Control System Design Considerations in a Modern Nuclear Power Plant

P. Foster, G. Raiskums, J. Harber, S. Tikku
Atomic Energy of Canada Limited
Mississauga, Ontario, Canada

Abstract

Applying new technologies is a challenge for instrumentation and control (I&C) designers to ensure that the overall principles of defence-in-depth, the independence of safety functions (credited in the safety case), and modern human factors engineering principles are maintained. This paper describes the Advanced CANDU Reactor® (ACR-1000®) I&C architecture, including the display/control systems and the design approaches employed to 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 the overall plant safety goals.

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 arrangements. In more recent CANDU designs, trip computer systems are used for certain shutdown system logic. In the newest reactor design, the ACR-1000, AECL is applying its expertise in computerized control and safety computers to take advantage of modern digital technology with limited use of HW relay logic.

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 first 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 system 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 safety related computer systems.

The advances in digital technology used in other industries must be considered for use in the ACR-1000 control system architecture to take advantage of such improvements. Enhanced information displays, data availability, networking, and internal maintenance diagnostics found in modern computer platforms improve the overall understanding of the control systems and the plant status. 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 license them for use in a nuclear safety application.

1.2 Concepts for developing the control system architecture

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 features of the ACR-1000 high-level I&C architecture support all of the redundancy, separation, qualification, and operational requirements associated with the various types of functions.

The I&C architecture, which provides monitoring and control of the process and safety systems, is primarily based on the fundamental defence-in-depth concept. The main function of the process 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. The use of robust designs ensures that no single failure in the I&C architecture can alter the plant parameters so that actuation of the safety systems is required. In case the first layer of defence is compromised, independence ensures that the second layer is not.

The ACR-1000 display/control systems are developed in accordance with modern design practices. Human factors considerations 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, Reference [2]) 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, the design and procurement of I&C components take electromagnetic interference considerations into account. 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 [3]), 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 safety-related function in any category, it is considered important to safety (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 ACR-1000 detailed design. They also determine the safety classification and qualification requirements for the target platform and the software work practices to be followed for implementation. Safety-related functions need to be traceable to the plant safety analysis.

The display/control systems are assigned to a safety class, consistent with IEC 61513 (Reference [4]), 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: the higher the class, the more stringent the requirements for the display/control system. Category A functions must be implemented in Class 1 display/control systems, whereas category B functions may be implemented in either Class 1 or Class 2 display/control systems, and category C functions may be implemented in either Class 1, Class 2, or Class 3 display/control systems. Independence among the classes is required to maintain the fundamental defence-in-depth concept.

For added defence-in-depth, the features of the ACR-1000 high-level I&C architecture are based on separating the essential functions (i.e., safety category A and B functions) into two safety groups: essential functional group 1 (EFG1) and essential functional group 2 (EFG2), with independent controllers/partitions and independent sets of signal channels. The arrangement of functions into EFG1 and EFG2 provides two functionally and physically independent pathways for shutdown, heat-sink management, and containment isolation. For further reliability, the systems/functions that provide back-up for each other utilize platforms with diverse design, manufacture, and/or maintenance techniques.

2. Control system architecture

The ACR-1000 design uses multiple distributed control systems (DCSs) to provide data acquisition and control logic for the majority of the plant functions as well as selected ITS functions, including some that are considered essential. The NSP DCS interfaces with the plant display system (PDS), plant annunciation system, and safety system monitor computers (SSMCs) to provide monitoring and alarms for the operator. The primary annunciation system is hosted on the PDS. The BOP DCS, which communicates with the NSP DCS, as well as the stand-alone controllers, which are used for minor process systems with simple control logic, are also considered part of the overall control system architecture. The safety systems are implemented in dedicated safety-qualified control systems, independent of each other but all monitored by the SSMCs. The safety systems and the SSMCs are separate from the DCS and the PDS. The conventional safety-qualified panel controls and displays (including "window tile" alarms) are used as back-ups to the essential functions. Figure 1 provides an overview of the I&C architecture of the ACR-1000 plant design.

The computerized portion of the ACR-1000 DCS is a modular digital system that uses a number of programmable controllers connected to common data communication networks designed in accordance with programmable electronic system (PES) standards and regulations. In addition to implementing the necessary control logic and loop control for plant and selected ITS functions and the input/output (I/O) communication with field devices, the DCS provides data acquisition for monitoring, alarm generation, display, and data recording functions performed by the PDS and SSMCs, which use PES components as well. The DCS also receives and executes operator commands, including commands for testing and calibration of field devices, entered via the PDS. The PDS is the main interface for the operator to monitor and control, via soft video display units (VDUs) and associated keyboards, the plant functions implemented in the DCS and has access to information on the SSMCs as well. The DCS is subdivided, to separate the plant and essential functions.

