

THE ROLE OF FUNCTION ANALYSIS IN CONTROL CENTRE DESIGN

E.C. Davey and M.P. Feher
AECL, Chalk River Laboratories,
Chalk River, Ontario, Canada, K0J 1J0
(613) 584-3311

ABSTRACT

An essential aspect of control centre design is the need to characterize:

- plant functions and their inter-relationships to support the achievement of operational goals, and
- roles for humans and automation in sharing and exchanging the execution of functions across all operational phases.

Function analysis is a design activity that has been internationally accepted as an approach to satisfy this need. It is recognized as a fundamental and necessary component in the systematic approach to control centre design and is carried out early in the design process.

A function analysis can provide a clear basis for:

- the control centre design for the purposes of design team communication, and customer or regulatory review,
- the control centre display and control systems,
- the staffing and layout requirements of the control centre,
- assessing the completeness of control centre displays and controls prior and supplementary to mock-up walkthroughs or simulator evaluations, and
- the design of operating procedures and training programs.

This paper will explore the role for and cost-effectiveness of function analysis in supporting each stage of control centre design. The development of improvements to next-generation CANDU control rooms will be used as an illustrative context for the discussion. The paper will also discuss the merits of using function

analysis in a goal- or function-based approach resulting in a more robust, operationally compatible, and cost-effective design over the life of the plant than with past practices.

INTRODUCTION

This paper describes the approach being taken and the benefits of applying function analysis in the development of the control centres for the Advanced CANDU plant.

The Advanced CANDU plant represents a class of CANDU plants that are being developed by AECL for utility use beyond the year 2000. To focus its Advanced CANDU design effort, AECL is building on past successful practice and evolving the basic CANDU plant design to meet evolving customer, regulatory and accepted human factors standards and design practices. The conceptual design of the control centres for the Advanced CANDU plant is being undertaken by the Control Centre Technology Branch at AECL's Chalk River Laboratories.

For the purposes of this paper, a 'function' is defined as the proper action that a person, system, or structure takes to fulfill a goal. The functions of interest in control centre development are the operational functions the shift operating team must supervise and control in operating the plant to achieve both safety and production objectives under all possible operating circumstances.

Function analysis is a design activity that is recognized as a fundamental and necessary component in the systematic approach to control centre design and is carried out early in the design process. ^{1, 2, 3} Function analysis is generally recognized to consist of three design activities:

- function identification - the identification and organization of functions and sub-functions necessary to support the achievement of overall plant safety and power production goals,

- function description - the characterization of specific information for each function necessary to support function implementation and usage (e.g., application context and performance attributes), and
- function assessment - analysis of the characterization to either define requirements of the function to meet human information needs, or, to assess the compatibility of the function against human information needs.

We believe that to successfully apply function analysis to control centre design, the approach taken must support the following objectives:

- the organization and description of plant functions should be developed from a plant operations perspective and should be expressed in familiar operational terms,
- an iterative approach to conducting the analysis should be followed that begins with the derivation of primary plant functions necessary to support the achievement of overall plant safety and power production goals and proceeds to successive function refinement and detail,
- the completeness and level of detail provided by the analysis should be sufficient to support the information needs of interface designers, procedure developers and trainers, and
- means should be established to easily and cost-effectively update the analysis to reflect the results of changes in plant design over the lifetime of the design, including the time during operational use.

BACKGROUND

CANDU nuclear power plants are large, complex electrical generation facilities that are operated under computer control. Overall plant operation is supervised from a central control room by human operators using computer displays, and conventional instrumentation and controls.

The basic design for current CANDU control centres was established in the early 1970s. Plants constructed since then have, for the most part, retained the same basic design. Several factors have led to the need to re-examine CANDU control centre design for plants to be built beyond the year 2000. These factors include:

- the changing roles and responsibilities for the 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
- competitive marketing pressures.

THE ROLE OF HUMANS IN CANDU PLANT CONTROL

A fundamental tenet of the operation of CANDU nuclear plants is that human operators are ultimately responsible as licensed authorities for the 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. The resources of the plant control centres are intended to provide the necessary means to monitor the state and performance of plant functions, and effect their control.

