

A DESIGN BASIS FOR THE DEVELOPMENT OF CANDU CONTROL CENTRES

M.P. Feher, E.C. Davey, and L.R. Lupton
Control Centre Technology Branch
AECL, Chalk River Laboratories,
Chalk River, Ontario, Canada, K0J 1J0
(613) 584-3311

M.J. MacBeth
Control Engineering, CANDU 9
AECL, 446A 2nd Ave. North
Saskatoon, Saskatchewan
Canada, S7K 2C3
(306) 665-5102

I. ABSTRACT

The basic design for current CANDU control centres was established in the early 1970's. Plants constructed since then have, for the most part, retained the same basic design. Several factors have led to the need to re-examine the CANDU control centre design for future projects. These factors include the 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, the opportunity for improved plant performance through the introduction of new technologies, and evolving customer requirements. This paper describes the design process for the development of control centres to be implemented in CANDU new plants beyond the year 2000, including the CANDU 9 product.

II. INTRODUCTION

The basic design of current CANDU control centres was established in the early 1970's. Plants constructed since then have, for the most part, retained the same basic design. To meet evolving client and regulatory needs, AECL has adopted an evolutionary approach to the design of future control centres. That is, the design will be enhanced to incorporate feedback from existing stations, reflect the growing diversity in the roles and responsibilities of the operating staff, and ensure that plant capital and operations, maintenance and administration (OM&A) costs are reduced through the appropriate introduction of new technologies. Underlying this approach is a refined engineering design process that cost-effectively integrates operational feedback and human factors engineering. This paper describes the design process as it is being used for the development of the CANDU 9 control centre, as well as for future control centres to be implemented beyond the year 2000.

Key elements of the design process are described in the following sections and cover the steps listed below.

- Specify design goals and principles.
- Establish the design basis.
 - Define operational, functional, and maintenance bases.
- Design the plant, including the control centre.
 - Establish requirements and designs.
 - Assess the operational impact of requirements and designs.
 - Evaluate the design.
- Provide support for the customer utility.
 - Transfer information for training and procedure development.

III. DESIGN GOALS AND PRINCIPLES

Three design goals have been identified to ensure designers meet product needs in the areas of licensability, and capital and OM&A costs.

- Safety - The control centre should be designed to support the operation of the plant safely in all operational states to maintain safety of the public and the facility staff. The control centre must be licensable and be able to maintain licensability over its intended life.
- 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).
- Operability/Maintainability - The design of the control centre and the design process 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.

The first two design goals are effectively addressed by the existing AECL design process. The third goal has resulted in a number of enhancements to the process and is the subject of the remainder of this paper.

The CANDU plant is designed such that the human operators are ultimately responsible as licensed authorities for its safe operation, and as employees for the productive operation of the plant. This requires that operators be supported in their roles as system supervisors, intervenors, and manual controllers, where appropriate. In recognition of this important role for humans in overall plant operation, design principles have been established to address their needs. Principles are statements that establish the need to define requirements and design features, and to guide designers throughout the design process. The following sub-sections present a summary of the principles established for CANDU control centre design.

A. Design for Available Plant Functionality

A function is defined as the proper action that a person, system, or structure takes to fulfill a goal.

Principle: Design to support operators in their need to know and understand:

- the plant functions to be monitored and controlled, and their performance goals,
- the relationship of each function to the primary safety and production goals,
- the relationship(s) of each function to other functions,
- the applicable state(s) of each function for each operating region of the plant,
- the initiating, on-going, and terminating conditions that define the bounds of operation for each function,
- the performance measures and criteria to be used in judging function performance, and
- the control and information needs for operators and automation to jointly perform tasks for each function in all operational situations.

B. Design for Plant Operability

Principle: Design to support operators within the overall context of plant operation, including:

- the fundamental operating regions of the CANDU, as based on process parameters and equipment configuration,

- the operational strategies used by plant staff to maintain stable operation, monitor the success of the automation, or intervene to maneuver the plant to desirable operating regions, and
- the roles and responsibilities of plant staff in applying applicable operational strategies to operating regions.

Principle: Design to support specific operator tasks in the areas of:

- overview awareness,
- process awareness,
- process control,
- manual control,
- process and process control diagnosis and planning,
- fueling the reactor,
- station operation planning and administration,
- equipment testing, and
- team interaction for common operational goals.

