AECL-10071

ATOMIC ENERGY OF CANADA LIMITED

ÉNERGIE ATOMIQUE DU CANADA LIMITÉE

A FRAMEWORK FOR OPERATOR SUPPORT SYSTEMS FOR CANDU

UNE BASE POUR LES SYSTÈMES DE SOUTIEN D'OPÉRATEURS DE SALLES DE CONTRÔLE-COMMANDE DE RÉACTEURS CANDU

L.R. LUPTON, J.J. LIPSETT and R.R. SHAH

Presented at: IAEA/NPPCI Specialists' Meeting on "Artificial Intelligence in Nuclear Power Plants", Helsinki, Finland, 1989 October 10-12

Chalk River Nuclear Laboratories

Laboratoires nucléaires de Chalk River

Chalk River, Ontario K0J 1J0

November 1989 novembre

ATOMIC ENERGY OF CANADA LIMITED

A FRAMEWORK FOR OPERATOR SUPPORT SYSTEMS FOR CANDU

by

L.R. Lupton, J.J. Lipsett* and R.R. Shah

Presented at: IAEA/NPPCI Specialists' Meeting on "Artificial Intelligence in Nuclear Power Plants", Helsinki, Finland, 1989 October 10-12.

Instrumentation & Control Branch
*Advanced CANDU Project
Chalk River Nuclear Laboratories
Chalk River, Ontario, Canada K0J 1J0
1989 November

AECL-10071

ÉNERGIE ATOMIQUE DU CANADA LIMITÉE

UNE BASE POUR LES SYSTÈMES DE SOUTIEN D'OPÉRATEURS DE SALLES DE CONTRÔLE-COMMANDE DE RÉACTEURS CANDU

par

L.R. Lupton, J.J. Lipsett* et R.R. Shah

RÉSUMÉ

La taille et la complexité des centrales électronucléaires se sont accru considérablement au cours de ces 20 dernières années. On reconnaît en général qu'on peut améliorer la sûreté et disponibilité des centrales en assurant davantage de soutien opérationnel aux opérateurs si on le fait sans les surcharger de renseignements superflus. Les progrès récents réalisés en technique informatique donnent des possibilités de mettre en oeuvre des systèmes de soutien d'opérateurs très différents de ceux basés sur les techniques plus classiques employées dans les salles de contrôle-commande de centrales. L'intelligence artificielle (IA) et les techniques connexes joueront particulièrement un grand rôle dans la mise au point de techniques ouvrant des nouvelles voies et permettant de traiter et présenter l'information. Notre opinion est qu'il faut intégrer ces techniques à la gestion globale et philosophie de contrôle-commande des centrales et ne pas les traiter comme des moyens de mise en oeuvre de solutions ponctuelles. On examine, dans cette communication, la philosophie fondamentale à l'origine de cette opinion ainsi que les objectifs de conception du centre de contrôle-commande du réacteur CANDU 3. Les systèmes de soutien des opérateurs s'intégreront à la philosophie globale de contrôle-commande en complétant les opérateurs. En outre, ces systèmes peuvent jouer un rôle en aidant les opérateurs à "contrôler la situation", organiser, gérer et planifier le fonctionnement des centrales. On y décrit quatre systèmes de soutien comportant la philosophie fondamentale.

Présentée à la Réunion AIEA/NPPCI des spécialistes sur "l'intelligence artificielle dans les centrales électronucléaires", à Helsinki, Finlande, 1989 octobre 10-12.

Instrumentation en contrôle
*Projet CANDU avancé
Laboratoires nucléaires de Chalk River
Chalk River, Ontario, Canada KOJ 1JO
1989 novembre

AECL-10071

ATOMIC ENERGY OF CANADA LIMITED

A FRAMEWORK FOR OPERATOR SUPPORT SYSTEMS FOR CANDU

by

L.R. Lupton, J.J. Lipsett* and R.R. Shah

ABSTRACT

The size and complexity of nuclear power plants has increased significantly in the last 20 years. There is a general agreement that both plant safety and availability can be enhanced by providing the operator with more operational support if that can be done without overloading him/her with unnecessary information. Recent advances in computer technology provide opportunities for implementing operator support systems that are significantly different from the ones based on the more conventional technologies used in plant control rooms. In particular, artificial intelligence (AI) and the related technologies will play a major role in the development of innovative methods for information processing and presentation. Our approach to these technologies is that they must be integrated into the overall management and control philosophy of the plant and are not to be treated as vehicles to implement point solutions. The underlying philosophy behind this approach and the design objectives and goals for the CANDU 3 control centre are discussed in this paper. Operator support systems will integrate into the overall control philosophy by complementing the operator. There is also a role for such systems in assisting the operator to be a "situation manager", organizing, managing and planning the running of the plant. Four support systems that incorporate the underlying philosophy are described.

Presented at: IAEA/NPPCI Specialists' Meeting on "Artificial Intelligence in Nuclear Power Plants", Helsinki, Finland, 1989 October 10-12.