Normally, the senior power plant operator (SPPO) and an assistant power plant operator (PPO) are the only two members of the shift crew resident in the control centre on a continuous basis. The SPPO under the direction of the supervisor for the shift, directs and controls all station activities to comply with station safety and production objectives. This responsibility includes:

- Direction for and control of all reactor and electrical generation activities to comply with station safety and production objectives.
- Continual monitoring and control of plant state within authorized safety and production limits.
- Review and authorization of work permits for all inspection, testing, and control activities associated with station operation.
- Communication with shift and station support personnel to schedule, initiate, track, and terminate work in support of station operation.
- Review of completed work reports and determination of the acceptability of the work completed.
- Communication with the utility power distribution control centre personnel to match station electrical production to energy demand needs.

- Preparation of a record of shift activities, and notification of the relief senior power plant operator of the status of the station and work activities.

The control system design for CANDU plants permits the plant to be manoeuvred 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, equipment failures or inappropriate operating actions can result in highly dynamic and not fully predictable behaviour of plant processes and systems.

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

- excellent detectors of signals in the midst of noise,
- can reason effectively in the face of uncertainty, and
- capable of abstraction and conceptual organization.

Operators thus 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 problems.

To support this role for operators, the control centre design must be structured to ensure that the relevant information on plant functions is defined and available in all operating situations.

THE ROLE OF FUNCTION ANALYSIS IN CONTROL CENTRE DESIGN

The Advanced CANDU control centre is being developed using an iterative model that includes:

- development of a design basis,
- creation and evaluation of design concepts,
- continual refinement of the basis and the design using feedback from development and operational experience, and
- support for transfer of validated concepts and design information to existing stations and design groups for station implementation.

We believe that an essential first step in the design of systems is the development of a design basis. The purpose of the design basis is to document the objectives and constraints for the system, and provide a guiding philosophy or framework for the subsequent system design activities. To provide relevant guidance over the lifetime of the system design and use, the design basis must undergo on-going refinement as the design evolves and improves.

The design basis for the Advanced CANDU control centre consists of:

- design goals to be achieved,
- design principles to be applied,
- an operational basis that characterizes plant operation,
- a functional basis that describes the plant functions and their preliminary allocation between humans and automation,
- high level design requirements based on regulatory and customer demands, and plant design constraints, and
- design input from the operating experience of existing CANDUs and supervisory control experience around the world.

A description of the functional basis of the plant is a key part of this design basis and is the outcome of performing a function analysis.

The functional basis consists of descriptions of the plant functions that the shift operating team must supervise and control in operating the plant to achieve safety and production objectives under all possible operating circumstances. These descriptions include:

- the plant functions to be monitored and controlled, and the performance measures and criteria to be used in judging function performance,
 - the applicable state(s) of each function for each operating region,
 - the initiating, on-going and terminating conditions that define the bounds of operation for each function,
 - the relationship of each function to primary safety and production objectives and to other functions, and
 - the roles of humans and automation in controlling and processing information to perform the component tasks for each function.
- a context for the design and description of systems from an operational and human-centered perspectives,
 - a basis for and description of the aspects of plant functions that control centre designers need to integrate into plant control centres,
 - a record of original design intent with which to judge options for design improvement, and
 - a basis for the detailed development of plant operating procedures (i.e., a concise description and representation of how systems, sub-systems, and equipment support multiple plant functions, and the context for their use in operation).

The components of the design basis are related to the functional basis in the following ways. Design goals define the performance objectives from which the purpose of all plant functions are derived. Design principles, establish preferred ways in which plant functions should be implemented to achieve overall design goals. The operational basis establishes the context for operation of plant functions by describing the operating regions (i.e., states) for the plant, the strategies employed to manoeuvre the plant and the roles and responsibilities of staff. High-level design requirements establish the need for specific functions, provide constraints to limit the design choices for implementation, and provide an impetus for changing plant functions as requirements evolve. The input from operating experience provides an additional impetus for change that leads to on-going improvement in plant functions.

The importance of these other components of the design basis to the discussion of function analysis is in the nature of the information required for adequate characterization of each plant function. For example, the needs of operators in a supervisory role and the goals of functions for different operating regions and different operational strategies define the types of information to be collected for each function to support designing to these other aspects of the design basis.

