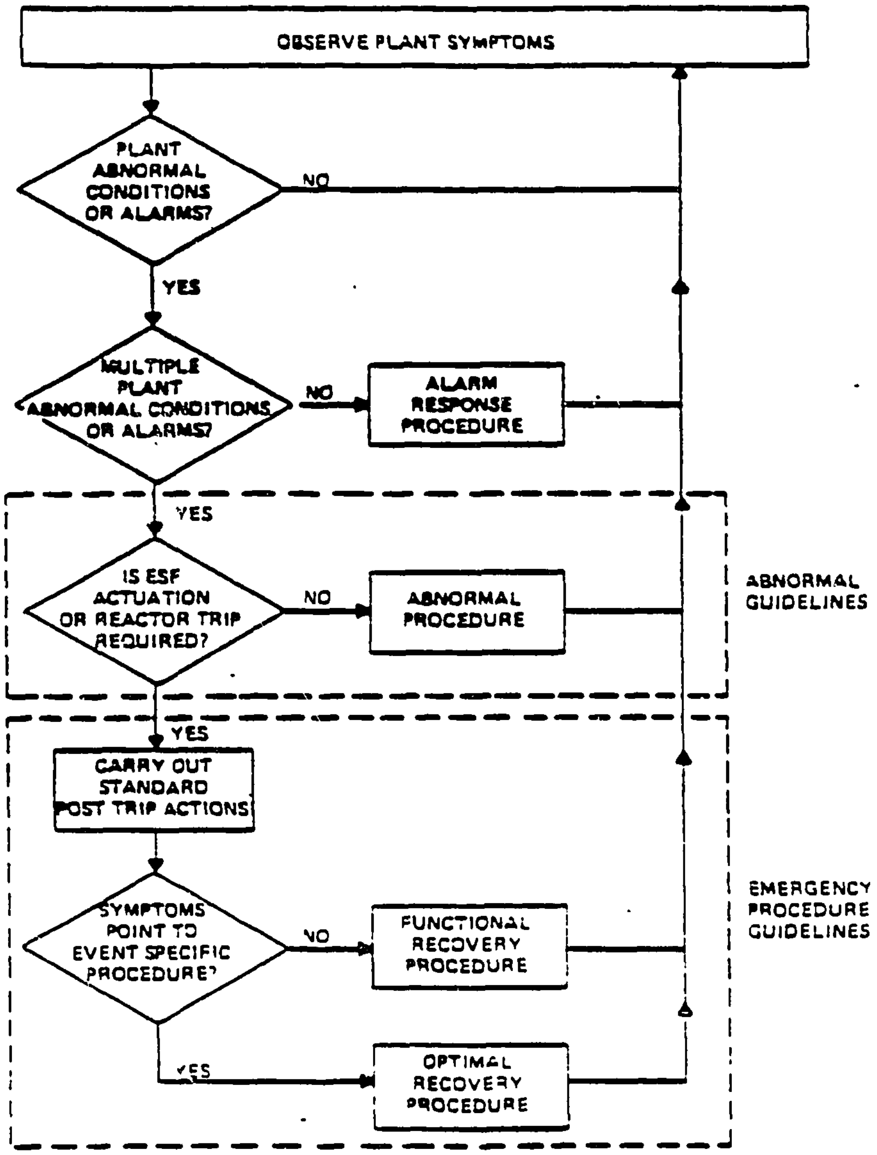
Event oriented automated response or successpaths are identified in all nuclear plant Safety Analysis Reports (SAR). In addition to the primary automated successpaths, the C-E Standard SAR (CESSAR) identifies an alternate automatic or semi-automatic successpath for all major analyzed events, to acccommodate a single failure in the primary successpath, if this should occur. If anything would go wrong in the sequence of actions during an event other than predicted, the operators of the plant, being well trained in event-oriented emergency procedures, would then provide the necessary additional actions to mitigate the consequences of the event.

Recent occurrences in the nuclear field however, have indicated that a strictly event-oriented response, (especially to rare, unexpected or unfamiliar events, e.g. when multiple failures would occur in one or more successpaths) might be undesired to prevent or limit the extent or consequences of the event. It's true, that given enough time the plant operators of any plant can solve any problem in any way. After all, operators are well qualified professionals. But if a plant's integrity is a function of how timely and how well a response is provided to an occurring event, it might be worthwhile to evaluate if there are ways that can assist the operator during those situations where he might have problems of "putting it all together" when time and quality of response are of the essence.

Combustion Engineering decided therefore first of all, to look at the basic cognitive process of an operator in responding to an emergency situation, and at his main tool that he uses during his response, the plant emergency procedures. Becoming aware of the fact that the emergency procedures did not address situations other than the events addressed by the procedures, the previously discussed concept of the Critical Functions was introduced to the procedures. The underlying reasoning here was, that if during the occurrence of an event, the operator would fail to recognize the event, and consequently would be unable to consult the appropriate emergency procedure, he would first attempt to bring and maintain the plant in a stable and safe condition, utilizing the Critical Function concept, before doing anything else. The resulting concept of the cognitive process of an operator during an emergency situation that emerged is illustrated in Figure 4.

Figure 4

OPERATOR'S COGNITIVE PROCESS AND SEQUENCE OF DECISIONS FOR OFF-NORMAL OPERATIONS



OBSERVE PLANT SYMPTOMS
PLANT ABNORMAL CONDITIONS OR ALARMS?
NO
YES
MULTIPLE PLANT ABNORMAL CONDITIONS OR ALARMS?
NO
ALARM RESPONSE PROCEDURE
YES
IS ESF ACTUATION OR REACTOR TRIP REQUIRED?
NO
ABNORMAL PROCEDURE
ABNORMAL GUIDELINES
YES
CARRY OUT STANDARD POST TRIP ACTIONS
SYMPTOMS POINT TO EVENT SPECIFIC PROCEDURE?
NO
FUNCTIONAL RECOVERY PROCEDURE
YES
OPTIMAL RECOVERY PROCEDURE
EMERGENCY PROCEDURE GUIDELINES

