

Design Principles for CANDU Control Centres

E.C. Davey and M.P. Feher
Control Centre Technology Branch
AECL, Ontario, Canada KOJ 1J0

Abstract: CANDU control centres must meet design goals in the areas of licensibility, capital, and operations, maintenance and administration (OM&A) costs. The principles and requirements associated with the licensibility (i.e., safety) and capital cost goals have been well specified in regulatory and AECL/utility project design practice for some time. However, the principles and requirements associated with plant operability and maintainability goals have evolved with utility operations experience and an improving understanding of the role of humans and automation in supervisory control systems.

This paper summarizes recent work to document design principles for CANDU control centres based on current CANDU utility operations experience, Canadian and international design standards, and supervisory control practice in nuclear and similar environments. Principles associated with plant operability are emphasized since principles in this area have been less well documented for use by designers in past practice.

Keywords: Nuclear power plant, CANDU, control centre, design principles, operability.

I. INTRODUCTION

The basic goals, principles and requirements for the design of CANDU control centres were established in the early 1970's. Plants constructed since then have, for the most part, retained the same basic design. However, several factors have led to the need to re-examine control centre requirements for future projects, both new plant designs and retrofits. These factors include:

- evolving utility operational requirements,
- changing roles and responsibilities of operations staff,
- an improved understanding of operational issues associated with supervisory control,
- an improved understanding of human error in operational situations, and
- opportunities for improved plant performance through the application of new and/or replacement technologies.

The basis for a control centre design can be specified by statements of design goals, principles and requirements. Design goals are statements of key objectives a control centre design must satisfy to meet overall plant needs. Principles describe preferred operational practices or features a control centre should embody in support of design goals. Requirements are specific statements of objectives a design must satisfy to be compliant with design goals and principles.

II. BACKGROUND

A. Design Goals

All aspects of a control centre design should be traceable to fundamental design goals. CANDU control centres must meet design goals in three primary areas:

- Safety - Licensibility

The control centre should be designed to support the operation of the plant safely in all operational states to maintain safety of the public, environment and the facility staff. The control centre must be licensible and be able to maintain licensibility over its intended life.

- Implementation Costs - Capital Cost

The control centre should be designed to minimize the cost of design, procurement, construction, and commissioning (including the costs of equipment and schedule). While the intent is to minimize capital cost where possible, the economic viability of any design or design change will be determined by balancing the economic benefits of specific control centre features in terms of improved production and reduced OM&A costs against the capital costs of implementation and ongoing cost of maintenance.

- Operability/Maintainability - Production and OM&A Cost

The design of the control centre should:

- provide an assignment of functions that effectively utilizes operator and system capabilities to achieve operational objectives,
- ensure the availability of plant functions when they are needed,
- provide for the planning and scheduling of maintenance and testing based on plant performance, and permit necessary system/equipment maintenance safely, quickly, and cost-effectively, and
- minimize the cost of operating and maintaining the plant.

B. Role of Design Principles

Designers employ design goals to establish a direction for, and as a means to assess, the overall effectiveness of a specific design. However, design goals by themselves are generally insufficient in specifying all intended aspects of design intent. Statements of design principles can serve to further specify the behaviours and features a design must support, and the manner in which specific design goals are to be achieved. Thus statements of principles can act as effective means to further express design intent to assist in the development and interpretation of specific design requirements.

C. The Strategy of CANDU Plant Control

CANDU plants employ both humans and automation as controlling agents for successful and safe plant operations. Thus, an understanding of the accepted roles for both controlling agents is fundamental to a discussion of specific control centre design principles.

The Role of Operators

CANDU plants are designed and operated with the understanding that human operators are ultimately responsible as licensed authorities for plant safety, and as employees for the productive operation of the plant. In this role, human operators plan, organize, direct plant operations, and configure automated systems to achieve operational objectives. This requires that operators be supported in their roles as system supervisors, intervenors, and manual controllers, where appropriate.

The control system design for CANDU plants permits the plant to be maneuvered from one operating region to another with little need for human control action beyond power setpoint changes. While the CANDU approach to computerized plant control has been very successful and safe, process disturbances can result in highly dynamic and not fully predictable behaviour of plant processes and systems.

