A DESIGN BASIS FOR THE DEVELOPMENT OF ADVANCED CANDU CONTROL CENTRES

M.P. Feher, E.C. Davey and L.R. Lupton
Control Centre Technology Branch
AECL Research, Chalk River Laboratories
Chalk River, Ontario, Canada K0J 1J0

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 marketing pressures. This paper describes the proposed design bases for the development of advanced control centres to be implemented in CANDU plants beyond the year 2000. Four areas have been defined covering design goals, design principles, operational bases, and plant functional bases.

Background

The Control Centre Technology Branch of AECL Research has undertaken the development of an advanced control centre for future CANDU plants. To guide the development activities, a basis for the design has been established consisting of:

- design goals to be achieved,
- design principles to be applied,
- an operational basis that characterizes plant operation, and
- a functional basis that describes the plant functions and their preliminary allocation between humans and automation.

These four components are briefly described below. Additional detail will be provided in the paper and presentation.

Design Goals

The design goals for the advanced control centre are grouped around six factors:

- Safety - to provide one or more control centres for the operators to control the plant safely in all operating regions so as to maintain the public and staff safety,
- Operability - to provide an assignment of control and monitoring functions to achieve operational objectives through the effective utilization of operator and system capabilities,

- Maintainability - to permit necessary system maintenance safely, quickly, and cost-effectively,
- Availability
  - to maximize the probability that the control centre functions as intended and when required,
  - to provide the operating team with the capability to monitor and control the plant as intended, and
  - to provide, when required, the controls required to return the necessary plant functionality to normal conditions, or the rules required to respond if no replacement functionality is available,
- Overall Consistency - to base the control centre design on clearly documented and well understood philosophies of design and operation, and
- Marketability - to incorporate design features that are commercially competitive and meet the expectations of potential customers.

Design Principles

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 (e.g., from 60% to 100% Full Power). 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 to avoid shutdowns. Even if the effects themselves could be predicted and modeled, the computational engine that can cope with such state variability in real time has not yet been constructed.

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

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

Operators thus provide 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. Also, 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. 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.

Each of these unique human attributes are compelling reasons to retain the human operator in a central position in the CANDU system.

Thus, a requirement of the advanced CANDU control centre design is that the human operators shall be 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. In recognition of this important role for humans in overall plant operation, design principles have been established in four areas covering:

- the roles of humans in supervisory control and plant automation,
- the role of human-machine interfaces in support of plant operation,
- human cognitive and physical capabilities and limitations, and
- approaches for preventing, accommodating and mitigating the consequences of human error.

Operational Basis

The plant control centre must support the supervision and control of the plant in all possible operating regions. The basis for this operation includes definitions of:

- the fundamental operating regions of the advanced CANDU plant based on process parameters and equipment configurations (e.g., electricity generation, poison prevent, load follow, zero power hot, etc.),
- the operational strategies used by plant staff to maintain stable operation in the regions, to monitor the success of the automation, or to intervene to manoeuvre the plant to desirable operating regions, and
- the roles and responsibilities of plant staff in each of the operating regions.

Functional Basis

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 both safety and production objectives under all possible operating circumstances. These descriptions include:

- the plant functions to be monitored and controlled,
- the performance goals of the various plant functions,
- the relationship of each function to primary safety and production objectives,

- the relationship(s) of each function to other functions,
- 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 performance measures and criteria to be used in judging function performance, and
- the roles of humans and automation for controlling and processing information to perform the component tasks for each function in all operational situations.

Conclusion

The paper will discuss in more detail the approach to establishing the operational and functional bases, and then conclude by describing the process to be used to apply the bases to the design of the advanced CANDU control centre.