Instrumentation & Control Branch
*Advanced CANDU Project
Chalk River Nuclear Laboratories
Chalk River, Ontario, Canada K0J 1J0
1989 November

AECL-10071

TABLE OF CONTENTS

1. INTRODUCTION

The effect of operator errors on plant safety and operation has been discussed extensively over the past ten years [1,2]. There is a general agreement that both plant safety and availability can be enhanced by providing the operator with more operational support, if that can be done without overloading him/her with unnecessary information.

Recent advances in computer technology provide opportunities for implementing operator support systems that are significantly different from the ones based on the more conventional technologies used in plant control rooms. In particular, artificial intelligence (AI) and related technologies will play a major role in the development of innovative methods for information processing and presentation. However, because significantly new approaches and technologies are involved, the solutions will have to evolve as these technologies mature further and gain acceptance in the control centre environment. Operator support systems will be integrated into the control centre of CANDU* 3 nuclear power plants [3] over the next 5 to 20 years.

Atomic Energy of Canada Limited (AECL) is developing a framework on which the newer approaches to operator support systems will be implemented. Our approach to these systems is that they must be integrated into the overall management and control philosophy of the plant and are not to be treated as point solutions. The underlying philosophy behind this approach and the design objectives and goals for the CANDU 3 control centre are discussed in sections 2 and 3 of this paper. Section 4 briefly describes specific operator support systems being developed as prototypes for gaining experience and for building a level of confidence and acceptance with the new technologies.

2. UNDERLYING PHILOSOPHY

The development of operator support systems requires designers to address the following issues:

- the balance between performance (availability) and safety goals (plant complexity),
- the balance between manual and automatic control (function allocation), and
- the inclusion of human factors (psychology, anthropometrics and task analysis), including human reliability.

Our experience to date has shown that each of these issues cannot be addressed independently. In this section, we will summarize the underlying philosophy that is being applied to the development and integration of operator support systems within the control centre of CANDU.

Over the past 25 years, nuclear power plants have increased in size and complexity, and the technology available to process information has advanced significantly, enabling considerably more information to be available to the plant operator than was previously possible.

The expansion of information has been beneficial since that has contributed to the increase in production capability and the safety of the plants. However, this large amount of information tends to be presented to the operator in the conventional manner, i.e., the philosophy behind information presentation is based on conventional panel-based control rooms. This approach, we believe, leads to the information overload that the operator is often faced with.

---

* CANDU: CANada Deuterium Uranium. Registered in the U.S. Patent and Trademark Office.

Information overload, combined with the stress of ensuring safety while meeting high production targets, is a concern since that combination can increase the potential for operator error.

We are developing new control centre concepts, incorporating such advanced technologies as artificial intelligence (AI) and expert systems, for CANDU that will help reduce this potential for human error. The key thrusts of this approach are:

- a better definition of the levels of automation,
- a comprehensive decision-making model,
- design of operator support systems using the application of human behaviour and reliability considerations, and
- presentation of information in the context of a plant situation or condition.

2.1 Levels of Automation

In modern plants, control is shared between the installed instrumentation and control systems and the humans who are in charge of the overall operation. The process of allocating plant control functions to the human operator or to the machine has, in general, been decided on a case-by-case basis. For the control centre for CANDU plants, we are identifying a more formal process.

In addressing the allocation of function to the operator and the machine, the following contradictory issues have to be resolved:

- errors made during manual operations are an important factor in initiating plant outages, and hence where possible, tasks should be automated;
- departures from prescribed tasks by knowledgeable operators sometimes ensure plant availability or safety;
- tasks that are fully prescribed and where the operator has no discretion should be automated;
- too much automation will leave operators with very little to do, leading to boredom, possible loss of operations skills and possible safety concerns.

We have re-examined the generalized control problem and have derived a hierarchy of activities [4]. This hierarchy parallels much of the structure of human behaviour (skill-based, rule-based and knowledge-based) defined by Rasmussen [5]. His structure was derived from observations in a control room situation involving mainly manual control. This parallelism is not surprising since, historically, automatic control has arisen from efforts to assist and expand human capabilities. We are currently developing a combined hierarchy to meet our needs.

Plant activities that involve the performance of knowledge-based tasks, such as planning, scheduling and review of operations, interpreting situations and devising new procedures, are defined as "creative" (see Table 1). These activities require the operator to be a "situation manager" and to utilize adaptability, training, experience, foresight, initiative and common sense while dealing with new situations, variants of previous ones and obscure events. There is considerable scope for machine assistance in this domain, the main criterion being to assist the process, not hinder it.

On the other hand, many activities exist where the response to a particular situation must be predetermined based on system behaviour that is fully understood and that can be mathematically defined. Examples of these actions are control systems and trip systems. These actions are fully implemented in hardware and this is referred to as "hard automation".

Table 1: Comparison of Levels of Automation

Behaviour Type	Intent	Definition of Functions Assigned to Operator	Definition of Functions Assigned to Machine	Responsibility for Action
Knowledge-Based	Creative Thought	Creative/Situation Management	Operator Support System	Operator
Rule-Based	Predetermined Response	Soft Automation	Operator Support System	Designer/ Operator
Skill-Based	Automatic/ Conditioned Response	Hard Automation	Hard Automation	Designer

There are other activities where the task is assigned to the operator, but he/she has no option but to carry it out exactly as specified. The operator must act accurately and reliably and, in a sense, is "hard automated" to have a very specific conditioned response.