Plant automation may also fail in unpredictable ways. Minor system or procedural anomalies can cause unexpected effects that must be resolved in real-time by human intervention. The combination of several of these anomalies can lead to complex plant responses, that are difficult to fully predict and provide solutions for in design. Consequently, the human's role in real-time state interpretation, intervention, diagnosis and restoration remains essential.

Though operators are far from perfect sensors, decision-makers and controllers, they possess three invaluable attributes [1]:

- excellent detectors of signals in the midst of noise,
- effective ability to reason in the face of uncertainty, and
- abstraction and conceptual organization of information.

Thus, operators provide to the CANDU system a degree of flexibility that can not now, and may never, be attained by

automation. They can cope with failures not envisioned by system designers. They are intelligent; they possess the ability to learn from experience and thus the ability to respond quickly and successfully to new situations. Automation can not do this except in narrowly defined and well understood domains and situations. Thus, the CANDU system has been made robust by the ability of humans to:

- recognize and bound the expected,
- cope with the unexpected, and
- innovate and reason by analogy when previous experience does not cover the immediate situation.

These unique human attributes are compelling reasons for the central and commanding position the human operator plays in the CANDU system.

The Role of Automation

Automation plays an essential role in the successful performance of CANDU plants. The purpose of automation is to perform monitoring, controlling and compensation activities under the direction of the human plant operators and in support of plant operational objectives. The key attributes of automation that have contributed to the success of the CANDU system are:

- vigilant and comprehensive monitors of plant process and equipment conditions,
- accurate and responsive controllers to changing plant conditions,
- reliable production and safety performance between planned service intervals,
- tolerant of individual equipment failures through the automatic detection and substitution of redundant and/or secondary functionality or placement of failed equipment in a safe state on the failure of key primary functions, and
- effective prevention and mitigation of human operating errors through control interlocks and control of permissible operating setpoint ranges.

For automation to be effective in this supporting role, there must be a good means of communication between the automation and the plant's human operators. For example, the operational intent of the human operators must be communicated to automated functions and the state, performance and health of automated functions must be communicated back to human operators. Any uncertainties or breakdown in this communication can lead to operational situations where the human operators and automation may not be working cooperatively to achieve common goals. The control centre interfaces and field panels serve as the primary means for effecting this communication.

III. DESIGN PRINCIPLES

Principles have been established for each of the three CANDU plant design goals. Principles associated with the safety and implementation cost design goals will not be

discussed in this paper because they are extensively documented in industry guides, standards and practice.

For the operability/maintainability goal, control centre principles have been established in the following areas:

- available plant functionality,
- plant operability,
- plant maintainability,
- accommodation of human capabilities and behaviours,
- supervisory control,
- automation,
- incorporation of operating experience, and
- transfer of design information to users.

The balance of this paper will outline some of the key principles that we have adopted in three of these areas.

A. Accommodation of Human Capabilities and Behaviours

Principle: Design to maximize the effectiveness of human attention.

Human attention is an enabling resource that permits many other cognitive processes. Overall attentional demand has limitations and requirements that should be heavily weighed during the design process to ensure the information demands placed on operators can be readily accommodated.

Principle: Design to support human behaviours for visual scanning and sampling of information displays.

In supervising plant operation, operators periodically scan and sample plant information displays. The frequency with which information displays are monitored is a function of:

- the operational objectives,
- the desired plant state,
- the degree of departure and rate of change of the actual plant state from the desired plant state, and
- the operator's knowledge of any discrepancy between desired and actual plant state.

Some monitoring behaviour is directed by immediate operational objectives and the current understanding of plant state in support of specific tasks. For such cases, information salience and the alerting of operators to departures from desired plant state by annunciation systems, play a pivotal role in directing operators attention to the monitoring task. In other cases, monitoring of information may be opportunistic based on information accessibility and salience.

Principle: Design to minimize the demands on short term memory.

Once a stimulus has been perceived, humans use short-term memory (STM) to store the sensory information before further processing can occur. Storage in STM is capacity and time limited, thus interfaces should be designed to minimize

the dependence on STM for retention of critical information by providing external representations of this information.