C. Design for Maintainability

Principle: Design to support the information and control needs of maintenance-related staff including:

- the presentation of information to operators, maintainers, and/or system responsible engineers regarding the health of a given system or component to identify root causes of failures or performance degradation (to the extent possible),
- support for the required testing for availability and performance, and
- support for the replacement or repair of systems/equipment/components as appropriate.

D. Design for Humans

Principle: Design for the cognitive capabilities of human operators including consideration for:

- human attention,
- demands on short term memory,
- storing and retrieving information from long term memory,
- known models of human decision-making,
- situation awareness, and
- the goal-based behaviour of operators.

Principle: Design for the ergonomic/physical capabilities of human operators, covering:

- anthropometric standards,
- human sensation and perception, and
- environmental limitations.

Principle: Design for supervisory control and plant automation.

The allocation of functions to humans and automation can be grouped into three distinct levels: control, information, and management/planning (Billings 1991). CANDU plants have typically focused on automation of control through the use of central control computers and microprocessor driven control loops. The CANDU 9 will begin to introduce more information automation and potentially some automation of planning functions for operating teams. Examples of automation of information that could be considered include: dynamically generated displays (i.e., alarm response procedures) based on the current plant operating region; dynamically linked display suites, or; sequence of control actions grouped into single control actions. It must be remembered that the licensed operator is responsible for the safety and production performance of the plant and therefore must be considered in the design and use of automation.

The following principles for automation (Billings 1991) are to be considered in the design:

- the human operator must be in command.
- to command effectively, the human operator must be informed of plant state and trends,
- the human operator must be able to monitor the automation,
- the automation must be predictable,
- the automation must be able to monitor the human operator, and

- the operator and the automation should have knowledge of each others intentions.

Principle: Design to address human error by:

- avoiding design features that are known to promote human error, for example:
 - lack of differentiation of controls,
 - lack of feedback on automation modes and states,
- reducing the probability of human error, for example:
 - providing feedback,
 - using coding to aid and constrain choices,
 - unambiguous labeling and identification,
- preventing the consequences of human error through human or automated error detection and intervention, for example:
 - mode-based interlocks,
 - human or automated data entry checking, and
 - presenting to operators the predicted results of the given instruction prior to implementation or with sufficient time for correction, and
- accommodating human error,
 - where no alternative design feature can be employed to reduce the probability of error, and the likelihood of error is considered unacceptable, then the designer must choose additional design features or functions that will accommodate the error, including
 - automatic reactor power reductions, and
 - automatic special safety system actions.

E. Design to Incorporate Operating Experience

Principle: Draw on the evolving CANDU and international experience base to identify relevant operational and design issues that need to be addressed and identify options for improving the control centre design in such areas as:

- operational requirements,
- operational strategies and practices,
- human cognition,
- support for decision-making and control actions,
- equipment, facilities, and layout,
- design philosophies, and design approaches and processes.

F. Design for Transfer of Information to Client Utilities

Principle: Document the design to support the transfer of information and technology to customer utilities to aid in the development of training programs, and operating and maintenance procedures.

IV. THE DESIGN BASIS

The design basis is a body of information that captures the functional, operational and maintenance bases for a given plant.

All “new” nuclear power plant designs are the product of evolution. Even the most advanced designs have evolved from past practice and design. AECL believes strongly on building on past successful practice and is most definitely using an evolutionary model for design. In order to evolve, a baseline for evolution is required. The model presented in Figure 1 presents the process of evolving from the reference plant design basis to the new plant design basis.

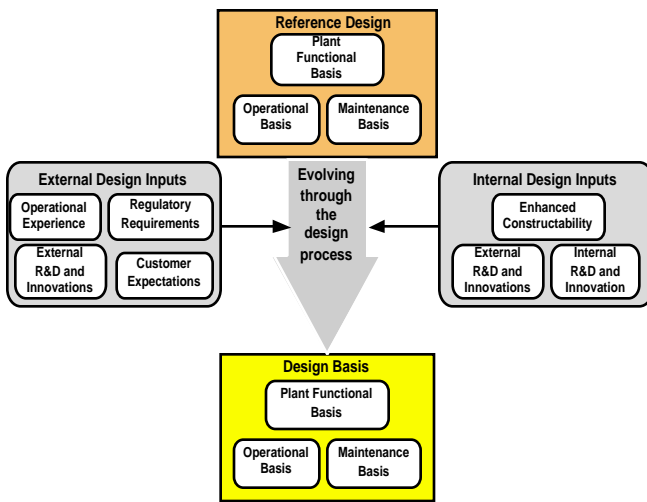


Figure 1: Evolving the design basis.