In other circumstances, hard automation (by man or machine) may not be the correct choice because it is too expensive, the technology does not exist or does not significantly exceed the reliability of the human, or there may be components of judgement required to deal with the circumstances. In these cases, the human must remain in the control and decision loop. This type of action or response is what we refer to as "soft automation". In this case, the operator must be provided with as much assistance as is practical so that the task will be done as accurately and reliably as possible.

Our intention is to implement operator support systems for assisting the operator in being the "situation manager" and to carry out the "soft automation" functions (see Figure 1). We believe that the AI and expert system technologies will have a significant role to play in implementing operator support systems that enhance the operator's inherent capabilities.

2.2 Decision-Making Model

Machine assistance can be introduced at various places in the information processing and control loop, and communication between the human and the machine could occur at many places. To provide a structure or framework for this we must examine the decision-making sequence to define sensible breaks and communication points.

First it is necessary to evaluate how information is used for control decision-making [4-9]. We are proposing a five-step sequence of discrete activities, each with unique requirements and characteristics:

- Track — Measure plant parameters, monitor equipment status,
- Compare — Compare current situation to goals, standards and desired condition,
- Identify — Identify primary and associative conditions,
- Diagnose — Determine root cause, reasons for differences, and
- Decide/Act — Derive or assess the corrective options, choose one for implementation.

The basic sequence forms a framework that can provide strategies for combining manual control, automatic control and management functions to treat the full range of control issues from single parameter control to the control of a complete plant. Figure 2 illustrates where the necessary goals, data and knowledge bases must be provided, where possible technologies could permit machine operations and how information flow paths can be organized to attack a problem.

In the situation management mode, the "Decide/Act" step would predictably require an internal loop to prepare a special procedure (even if it is only in the head of the operator) consisting of a plan of attack, assessing available resources, predicting consequences, and a sequence of action. Using Rasmussen's model [5], we propose to expand the Decide/Act step to:

• Interpret	Interpret the consequences for current task, safety, efficiency, etc.,
• Evaluate	Evaluate performance criteria,
• Define Task	Select change of system condition,
• Formulate Procedure	Plan sequence of actions, and
• Execute	Manipulate system (including feedback).

We are still evaluating the significance and completeness of the sequence as applied to combined man-machine operations.

2.3 Context-Sensitive Information

The CANDU 3 plant incorporates data highways and distributed control for all control functions. This distributed system architecture enables the adoption of the "soft" control room concept (also referred to as cockpit-type control [10]), where CRT's are used for presentation of plant information as well as for executing control operations. This concept provides the opportunity to present the operator with information that is most relevant to the task in hand. The other background information is not "hidden", but rather is available on demand. Relevance implies that there are contexts that change with operating circumstances. This useful concept of context sensitivity can be applied in many ways, such as:

- prioritizing the importance of plant data according to a set of predefined reactor states, conditions, and controlled trajectories between states,
- graphical presentation of operating parameters showing plant condition or trajectory within the acceptable domain, and
- information presentation by function, system or suitable combinations.

By applying this concept throughout the design of the plant, including the operator support systems, we ensure that the operator has access to, and can properly interpret, the correct information within the context of the tasks to be performed to achieve the desired performance and safety goals.

3. DESIGN OBJECTIVES AND GOALS

The CANDU 3 design incorporates a number of new approaches. Specifically, the design of the control centre will address the underlying philosophy outlined above. The highlights of the design objectives and goals for the CANDU 3 control centre are briefly presented below. These objectives and goals are presented in the form of targets that will be achieved over a number of years, and will require close interaction with the designers and operation staff.