We have found that function analysis is a cost-effective means for documenting plant functionality as well as providing guidance to system and control centre designers because it provides:

- a concise and complete reference of plant functionality to support effective communication between plant systems and control centre designers,

ADVANCED CANDU FUNCTION ANALYSIS

A. Analysis Approach and Organization

The AECL CANDU 6 reference design was used as the initial basis for developing the function analysis for the Advanced CANDU plant. Two decisions directed the scope and perspective of the subsequent analysis:

- A single hierarchical function decomposition was used to provide coverage of the plant functions required in all operational regions and in support of the operational strategies for the plant, and
- Safety and production perspectives were represented in an integrated manner within the function decomposition, rather than providing separate decompositions for the two perspectives independently, because plant operation is rarely governed exclusively by safety functions alone.

B. Function Identification

The major functions of a nuclear power plant that are related to the achievement of safety and production objectives were used as the starting basis for the function analysis (see Figure 1). To achieve operating objectives, station management monitors and directs five functions:

- establish production and safety setpoints and margins,
- establish operating practices and procedures,
- operate the plant to setpoints to achieve safety and production objectives,
- maintain operability and efficiency of plant equipment, and
- train plant staff.

Performance of the third of these goals is the responsibility of the station operations team. The plant control centres serves as the focus for the operations team activities.

This third function was in turn broken down to lower level functions consistent with the way the CANDU 6 plant is constructed and operated. A hierarchical representation of functions with respect to energy production, transport, conversion, and distribution was used to identify and document individual functions and supporting hierarchical relationships. This process of identifying successively lower-level functions was continued through several levels of decomposition. The decomposition process was stopped when the lowest level functions represented the most elementary level at which control centres personnel would supervise or control a plant function.

C. Function Description

Function description involves the characterization of information for each function necessary to support function assessment, implementation and use. For the Advanced CANDU plant the following types of information are being used to characterize each function:

- identification information (e.g., function name and catalog reference number),
- context information (e.g., the state of the function for each combination of plant operating region and operating strategy),
- performance assessment attributes (e.g., measures of and criteria for success),
- implementation attributes (e.g., strategies for performing the function),
- operational attributes (e.g., conditions for function operation),
- allocation attributes (e.g., a description of how tasks in support of each function are shared between humans and automation, and criteria that result in changes to the allocations),
- relationship attributes (e.g., affinity, priority or hierarchic relationships among functions), and
- interface information attributes (e.g., information concerning each function that needs to be conveyed through control centre interfaces).

Examples of the information used to describe the function 'Control liquid zones' is provided in Table 1.

We are currently refining the approaches for identifying and describing functions. For example, to more effectively characterize the allocation of a function between humans and automation we have found it advantageous to use models of closed loop control, supervisory control and decision-making to provide a reference framework and vocabulary for characterizing the roles assigned to humans and automation.

C. Function Assessment

Function assessment involves the analysis of the information used to characterize functions to:

- define requirements of the function to meet human information needs, and
- assess the compatibility of the function against human information needs.

Although we are only in the early stages of the conceptual design of the Advanced CANDU control centre, we have found the information contained in the function analysis invaluable for:

- reviewing and assessing the information needs of control room staff in all operating situations,
- assessing the task burdens imposed on control room staff in different operating situations, and
- identify areas for and assessing the potential of increased control or information automation in better supporting the control room crew to meet plant operational objectives.

CONCLUSIONS

The approach to developing and applying function analysis outlined in this paper is being used for the conceptual design of the control centres of the Advanced CANDU plant. AECL will continue to refine and adapt this basic systems development method to meet evolving project needs.

REFERENCES

1. "Human Factors Guide for Nuclear Power Plant Control Room Development," Electric Power Research Institute report NP-3659, Palo Alto, California (1989).

2. "Design for Control Rooms of Nuclear Power Plants,"
 International Electrotechnical Commission standard
 IEC 964, Geneva, Switzerland (1989).

3. "Human Factors Engineering Program Review
 Model," United States Nuclear Regulatory
 Commission report NUREG-0711, Washington, D.C.
 (1994).

