Evolution of the Enhanced CANDU-6 Monitoring and Control System Design

P. Foster, J. Harber, S. Tikku, A. Xing
Atomic Energy of Canada Limited
Mississauga, Ontario, Canada

Abstract

This paper describes the enhancements being made to the instrumentation and control (I&C) architecture and design approaches for the display/control systems in the Atomic Energy of Canada Limited (AECL®) Enhanced CANDU 6® (EC6®) plant design. These enhancements and design approaches ensure that the fundamental premise of independence between safety and process control is not compromised and that the reliability targets for each layer of protection are fulfilled to meet overall plant safety goals.

Advances in digital technology and modern human factors engineering principles must be considered by I&C designers without sacrificing the overall principles of defence-in-depth and the independence of safety functions (credited in the safety case). AECL has put a significant amount of effort into applying new technologies to the existing CANDU® 6 (C6) design while taking precautions to retain the original design intent and support the documented safety case.

1. Introduction

AECL is recognised as an innovator in successful implementation of computerized monitoring and control systems for process control and safety applications in nuclear power plants. In most of the operating CANDU designs, process control of plant systems is accomplished by a combination of digital control computers (DCCs), analogue control devices, and hardwired (HW) relay logic. In more recent CANDU designs, trip computer systems are used for certain shutdown system logic. Based on innovations introduced in AECL's newest reactor design, the Advanced CANDU Reactor®, AECL is enhancing its successful C6 design by applying its expertise in computerized control and safety computers to take advantage of modern digital technology (but still retaining conventional HW relay logic where appropriate). These enhancements to the C6 I&C functions are a part of the EC6 design project at AECL.

1.1 Background

From the very early days of design and construction of nuclear reactors in Canada, some key safety criteria and principles were established as part of the Canadian licensing framework. An important one was the high-level defence-in-depth concept of the plant being considered to consist of multiple layers, with the main three being the process system, the protective system (either for shutdown, initial cool down, or decay heat removal), and the containment system. The premise was that if these systems acted independent of one another, and each was of appropriate reliability, the chance of a significant release of radioactive material to the public domain would be kept extremely small [1].

In existing CANDU designs, process control at the highest level is performed by dual redundant DCCs, which execute a set of programs for monitoring, operator display, annunciation, and control of the reactor and important plant process functions. At a lower

level, conventional control devices such as analogue controllers and HW relay logic handle individual device control functions. The application programs for the DCCs are written in simple programming languages such as assembler, while the lower level device control logic is written in a symbolic language or is performed in HW relay logic.

AECL has also made advances in the application of computerized systems by developing and implementing multiple diverse trip computer systems in its more recent CANDU designs. In implementing computerized safety systems, AECL has produced, in consort with Canadian utilities, software development and qualification standards and internal software development practices for design of computer systems in important to safety (ITS) applications.

The advances in digital technology are being considered for use in the EC6 I&C architecture to take advantage of such improvements (for both process and safety systems). Enhanced information displays, data availability, networking, and internal maintenance diagnostics found in modern computer platforms increase the operator awareness and the plant availability and provide more flexibility in controlling and maintaining the plant. They provide the advantages associated with integrated control rooms for the operators to effectively operate the units in both normal and abnormal modes, and allow smarter solutions to meet plant performance and safety goals. However, these advantages must always be balanced against the requirements for independence between the various layers of defence and the complexity that computer systems bring with them in terms of the effort to approve them for use in a nuclear safety application.

1.2 Concepts for developing an I&C architecture

The features of the EC6 high-level I&C architecture support all of the redundancy, separation, qualification, and operational requirements associated with the various types of functions.

In general, control functions serve production or safety purposes, or sometimes both. In nuclear power plant designs, production functions are typically in continuous operation, whereas many safety functions are poised and ready to actuate a device or multiple devices based on some sort of conditioning and voting strategy. Functions that actuate on demand can make independent decisions to actuate each device individually, or a single decision to actuate all of the devices together with a common signal. In some cases, the same device is used for both production and safety purposes but has appropriate override logic such that the safety function always has priority.