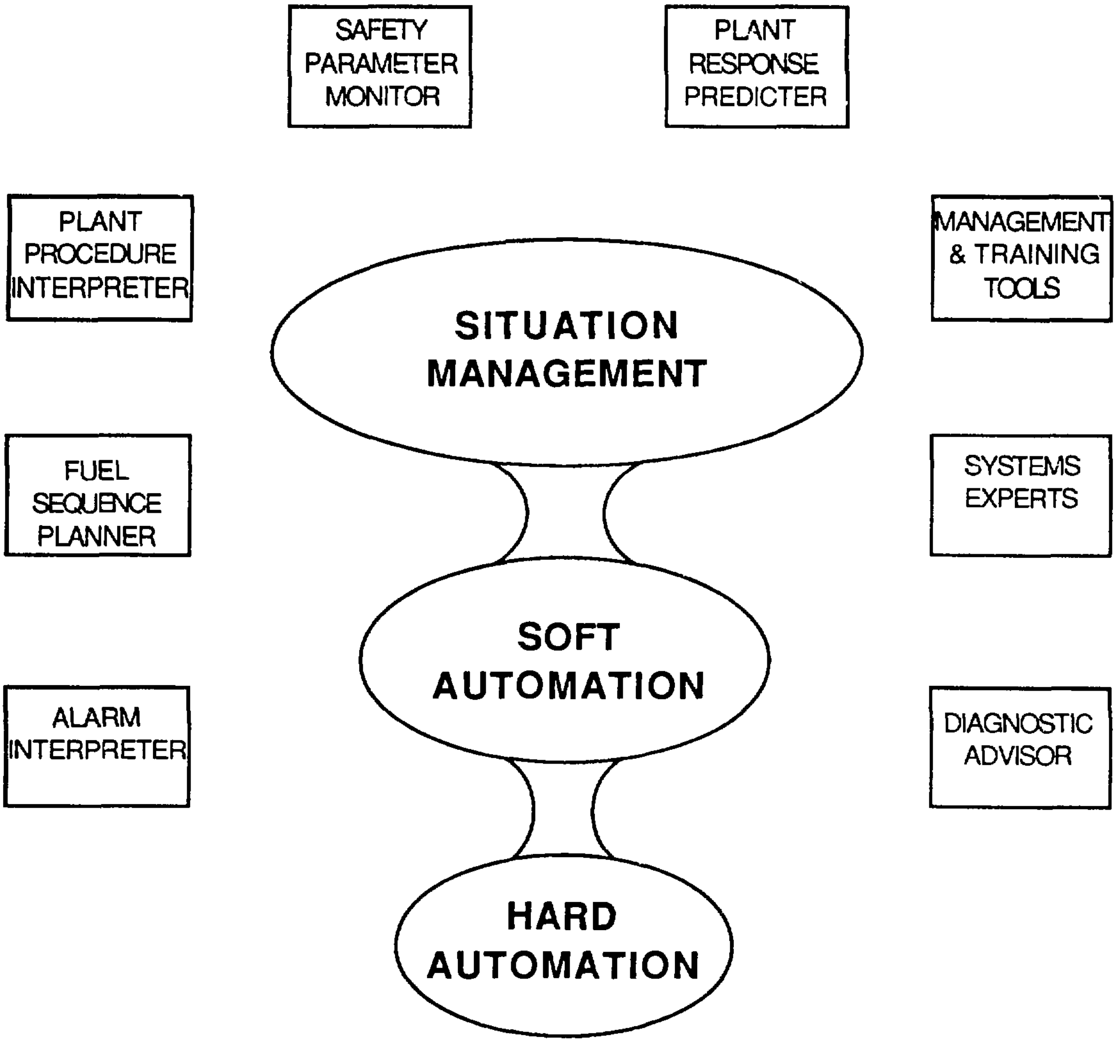

Figure 1: A Model for Operator Support Systems

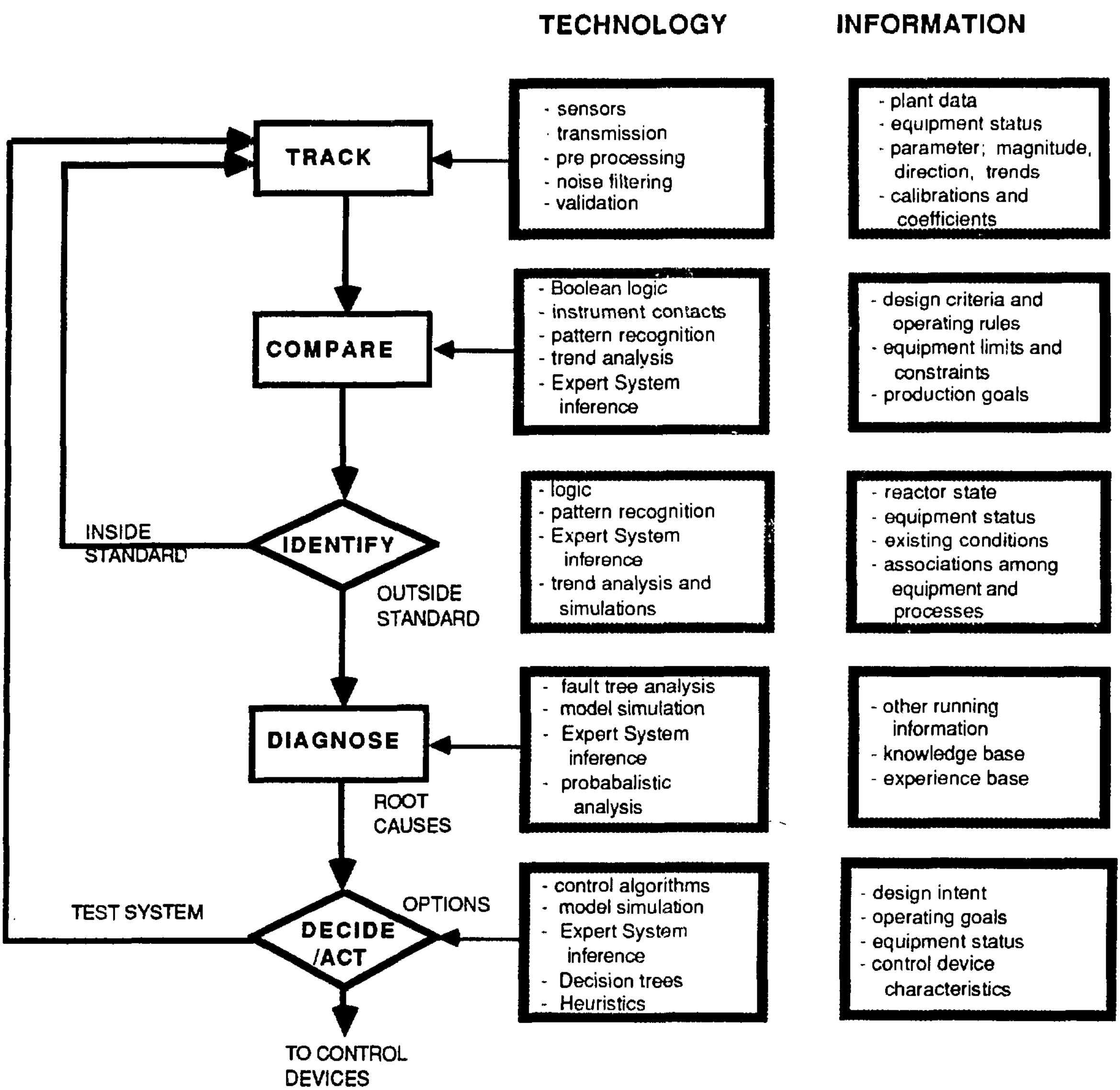

Figure 2: Decision Sequence with Associated Technologies and Information Bases

3.1 Cost Reduction

The control centre has to be simple and compact so as to avoid capital cost and schedule risk.

3.2 Elevate the Role of the Operator

Apply additional automation selectively in order to remove tedious distracting activities and provide the operator with tools to function on the level of a situation manager who plans, organizes activities and solves problems.

3.3 Systematic Design Process

High-level operational objectives should drive the detailed design of the cognitive and physical man/machine interfaces. The design should be based on an analysis of the goals and functions for the control centre covering all operational states and accident conditions. The analysis should be carried out to define the detailed design requirements, including man-machine interfaces, procedures, staffing and training systems. Standard methodologies (e.g., International Standard for Design for Control Rooms of Nuclear Power Plants, IEC 964 [11]) should be adapted to suit CANDU 3 needs.

3.4 Design to Reduce Operator Error

Information presented to the operators should reflect the context of the specific objectives and tasks relevant to each particular situation. This approach will help the operator absorb and interpret the data and define actions correctly and rapidly.

3.5 Input from Operating Staff

To ensure that the control centre design satisfies the plant operator's needs, the knowledge of plant operating staff should be incorporated in the design by having the experienced operating staff as members of the design teams.

3.6 Flexibility

The control centre should be flexible to enable designers to incorporate the operations input. Thus, where possible, information should be presented and control actions executed through interfaces, such as CRT displays, that can be optimized as the design progresses. A "soft control" philosophy will also give the designers considerable flexibility in arrangements of panels (predominantly CRT based).

The control centre should have a minimum number of standardized components in a flexible interface, that can be tailored to suit different operating philosophies and methodologies.

3.7 Integration of Control Centre Functions