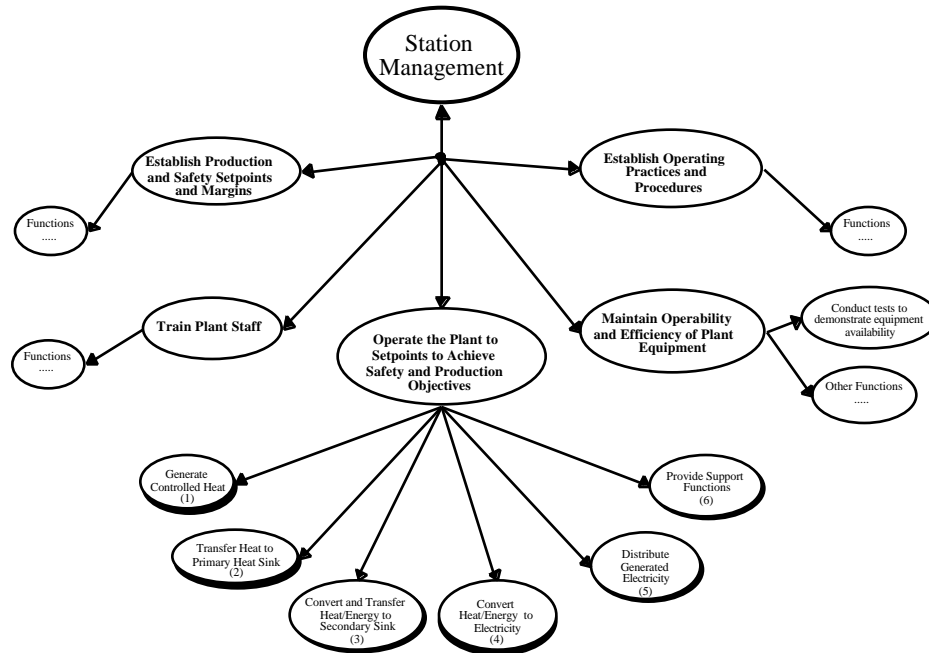


Figure 1: Major Functions of the Advanced CANDU Plant.

Table 1: Example Function Information.

Identification Information	
Name	Control liquid zones
Reference #	1.2.1
BSI Reference(s)	63480

Applications Context Information	Plant Operating Strategies			
	Normal	Abnormal	Upset	Emergency
Plant Operating Regions				
Electric generation	active	active	active	active
Guaranteed shutdown	inactive	inactive	inactive	inactive
Low power cold	active	active	active	active
Zero power hot	active	active	active	active
Poison prevent	active	active	active	active
Raise reactor power to achieve criticality	active	active	active	active
Warm-up	active	active	active	active
Raise reactor power and dump steam to condenser	active	active	active	active
Raise reactor power and provide steam to turbine	active	active	active	active
Lower reactor power and remove steam from turbine	active	active	active	active
Lower reactor power and dump steam to condenser	active	active	active	active
Cooldown	active	active	active	active
Lower reactor power below criticality	active	active	active	active

Table 1: Example Function Information (continued).

Performance Assessment Attributes	
The goal or objective for the function.	<ul style="list-style-type: none"> - Continuous control of spatial power, and - Continuous control of small changes to bulk power (i.e., power errors < 3%).
Measures for judging goal achievement.	<ul style="list-style-type: none"> - Neutron flux measurements in several regions of core, and - Calculated bulk power and power error.
Criteria for judging goal achievement.	<ul style="list-style-type: none"> - Absence of flux tilts, and - Stability of individual zone levels at a fixed power setting.
Measures for judging if the function is being performed as expected.	<ul style="list-style-type: none"> - Zone levels, - Zone header pressures, and - Zone compartment flow rates.
Criteria for judging if the function is being performed as expected.	<ul style="list-style-type: none"> - Zone level movement in relation to power manoeuvres, and - Zone header pressures and zone flow rates at nominal values.
Performance influencing factors and their expected effects.	<ul style="list-style-type: none"> - Flux detector response and calibration, - Overall core reactivity (i.e., fuel plus moderator), - Position of absorbers and adjusters, and - Spatial distribution of fuel reactivity in all core regions.
Implementation attributes	
Primary strategy to be employed in performing the function.	<ul style="list-style-type: none"> - Division of core into 14 regions and control of neutron flux in each region by flooding or emptying the water level in each zone compartment to decrease or raise the regional neutron flux respectively. - Co-ordinated raising or lowering of zone levels in response to power errors.
Alternatives strategies within the bounds of the function for achieving the function goal.	<ul style="list-style-type: none"> - Manual control of up to two zones at a time to assist in overcoming fueling flux transients.
Criteria for selecting among the alternative strategies.	<ul style="list-style-type: none"> - To be determined.
Operational attributes	
Support functions that must be available.	<ul style="list-style-type: none"> - Helium cover gas, - Instrument air supply, - Class I 48 Vdc power, - Demineralized water supply, and - Chilled cooling water.
Initiating conditions for the function.	<ul style="list-style-type: none"> - Removal of reactor from guaranteed shutdown state.
On-going conditions or constraints for the function.	<ul style="list-style-type: none"> - Availability of at least one digital control computer running reactivity control program, - Availability of flux mapping calibration and flux detectors in all regions, and - Availability of water supply at 750 kPa.
Side or secondary effects of performing the function.	<ul style="list-style-type: none"> - Differential fuel burnup in different regions of the reactor core.
Terminating conditions for the function.	<ul style="list-style-type: none"> - Reactor returned to guaranteed shutdown state or reactivity control program not available to run in at least one digital control computer.