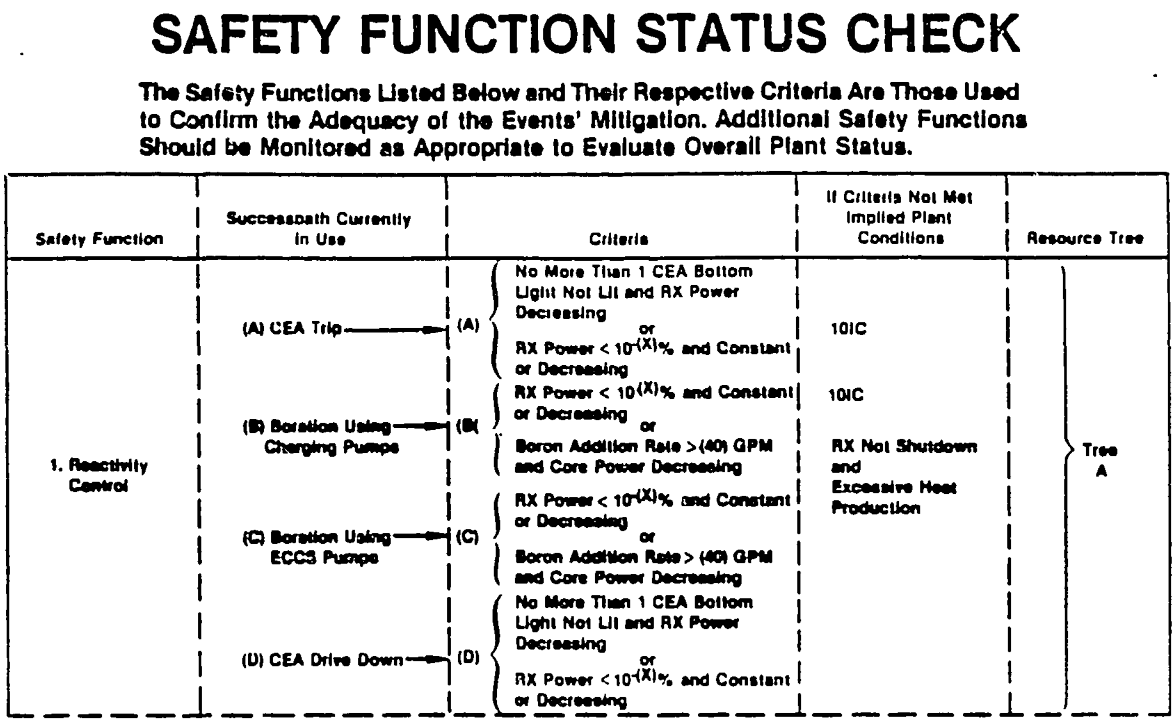
Utilizing this concept, an intense three-and-one-half year of effort was undertaken in cooperation with, and under sponsorship of the CE PWR Owner's Group, to prepare a set of Emergency Procedures Guidelines[11] which addressed "optimal recovery" (event-oriented) as well as "functional recovery" response to emergency situations.

As can be observed from Figure 4, the operator's cognitive process goes through several stages in order to relate a plant happening with the appropriate plant procedures. If the operator is unable to relate a specific symptom set to a specific plant procedure, the operator must revert to a functional recovery procedure which is based on the Critical Safety Function concept. The functional recovery procedure includes the identification of the status of the Critical Safety Functions, and the accomplishment of these functions if they should be challenged or in jeopardy. To accomplish the functions, the operator must evaluate the available successpaths and select the most appropriate one for the purpose.

To assist the operator's cognitive process when performing a functional recovery procedure, the C-E Emergency Procedure Guidelines promote the use of a check list to determine the status of each Critical Safety Function. Going down the list, the operator can check for each critical function the criteria associated with the primary successpath in use for that function. Table 5 shows the Safety Function Status Check for the Reactivity Control critical safety function. If a function does not meet the criteria, then the operator subsequently consults the appropriate "Resource Assessment Tree" (listed in the right hand column of Table 5). Figure 5 illustrates a part of the Resource Assessment Tree A for the Reactivity Control Critical Safety Function. The tree pictorially displays all the generic successpaths that can accomplish this particular Critical Safety Function. The EPGs contain pictorial presentations of the Resource Assessment Trees for the accomplishment of each critical safety function.

Each successpath further shows the major components and their minimum operating requirements (e.g., minimum usable tank level, electical power available, etc.) for that path, assisting the operator to choose an alternate successpath if necessary. The operator will normally work from left to right on the tree implementing or attempting to implement each successpath until the criteria are met. The path with the highest priority will be that path which is capable of meeting the success criteria (e.g., only the ECCS is capable of meeting some success criteria if a LOCA is in progress).

When the appropriate criteria of each of the safety functions are met, the plant is in a stable condition and the operator consults the Long Term Actions to assess what further action should be taken. Also at this time the operator might start paying attention to the cause of the event, potential restoration of the primary successpath if this proved to be a problem, etc.



SAFETY FUNCTION STATUS CHECK

The Safety Functions Listed Below and Their Respective Criteria Are Those Used to Confirm the Adequacy of the Events' Mitigation. Additional Safety Functions Should be Monitored as Appropriate to Evaluate Overall Plant Status.

Safety Function	Successpath Currently in Use	Criteria	If Criteria Not Met Implied Plant Conditions	Resource Tree
1. Reactivity Control	(A) CEA Trip	(A) No More Tlian 1 CEA Bottom Light Not Lit and RX Power Decreasing or RX Power < $10^{-(X)}$% and Constant or Decreasing	10IC	Tree A
	(B) Boration Using Charging Pumps	(B) RX Power < $10^{(X)}$% and Constant or Decreasing or Boron Addition Rate >(40) GPM and Core Power Decreasing	10IC RX Not Shutdown and Excessive Heat Production	
	(C) Boration Using ECCS Pumps	(C) RX Power < $10^{-(X)}$% and Constant or Decreasing or Boron Addition Rate > (40) GPM and Core Power Decreasing		
	(D) CEA Drive Down	(D) No More Tlian 1 CEA Bottom Light Not Lit and RX Power Decreasing or RX Power < $10^{-(X)}$% and Constant or Decreasing		

Table 5: EPG Safety Function Status Check list shown for Reactivity Control critical safety function.

It can readily be seen that to successfully achieve a stable plant condition during the occurrence of an adverse event, especially with a potentially simultaneous occurrence of multiple failures of succsspath components, a considerable mental activity is required from the operator. It is therefore no surprise that several attempts have been made by the nuclear industry to provide so-called diagnostic aids. Most of these aids, identified as Safety Parameter Display Systems (SPDSs) are intended to provide the operator with more integrated plant status information from which he can further perform his diagnostics to come up with the knowledge required to take action(s).

C-E, realizing that performing diagnostics is appropriate when one has the time but undesireable otherwise, made the decision to supplement the operator's cognitive process by implementation of this process in a computer. The result, the Critical Function Monitoring System (CFMS), provides essentially a computer implementation of the operator's cognitive process to determine the status of the critical functions. The system further provides guidance to the operator to identify the appropriate successpath to accomplish a critical function in jeopardy. The next chapter discusses the CFMS in some more detail.