The I&C architecture, which provides monitoring and control of the process and safety systems, is primarily based on the fundamental concept of defence-in-depth. In case the first layer of defence is compromised, independence ensures that the second layer is not impacted.

The main function of the process control systems is to keep the plant parameters within the normal operational range during operational conditions. Information and controls are available for automatic or operator-assisted actuation of corrective control actions in case the plant parameters depart from the normal operational range. The setpoints for alarms and/or automatic actuations allow mitigating actions to be performed and completed so that the limits for the actuation of the safety systems are not reached. With the use of robust designs, single

failures in the I&C architecture generally do not alter the plant parameters to the point where actuation of the safety systems is required.

The EC6 control systems and human system interfaces (HSIs) are developed in accordance with modern design practices. Human factors considerations, namely NUREG 0700 [2], are one of the primary focuses. The functions assigned to the operators and to automation are allocated according to a functional analysis of the control functions needed during the various plant states and operating modes and considering the limitations of human capabilities.

The specifications for all monitoring and control application functions are documented in a function block representation, based on IEC 61131-3 [3], rather than in computer program specific terms so that they are platform independent and are readily understood and reviewable by the I&C functional engineers, process engineers, and plant operators. Furthermore, standardization of I&C components across both the nuclear steam plant (NSP) and balance of plant (BOP) is utilized in order to reduce plant maintenance and operating costs over the life of the plant.

Functional categorization is used as a basis for allocating functions within the I&C architecture. The various I&C functions are categorized in terms of safety significance into safety function categories A, B, or C, in accordance with the project design guidelines, based on IEC 61226 [4], otherwise are deemed non-safety. Once categorized, each function is designed and implemented in accordance with the requirements associated with the category assigned to the function. If a system consists of a function in any category, it is considered ITS. If a component serves multiple functions, it is designed according to the category of highest importance associated with these functions.

Although the safety category may not affect the way the functional specifications are defined, they are an important input in determining the allocation of functions to the target hardware in the EC6 detailed design. They determine the safety classification and qualification requirements for the target platform and the software development work practices to be followed for implementation. ITS functions need to be traceable to the plant safety case.

The display/control systems are assigned to a safety class, consistent with IEC 61513 [5], to provide a general basis for implementing the functions as follows:

- Class 1 for Safety Function Category A functions (such as those belonging to the safety systems).
- Class 2 for Safety Function Category B functions (such as those belonging to safety support systems, systems that back-up safety systems, and other mitigating systems).
- Class 3 for Safety Function Category C functions (such as those belonging to process systems that are ITS).

The safety classes are listed in order of importance as the higher the class, the more stringent the requirements are for the display/control system. The Category A functions must be implemented using class 1 platforms, whereas the Category B functions may be implemented using either class 1 or class 2 platforms, and so on. Since some of the different layers of

protection credited for defence-in-depth have different safety function categories, independence among the safety classes helps maintain the fundamental defence-in-depth concept. The EC6 I&C architecture uses this philosophy.

In keeping with the existing principles of CANDU designs, plant safety functions are divided into two safety groups, group 1 (G1) and group 2 (G2), with the fundamental principles of control, cool, contain, and monitor in each group. The allocation into two groups provides two functionally and physically independent means for maintaining the key safety functions during common-mode events. For further reliability, the systems/functions that provide back-up for each other utilize platforms with diverse design, manufacture, and/or maintenance techniques.

2. EC6 overall I&C architecture

As discussed earlier, CANDU plant designs have typically used a pair of redundant DCCs to control and coordinate high level plant monitoring and control functions. The DCC logics were programmed in a low level assembly language and interfaced to individual loop controllers and relay logic for low level control functions such as operating end-device actuators. The DCCs were independent of the safety systems. A limited number of soft display screens and data entry keypads were provided for use by plant operators.

The EC6 NSP design has a more graded approach to safety, as per the functional categorization rules. A distributed control system (DCS) is used to provide data acquisition and control logic for the majority of the process and reactor control functions as well as many ITS functions. This DCS is divided into the plant control subsystem (PCSS), which is used for process systems and the reactor regulating system, and the essential control subsystem (ECSS), for safety support, back-up and other mitigating systems. As always, independent logic platforms are used for the safety systems. Figure 1 provides an overview of the I&C architecture of the EC6 plant design. The BOP controllers (which communicate with the NSP DCS), as well as other stand-alone controllers, are not shown.