The control centre should integrate display and control systems, all man/machine interfaces and operating procedures.

3.8 Keep the Operator in Touch with the Plant

Provide information and activity that will keep the operator alert and in touch with the plant, using information other than that normally available in the control panels.

4. OPERATOR SUPPORT SYSTEMS

The design objectives and goals discussed above lead to several new operator support systems that are being considered for the CANDU 3 control centre, and each is described below. These new systems are, however, still unproven in the control centre environment, and therefore we are developing prototypes to gain experience in applying them. The prototypes will be evaluated by operators in real plant environments, or using simulators, to obtain operational feedback and to gain acceptance of the new approaches. Introduction of all these support systems into the plant will extend over several years.

A number of other operator support systems have also been identified (see Figure 1), but these systems will be implemented in the future [12].

4.1 Information Displays and Interfaces for Control Execution

The CANDU 3 control centre will incorporate a "soft control" concept where CRT displays are used for data display, annunciation and for control execution functions. This implies that the same CRT's will be used to provide the operator with an overview of the plant, the safety margins and the operating envelopes at a glance. Conventional CRT display techniques for presenting information have been reasonably effective in past CANDU designs [13]. The last decade has seen major advances in display technologies, and the new technologies associated with CRT displays offers opportunities for information presentation that were not available in the past. The purpose of our development activity is to use these improved information presentation tools (e.g., windows, icons and interactive multimedia - integrated graphics, text, sound, animation, etc.) to produce innovative display formats to present information efficiently and effectively. The displays will be designed to exploit the unique cognitive capabilities of humans, and their ability to relate geometric shapes or patterns to meaningful events [14,15]. Where possible, we will be building on the work of others and are prepared to enter into technology transfer agreements to advance the development of international standards.