2.1 Functional partitioning

In the ACR-1000 I&C design, control functions are divided into groups, with each group of functions, known as a partition, 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.

Generally, a partition is a combination of control system components that are dedicated to a particular set of control functions and have some form of independence from components belonging to another partition. Some partitions are capable of communicating with others. Functional partitioning of the NSP DCS as well as the safety system components is necessary, to facilitate construction and maintenance (smaller, simpler entities), to limit the worst-case consequences of a major failure, and to separate mitigating functions from power production functions. Functional independence reduces common-mode failures of systems that are required to mitigate a particular initiating event, while offering maintainability and high availability for the various monitoring and control functions.

2.1.1 Nuclear steam plant distributed control system

The NSP DCS is subdivided into the plant control subsystem (PCSS) for plant functions and the essential control subsystem (ECSS) for essential functions. As with any PES, both of these control systems have control functions implemented using software programs in small, powerful, digital processor modules. Limited functionality of the ECSS (i.e., some voting logic, priority override logic, and other simple functions) is implemented in HW control circuits.

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 four basic partitions that provide a degree of functional separation. These are named according to the major systems/functions that are implemented in them:

- Heat transport system (HTS) and moderator system partition for primary side heat sinks.
- Steam generator (SG) and feedwater partition for secondary side heat sinks.
- Reactor Regulating System (RRS) partition for reactor power control.
- Monitoring partition for pure monitoring functions.

The PCSS monitoring partition does not include any control logic as it is only used for acquisition of (health/status) process system data. Monitoring functions that require multiplexing of a relatively large number of measurement signals from a remote location (e.g., fuel surveillance, channel temperature monitoring, etc.) or that are part of an integrated monitoring package (e.g., seismic instrumentation, standby generators, etc.) may use stand-alone controllers.

The ECSS, which provides all of the essential functions that are not provided by the safety systems, such as those from safety support, back-up, and other mitigating systems, is a Class 2 PES. The ECSS has two basic partitions separating functions in the two essential groups (EFG1 and EFG2) and preserving the independence between the two pathways for shutdown, heat-sink management, and containment isolation.

The PCSS and ECSS partitions are designed to provide high reliability and data security, and include comprehensive self-checking, diagnostics (i.e., fault detection), 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. The communication networks are intrinsically fibre-optic based and use optical isolation, where appropriate, to provide protection against possible cross-link faults between the different partitions or between channelized processors in the same partition.

2.1.2 Safety systems

Each safety system uses a dedicated control system, which may be a PES, a HW control circuit, or a combination of the two. Many of the control 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. To conform to reliability and separation requirements, the voting logic is completely HW for all safety systems, including the shutdown systems. All of the key safety system functions can be manually initiated from the conventional control panels as well.

The safety systems are designed to Class 1 requirements. Each safety system is implemented in a dedicated Class 1 control system, functionally and physically independent of the PCSS and ECSS. The control systems for the safety systems, along with the Class 2 ECSS, are designed to survive postulated accident conditions through seismic qualification, and enhanced functional and physical separation. Adequate self-diagnostics are used for safety systems and other ITS systems. The analysis of the coverage of the self-diagnostics includes separate assessments for hardware and software faults. Features used to support testing are incorporated into the system designs where appropriate, without compromising reliability due to undue complexity. These control systems are designed to an even higher availability target than the Class 3 PCSS. Figure 2 provides an overview of the various control platforms in the ACR-1000 plant design, showing the overall configuration of these systems and the interconnections between the systems.

2.2 Display systems

The plant annunciation system consists of coverage for all alarms and status signals detected in the PDS, as well as in the SSMCs. Hence, these signals are merged into a common presentation for the operators and other plant staff. The plant annunciation system includes a primary system as well as a back-up system. The primary annunciation system is implemented using an application hosted on the PDS. This separates the annunciations into an alarm list and a status list, and displays the appropriate messages. 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 that are displayed by the SSMCs are also displayed in the back-up annunciation system, which is implemented using modern HW “window tile” technology, but similar to that traditionally used.