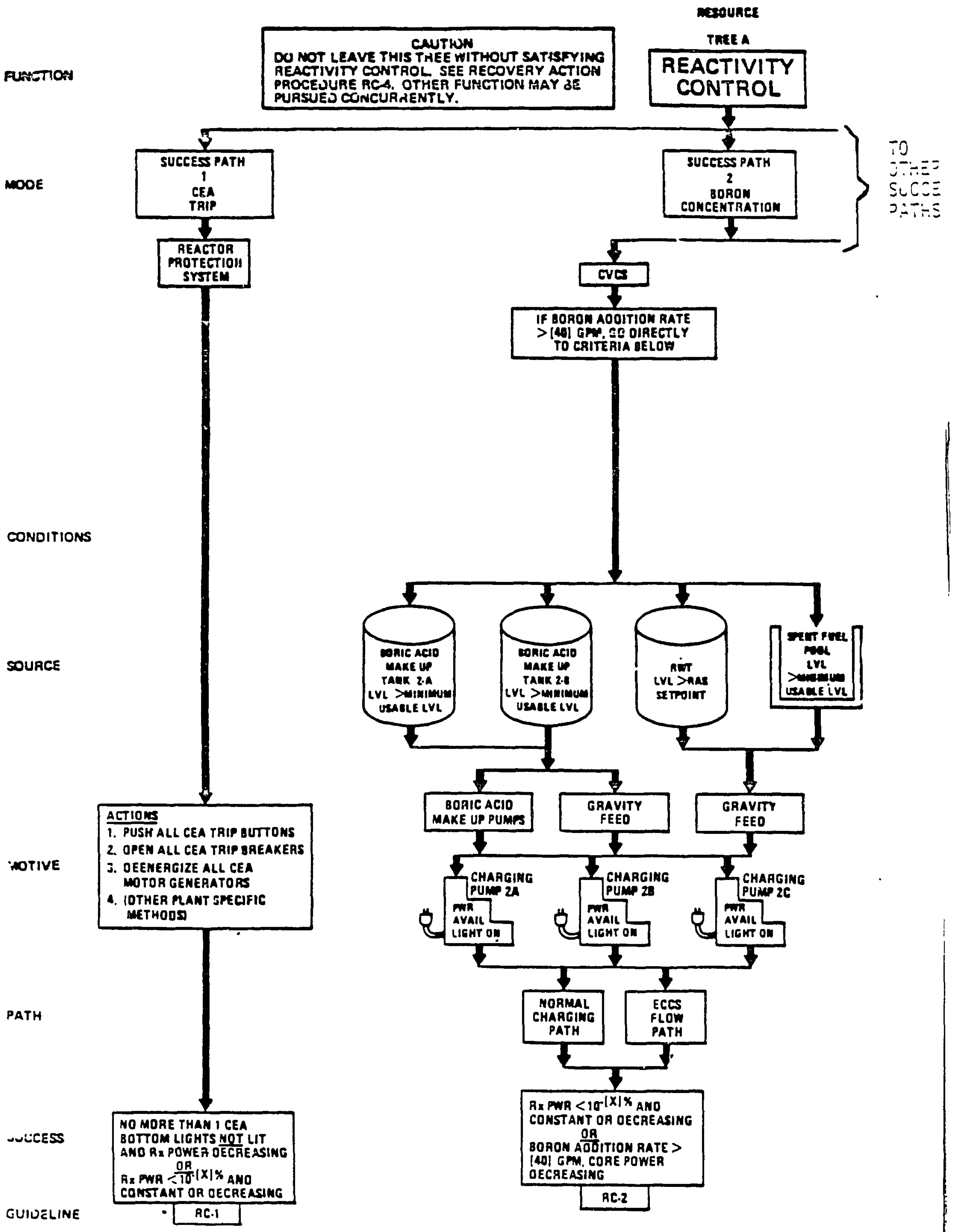

RESOURCE
TREE A
FUNCTION
CAUTION
DO NOT LEAVE THIS TREE WITHOUT SATISFYING REACTIVITY CONTROL. SEE RECOVERY ACTION PROCEDURE RC-4. OTHER FUNCTION MAY BE PURSUED CONCURRENTLY.
REACTIVITY CONTROL
MODE
SUCCESS PATH 1 CEA TRIP
SUCCESS PATH 2 BORON CONCENTRATION
TO OTHER SUCCESS PATHS
REACTOR PROTECTION SYSTEM
CVCS
IF BORON ADDITION RATE > [40] GPM, GO DIRECTLY TO CRITERIA BELOW
CONDITIONS
SOURCE
BORIC ACID MAKE UP TANK 2-A LVL >MINIMUM USABLE LVL
BORIC ACID MAKE UP TANK 2-B LVL >MINIMUM USABLE LVL
RWT LVL >RAS SETPOINT
SPENT FUEL POOL LVL >MINIMUM USABLE LVL
MOTIVE
ACTIONS
1. PUSH ALL CEA TRIP BUTTONS
2. OPEN ALL CEA TRIP BREAKERS
3. DEENERGIZE ALL CEA MOTOR GENERATORS
4. (OTHER PLANT SPECIFIC METHODS)
BORIC ACID MAKE UP PUMPS
GRAVITY FEED
GRAVITY FEED
CHARGING PUMP 2A
PWR AVAIL LIGHT ON
CHARGING PUMP 2B
PWR AVAIL LIGHT ON
CHARGING PUMP 2C
PWR AVAIL LIGHT ON
PATH
NORMAL CHARGING PATH
ECCS FLOW PATH
SUCCESS
NO MORE THAN 1 CEA BOTTOM LIGHTS NOT LIT AND Rx POWER DECREASING OR Rx PWR < 10^-[X]% AND CONSTANT OR DECREASING
Rx PWR < 10^-[X]% AND CONSTANT OR DECREASING OR BORON ADDITION RATE > [40] GPM, CORE POWER DECREASING
GUIDELINE
RC-1
RC-2

Figure 5: Part of Resource Assessment Tree for the Reactivity Control Critical Safety Function[11].

84.

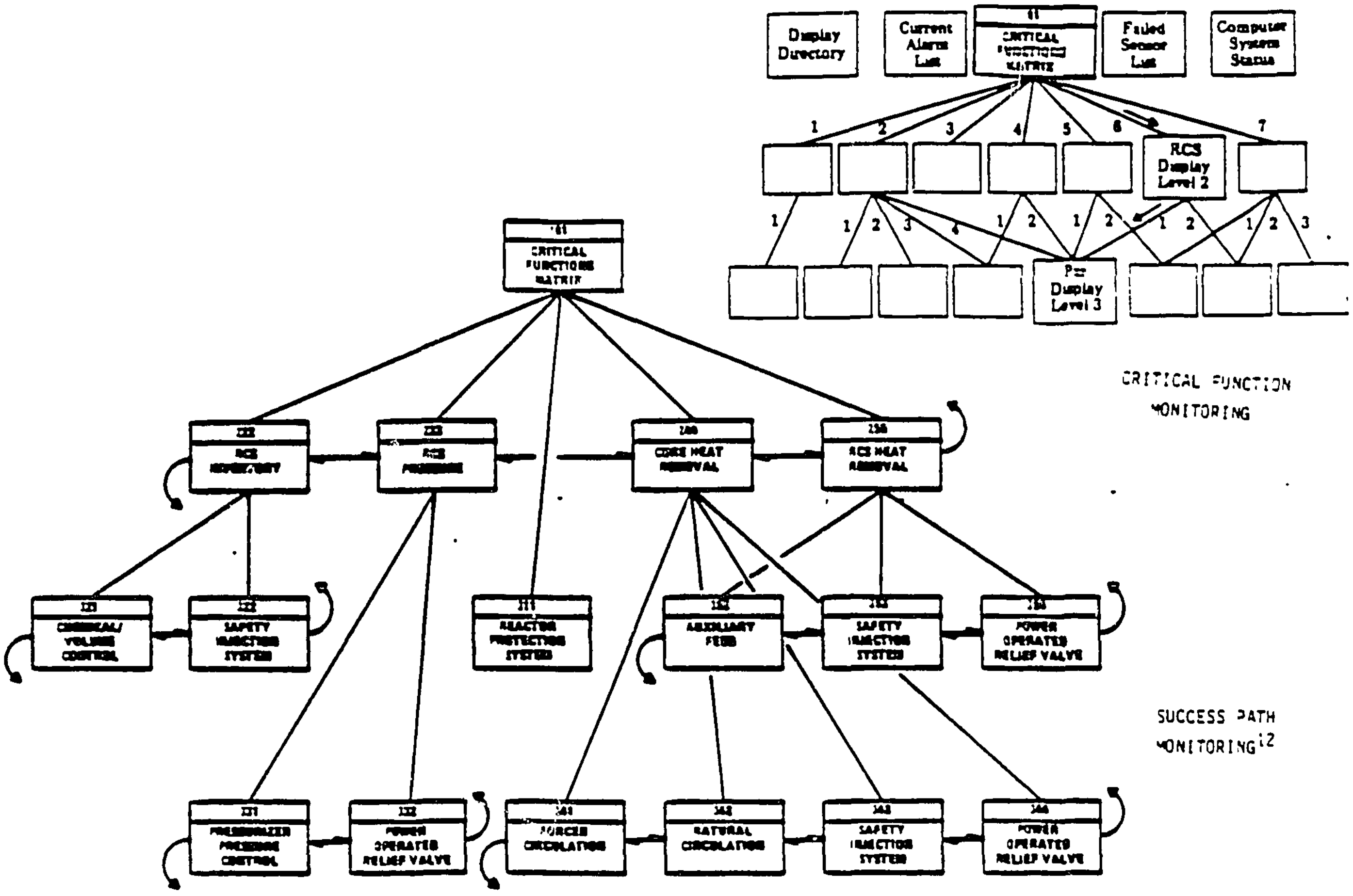
THE CRITICAL FUNCTION MONITORING SYSTEM (CFMS)

