Electrical, Control and Information Systems in the Enhanced CANDU 6®

J. de Grosbois, G. Raiskums, M. Soulard
Atomic Energy Canada Ltd.
2251 Speakman Drive, Mississauga Ontario Canada,
Email: degrosboisj@aecl.ca

Abstract

This paper describes the electrical, control, and information system (EC&I) design feature improvements of the Enhanced CANDU 6® (EC6®). These additional features are carefully integrated into the EC6 design platform, and are engineered with consideration of operational feedback, human factors, and leveraging the advantages of digital instrumentation and control (I&C) technology to create a coherent I&C architecture in support of safe and high performance operation. The design drivers for the selection of advanced features are also discussed. The EC6 nuclear power plant is a mid-sized Pressurized Heavy Water Reactor design, based on the highly successful CANDU 6 family of power plants, and upgraded to meet today's Canadian and international safety requirements and to satisfy Generation 3 design expectations.

1. Introduction

CANDU nuclear power plants are designed and built by Atomic Energy Canada Ltd. (AECL). AECL is composed of two main divisions: Commercial Operations, the commercial part of the organization (which includes "CANDU Services" who provide full service capability to the existing CANDU fleet and "Product Development" who are a full scope design engineering group responsible for reactor development and the new build program); and a world-class nuclear R&D lab at Chalk River Labs (CRL). CRL supports extensive R&D faculties including hot cells, fuel fabrication and test facilities, research reactors, isotope production facilities and waste management facilities. AECL is a unique and tightly integrated technology-driven organization with a strong nuclear knowledge base across many engineering and science disciplines. In addition, AECL also has a strong network of new build partners and a flexible supply chain network capable of adapting to meet demand cycles. The CANDU Owner's Group (COG) is a well coordinated and active CANDU operator's network that provides a wide range of utility services including training, knowledge transfers, community of practice programs, as well as co-funded R&D.

There are currently 29 operating CANDU reactors world-wide. This includes 20 in Canada, 4 in Korea, 2 in China, 2 in Romania, and 1 in Argentina. The first standard design CANDU 6 plant in Canada was Point Lepreau in New Brunswick. It was licensed and started operation in 1983. There are now 11 standard CANDU 6 design reactors operating successfully and safely throughout the world, all designed and built by AECL. These plants are economic to operate and achieve high production reliability. Incremental improvements have been made to each successive CANDU 6 new build. The most recent CANDU 6 plant to go into operation was Cernavoda 2 in Romania, which came on-line in 2007.

The EC6 design is an evolution of the very successful CANDU 6 design (i.e., the Reference Design). It has been designed to retain the fundamental and proven characteristics of CANDU 6 while further enhancing safety to meet latest codes and standards and improving operability. It retains the fundamental design of the CANDU 6 reactor core – a heavy-water moderated, heavy-water cooled pressure tube reactor using natural uranium fuel. Included in the enhancements are several innovations developed under the Advanced CANDU Reactor (ACR®) development program, improvements made to existing CANDU 6's as part of recent refurbishments, and other changes specifically designed for the EC6.

EC6 is designed to meet the latest (more demanding) requirements of the Canadian Nuclear Safety Commission (CNSC) for new nuclear power plants in Canada as defined in the RD-337 standard [1]. The EC6 is also designed to meet higher operational targets of a 94% year-to-year capacity factor, a 1% forced outage rate, and to achieve a 60-year plant design life. Careful consideration of operating experience feedback in the design, systematic elimination of single points of vulnerability, human factors engineering, and design for maintainability and reliability have all been incorporated in the design to ensure these targets are met. Finally the design addresses various equipment obsolescence and modernization objectives. These new features strengthen existing and already proven CANDU 6 features to provide an enhanced plant design that achieves very high reliability of safety functions and meets Canadian and international safety goals.