The information display system is being designed to enable customization by the plant operating staff to tailor the displays and the display formats to meet the station-specific needs.

We are exploring the concept that the commands used to access plant information--such as change displays and display formats, select and deselect parameters, access procedures, initiate control actions and request background information--will be based on a common syntax. The commands could be accessible via menus and icons, and would allow convenient recovery from data entry errors. The operator should be able to use one syntax to perform all his/her tasks via the plant information and control computer system.

The need has been identified for large, dynamic, overview displays in the control centre to provide plant operators with an "information wall" that can be viewed and read from anywhere in the control room. The displays on the "information wall" would be selectable by the operators and shift supervisors, and would show the process flowsheets with the current equipment and system status, critical plant parameters, etc. Prototype large format display systems are being evaluated. Operator requirements for information to be available on such displays are being discussed with CANDU utilities.

To address some concern that increased automation will isolate the operator more and more from the plant , we are exploring the option of providing the operator with information other than of the kind displayed on the CRT screens, e.g., video images of and sound from strategic areas of the plant. Such information would enable the operator to make use of the human senses and sensibilities to obtain a better feel for the plant using other input sources.

4.2 "Smart" Alarm Processing and Presentation

The current alarm annunciation systems in nuclear power plants are generally designed to be activated as soon as a parameter transgresses a predefined limit. Therefore, a control centre during a plant upset condition presents a rather stressful environment for the operator. Alarms are pouring in, lights are flashing, displays are scrolling and printers are spewing out alarm messages. Under these conditions, the operator has to interpret the plant state, identify the root cause of the event and take timely and correct action to mitigate the consequences of the event.

In current reactor designs, alarms are usually annunciated even if, under a given plant state, the parameter is where it should be. For example, in a CANDU design, an alarm message will be generated when the Emergency Core Cooling (ECC) tank level falls below a specified level. At full power production, this message is important as it indicates an impairment to a safety system. However, the same message will be generated if ECC is used, though the context is exactly opposite to the previous case, and it now indicates that ECC has been successful. Depending on the circumstances, the operator may have to filter out this type of extraneous information while attempting to analyze the situation.

Attempts have been made at conditioning and categorizing alarms to reduce the volume of data for the operator [16]. These attempts have been only partially successful as the designs have tended to produce systems that:

- are strong in their fault coverage and their detailed technical correctness, but less strong in their integration across system boundaries, and in their prioritization from an overall plant perspective, and
- mix maintenance messages, diagnostic information, operational action commands, short- and long-term warnings, and equipment status change indications.

Where suppression of messages has been performed, the higher-level message stating that the filtering has been performed usually has not been created.

We are exploring the development of alarm processing techniques that will evaluate and categorize alarm information based on plant states and plant operating status to generate composite and advisory alarm messages [17]. The operator would be presented with alarm information relevant to the current situation, and thus he/she would be able to concentrate on the essential messages and interpret the situation without being distracted by extraneous data.

Expert systems could be used to carry out the alarm processing functions and alarm messages would be presented to the operator in formats that would simplify interpretation. The operator will have easy access to all the alarm data and will be able to sort alarms using criteria that can be easily defined and modified.

In addition, the station operation staff will be able to conveniently tailor alarm processing and presentation to suit the station-specific needs.

4.3 On-Line Fault Diagnostic Systems

The failure of system operation, as designed, eventually precipitates a number of alarms that have to be interpreted and the root cause of the failure diagnosed. With 6000 measured and calculated variables in a CANDU plant, there are operational circumstances when an event can result in a flood of alarms. Such information overloads present severe demands on the operator, who must attempt to diagnose the fault and take timely and correct action.

We are developing prototype on-line diagnostic systems that will provide plant operators with advice on root causes of alarms and will give operators a capability to predict potential failures. An early prototype has been developed for a small heat transfer circuit and is based on a model representation using the qualitative physics of De Kleer and Brown [18], and first-principles diagnosis using constraint suspension [19]. Temporal information was integrated into the diagnosis by using a type of directed graph to record event dependencies. This graph was used to dynamically alter the qualitative model to reflect changes in the system over time. Although not completely formal, our method has successfully integrated the time diagnostic information to identify the faulty components in several tests. The number of spurious candidates was low. More work is planned in the area of combining the qualities of this approach with conventional expert systems.

We are starting the development, jointly with Hydro Quebec, of an on-line diagnostic system for determining the root cause of shut down system trips for the Gentilly 2 nuclear power plant. This system will make use of expert system technology and could include qualitative model-based reasoning and knowledge-based simulation. The system will be tested initially using a full-scope simulator and then evaluated in the Gentilly 2 control room.

4.4 Computer-Assisted Procedures

Since the operator in the CANDU 3 control centre will be presented with plant information on CRT display screens and will be able to carry out the necessary control action from the CRT's, plant operating procedures will be available through the same medium. This capability will provide plant operators with a highly interactive on-line access to plant operating procedures, together with all relevant information in a convenient format.