One proposed solution to improve the man-machine interaction during rare or unfamiliar situations in nuclear power plants has been to provide the operating crews with an aid that could provide an integrated display of a minimum number of critical plant parameters. Such aid, generally identified as a Safety Paremeter Display System (SPDS) [3], was expected to provide a timely and correct determination of the safety status of the plant, specifically during adverse plant conditions.

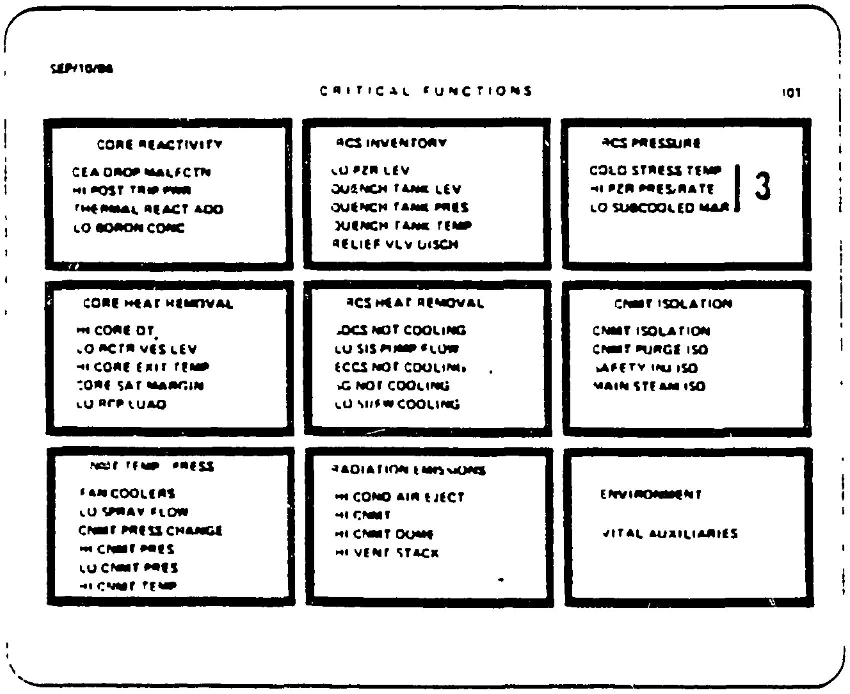
The CFMS distinguishes itself from other SPDS designs by machine implementation of sophisticated plant dynamics oriented algorithms[20] assisting the basic operator's cognitive process as discussed earlier, to recognize the status of a selected number of critical functions and the successpaths to accomplish these functions. In this context, a critical function has been defined as a group of actions, human or otherwise, which must be accomplished at all times to keep the plant in a stable and safe condition[8]. The minimum set of critical safety functions monitored by the CFMS are:

- reactivity control
- reactor coolant inventory
- reactor coolant pressure control
- reactor core heat removal
- secondary heat removal
- containment pressure and temperature control
- containment isolation

The CFMS interfaces with the operator through a color graphics video display system and controlling key pad. The display system includes a simple three-level display hierarchy as shown in Figure 6. The top level 1 display provides the critical function status type information as shown in Figure 7. The intermediate level 2 displays provide the information on the availability status of the successpaths to accomplish a particular critical function as shown in Figure 8. The lower level 3 displays supply the details on a particular successpath chosen by the operator, as shown in Figure 9. The algorithms and the display development for the level 2 and 3 displays were developed in cooperation with EPRI[12].



Fiqure 6: Basic CFMS Video Display Hierarchies



SEP/10/86

CRITICAL FUNCTIONS 101

CORE REACTIVITY CEA DROP MALFCTN HI POST TRIP PWR THERMAL REACT ADD LO BORON CONC	RCS INVENTORY LO PZR LEV QUENCH TANK LEV QUENCH TANK PRES QUENCH TANK TEMP RELIEF VLV DISCH	RCS PRESSURE COLD STRESS TEMP HI PZR PRES/RATE LO SUBCOOLED MAR 3
CORE HEAT REMOVAL HI CORE DT LO RCTR VES LEV HI CORE EXIT TEMP CORE SAT MARGIN LO RCP LOAD	RCS HEAT REMOVAL SDCS NOT COOLING LO SIS PUMP FLOW ECCS NOT COOLING SG NOT COOLING LO SI/FW COOLING	CNMT ISOLATION CNMT ISOLATION CNMT PURGE ISO SAFETY INJ ISO MAIN STEAM ISO
CNMT TEMP PRESS FAN COOLERS LO SPRAY FLOW CNMT PRESS CHANGE HI CNMT PRES LO CNMT PRES HI CNMT TEMP	RADIATION EMISSIONS HI COND AIR EJECT HI CNMT HI CNMT DOME HI VENT STACK	ENVIRONMENT VITAL AUXILIARIES

Fiqure 7: Level 1 CFMS Critical Function Status Video Display[12]

86.

In addition to the primary displays to assist an operator utilizing the Critical Function concept when responding to a plant situation, each of the display levels includes a reportoire of operational displays. These operational displays provide overview as well as more detailed information which is useful for successpath diagnostics and restoration and validation of system internal cognitive models, if so desired by the operator.

The display system is largely "self-directing" in nature through applied sectoring techniques, such that an operator is guided to the most appropriate display by simple key pad operation. The key pad also allows the operator to traverse the display hierarchy in any desired manner.