As part of the EC6 Project design improvements, the instrumentation, controls, electrical, and plant information systems are being significantly upgraded and modernized to take advantage of proven technological advancements and to enhance plant safety, production reliability, and economics. This paper describes these design improvements. The following topics will be covered:

- I&C design philosophy and architecture:
  - Basic principles
  - The overall architecture
  - Electrical systems
  - Defense in depth
  - Prevention of common cause failure
  - Design philosophy for MCR upgrades
- Specific I&C design enhancements:
  - Drivers for design changes
  - Enhancements to the main control room (MCR), secondary control area (SCA) and the technical support centre (TSC)
  - Enhanced use of modern digital control systems
  - Main control room (MCR) control/safety panels
  - Plant display system (PDS)
  - Digital safety systems
  - Safety system testing and monitoring

To provide a full context for this discussion, the following section describes the overall design philosophy and architecture of the instrumentation, control, and electrical systems of the EC6 plant design.

2. I&C Design Philosophy and Architecture

The following section explains the basic I&C design principles and features of the EC6. The I&C architecture including electrical systems is described, the categorization approach is outlined, and the defense in depth and common cause failure defenses are summarized.

2.1 Basic Principles

A key safety principle behind the EC6 I&C design (dating back to the original CANDU 6 design) is the defense-in-depth concept of the nuclear plant design. This consists of multiple layers, with the first three being the process system, the protective system(s) and the containment system. The design is such that these systems act independent of one another, and as each is high reliability, the probability of a significant release of radioactive material to the public domain is extremely small [1]. Thus a fundamental principle in the I&C architecture is to ensure independence between safety and control is not compromised.

From the very outset, this led to the requirement for the safety systems to be physically and functionally separate and independent from the control systems - and from each other. CANDU power reactors employ two equally capable reactor shutdown systems (SDSs), each capable of shutting down the reactor using entirely separate means during any postulated accident condition (see Figure 3).

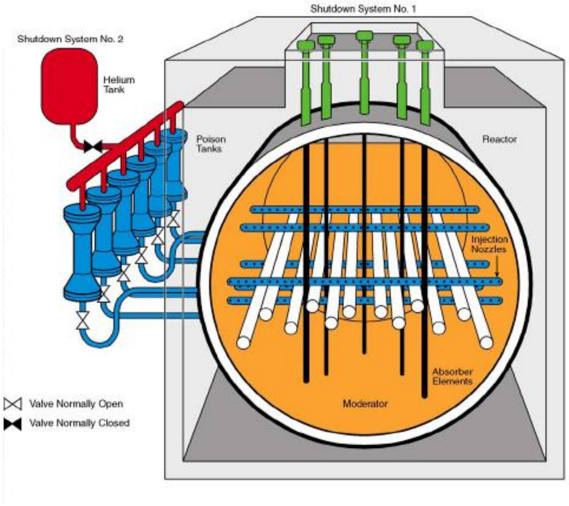

Figure 3. CANDU Shutdown Systems

Over the years, with increasing design and operating experience, and with ongoing evolution of the CANDU reactors, the original design has undergone several refinements; however these key safety principles have remained and are retained in the EC6 design.

2.2 The Overall Architecture

The reactor and process control systems are backed up by the special safety systems, which include the two shutdown systems, the emergency core cooling system, emergency heat removal system, and the containment system. Each of these safety systems operates completely independent of the other and independent of the reactor and process control systems. The two SDSs are independent and diverse from each other (including fully separate and diverse voting, actuation and shut-down mechanisms) and each employ triplicated (3-channel) computerized trip channels. Two out of three voting logic is employed between channels in each SDS. The emergency core cooling and the containment systems also employ redundant channels and will include at a minimum, computerized testing and, where appropriate, digital safety logic.

The EC6 control room features an array of panels for operator interface and is closely based on the reference CANDU 6 design (shown in Figure 4). The instrumentation and controls on the panels are grouped on a system basis, with a separate panel allocated to each special safety system. For EC6, a combination of digital and conventional display and annunciation instrumentation will be provided for all safety and production systems. In general, the CANDU 6 allocation of systems to the operator interface panels is preserved in the EC6 design with a minimal number of changes. Independence between control and safety systems is implemented at the sensor level and is preserved all the way through the wiring and logic to the operator interface level.