The intention is not to just computerize the procedures, i.e., have the procedures presented on CRT's in the same format as would be shown on paper, but rather to incorporate significant information processing and analysis capabilities to provide the operating staff with an "intelligent" tool that will truly assist the operator in monitoring and executing the procedures.

The decision-making model outlined in section 2.0 can be grouped into the following three high-level divisions:

Detection	-	Track, Compare,
Identify Procedure	-	Identify, Diagnosis, Interpret, Evaluate, Definite Task, Formulate Procedure, and
Action	-	Execution (including feedback).

Using these divisions, the implementation of the decision-making model and the context of Emergency Operating Procedures (EOP's) within the model in existing CANDU plants and CANDU 3 can be shown in a simple manner (see Table 2). In existing CANDU plants, the tasks of the three high-level divisions of the decision-making model are supported by separate systems with the operator providing the integration between each part. In this approach, procedures are the paper-based instructions that are used to direct the actions to be performed by the operator to return the plant to a safe state.

Point Lepreau Generation Station (GS) has enhanced the implementation of the model by adding an Emergency Conditions Monitor (ECM) to the Digital Control Computers (DCC's) to advise the operator when the entry conditions have been met for each EOP and to monitor governing conditions within each EOP, once initiated [20,21]. Procedures are still paper-based and significant demands are placed on the operator to integrate them with the other two parts of the model.

For CANDU 3, we propose to:

- integrate all three aspects of the decision-making model in the man-machine design of Plant Display System (PDS),
- define the tasks to be performed by the computer and by the operator based on a functional analysis of the plant (including task and job analysis) [11], and
- treat the complete environment as 'a procedure'.

This integration will ensure that there is complete traceability from the Probabilistic Safety Analysis (PSA) and functional analysis of the plant to the EOP's (as defined in [11]).

The above discussion has focussed on EOP's. The same logic will be applied to normal operating procedures.

Table 2: Decision-Making Model for CANDU Emergency Operating Procedures

Plant	Implementation of Decision-Making Model			Comment
	Detection	Identify Procedure	Action	
CANDU 6	By Annunciation System (DCC's)	By Operator	By Operator (Paper-based EOP's)	Three parts of model not integrated - procedures address 'Action' and sometimes 'Identification'
Point Lepreau GS (Proposed for EOP's)	By Annunciation System (DCC's)	By Emergency Conditions Monitor (ECM) (DCC's and SDS computer)	By Operator (Paper-based EOP's)	First two parts integrated - procedures address 'Action'
CANDU 3	By PDS (Annunciation System)	By PDS (Annunciation System)	By Operator interaction with PDS	All three parts integrated - procedures encompass all three elements

The CRT displays could employ interactive multimedia technologies, such as hypermedia, to provide an easy-to-use interface for operators to access and manoeuvre through the procedures.

The system will be developed as a "shell" so that designers and station staff can conveniently customize the procedures to suit the station-specific needs without having to launch a major software upgrade.

While assistance with normal operating procedures is needed to reduce operating errors and enhance plant availability, a system to assist with emergency operating procedures (EOP's) was considered to be most urgent for addressing operator needs under more stressful situations during major plant upsets.

The shell will support the EOP "standard" drawn up by the Joint Task Group of the CANDU utilities [22,23], and the EOP system will be intimately tied to the Plant Display System (PDS) of CANDU 3.

The shell for EOP's will be designed such that it can be expanded to eventually incorporate normal procedures at a later date.

We are currently implementing a prototype computer-assisted EOP for Loss of Instrument Air for Point Lepreau GS that will be tested in their control centre. The plant operators will be able to compare the performance of the computer-assisted procedure with the conventional paper-based procedure. This evaluation is expected to provide valuable feedback for the designers and will give the operators an opportunity to experiment with the new technology.

5. CONCLUSIONS

The size and complexity of nuclear power plants has increased significantly in the last 20 years. The continued advancement of computer technologies offers new opportunities for machine assistance to the operator at a time when human error is being increasingly recognized as a key component in industrial accidents.

The underlying philosophy leading to the integration of operator support systems in CANDU addressed the issues of the balance between performance and safety goals, the balance between manual and automatic control and the inclusion of human behaviour and reliability issues. Operator support systems will integrate into the overall control philosophy by complementing the operator. There is also a role for such systems in assisting the operator to be a "situation manager", organizing, managing and planning the running of the plant.

Design objectives and goals for the CANDU 3 control centre have been summarized and four support systems that incorporate the underlying philosophy have been described. Considerable effort is still required to gain experience, confidence and acceptance with these new systems incorporating advanced technologies.

6. ACKNOWLEDGEMENTS

The authors wish to acknowledge the contributions of R.A. Olmstead, R.E. Ashwell and J.E.S. Stevens towards the development of the concepts described in this paper. The authors wish to thank R.F. Moore for the numerous discussions on the practical aspects of our work and for providing references to work by others in this field. The contributions of the operations and technical staff at Hydro Quebec's Gentilly 2 NGS and at New Brunswick Electric Power Commission's Point Lepreau GS are also acknowledged .

7. REFERENCES

1. "An Analysis of Root Causes in 1983 and 1984 Significant Event Reports", Institute of Nuclear Power Operators Report, INPO 85-027, 1985 July.