Principle: Design to support the goal-based behaviour of operators.

Human operators are assigned the prime responsibility for all aspects of plant operation. All decision-making performed by operators is based on a set of safety and production goals established by licensing officials and members of plant management. Given a specific plant status, operator task responses are structured so as to achieve these goals. Thus this goal-based behaviour should be supported in the design.

Principle: Design to avoid, reduce, prevent and accommodate human error.

A number of human characteristics lead to error initiating behaviours. In practice, most of these errors are detected and corrected by the individual committing them before the consequences of the error are important. Thus, information systems should be designed to assist operators in detecting errors, and controls should provide protection against inadvertent operator actions that can have large consequences.

B. Supervisory Control

CANDU operational practice assigns the control room crew full responsibility and authority to control all aspects of plant operation. Yet to achieve specific safety and production requirements, most middle and lower level plant functions are highly automated. Even so, functions are rarely allocated exclusively to an operator or automation. In most cases, the performance of each function is shared on some basis. To carry out their responsibility and meet production and safety goals, operations staff must be supported by information and control systems that allow them to actively supervise a highly automated process system, be responsively informed of off-normal conditions, and have the capability to intervene and substitute compensatory functions if automated functions are inadequate or should fail. Thus, successful supervisory control requires the co-operative control and monitoring of plant functions by both operators and automation.

The allocation of functions to humans or automation can be grouped into three distinct levels: control, information, and management [1]. CANDU plants have typically focused on automation of control through the use of central control computers and microprocessor driven control loops. Little automation of the information has been established in past implementations and virtually no automation of planning functions has been attempted. However, current changes to existing CANDU control centres dictated by both safety and production efficiency concerns are leading to the introduction of many examples of information and management automation. It is anticipated that the operational benefits of increased plant automation in the next ten years will be realized by further automation of information and work management systems in support of operator tasks.

The following design principles for supervisory control adapted from the work of Charles Billings [1] have been adopted to guide the development of future human-machine systems for CANDU control centres.

Principle: The human operator must be in command.

To be in command of the plant, the operator must be involved in plant operation. To be involved, the operator must have an active role, whether the role is to control the plant directly or to manage the human and machine resources to which control has been delegated.

Principle: To command effectively, the human operator must be informed of plant state and trends.

Without information about the conduct of operation, involvement becomes random. The operator in command must have a continuing flow of relevant information concerning the state and progress of the operation of the plant to maintain involvement with it.

Principle: The human operator must be informed about and be able to monitor the automation.

The need to be informed about the state of automated systems and the ability to monitor the automated systems is necessary both to permit the operator to remain "on top of" the situation and confirm that the automated functions are performing as expected. Automated systems are fallible and can be expected to fail in unpredictable ways at unpredictable times.

Principle: The automation must be predictable.

The operator must be able to evaluate the performance of automated systems against an internal model formed from the observed normal behaviour of the systems. Only if the systems normally behave in a predictable fashion can operators be expected to rapidly detect departures from normal behaviour and thus recognize problems when they occur.

Principle: The automation must be able to monitor the human operator.

Operators are not infallible either, and their failures may likewise be unpredictable, even though a good deal has been learned about human behaviour and error modes. For that reason, it is necessary that the automation monitor the operator and intervene as appropriate, where operator actions could lead to large safety or production consequences.

Principle: The operator and the automation should have knowledge of each others intentions.

Cross-monitoring can only be effective if the monitor understands what the operator of the monitored system is trying to accomplish. To obtain the benefits of effective

monitoring, the intentions of the human or the automated system must be known and communicated.

C. Automation

This section extends the previous discussion by outlining specific principles for the design of automated functions in support of co-operative human-machine systems. Four groups of principles are described: general, control, information and management automation principles corresponding to the levels of automation previously described. Principles in the 'general' category apply to all three levels of automation.

General Automation Principles

Principle: Design so that automation does not remove the operator from the command role.

The increasing application of automation in nuclear plants has the potential to remove the operator from the chain of command in some operational situations. To ensure the operator remains in command, where safety permits, automated systems should be designed to inform the operator of impending changes to plant operating configuration and the likely consequences, and require operator consent or acknowledgment of the change before action to implement the change is taken.