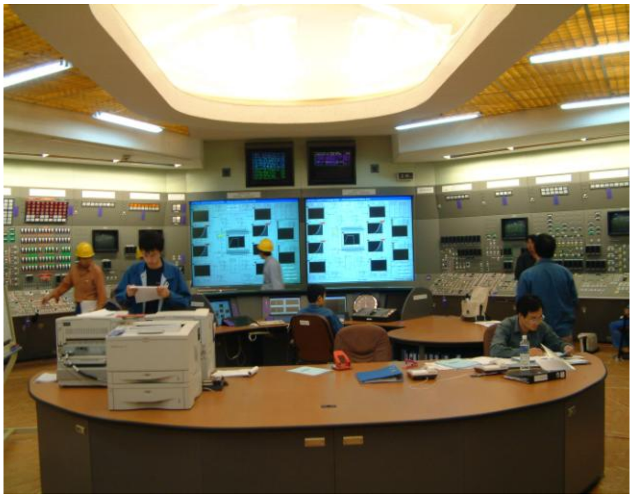

Figure 4. The CANDU 6 Main Control Room

Similar to the proven CANDU 6 design, the control room panels of the EC6 design are complemented with central large screen displays, dedicated alarm annunciation displays and an operations console. The central large screen displays serve to improve situational awareness with an uncluttered and integrated plant monitoring capability. Important safety system information is available via a combination of hardwired panel indicators and soft panel displays on the safety panels and this information is also made available to the computer-based central annunciation, computer-based procedures and plant display system.

A computerized and seismically qualified safety monitoring system (SMS) receives data from the trip computers and the partitions belonging to the essential control subsystem of the distributed control system (DCS) and provides the safety parameter display and post accident monitoring (PAM) functionality. In addition, each of the post accident monitoring parameters can also be monitored by hardwired means on the safety panels and this is fully independent of the SMS.

There are manual hardwired controls in the main control room (MCR) and secondary control area (SCA), not only to shutdown the reactor but also to perform several other key safety functions. These manual hardwired controls work backup the automated functions of the safety systems.

The plant annunciation system includes a primary system as well as a back-up system. The primary annunciation system is implemented as a computer-based message list system. The alarms of high safety significance are also provided in an independent back-up annunciation system, which is implemented using modern hardwired "window tile" technology.

The EC6 design uses multiple distributed control system (DCS) equipment subsystems to provide data acquisition and control logic for all plant production functions as well as many important to safety (ITS) functions. The nuclear steam plant (NSP) DCS interfaces with the plant display system (PDS), plant annunciation system, and SMS to provide monitoring and alarms for the operator. The control, normal monitoring and safety monitoring functions are in separate independent systems for high reliability and as an added defence against common cause failure. Figure 5 provides an overview of the EC6 I&C Architecture.