Table 1: Example Function Information (concluded).

Allocation attributes	
Control tasks allocated to humans (e.g., setpoint adjustment, selection of control modes).	<ul style="list-style-type: none"> - Selection of automatic or manual control of up to two zones. - Selection of compensation means if function is not being performed as expected.
Control tasks allocated to automation (e.g., continuous control to setpoint).	<ul style="list-style-type: none"> - Filling or emptying of zone compartments in response to spatial or bulk power error demands.
Criteria that result in changes to the control allocations between humans and automation (e.g., mode changes, equipment unavailability).	<ul style="list-style-type: none"> - During fueling manual control of up to two zones may be advantageous to address step changes in zone reactivity as a result of new fuel introduction.
Information tasks allocated to humans	<ul style="list-style-type: none"> - Supervisory monitoring of zone level values and movement, assessment of function performance values against performance criteria.
Information tasks allocated to automation	<ul style="list-style-type: none"> - Calculation of individual zone level deviations from average zone level to achieve spatial control, - Monitoring of parameters, and - Annunciation of performance discrepancies.
Criteria that result in changes to the information allocations between humans and automation.	<ul style="list-style-type: none"> - To be determined.
Relationship attributes	
Hierarchic relationships between functions.	<ul style="list-style-type: none"> - Refer to function hierarchy.
Priority relationships between functions.	<ul style="list-style-type: none"> - For power errors $< \pm 3\%$ control liquid zones provides bulk power control exclusively. - For power errors $> \pm 3\%$ bulk power control is achieved by a combination of adjuster and liquid zone control. - On activation of any shutdown function (i.e., SDS1 or SDS2) liquid zones are filled to 95% filled and held at this value until the shutdown systems are reposed.
Substitutional or preference relationships between functions with the same goal.	<ul style="list-style-type: none"> - None identified.
Affinity relationships between functions that share common grouping or categorization aspects.	<ul style="list-style-type: none"> - Goal affiliation - Generate heat. - System affiliation - Reactor. - Group affiliation - Group 1.
Interface information attributes	
Instruments applicable to the function.	<ul style="list-style-type: none"> - Flux detectors, - Zone level instruments, and - Liquid zone header pressure instruments.
Measured and calculated plant variables applicable to the function.	<ul style="list-style-type: none"> - Average neutron flux in each zone, - Average zone level, - Zone levels in each compartment, and - Zone deviations of each compartment from average.
Recommendations and rationale for control centres and field panel annunciation.	<ul style="list-style-type: none"> - Abnormal supply header pressures - inability of function to be performed with expected filling/emptying response times. - Abnormal zone level in response to calculated level. - Helium header pressure abnormal. - Recombiner temperature abnormal.
Recommendations and rationale for the types of control room displays for the function.	<ul style="list-style-type: none"> - Spatial presentation of zone levels and deviations. - Bulk power history and power error in relation to liquid zone control range. - Spatial power history in relation to liquid zone control range.