Principle: Design so that automation maintains and enhances the operators situation awareness of the plant.

A key task of human operators is to maintain an awareness of the state of the plant. This awareness is called situation awareness (SA) in the aviation and supervisory control fields. Plant systems are designed to provide operators with information to help them determine the current state of the plant, and also to help predict changes in plant state. Because SA is a dynamic process and plant systems are complex, there is a need to support communications between the plant systems and the human operator, so that accurate SA is always maintained.

Principle: Design so that automation is comprehensible and easy to operate.

Automated systems that are comprehensible and simple to use will promote use and impose few memory burdens on users who must configure them. The memory burdens (e.g., information on modes and interactions) imposed on operators by complex systems can be considerable.

Principle: Design with the assumption that operators will be reliant on automated systems.

Once operators have become familiar and developed trust in particular automated functions, they will become increasingly reliant on their use. As a consequence, infrequent problems or failures that may develop with such systems may not be detected promptly as operator's suspicions concerning the system may be lowered based on long-term

successful experience. Special consideration should be given in design to ensure high visibility for failures of automated systems and to provide means for operators to verify and confirm the correct functioning of automated functions.

Principle: Design so that operators are involved in operation, requiring of them meaningful and relevant tasks, regardless of the level of automation utilized.

High levels of automation have the potential to decrease operator involvement in overall plant supervision and control. Operator involvement can be maintained and promoted by designing automated systems so that their internal operation is readily observable, and changes in modes and relationships are effectively communicated and approved by operators as part of regular operation.

Principle: Design so that options are available to operators to transition gracefully to backup functions.

In many cases, operators are the prime means available to intervene and select a compensatory function when an automated function fails. To minimize the impact of the initial failure and the potential for additional disturbance in transitioning to a compensatory function, automated systems should be designed to fail gracefully and options for function replacement should be chosen that are readily configurable to match process requirements and operator capabilities.

Principle: Design so that training in the use automation is simple.

A key determinant in the successful application of automated systems is the availability and effort involved in training operators in system use. Systems that are simple to train and learn promote the full use of their capabilities.

Control Automation Principles

Principle: Design so that control automation will not perform or fail silently.

Operators monitor plant processes and systems using several monitoring behaviours. During normal operation, they are expected to perform many duties and so can not be expected to be continuously aware of the status of all automated systems moment to moment. Between periodic samples of plant status, plant processes and systems are assumed to be performing normally unless a specific indication indicates otherwise. Automated systems should communicate their status and changes in function to supervising operators to ensure failures will not go unnoticed.

Principle: Design so that control automation is limited in its authority.

Control automation must always work in support of operator goals. Control automation should not be designed to work independently of the operator, or working to achieve

goals that are inconsistent with operator objectives and overall plant safety.

Principle: Design so that operators have the authority to override normal operating limits when required to re-establish or preserve plant safety.

As the final authority for plant operation, operators must have the capability to exercise the full-range of control over plant functions if needed to accomplish safety objectives. Thus, automation that may provide administrative or interlock controls to restrict the normal operating envelope must be capable of being over-ridden in an emergency to support safety-directed operator responses.

Information Automation Principles

Principle: Design to present information in situational context.

Information should be presented in a manner consistent with the current plant operating situation. As the plant situation changes, the relevance and importance of specific information will change and the presented information should reflect this.

Principle: Design to provide direct support for operator tasks.

Information should be designed to directly support operator tasks to minimize the effort to use it. This can involve the organization of plant status information in a manner consistent with task use and the inclusion of information attributes (e.g., indications of acceptable ranges and operating limits) that assist in information interpretation and use.

Principle: Design to differentiate between valid and invalid indications of process conditions.

Information systems should be designed to confirm the validity of information that is sensed prior to presentation to operators for decision-making use. This can substantially simplify plant monitoring, disturbance analysis and fault detection tasks. Signal validation techniques based on a number of comparison and correlation techniques between plant parameters are capable of making validity determinations on a reliable basis.

Management Automation Principles

Principle: Design to permit use of information from different systems.