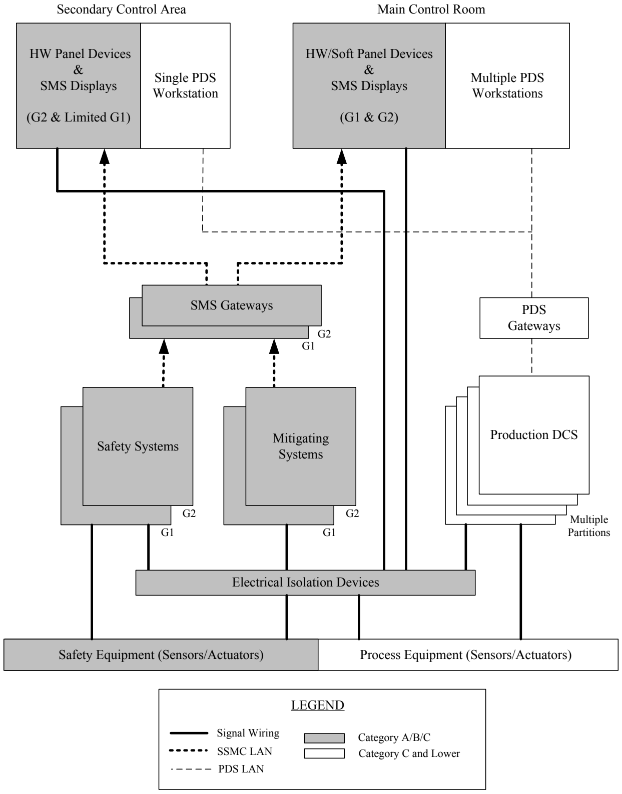

Figure 5. EC6 I&C Architecture

2.3 Electrical Systems

The emergency power supply (EPS) part of electrical distribution system for EC6 has been expanded to meet the automatic start and single failure criteria (SFC) requirements of CNSC RD-337 [1], Section 8.9. The EPS distribution system has been connected to Class III system so as to distribute both normal Class III power and emergency power to the critical loads. Provisions have been added to allow testing of the EPS under load conditions. Seismically qualified uninterruptible power supplies (UPSs) have been added to ensure the automation of start-up and control of all essential loads and the powering of essential loads.

The EC6 EPS is fully automated. As well, a full manual mode of operation control is retained. The safety loads are automatically connected to EPS on a design basis event (DBE). To meet SFC each unit in EC6 has a dedicated pair of redundant EPS standby generators. In addition manual tie-in breakers between the redundant buses of the two units enhance availability of the EPS in each Unit.

The defense in depth is achieved as follows:

- The EPS is an entirely separate system for each unit in the typical 2-unit EC6 configuration,
- EPS loads are normally supplied from Class III power with backup from EPS standby generators for a DBE,
- Manual tie-in breakers are provided between redundant EPS buses of the two units.

The Severe Accident Recovery & Heat Removal System (SARHRS) has been added to the EC6 design and is supplied by a dedicated diesel generator independent of EPS.

2.4 Defense in Depth

The layers of defence are primarily the process control system, the protective systems that include the shutdown systems and the cooling systems, and the containment system. The control system operates continuously to maintain plant parameters within operational limits. If it fails for any reason to do this, a separate Class 2 mitigating controller (i.e., the “essential control” sub-system) will independently reduce reactor power (i.e. a fast power “step-back” function). In the unlikely even that this function fails; the reactor shutdown systems will activate. In the very unlikely event of a design basis accident, the cooling systems continue to cool the fuel and the containment system provides the physical barriers to radiological release and thus allows time for other actions to be taken by reactor operators (i.e., further mitigation measures). A minimum complement of independent monitoring and supervisory control capability is additionally provided to help perform tasks for achievement of key safety functions.

2.5 Prevention of Common Cause Failure

For the different layers of defence to be truly independent, care has to be taken to design them to be immune to common cause failures (CCF). This becomes especially pertinent in the context of computer based systems because of additional vulnerabilities caused by the use of digital technologies in any design. Failures can be compounded by use of the same technology (manufacturer, product design) across different systems, as latent software / hardware / communication faults or external stressors such as electromagnetic interference (EMI) can simultaneously render multiple systems ineffective. Although less likely, it is possible for CCF to defeat redundancy or separate layers of defence. As a consequence, the principle of design diversity gains importance, particularly for safety systems.

In the EC6 plant design (consistent with the CANDU 6 design philosophy), to provide defence against low probability common cause events such as fires or missiles (turbine blades, aircraft strikes etc), the station safety, post shutdown, and safety support systems are separated into two groups with strong separation that are physically and functionally independent of each other. This is in addition to the normal separation provided between redundant channels of a channelized system. Each of these groups includes equipment to shutdown the reactor, remove decay heat if the process systems are intact, or if they are not intact, to prevent or minimize release to the public, and, to supply the necessary information for post accident monitoring. Measurements and control/instrumentation cabinets for Group 1 are connected to the MCR for implementation of the control logic and monitoring, whereas Group 2 is primarily connected to SCA (see Figure 6). Group 2 equipment is also siesmically qualified to withstand DBEs. Electrically buffered information and actuation signals are made available from each group to the other control room.