The PCSS interfaces with the plant display system (PDS) and the primary annunciation system (which is hosted on the PDS) to provide monitoring, alarming, and some high-level input capabilities for the operator during normal operation. The ECSS and the safety systems are all monitored by the safety monitoring system (SMS). The safety systems, ECSS, and SMS (i.e., the functionality used during accident conditions) are independent of the PCSS and the PDS. The controls and displays (including window tile alarms) on the system panels are the primary HSIs for all process and safety functions, similar to previous CANDU reactors.

The EC6 PCSS is a modular digital system that uses a number of programmable controllers connected to a common data communication network designed in accordance with programmable electronic system (PES) standards and regulations. In addition to implementing the necessary process system control logic and the input/output (I/O) communication with field devices, the PCSS provides data acquisition for display, alarm generation, data recording, and data analysis functions performed by the PDS, which uses PES components as well.

The PDS is the interface used by the operator for monitoring and supervisory control, via video display units (VDUs) and associated keyboards, of some high-level group control functions executed by the PCSS. The PDS can accept operator inputs for setpoint entries and mode selections as well as for testing and calibration of field devices. The SMS, on the other hand, is used for monitoring purposes only.

2.1 Control systems

In the EC6 I&C design, control functions are divided into suites of functions, known as partitions, having a defined set of functional properties. The partitioning relates, in one manner or another, to the traditional control, cool, contain, and monitor philosophy. However, as far as practicable, two systems that have a relatively complex interface are assigned to the same partition.

In this context, a partition is a set of processors, digital components, and/or HW devices that are dedicated to a particular set of control functions and have some form of independence from components belonging to another partition. Partitions are sometimes capable of communicating with others, with appropriate signal buffering. Functional partitioning is necessary to facilitate construction and maintenance (smaller, simpler entities) and to limit the worst-case consequences of a common-mode event.

The communication networks are typically fibre-optic based and use optical isolation, where appropriate, to provide protection against possible cross-link electrical faults between the different partitions and between the control and display systems.

2.1.1 Plant control subsystem

The PCSS provides monitoring and control functions for process functions. As with any PES, the PCSS has control functions implemented using software programs in small, powerful, digital processor modules. The PCSS is a Class 3 PES and can therefore be used to implement ITS functions as long as they are suitable for this safety class. The PCSS has multiple partitions that provide a degree of functional separation between the primary side heat-sink (heat transport system), secondary side heat-sink (steam and feedwater system), reactor power control (reactor regulating system), and service (utility) functions.

The utility partition includes automatic testing and calibration logic, maintenance-related data acquisition associated with the process systems (e.g., health/status of pumps), and other pure monitoring functions (e.g., fuel surveillance and channel temperature monitoring).

Systems/functions that are part of an integrated package (e.g., seismic instrumentation, gas analysis system, meteorological monitoring, etc.) typically use stand-alone conventional or PES-based implementation, and are not considered partitions of the PCSS.

2.1.2 Essential control subsystem

The ECSS, which is a Class 2 PES, provides all of the Category B functions that are not provided by the safety systems, such as those from safety support, back-up and other mitigating systems. Limited functionality of these systems (i.e., external voting logic and

priority logic) is implemented in HW control circuits. The ECSS functions assigned to safety group G1 are independent of those associated with G2 in order to preserve the independence between the two means for shutdown, heat-sink management, and containment.

The ECSS controllers are designed to provide high reliability and data security, and include comprehensive self-checking, diagnostics (i.e., fault detection), modular redundancy, and switchover features, to provide a high degree of immunity to random component failures. PES components continuously monitor plant parameters for the validity of their input and output signals and internal operation, and give an alarm signal when needed.

2.1.3 Safety systems

Each safety system uses a dedicated safety-qualified logic platform, which may be a PES, a HW control circuit, or a combination of the two. Some of the functions belonging to the safety systems have minimal complexity and therefore use traditional HW relay logic. Relatively complex functions are more likely to be computerized. This is the case for certain functions belonging to the shutdown systems, which utilize trip computers. All of the key safety system functions can be manually initiated from the conventional control panels.