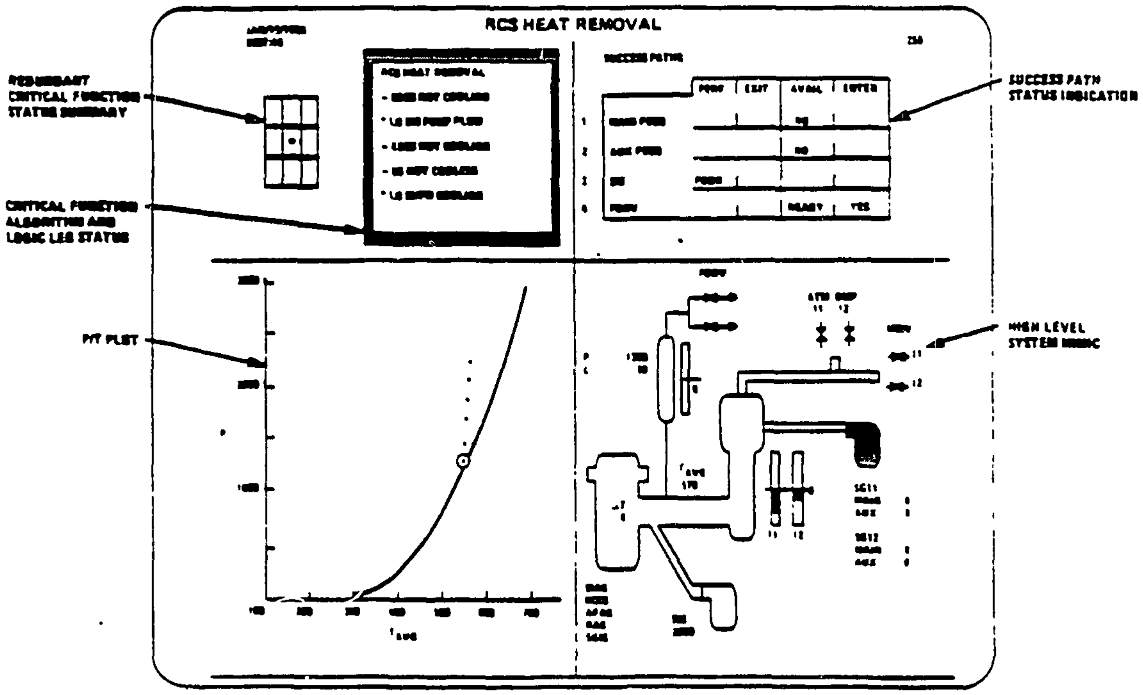

RCS HEAT REMOVAL
REDUNDANT CRITICAL FUNCTION STATUS SUMMARY
CRITICAL FUNCTION ALGORITHM AND LOGIC LED STATUS
P/T PLOT
SUCCESS PATH STATUS INDICATION
HIGH LEVEL SYSTEM MIMIC
EXIT
AVAIL
ENTER
NO
NO
READY
YES
ATM DMP
11
12

Figure 8: CFMS Level 2 Successpath Availability Video Display[12]

87

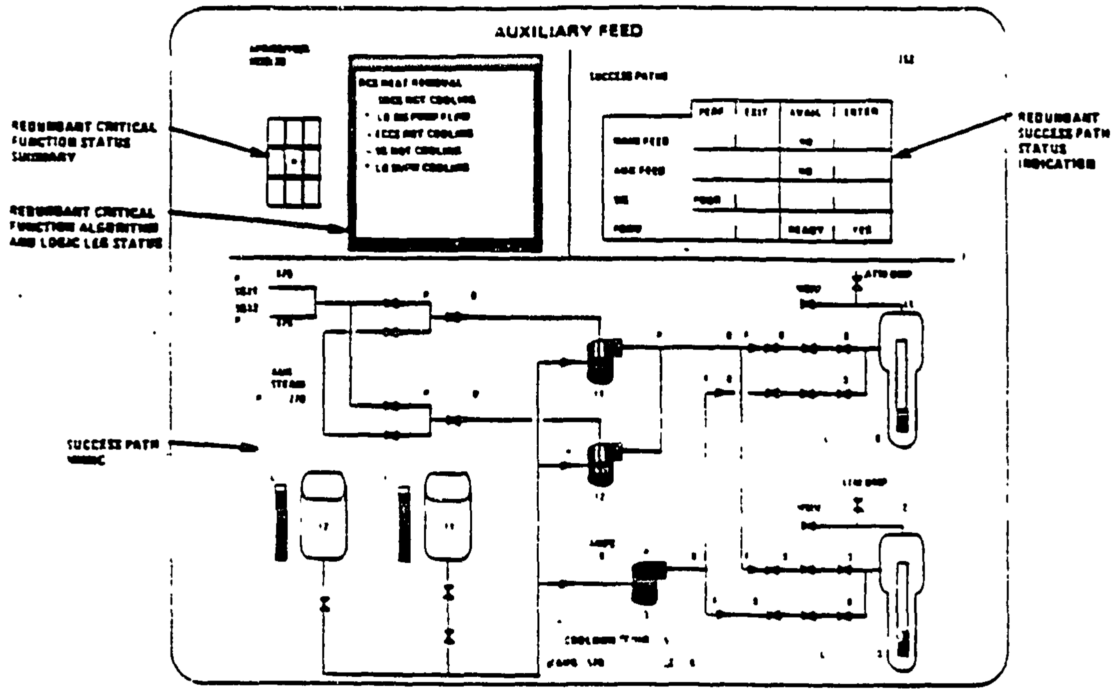

AUXILIARY FEED
REDUNDANT CRITICAL FUNCTION STATUS SUMMARY
REDUNDANT CRITICAL FUNCTION ALGORITHM AND LOGIC LEG STATUS
SUCCESS PATH MIMIC
REDUNDANT SUCCESS PATH STATUS INDICATION

Figure 9: Level 3 CFMS Selected Successpath Video Display[12]

The CFMS has been installed in several operating plants in the U.S. Preliminary experience with the CFMS has indicated so far, that the device has been well accepted by the operating crews as an aid to timely assess the status of the plant.

To confirm the effectiveness of the CFMS during adverse plant conditions, as speculated by the designers of the system, a full scale experimental validation[13] of the critical Function Monitoring System (CFMS) was carried out by the Halden Project in co-operation with the manufacturer, Combustion Engineering, the Technical Research Centre of Finland (VIT) and Imatran Voima OY (IVO). The experiment took place at the PWR training simulator situated at the IVO Loviisa nuclear power plant in Finland. The project, which lasted more than 18 months, covered all essential details:

88

initial planning, development of a CFMS training program, specification and installation of data recording equipment, practical training of operating crews, experimentation and data collection, data processing, analysis and evaluation. The subjects were twelve crews of experienced operators from the Loviisa nuclear power plant, undergoing their semi-annual retraining at the simulator. The experiment, which employed a 'within group comparison' design, made substantial use of both video and audio recordings, in addition to computer derived measurements. Two transients were developed which presented the operators with two equivalent, severe and complex plant disturbance scenarios. The analysis combined quantitative and qualitative methods, and used a detailed timeline description as the basis for answering questions about the impact of the CFMS. In terms of the overall quantitative analysis, two specific hypotheses were investigated: (1) that operators using the CFMS would maintain critical functions more effectively, and (2) that effective maintenance of critical functions was equivalent to improved plant safety. Both the overall results and the more detailed qualitative investigation of timeline data supported these hypotheses. In addition, the CFMS project demonstrated successfully the validation methodology developed at Halden.

This brief discussion highlights the efforts necessary to develop and validate a typical knowledge-based hierarchy before it can be included in the knowledge-base of a minimum attention control center. During the past several years, and particularly after actual installation in a plant, the operating staffs rapidly became to like the CFMS knowledge-based displays. In a sense, most humans rather prefer to work with knowledge than information or data. Consequently a certain dependency by the operating staffs on the system can be expected in due time. Such dependency naturally raises concern on the potential reliability of the knowledge provided. Combustion Engineering therefore conducts an extensive software verification and validation program[21] for the CFMS, which was developed from an ANSI standard[22]. In addition, basic signal validation techniques are utilized on the plant signal inputs to the system, more elaborate techniques[23] being under investigation.