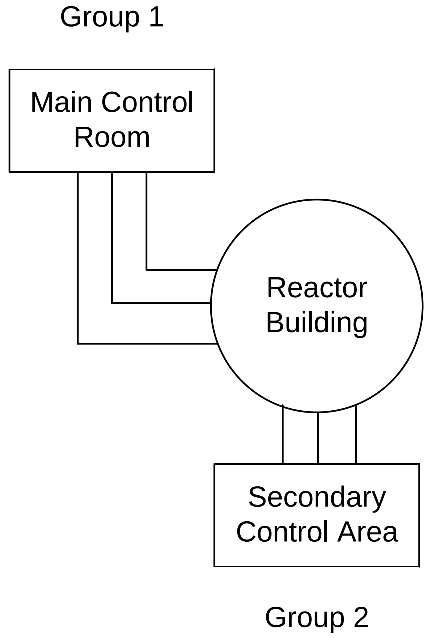

Figure 6. CANDU Two Group Separation

Each safety shutdown system (SDS1 and SDS2) uses a separate hardware platform from different vendors. In addition, there is software diversity between the two systems (different program organization, software environment, compilers, application language, etc.), and the two systems use different product architecture. Furthermore, the use of functional diversity (different underlying mechanisms such as rod insertion versus poison injection, etc.), and signal diversity (different sensors or reactor process parameters etc.) contribute in ensuring that the two shutdown systems meet their reliability goals.

Functional and electrical isolation are maintained between the Class 1 shutdown systems and the Class 2 monitoring and controls systems by the use of qualified isolator connections only. These isolation devices are considered to be part of the Class 1 shutdown systems and are rigorously qualified accordingly. Qualification includes functional isolation to ensure that any failure of the Class 2 system or of the communications prototcol or link itself will not affect the safety function of the Class 1 system.

2.6 Design Philosophy for MCR Upgrades

The existing CANDU 6 MCR design is based on a conventional "operate at the panel" philosophy. The EC6 design, while incorporating digital device control enhancements and providing an upgraded plant display system with advanced alarm annunciation and computer based procedure support, deliberately retains this proven design philosophy in what is referred to as a "hybrid MCR" design. This means it incorporates the advantages of modern digital control systems without total reliance on software based controls from a centralized operator console. The centralized operator console provides monitoring and test function support, and limited supervisory capability only. Digital signal exchange between device and group control functions enable a feature rich implementation of the alarm annunciation system, computer based procedures and plant display system.

3. Specific I&C Design Enhancements

The following section describes the motives and objectives of the EC&I enhancements and highlights the specific changes being made relative to the CANDU 6 reference design.

3.1 Drivers for Design Changes

There are several important drivers for change behind the EC6 EC&I enhancements. These include:

- the need for compliance with new and more stringent licensing requirements in Canada for new reactor builds (i.e. as specified in the CNSC RD-337 [1] standard),
- improvements to enhance plant safety margins,
- improvements to address customer feedback and deficiencies identified from operating experience reviews,
- improvements to achieve higher plant performance targets, reduce capital costs and achieve more economic life-cycle operation, and
- design changes to address obsolescence, take advantage of proven advances in equipment technology, improve maintainability, and achieve longer plant-life.

3.2 Enhancements to MCR, SCA and TSC

The EC6 Main Control Room (MCR) is designed to allow operators to control, cool, and shutdown the plant during all plant operational states, and accident conditions including normal operation, Anticipated Operational Occurrences (AOOs), Design Basis Accidents (DBAs), and Beyond Design Basis Accidents (BDBAs). The design of the MCR is based on the philosophy of having sufficient displays, controls and annunciation to allow the plant to be safely operated and support measures to be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of AOOs, DBAs, and to the extent practicable, following beyond DBAs. The MCR will have the required controls to manually initiate any safety functions which are also initiated by automatic control logic. The MCR contains traditional control panels, computerized control and display workstations, large screen displays, and communication equipment. There are three main MCR instrumentation panel groups: one for the reactor and turbine, including the safety systems; one of the electrical distribution systems and switchyard, including miscellaneous auxiliary systems; and one for fuel handling systems.