The safety systems are designed to Class 1 requirements. Each safety system is implemented as a dedicated Class 1 logic system, functionally and physically independent of the Class 2 and Class 3 systems. The reliability of the logic platform allows the overall availability target of the safety system to be met. The safety systems, which are divided appropriately into safety groups G1 and G2, are designed to survive postulated accident conditions through enhanced functional and physical separation. Adequate self-diagnostics are used. The analysis of the coverage of the self-diagnostics includes separate assessments for hardware and software faults. Features used to support automatic testing are incorporated into the safety system designs where appropriate, without compromising reliability due to undue complexity.

2.2 Display systems

The PDS components, which are not credited to be operational during accident conditions, are designed to Class 3 requirements. The PDS is primarily responsible for monitoring the plant parameters collected by the PCSS, but has access to all important safety information using buffered digital links. An important application hosted on the PDS is the primary annunciation system.

The primary annunciation system consists of coverage for all alarm and status signals detected in the plant. Hence, these signals are merged into a common presentation for the operators and other plant staff. The alarm list displays the messages in priority order based on consequence and response factors, whereas the status list displays the messages in chronological order. Another feature of the primary annunciation system is message coalescing, which consolidates multiple similar alarms (representing a known event) into a single annunciation message. The alarms of high importance also displayed in the back-up annunciation system, which is implemented using modern window tile technology.

The Class 2 SMS is used during all plant states, including postulated accident conditions. The safety systems and ECSS interface to the SMS through unidirectional network links, which are

configured for upward communication, such that the data only flows to the SMS. There is no communication between the SMS and the PCSS.

The SMS provides all the health measures and diagnostic information associated with the safety systems using qualified VDUs backed up by conventional HW displays. Also within the SMS envelope for the EC6 design are the parameters required for post-accident monitoring (PAM). The information includes trending of the various parameters and display of their respective safety limits to indicate the available margins. Using the SMS, the operators are able to determine the safety state of the reactor unit and obtain a comprehensive assessment of the accident conditions.

During transient plant operating conditions associated with accident scenarios, the operators continuously monitor the status of the plant using the SMS VDUs. Based on this information, along with cross-checking the data displayed on the PDS and the control actions taken by the PCSS, the operators determine the health of the plant. If the operators determine that the PDS and/or PCSS are/is not functioning properly, then they have the ability to gracefully bring the plant to a hot shutdown state based on the functions available on the SMS and/or HW display and control panels, along with any necessary field actions (including controls at the motor control centres).

2.3 Instrument channelization concepts

An EC6 instrumentation channel comprises interconnected hardware and software components that process one of the duplicated or triplicated signals associated with a single parameter. A channel may include the sensor, data acquisition, signal conditioning, data transmission, logic, and control actuator. This defines a subset of instrumentation that can be unambiguously tested or analyzed from end to end.

The instrumentation channels provide physical separation between safety systems (each safety system has its own set of channels), between groups, between safety systems and process control systems, and between redundant components within individual systems. The EC6 design, which retains the CANDU two-group philosophy, separates and assigns separate triplicated channel sets to each group. Using appropriate layout, barriers, and/or orientations, adequate physical separation between the G1 and G2 channels is achieved.

To reduce the number of instruments used in the EC6 design, signals available from safety and mitigating systems are, where appropriate, buffered to process control systems that use the same signals for production purposes. Furthermore, there are cases where the same end-device is used for both production and safety purposes and control interconnections (priority logic) are required. The channelization rules include restrictions on which channels are allowed to share or combine signals. When sharing, an appropriate isolation device is used and all shared components up to and including the isolation device are designed to the requirements of the system with the higher safety category.

Routine channelized testing and maintenance of I&C components, particularly of the safety systems, is performed when the reactor is at power and will not require plant outages. Overlapping tests, which may include periodic calibration as well as continuous monitoring

(including during transients) of certain loop components, will ensure the entire channel is functioning appropriately.