CE-NUMACC^{TM} NUCLEAR MINIMUM ATTENTION CONTROL CENTER

CE-NUMACC is Combustion Engineering's latest entry in its quest of improving plant safety through improved man-machine interaction. CE-NUMACC is a natural follow-up of the CE NUPLEX-80^{TM} Advanced Nuclear Control Complex[11] developed during the '70's. CE-NUMACC is of advanced state-of-the-art and is being developed as a cognitive system of which the elements are not only cognitive by themselves, but also cognitively coupled to each other.

To promote the cognitive aspects of CE-NUMACC, the guidelines as identified in Table 1 are being applied intensively. Hereto, the Critical Function concept is being applied as the underlying cognitive concept. In addition, a visualization of the internal image or model of the process further promotes the cognitive coupling between the operating staff and the plant.

Table 6 summarizes the basic features of CE-NUMACC.

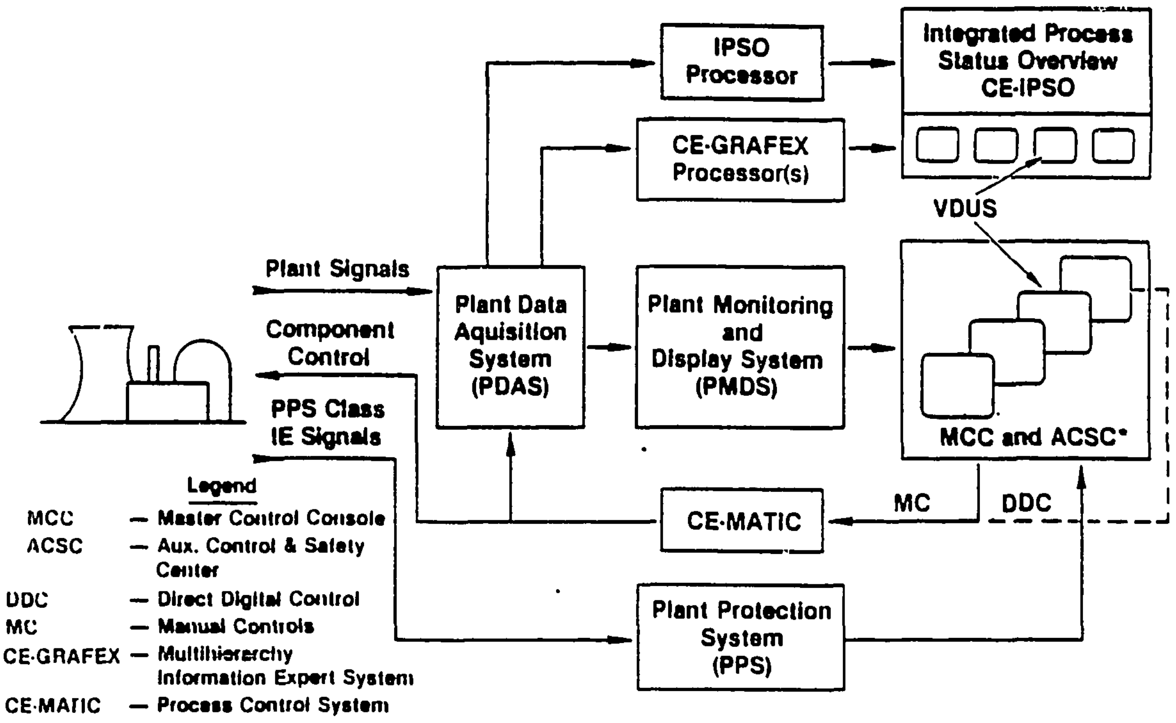
TABLE 6
CE-NUMACC^{TM} BASIC FEATURES

- BASIC NUPLEX-80^{TM} FUNCTIONAL AND DESIGN CRITERIA
- NUPLEX-80 PLANT MONITORING, CONTROL AND DIAGNOSTICS TECHNOLOGY UPGRADED
- INTEGRATED CRITICAL FUNCTION/SUCCESSPATH STRUCTURE
- LARGE FORMAT DYNAMIC INTEGRATED PROCESS STATUS OVERVIEW (CE-IPSO^{TM})
- MULTI-HIERARCHY COLOR GRAPHICS VIDEO KNOWLEDGE-BASED EXPERT SYTEM (CE-GRAPHEX^{TM}) TO SUPPORT CE-IPSO
- COMPUTER-BASED PLANT PROTECTION SYSTEM
- COMPUTER-BASED COMPONENT CONTROL SYSTEM (CE-MATIC^{TM})

As can be observed from Table 6, the well established NUPLEX-80 functional and design criteria have been maintained for CE-NUMACC. Also the PMS (Plant Monitoring System), PADS (Plant Alarm and Display System) and PDAS (Plant Data Acquisition System) have been upgraded to the latest state of the art.

The major differences between NUPLEX-80 and CE-NUMACC are the implementation of an Integrated Process Status Overview (CE-IPSO) with supporting multi-hierarchy color graphics video display expert system, CE-GRAPHEX, and CE-MATIC, which is an upgraded version of the NUPLEX-80 SSCCS (Solid State Component Control System), utilizing such innovations as multiplexed I/O's and DDC (Direct Digital Control) capabilities. Figure 10 shows a typical block diagram of CE-NUMACC as currently under development.

Figure 10: Typical Block Diagram CE-NUMACC


IPSO Processor
Integrated Process Status Overview CE-IPSO
CE-GRAFEX Processor(s)
VDUS
Plant Signals
Component Control
PPS Class IE Signals
Plant Data Aquisition System (PDAS)
Plant Monitoring and Display System (PMDS)
MCC and ACSC*
MC
DDC
CE-MATIC
Plant Protection System (PPS)
Legend
MCC — Master Control Console
ACSC — Aux. Control & Safety Center
DDC — Direct Digital Control
MC — Manual Controls
CE-GRAFEX — Multihierarchy Information Expert System
CE-MATIC — Process Control System

As shown, the plant signals are being collected and processed by PDAS, the Plant Data Acquisition System. This system is utilizing multiplexing as well as conventional techniques to acquire and transmit the plant data, depending on the ultimate use of the signals. As such, the PDAS interfaces with the Plant Monitoring and Display System (PDMS), CE-GRAPHEX and with CE-MATIC.

The PMDS provides a comprehensive monitoring and display function of the NSSS & BOP performance, much like a traditional plant computer. The information generated by this system is displayed on color graphics video monitors which are strategically located on the NUPLEX-80 like Master Control Console (MMC) and the Auxilary Control and Safety Center Panels of the Control Center.

The CE-GRAFEX™ is the cognitive "nerve center" of CE-NUMACC and includes a reportoire of operator and plant management information aids, such as the CFMS, COLSS[15], VISIONS[16], ISIS[17], etc. These aids are currently envisioned in dedicated stand-alone computer-based modules, or a common host computer system. The intelligence embedded in each aid module can be invoked by the user in the form of a dedicated information hierarchy displayed on three color graphics video monitors, located in or near the Integrated Process Status Overview (CE-IPSO). Figure 11 represents a simplified representation of CE-GRAPHEX.