The MCR includes interfaces for the advanced annunciation system. This includes both window alarms, located on the control panels and video display units for the computerized alarm system. Functionality for the computerized alarm system is accessed through the PDS. Communication devices are available in the MCR to communicate directly with the TSC and SCA as required. Communication is also available to make emergency announcements over the plant public address system.

The function of the SCA is to provide the necessary displays and controls to put and keep the plant in a safe shutdown state if the MCR is ever unavailable. The SCA contains the required indications and controls to perform the following functions:

- shut down the reactor and maintain it in a safe shut down state,
- remove heat from the reactor core,
- limit release of radioactivity material by maintaining the containment barrier, and
- monitor the plant conditions and perform actions necessary to maintain the above functions.

The SCA will have the required controls to manually initiate any safety functions which are initiated by automatic control logic.

In existing CANDU 6 plants, the SCA is qualified to remain functional during and after a Design Basis Event (DBE) earthquake. In the EC6 the monitoring and control of critical safety functions from the MCR and the monitoring of critical safety functions from the Technical Support Centre (TSC) are also seismically qualified to remain operational during and after DBEs. Other MCR supporting systems such as electrical power, lighting, and heating ventilation and air conditioning (HVAC) will be updated from the original CANDU 6 design to provide a habitable MCR complex during all plant operational and design basis accident states.

The MCR includes indications and controls capable of monitoring and controlling the plant safety systems as well as control systems. A seismically qualified safety monitoring system (SMS) which provides displays containing safety parameter information, post accident monitoring information and detailed status information regarding the safety and safety support systems will be provided in both the MCR and the Secondary Control Area (SCA). The upgrades to the MCR design will maintain the original plant design’s group separation philosophy, namely Group 1 systems will reside in the MCR and are generally non-seismically qualified, while Group 2 systems will reside in the SCA and are credited to remain functional during and after a design basis event (DBE) earthquake. Group 2 functionality available in the MCR (including display and manual actuation) will still maintain buffered and isolated signal connections to/from the Group 2 I&C system equipment which remains located in the SCA. Access to any functions credited for DBE earthquake that are available from the MCR are thus provided through the Group 2 systems in the SCA, and the bufferred and isolated Group 2 signal connections to/from the MCR and SCA will be via a seismically qualified route and powered by a seismically qualified source. Similarly, Group 1 functionality located in the SCA (including display and manual actuation) will maintain buffered and isolated signal connections to/from the Group 1 I&C system equipment which remains located in the MCR control equipment room (CER).

The SCA contains safety grade indications and controls to allow an operator to achieve and maintain safe shutdown of the plant following an evacuation of the MCR. The SCA is a unitized, seismically qualified facility only utilized for the scenarios where the MCR complex becomes uninhabitable (e.g. a fire in the MCR complex). This is in contrast to the CANDU 6, where transfer of plant control to the SCA is the usual response to a DBE earthquake, and relocation of the operator to the SCA is assumed.

The SCA will contain a dedicated Secondary Control Room (SCR). For human factors reasons, the SCR safety panels will be similar in design to the corresponding MCR backup and safety panels to provide the same operational interface (with the exception of any testing functions). In addition to the conventional controls, the SCR includes SMS displays similar to those in the MCR.