This process is being used in the design of the new CANDU 9 control centre, an evolution from the CANDU 6 plant combined with the functionality from the Darlington station of Ontario Hydro. As well, the approach is being applied to the design of an advanced CANDU 6 plant for future sales.

A key part of the evolution of the design is the feedback from the experiences of existing plants. AECL project procedures for the preparation of requirements and design descriptions require operating experience reviews. Feedback into the design has been formalized to include:

- analysis and recommendations from a Design Feedback Committee that includes representatives with experience in operations and maintenance from existing operating stations, as well as staff from design and R&D disciplines,
- interviews and contacts with existing CANDU station staff,
- reviews of station design change notifications, and
- reviews of the CANDU Owners Group databases that include significant event reports and engineering change proposals.

The following sub-sections present each of the key elements of a design basis.

A. Functional Basis

The functional basis establishes the processes and equipment available to support operational goals and objectives. The material is produced by performing a function analysis that:

- is part of a systematic approach to design,
- establishes a description of the plant functions that provide compliance with utility production and regulatory principles and requirements,
- establishes the inter-relationships between plant functions,
- describes the degree to which the performance of each function is shared and exchanged between the control room team and automation in all phases of plant operation,
- records the objectives, performance requirements, and constraints of the plant,
- defines the roles and information needs of humans and automation in sharing function performance,
- records the attributes for the health of a given system or component in support of monitoring, diagnosis, and prediction for assessing system performance and providing input to the maintenance planning process,
- provides a framework to promote completeness in analysis by system designers, and
- provides a cost-effective means for communication between design teams, operations, maintenance, and training.

B. Operational Basis

The operational basis contains a description of the domain of operation and represents the context(s) in which operators make decisions and perform tasks given the plant functions available to them. In doing so, the operational basis:

- establishes the context to design for operational tasks,
- provides a high level task description of roles and responsibilities (typically information needs based on responsibilities), and
- provides a framework to promote completeness of the design in support of operations.

The operational basis includes definitions of:

- the fundamental operating regions of the plant based on process parameters and equipment configurations (see Figure 2),
- the operational strategies used by plant staff to maintain stable operation, to monitor the success of automation, or to intervene to maneuver the plant to desirable operating regions (see Figure 3), and
- the roles and responsibilities of plant staff in applying applicable operational strategies to the various operating regions.

The term “operating region” refers to an envelope that characterizes plant operation, rather than a single finite operating state. Each operating region can be characterized by combinations of ranges of specific plant parameters and configurations of plant functions and equipment.

The operating regions for a CANDU plant can be grouped into long-term stable regions, time-limited stable regions, and transitional regions. Figure 2 presents a summary of the operating regions defined for a CANDU plant.