As can be seen from Figure 11, the inherent critical function based cognizance of the algorithms can be tuned to the cognitive process of the operator such that a self directed display of information on the VDUs can be achieved. The artificial intelligence embedded in such concept further promotes congruence between the system's and the operator's internal models.

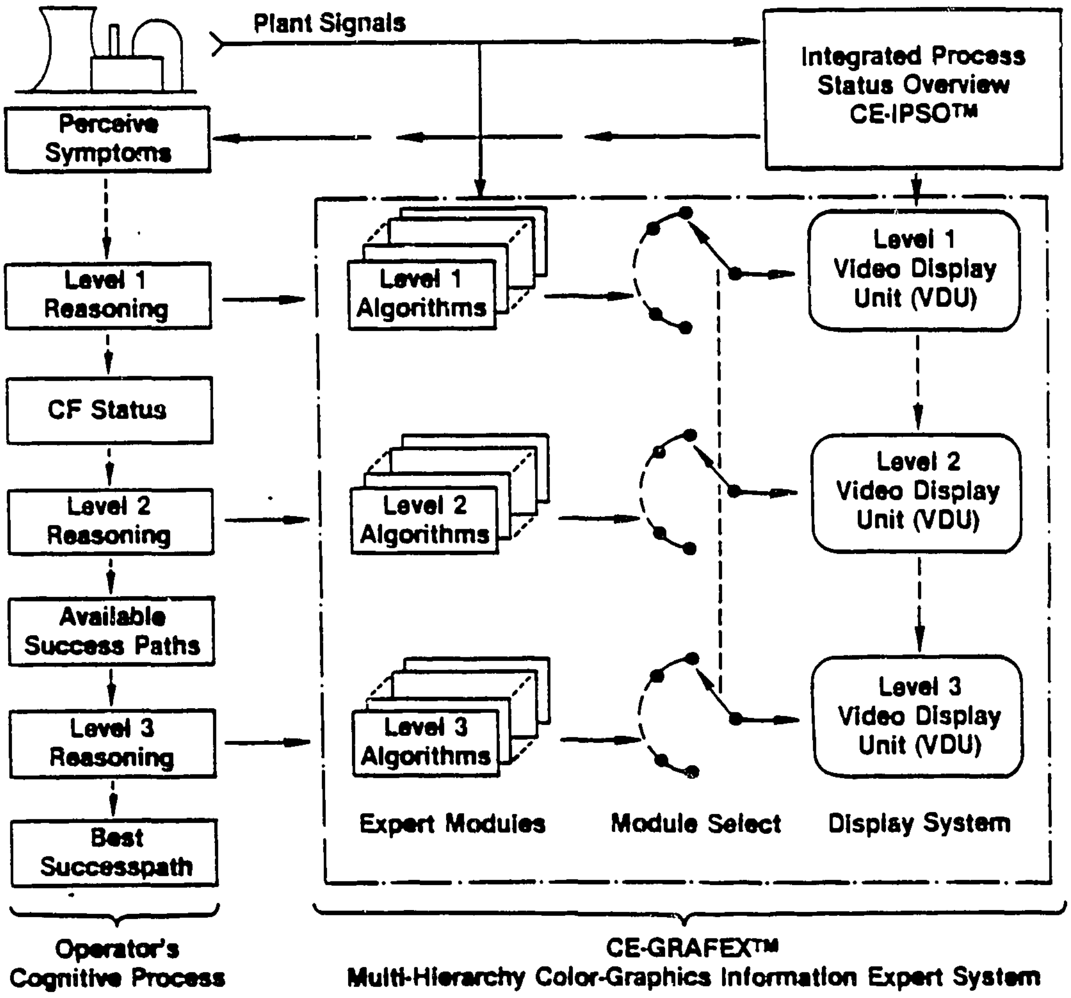


Figure 11: A Simplified Representation of CE-GRAPHEX™

92

The CE-IPSO[18] provides a permanent top level status overview of the process and functions much like an expert manager in a society of individual experts in a human expert system[19]. The overview is semi-dynamic, and is driven by the data-outputs of PDAS or by expert-system like algorithms calculating selected process status information (e.g. plant mode of operation, mass/energy flow balances, etc). A user can interact with CE-IPSO by means of a touchpanel located on the CE-NUMACC workstation. This touchpanel includes a reduced mimic of the CE-IPSO process map, providing a one-touch stroke capability to acccess each individual CE-GRAPHEX display hierarchy if so desired. In addition to the touchpanel, the center control panel of the workstation includes a Page Control Module (PCM) to access the display pages in each individual display hierarchy, and a joystick to access a software-based version of the CE-IPSO process map. Figure 12 provides a conceptual presentation of the CE-IPSO, Integrated Process Status Overview/CE-NUMACC workstation arrangement.