3.3 Digital Control Systems

Modern digital control systems technology is deployed in the EC6 to achieve an integrated architecture. However, careful use of redundancy and sub-system partitioning in the design provides defense against common cause failures and single points of failure. Communication links respect the segmentation rules to minimize inter-dependencies between functional partitions and redundant trains. This provides a robust design immune to random faults. The DCS platform is qualified to handle both Class 2 and 3 functions. In addition to DCS technology, several important architectural changes have been made to the digital control systems of the CANDU 6:

- the fuel handling control and display systems, although implemented using the same DCS and PDS platform technology, have been made a fully separate partition with an independent digital sub-system to implement safety interlocks.
- All important to safety mitigating functions previously in the digital control computers are now implemented in a separate Class 2 mitigating controller, which along with some other Category B functions is referred to as the “essential control sub-system”.
- Fully digital device control sub-systems will interface via digital communications with the digital group controls.
- Read-backs are provided from the digital device control sub-systems (including panel status information) to the PDS, the advanced alarm annunciation system, and the computer based procedures. This enables improved situational awareness and provides richer operator support functions.
- Use of local input/output stations and redundant digital control bus communications will simplify plant wiring.

3.4 MCR Safety and Control Panels

A number of changes are made to the MCR panels to address process system design improvements (such as accomodating the new SARHRS design), to accommodate the digital enhancements to the safety systems, computerized safety system testing, changes to support digital device control and component obsolescence issues. At the same time, the design objective is to retain the allocation of functions to panels except where obvious human factor or operational or safety benefit is realized. As a result, EC6 design will be combining modest use of “touch panel” display technology with conventional hardwired panel instrumentation in what is referred to as a “hybrid MCR” design that optimizes safety and reliability. The implementation follows strict design guides developed to ensure a consistent approach to human machine interface design and logic implementation, while retaining necessary independence of redundant equipment and electrical supplies and ensuring adequate defenses against single points of failure and common cause failure. Careful consideration to classification of control loops based on safety function categorization is given through-out the design process.

3.5. Plant Display System (PDS)

Building on the success of the Qinshan CANDU 6 PDS, the EC6 will add significant additional display support in the PDS. A full implementation of the CANDU Advanced Message List System (CAMLS) will provide advanced alarm annunciation and management. This system provides rule-based processing of alarms to filter, sort, and prioritize their display to the operator in a more meaningful format. This means during abnormal conditions, alarm flooding is eliminated and situational awareness is improved to reduce operator response times and likelihood of human error. Operators have the choice of alarm display formats including priority-based or time-sequential displays.

Computer based procedures provide operator assistance in performing both routine testing or infrequent tasks (e.g. emergency operating procedures). CBPs walk the operator through a sequence, log his/her progress, warn of deviations or incomplete steps, and log a history. Read-backs from the control panels and from digital device controllers confirm the equipment states are correct and operator actions have been completed. Links to operating manuals and other supporting documentation are provided.

3.6. Digital Safety Systems

Two completely independent and diverse Class 1 shutdown systems, SDS1 and SDS2, are used in CANDU reactors. Each system contains three independent safety channels arranged in a 2-out-of-3 voting system. Channelized instrumentation is used to monitor a number of plant neutronic and process variables. If variables in any two channels of a single system are outside pre-determined envelopes, a shutdown is initiated. In all existing CANDU 6 plants except one, neutronic trips are hardwired while process trips are implemented in digital trip computers. Hardwired relay logic provides fast response for neutronic trips and trip computers provide intelligent trip logic (such as power-dependent setpoints) for process trips. Improvements in EC6 include:

- digital neutronic trips (including computer-assisted neutronic amplifier gain calibrations),
- faster digital platforms for both SDS1 and SDS2, and
- additional fast neutronic linear rate trips and additional process trips.

These improvements in EC6 provide improved trip coverage, improved trip margin (improved plant performance), and reduced operation and maintenance costs. In addition, this change addresses obsolescence concerns, facilitates operation and maintenance by permitting less error-prone (and more rapid) computer-assisted calibration of the in-core flux detectors. Incoporating digital neutronics trips in the EC6 design provides the ability to respond more quickly to changes in reactivity configuration, and accommodates possible future changes to the trip logic. This approach was implemented at the Darlington CANDU design and has been demonstrated through years of operational experience to be effective in terms of high reliability (with few failures and human error related events), and improvement in trip margins.