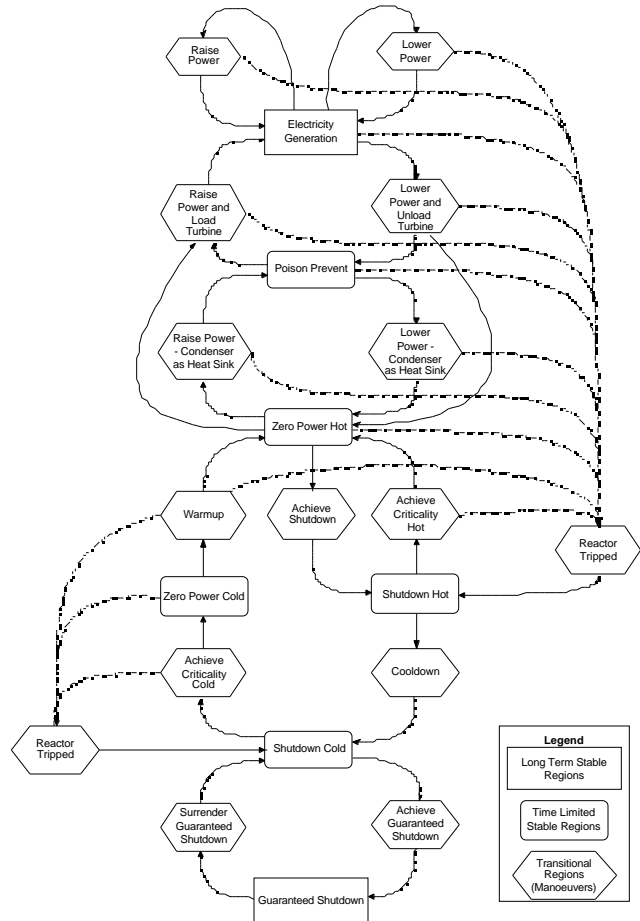


Figure 2: Operating regions of a CANDU plant.

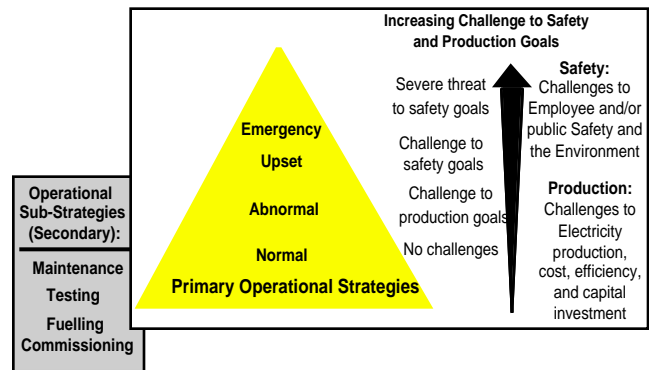


Figure 3: Operational strategies of a typical CANDU.

C. Maintenance Basis

The maintenance basis provides a framework to support system designers in establishing maintenance related design requirements and design features. As such, the document establishes:

- maintenance goals and principles for design, and
- assumed maintenance strategies and process including
 - maintenance-related tasks such as
 - planning/scheduling,
 - historical process analysis,
 - data access and collection,
 - data visualization, performance analysis and diagnosis,
 - reporting and documentation,
 - historical event analysis,
 - operational/on-line monitoring and analysis,
 - system testing,
 - implementation,
 - work package definition,
 - work control,
 - component/system maintenance tasks,
 - communication/co-ordination, and
 - maintenance personnel roles and responsibilities.

V. THE DESIGN

The process of designing a control centre is complex due to the number of individual systems that must come together in the room to provide an integrated interface to the plant. The following sub-sections summarize the approach taken to incorporating human factors into the design process in a cost-effective manner.

A. Establishing Requirements and the Design

Figure 4 summarizes the relationship between elements of the design basis and the resultant requirements for the control centre.

When designing the control centre the requirements and the design basis are combined with more detailed task analyses and specific design guides to complete the design. The following two sub-sections briefly describe the use of task analysis and design guides.

1. Task Analysis

A tasks analysis is highly related to a function analysis. A function analysis describes the functions available to operators to control and maneuver the plant. A task analysis describes the sequence and timing for combining the functions to complete a given task. A series of tasks are required, in series and/or in parallel, to fulfill an objective or goal.

The objectives of task analysis are to:

- identify and organize operator tasks to achieve a specific operational goals,
- establish the inter-relationships and sequence between tasks in support of the operational goals,
- describe the operational properties of each task including their assignment to specific personnel, and
- describe the information needs of operators who are to perform the defined tasks, and
- to provide the information in an organized framework to designers of control rooms, procedures and training programs.

2. Design Guides

Design guides help to maintain consistency and continuity across all interfaces within a plant as design requirements are translated into implementation features. Example of topics covered by control-room related design guides include:

- labeling and identification,
- information coding conventions - colour, flashing, audibles, etc.
- selection/design of graphic display objects,
- display navigation,
- panel layouts and device selection,
- input to function and task analyses by process and control designers, and
- design features for maintenance.

B. Assessing the Operational Impact of the Requirements and Designs

Design documentation is reviewed by the control centre and human factors team to assess:

- the impact of the design on the operational model (described in the operational basis),
- the allocation of the functions to humans and automation for individual systems, and
- the suite of integrated functions and their allocations.