2. "An Analysis of Root Causes of Significant Events Identified in 1985", Institute of Nuclear Power Operators Report, INPO 86-022, 1986 September.

3. "CANDU 300 Technical Outline", Atomic Energy of Canada Limited Report, PPS-74-01010-003, 1989. (Note - since being published, the name of the generic design for the power plant has been changed to CANDU 3.)

4. J.J. Lipsett, R.A. Olmstead and J.E.S. Stevens, "Balancing the Roles of Humans and Machines in Power Plant Control", Atomic Energy of Canada Limited Report, AECL-9955, 1989 May.

5. J. Rasmussen, "Information Processing and Human-Machine Interaction - An Approach to Cognitive Engineering", Noth-Hollan Series in System Science and Engineering, Series Volume 12, Andrew P. Sage (Ed), Elsevier Science Publishing Co., Inc., New York, NY, 1986.

6. J.A.G. Hale, "Goal Oriented Decision Support", from "Computer Assisted Decision Making", G. Mitra (Ed.), North Holland, New York, N.Y., pp 35-48, 1986.

7. B. Papin and G. Beltranda, "Computer Monitoring Systems: Design requirements for a Better Impact on Plant Operation", Presented at the IAEA Technical Committee Meeting on "User Requirements for Decision Support Systems", Vienna, Austria, 1988 November/December.

8. B. Wahlstrom, "On the Design of Decision Support Systems", Presented at the IAEA Technical Committee Meeting on "User Requirements for Decision Support Systems", Vienna, Austria, 1988 November/December.

9. D. Woods, Ohio State University, Private communication, 1988 August.

10. H. Hofmann, "Cockpit Concept: Small and Simple", Nuclear Engineering International, p 43-44, 1989 July.

11. "Design for Control Rooms of Nuclear Power Plants", International Electrotechnical Commission Report, IEC 964, 1989 March.

12. L.R. Lupton, R.A.J. Basso, L.L. Anderson and J.W.D. Anderson, "Expert Systems Use in Present and Future CANDU Nuclear Power Supply Systems", Proceedings of the EPRI Conference on Expert Systems Applications for the Electric Power Industry, Orlando, Florida, 1989 June, (AECL-10073 to be published).

13. R.A. Olmstead, "Safety Aspects of the CANDU Man/Machine Interface", Presented at the IAEA Workshop on Safety of Nuclear Installations of the Next Generation and Beyond, Chicago, IL, 1989 September.

14. W.E. Gilmore, "Human Engineering Guidelines for the Evaluation and Assessment of Video Display Units", NUREG/CR-4227, 1985 July.

15. K. Boff, L. Kaufman and J. Thomas, "Handbook of Perception and Human Performance", Wiley Interscience, 1986.

16. R.A. Olmstead, J. Pauksens and W. Goddyn, "New Approaches to Alarm Annunciation for CANDU Power Plants", Proceedings of the 1989 Canadian Nuclear Society Annual Conference, Ottawa, Ontario, 1989 June.

17. Y. Fujita, "Improved Annunciator System for Japanese Pressurized-Water Reactors", Nuclear Safety, (30), pp 209-221, 1989 April.

18. J. De Kleer and J.S. Brown, "A Qualitative Physics Based on Confluences", Artificial Intelligence (24), pp 7-83, 1984.

19. R. Davis, "Diagnostic Reasoning Based on Structure and Behaviour", Artificial Intelligence (24), pp 347-410, 1984.

20. H. Storey, B.K. Patterson, A.R. Johnson and D.L. Stafford, "A Computerized Monitoring System for Emergency Operating Conditions at the Point Lepreau Generating Station", Presented at the 1988 Canadian Nuclear Society Annual Meeting, Winnipeg, Manitoba, 1989 June.

21. A.R. Johnson, B. Patterson and W. Pilkington, "Man-Machine Interface Improvements for Emergency Operating Procedures at Point Lepreau", Proceedings of the IAEA Specialists' Meeting on Man-Machine Communication for Emergency Operation in Nuclear Power Plants, Schliersee, F.R.G., 1989 October.

22. Final Report of the Joint Utility Task Group on Emergency Operating Procedures, CANDU Owners Group, 1987 June.

23. Emergency Operating Procedures Standards for Canadian Nuclear Utilities, Revision 0, Prepared by the Joint Utility Task Group, CANDU Owners Group, 1987 June.

ISSN 0067-0367

To identify individual documents in the series we have assigned an AECL- number to each.

Please refer to the AECL- number when requesting additional copies of this document

from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada
K0J 1J0

Price: A

ISSN 0067-0367

Pour identifier les rapports individuels faisant partie de cette série nous avons assigné un numéro AECL- à chacun.

Veuillez faire ment' n du numéro AECL- si vous demandez d'autres exemplaires de ce rapport

au

Service de Distribution des Documents Officiels
L'Energie Atomique du Canada Limitée
Chalk River, Ontario, Canada
K0J 1J0

Prix: A

3266-89