2.4 Operator interface and control hardware locations

The development of the operator interfaces in the main control room (MCR) and secondary control room (SCR) involves the coordination of many plant system designs in terms of data management, annunciation strategies, and display of information on the operator workstations. The designs of all HSIs consider modern human factors engineering concepts consistent with the design of modern nuclear plants.

The MCR facilitates the HSIs and procedure-based activities necessary for the reactor unit to be monitored and controlled safely and reliably by the operator. The NSP, BOP, and fuel handling (FH) operational activities all take place in the MCR. The NSP and BOP activities are integrated, whereas the FH activities are essentially independent. The HSIs encompass an assortment of computer consoles and conventional panels with embedded display screens, some of which belong/connect to the PDS and some to the SMS. Located in close proximity to the MCR is a control equipment room (CER), which contains logic cabinets for safety group G1 functions as well as equipment and connections (gateways) for the PDS and G1 SMS local area networks (LANs).

The SCR is used as a back-up control station during MCR uninhabitable conditions (i.e., situations preventing the operator from accessing the display and control functions available in the MCR). The EC6 SCR features display, alarm, and manual control devices that allow the operator to ensure safe reactor shutdown and proper long-term heat-sink management. This includes all safety group G2 functions and a limited set of G1 functions, such as basic monitoring and manual control of the safety systems. These functions are mainly performed using the conventional HW display and control panels along with the SMS. There is another CER near the SCR containing logic cabinets for safety group G2 functions as well as equipment and gateways for the G2 SMS LAN.

There are several remote field control facilities, separate from the control rooms, distributed throughout the field, to provide local control, monitoring, and annunciation (for infrequent manual operations and maintenance purposes). The remote field control facilities consist of panels with soft and/or conventional HSIs. An important feature of local annunciation is control discrepancy indications, which provide local alert to differences between device and selected control state. Alarms from local annunciation stations are forwarded to the PDS for presentation in the MCR.

2.5 Enhanced functionality of the EC6 plant design

The introduction of modern technology into a mature plant design permits the plant designer to retain the proven functionality of an existing design while providing new features typically found in a new plant design. For the EC6 plant design, the proven functionality of the existing control programs and HW logic is translated to new platforms. Modern system and software development processes and tools (including advanced simulation techniques) assist I&C designers in implementing the control strategies used in the C6 plant design. Additional

operational and maintenance benefits are realised by the increased use of digital platforms to implement safety functions in the EC6 plant design.

Modern display and control systems provide extensive operating, maintenance, and diagnostic information along with simplified interfaces to operational support systems. Advanced monitoring systems such as alarm prioritization, safety parameter trending, and data analysis tools improve the operator's ability to quickly and effectively diagnose and respond to plant upsets. Situational awareness of the overall plant status for the operator and maintainers is improved by these advanced monitoring systems used both on-line and off-line. Further, operator-assist functions such as automated safety system testing and computer-based procedures reduce the workload on plant operators and assist in their decision making.

3. Conclusions

AECL has a long history of successful computer applications for CANDU nuclear power plants. Modern digital methodologies, latest standards in the nuclear industry, and the experience that has been gained by AECL in implementing computer systems are being applied to defining I&C requirements for a modern nuclear power plant.

AECL has incorporated more digital technology into its existing C6 design to take advantage of its many benefits. The control system architecture for the EC6 has evolved from previous CANDU designs to provide the optimum balance of safety and production goals. This is done by applying modern technological advancements such as a DCS (functionally partitioned for improved reliability), and modern information and status displays in a systematic manner based on safety significance.

4. References

[1] D.G. Hurst and F.C. Boyd, "Reactor licensing and safety requirements", 12th Annual Conference of the Canadian Nuclear Association, Ottawa, June 1972, 72-CAN-102.

[2] NUREG 0700, "Human-System Interface Design Review Guidelines", Revision 2, US Nuclear Regulatory Commission Regulation, May 2002.

[3] IEC 61131-3, "Programmable controllers - Part 3: programming languages", Edition 2.0, January 2003.

[4] IEC 61226, "Nuclear power plants - instrumentation and control systems important to safety - classification of instrumentation and control functions", Edition 3.0, July 2009.