The results of the assessments are discussed with process and control system designers to establish changes to the process or control designs, and/or to the operational, functional and maintenance bases as required.

C. Evaluating the Design

The control centre design will be evaluated by a variety of methods, including the use of a full scale mock-up of the control room driven by a simulator. The following approach will be used for the evaluations:

- early evaluations will be performed to provide feedback to design at each iteration,
- evaluation will be performed within an operational environment with reasonable fidelity,
- the evaluation will include realistic replication of staff roles, responsibilities and communication,
- evaluation at different stages of design will apply both static and dynamic models/prototypes as appropriate, and
- evaluation will focus on the impact of design features versus evaluating or demonstrating performance adequacy for specific events.

VI. SUPPORT FOR THE CUSTOMER UTILITY

Inherent in the revised design process is the ability to transfer information to the client utility to support the development of operating and maintenance procedures, and training programs and manuals. Key to this information transfer are the three basis documents plus the task analyses for the specific design.

- The operational and maintenance bases answer:
 - when to do tasks? - operational contexts
 - who performs tasks? - roles and responsibilities based on operating strategies.
- The functional basis answers:
 - what is available to use? - functions available for different operational contexts and their attributes.
- The task analyses answers:
 - how to perform tasks? - sequence and timing of applying functions to meet operational goals.

VII. SUMMARY

This paper has described a design process that is being used for the development of the CANDU 9 control centre, as well as for future control centres to be implemented beyond the year 2000. The process provides a sound basis for evolving future control centres from current operating designs ensuring that plant capital and operations, maintenance and administration (OM&A) costs are reduced.

REFERENCES

- Billings, C.E. (1991). Human-Centred Aircraft Automation: A Concept and Guidelines. NASA Technical Memorandum 103885. NASA, Ames Research Centre.

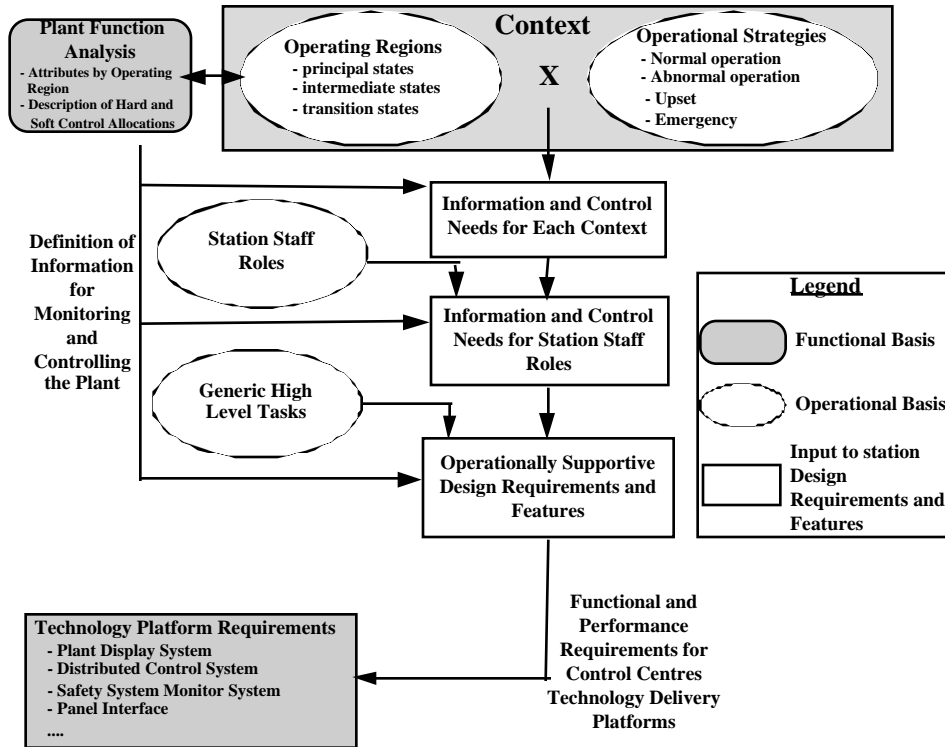


Figure 4: The process of establishing design requirements.