Operators are expected to work with and share information from several control room systems. To minimize the secondary burdens of mental integration of information, manual re-entry of data, or transcription of information from one system to another, systems should be designed to

facilitate information integration and exchange based on operator needs to do so.

Principle: Design to support the additional operator tasks beyond direct supervision and control of the plant.

Operators perform several tasks in addition to those associated with direct supervision and control of the plant. Tasks associated with work protection and management, maintenance, resource assignment, reporting, testing and routine inspections occupy a large part of the operators shift time. Current CANDU stations have been fielding and are developing a number of information system applications that are designed to provide additional support for these tasks.

IV. FUTURE PRINCIPLE DEFINITION

Within the past few years there has been renewed interest and emphasis in the importance of control centre operations and in particular the preferred behaviours of supervising staff. Recent workshops conducted by the Institute of Nuclear Plant Operations (INPO) [2] and Ontario Hydro [3] have focused on discussing key control centre functional and performance issues. We have been following and participating in the discussion of these issues and are beginning to see the emergence of additional control centre principles related to plant operability. Examples of these principles include:

Principle: Structure the workplace and responsibilities so that key individuals can provide undistracted supervision of plant operations.

Analysis of accidents in a number of domains has highlighted the risk to personnel and environmental safety and plant investment that temporary loss of supervisory oversight can result in. To minimize the potential of such incidents in the future, control centres should be designed to support those individuals in supervisory oversight roles.

Principle: Structure displays and decision-making aids to promote conservatism in control room decision-making and operating actions.

To maintain operating margins, protect plant investment and reduce the creation of latent event initiating or contributory factors, operating actions must be relevant for the operating situation and well planned. Conservative operating behaviours promote the achievement of these objectives and control centre displays and controls should be designed to support this practice and reduce the need to 'cut corners' in the face of competitive production pressures.

V. CONCLUSIONS

This paper has summarized recent work to document design principles for CANDU control centres. The documentation of these principles is part of a current effort to establish a more complete and operationally-based design basis for future control centre improvement initiatives. The principles outlined in this paper are currently being applied to guide the conceptual design of the next generation of

CANDU control centres as well as assist with ongoing station improvement projects. AECL is continuing to refine the definition of these principles in support of achieving control centre facilities that better support utility operating objectives.

VI. ACKNOWLEDGMENTS

Many people have assisted the authors in understanding and documenting principles for CANDU control centres based on current practices and future operational needs. The authors gratefully acknowledge the experiences and insights shared by utility and design colleagues within the CANDU community who have assisted us in this task.

VII. REFERENCES

- [1] C.E. Billings, *Human-Centred Aircraft Automation: Principles and Guidelines*, NASA Technical Memorandum 110381, NASA Ames Research Centre, 1995.
- [2] Z.T. Pate, "The Control Room," *Proceedings of the INPO 1995 CEO Conference*, Institute for Nuclear Power Operations, Atlanta, Georgia.
- [3] B. Strickert, "Safety Culture and Control Room Implications," *Summary Report of the Control Room Operations Workshop*, Ontario Hydro report N-REP-22603-0136-R00, Ontario Hydro, 1996.

VIII. BIOGRAPHIES



Eric Davey is a human factors engineer with the Control Centre Technology Branch at AECL's Chalk River Laboratories. He has over twenty years of nuclear plant experience in operations analysis, instrumentation and computer systems development and control centre applications. For the past ten years, he has worked closely with staff from several CANDU utilities to develop and evaluate control centre improvements to better support Operations staff in both normal and abnormal plant conditions. Eric received his formal education at the Universities of Toronto in Electrical Engineering (B.A.Sc., 1972) and the New Brunswick in Biomedical Engineering (M.Sc.E., 1974).



Mark Feher is a human factors engineer and the Section Head of the Human Machine Systems Development Group for the Control Centre Technology Branch at AECL's Head Office. He has over fifteen years of nuclear plant experience with both Canadian and United States utilities and regulators. For the past four years, he has led several project teams in developing improved annunciation systems

and operations centred design approaches for CANDU control centres. Recently he has been appointed lead technical responsibility for all AECL control centre development projects. Mark received his formal education at the University of Toronto in Industrial Engineering (B.A.Sc., 1982).