[5] IEC 61513, "Nuclear power plants - instrumentation and control for systems important to safety - general requirements for systems", Edition 1.0, March 2001.

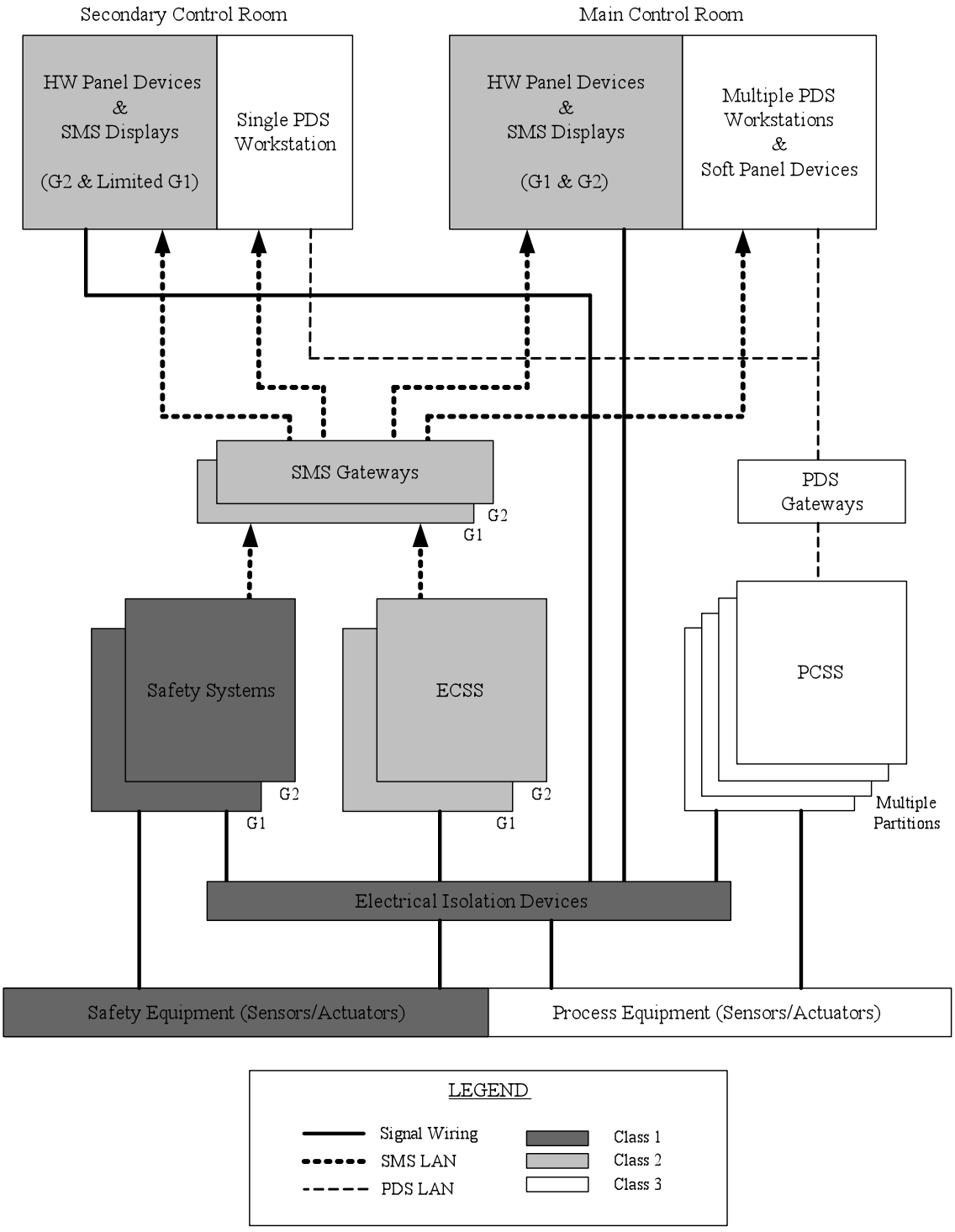

Figure 1 - Overview of the I&C Architecture in the EC6 Plant Design