The emergency core cooling (ECC) is a third safety system currently in the CANDU 6 design that contains Class 1 safety functions. The ECC trip logic functions and test functions in previous CANDU 6 (C6) plants were implemented using hardwired relay and timer logic circuits. The proposed design change implements the logic of the ECC system in channelized digital controllers. The ODD and EVEN separation of the existing ECC logic will be retained and all existing performance requirements will be met, with improved self-testing capabilities, and additional component status and diagnostic information. Partial ECC computerization has been previously successfully implemented at the Darlington CANDU station. A fully digital implementation of the ECC system would enable future changes to the Class 1 logic. The digital implementation of the ECC logic simplifies interfaces to operator display systems, improves the performance and coverage of ECC availability testing, and provides more comprehensive status and diagnostic information for the ECC system.

The fourth Class 1 safety system is the containment system. In the CANDU 6 this system is a conventional relay-based design. In the EC6, at a minimum the test functions of this system will be a digital implementation. Finally, the Class 2 emergency heat removal system (EHRS) is the newly added fifth safety system in the EC6. It too will at minimum have its test functions implemented with digital technology.

3.7 Safety System Testing and Monitoring

In CANDU 6 reactors such as Qinshan, safety system testing (SST) is performed by operating many hand-switches and pushbuttons on the MCR safety panels. This change will simplify the safety panels and testing procedures. It will also save operator time and help to reduce the likelihood of operator error. Hardwired panel instrumentation for testing will be replaced by computer-assisted testing similar to what is implemented in the Darlington CANDU design where testing is semi-automatic via a computer system. Some pushbuttons are retained on the safety system panels for test initiation (channel trip and interlock functions) but the operating sequences of the various tests are computerized. The operator initiates the test before being guided by a computerized menu as the computer-based procedures (CBPs) are run. The operator can interrupt the tests or pause the tests for any length of time at various hold-points but does not have to make any decisions other than stop/go. In this fashion, the tests are semi-automatic in nature. The procedure-based automation (PBA) provides the detailed decision-making and controls the outputs for direct tests of individual end-devices and control components (e.g., valves, pumps, shut-off rods, and relay contacts), for electrical injection of simulated signals (e.g., into the neutronic amplifiers) and for entire loop tests.

The EC6 plant design will also provide computerized on-line monitoring of safety system pressure, level, and flow measurement instrumentation to provide added confidence between scheduled calibration/test intervals.

4. Conclusions

The EC6 plant is an innovative design that improves upon the proven safety and performance of the CANDU 6 and incorporates important design improvements to meet Canadian and international new build requirements for Gen III plants. Several important design improvements to the I&C systems have been made. These enhancements and their benefits have been described. Collectively, all of these changes will enable higher plant performance, improve safety, reduce operator errors, and improve overall plant life-cycle economics.

5. References

[1] CNSC Regulatory Standard RD-337: Design of New Nuclear Power Plants. November 2008.

[2] IEC 61513 - 2001, Nuclear Power Plants - Instrumentation and Control for Systems Important to Safety - General Requirements for Systems.

[3] IEC 62138 - 2004, Nuclear Power Plants - Instrumentation and Control Important to Safety - Software Aspects for Computer-based Systems Performing Category B and C Functions.

[4] IEC 60880 - 2006, Nuclear Power Plants - Instrumentation and Control Important to Safety - Software Aspects for Computer-based Systems Performing Category A Functions.

[5] CSA N290.14-07, Qualification of Pre-developed Software for use in Safety-related Instrumentation and Control in Nuclear Power Plants.

[6] CSA N290.13-05, Environmental Qualification of Equipment for CANDU Nuclear Power Plant.

[7] CSA N286.7-07, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants.

Acknowledgments

The EC6 electrical, control, and instrumentation system design team leads: S. Tikku, J. Harber, A. Xing, R. Brown, R. Leger, S. Inamdar, and K. Doerffer, and their respective design team members.