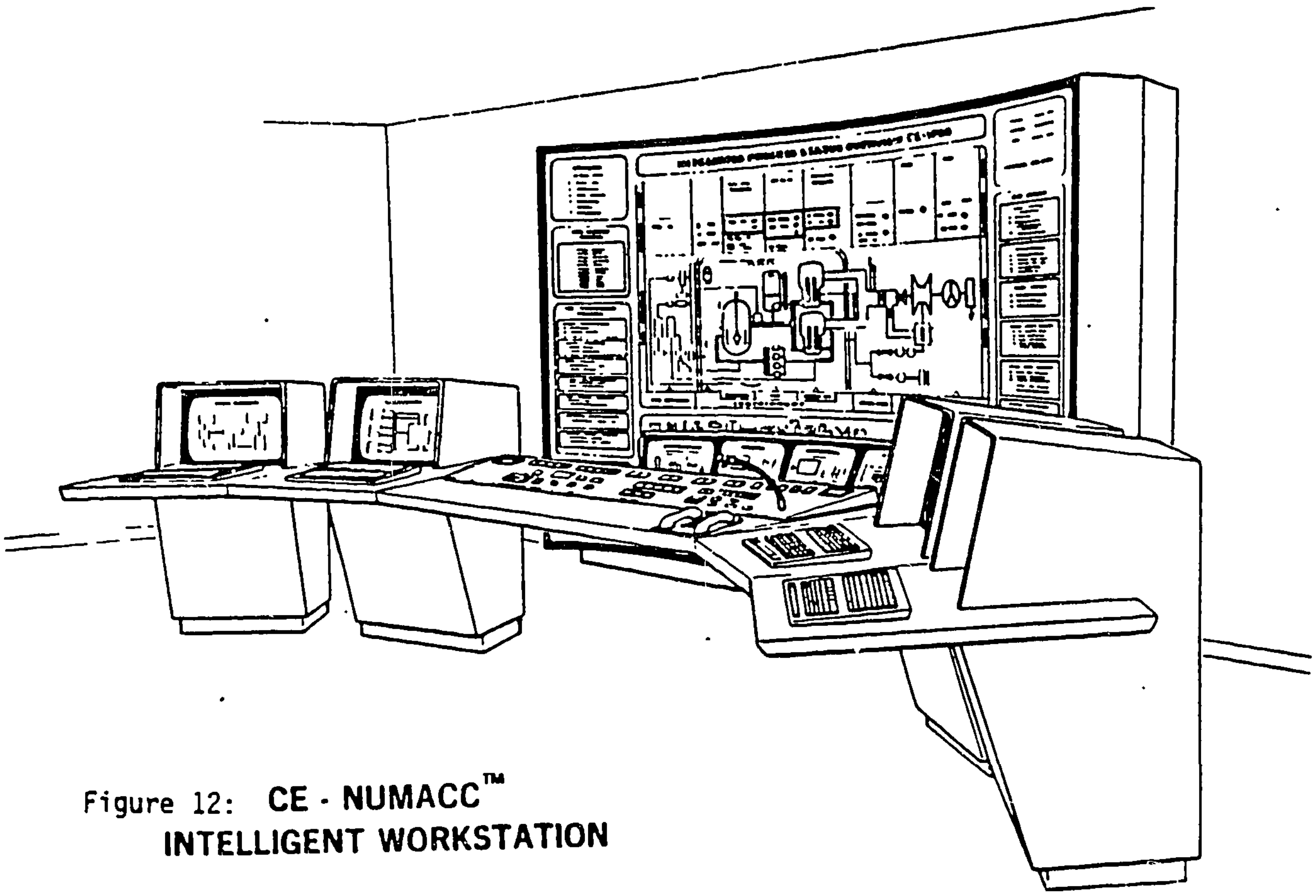


Figure 12: **CE - NUMACC™ INTELLIGENT WORKSTATION**

The CE-MATIC represents CE's latest apprach to the control of a process and its components. The approach includes selected multiplexed DDC (Direct Digital Control) by means of a trackerball from the PMDS color graphics video displays. The system is characterized by a sophisticated multi-redundant data bus and signal isolation structure, promoting a reliable and safe transmittal of safety grade or other informative and control signals.

CONCLUSIONS

Control Centers of nuclear power plants have been progressing from mostly data-driven to more information-driven media for interacting with the plants by the operating staffs. Utilizing the recent advances of the digital computer technology, a better understanding of the human cognitive aspects, and the potential of Artificial Intelligence and Expert System techniques, the obvious next step is a knowledge-driven interaction with these plants. Such interaction will promote a less attentive and therefore a higher human reliability of the operating staffs. The minimum attention control center concept described in this paper promises to enhance a more knowledge-based interaction process based on criteria essential for a natural interaction between intelligent agents. In particular the underlying Critical Function concept and the visualization of a shared dynamic "intelligent" knowledge base is expected to reshape the ways man is interacting with his machines...

THE FUTURE

In light of the current rapid advances of computer technology and applications in general, significant advances in the monitoring, control and diagnostics of nuclear power plants can be expected. These advances will most likely include nearly fully automated plants largely depending on intelligent knowledge-bases to maintain the safety and efficiency of these plants. Human interaction is not expected to occur other then during those rare occasions where human ingenuity must provide the last stand. Considering the current global interest in Artificial Intelligence and Expert Systems, there seems to be little doubt that future control centers of nuclear power plants will utilize these technologies to the maximum extent possible for further assurance of safe and economic power generation by these plants.

ACKNOWLEDGEMENTS

The author would like to thank J. E. Myers for his kind review of this paper. Also thanks to P. Gaudio for his contribution of the CFMS successpath monitoring displays to tne paper, to S. A. Morray and P. T. Gilbert for the artwork, and to Linda Cyr for arranging and typing of the final manuscript.

REFERENCES

1. Proceedings IAEA Specialists' Meeting on Control Room Design, IEEE-75CH1065-2, (7/75).
2. C. H. Meijer, et. al., "Applied Human Engineering to Improve the Man-Process Interaction in a Nuclear Power Plant", IEEE Symposium on Nuclear Power Systems, Orlando, Florida, (11/80), C-E Publication TIS-6704.
3. D. D. Woods, et. al., "Evaluation of Safety Parameter Display Concepts", Volumes I and II. EPRI Final Report NP-2234, February 1982.
4. C. H. Meijer, et. al., "Operational Aids to Improve the Man-Machine Interaction in a Nuclear Power Plant", American Nuclear Society, Annual Meeting, Las Vegas, (6/80), C-E Publication TIS-6649.
5. "An Overview of Computer-based Natural Language Processing", U.S. Department of Commerce, Publication no. NBSIR 83-2687 (4/83).
6. B. Chandrasekaran, et. al., "An Approach to Medical Diagnosis Based on Conceptual Structures", Proceedings of the International Conference on Artificial Intelligence, August 20-23, 1979, Tokyo, Japan.
7. G. A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capability for Processing Information", Psychological Review, Vol. 63, pp. 81-97, (1956).
8. W. R. Corcoran, et. al., "The Critical Safety Functions and Plant Operation", Nuclear Technology, Vol. 55, December 1981, CE Publication TIS-7158.
9. R. A. Fortney, et. al., "Safety Function and Protection Sequence Analysis", ANS Winter Meeting (November, 1973).
10. L. P. Goodstein, et. al., "Man-Machine Systems Design Criteria in computerized Control Rooms", ASSOPO 80, IFIP/IFAC Symposium, Trondheim, Norway, June 16-18, 1980.
11. Combustion Engineering Emergency Procedure Guidelines, CEN-152, REV. 01, Volume 1 & 2, November 1982.
12. P. J. Gaudio, Jr. et. al., "Improved On-line Operational Support using Successpath Monitoring", ISA/NRC/EPRI Symposium on New Technologies in Nuclear Power Plant Instrumentation and Controls, Washington, D. C., November 1984 (To be presented).

13. B. Wahlstrom, et. al., "Experimental Validation of Operator Support System Using A Training Simulator," IAEA International Symposium, Marseilles, France, 2-6 May 1983.

14. K. R. Rohde, "NUPLEX-80^{TM}-The Combustion Engineering Advanced Control Complex", ANS Nuclear Technology Exhibit, Beijing, People's Republic of China, May, 1984.

15. R. W. Knapp, "Digital Core Monitoring and Protection Systems", IAEA Specialists' Meeting on Nuclear Power Plant Control Problems associated with Load Following and Network Transients", Cadarache, France, January 26-27, 1977.

16 D. Bollacasa, et. al., "Visions-Versatile, Interactive Simulator of Nuclear Systems", ANS Winter Meeting, San Francisco, CA, (11/12 1981).

17. ISIS, "An Integrated Station Information System", private communication J. Herbst, Combustion Engineering, 1984.

18. C. H. Meijer, "CE-IPSO, An Integrated Process Status Overview Display for Nuclear Power Plants", Halden Project Workshop on Computerization of Procedures and on Information.Presentation, Halden, Norway, June, 1984.

19. C. H. Meijer, "Potential Applications of Knowledge Based Expert Systems to Industrial Environments", Fourth CE-Corporate Technology Awareness Conference, Atlanta, Georgia, May, 1983.

20. D. L. Harmon, "Critical Function Monitoring System Algorithm Development", IEEE and PLASMA Sciences Society (Nuclear Science Symposium), San Francisco, CA, August 1983.

21. J. M. Christens, Jr. et. al., "Insights and experience gained from the development of an Internal and Independent Verification & Validation Program", ANS Annual Winter Meeting, Oct/Nov 1983, CE-Publication, TIS-7522.

22. ANSI/IEEE-ANS-7.4.3.2, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations July 6, 1982.

23. C. H. Meijer, et. al., On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytic Redundancy, EPRI Final Report NP-2110, November 1981.