The PDS components, which are not credited to be operational during accident conditions, are designed to Class 3. The PDS is primarily responsible for monitoring PCSS parameters. The SSMCs, on the other hand, are designed to survive postulated accident conditions and use Class 2 components. The Class 1 and Class 2 control systems interface to the SSMCs through unidirectional communication links. Although the PDS is Class 3, it is capable of receiving signals from the SSMCs using buffered digital communication links. Therefore, all information can be passed to the PDS for display, with no direct link between the safety systems and the PDS. There is no communication between the PDS and the ECSS and between the SSMCs and the PCSS.

The SSMCs provide all the health measures and diagnostic information associated with the safety systems using qualified soft VDUs backed up by conventional HW displays. Also within the SSMCs envelope for the ACR-1000 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 SSMCs, the operators are able to determine the safety state of the unit and obtain a comprehensive assessment of the accident conditions. All of the digital communication links are configured for unidirectional communication, from the essential and safety systems to the SSMCs.

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

2.3 Instrument channelization concepts

An ACR-1000 control channel comprises interconnected hardware and software components that process one of the duplicated, triplicated, or quadruplicated signals associated with a single parameter. A control channel may include the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic. This defines a subset of instrumentation that can be unambiguously tested or analyzed from end to end. The components/functions associated with the PCSS and PDS use plant control channels, whereas the components/functions associated with the ECSS, safety systems, and SSMCs use essential control channels.

The essential control channels are seismically qualified to design basis earthquake (DBE) Level B and, in terms of separation of equipment and signal cables, have more restrictions than the plant control channels. To reduce the number of instruments used in the ACR-1000 design, signals available from essential channels are, where appropriate, buffered to plant channels that use the same signals for production purposes.

For safety and high reliability applications, the ACR-1000 I&C design uses four channels of instrumentation with a two-out-of-four voting strategy (i.e., two of the four channels must be outside of the acceptable limits in order to trip/actuate the system). To perform on-line testing in this design, the operator will “bypass” the channel, using controls in the main control room (MCR) resulting in the actuation logic performing as two-out-of-three.

Routine channelized testing and maintenance of I&C components is performed when the reactor is at power and will not require plant outages. Periodic testing, as well as continuous monitoring (including during transients), will ensure the entire channel, including the measurements to the actuation devices themselves, is functioning appropriately.

2.4 Layout concepts

The four-division configuration of the essential electrical system and the four-channel approach used for control components and devices are aligned with the four-quadrant layout concept. The intention of the four-quadrant concept is to physically separate certain safety and safety support systems, along with their electrical (switch gear, motor control centres, batteries, cables, etc.) and control equipment, into four quadrants within the reactor auxiliary building (RAB) as shown in Figure 3.

There is one field control equipment room (FCER) located in each of the four quadrants of the RAB. The FCERs are remote from the MCR and close to the systems being monitored and/or controlled (i.e., close to the reactor building), reducing the quantities of cables, raceways, etc. The FCERs are multi-level structures with the elevations separated by fire barriers. The separated elevations are used to maintain independence between the appropriate control systems. The PCSS I/O as well as the stand-alone control equipment belonging to process systems/functions that are not part of the PCSS are physically separated from the ECSS I/O and safety system control equipment.

Most of the DCS inputs and outputs (both analogue and digital) are controlled by the device processors via channelized remote I/O stations located, along with other control equipment, in the FCERs. The use of remote I/O helps support the separation of channels and allows for a less complex cabling system and ease of maintenance.

2.5 Operator interface and control hardware locations

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

The MCR facilitates the human-system interfaces (HSIs) and procedurally 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 NSP and BOP HSIs encompass an assortment of computer consoles, conventional panels, and large-screen displays, some of which belong/connect to the PDS and some to the SSMCs. Located in close proximity to the MCR is the central control equipment room (CCER), which contains PCSS components (and a limited number of ECSS components) as well as equipment and connections (gateways) for the PDS local area network (LAN).

The secondary control room (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 ACR-1000 SCR features display, alarm, and control functions that allow the operator to ensure safe reactor shutdown and proper long-term heat-sink management. This includes basic monitoring and manual control of the safety systems and other ITS systems/functions, as well as the emergency diesel generators. These functions are mainly performed using the SSMCs along with the conventional HW display and control panels. The PDS, which is not credited for accident conditions, provides additional functionality when available.

There are several remote field control facilities, separate from the FCERs, 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 computer consoles and/or conventional panels. 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 may be forwarded to the primary annunciation system for presentation at the main console.

Process systems that are not controlled and/or monitored via the DCS/PDS use either a stand-alone PES (e.g., programmable logic controller), a HW control circuit, or are operated manually. These systems typically have local readouts and gauges for field monitoring. This equipment is located as close to the system as possible, and/or in the nearest FCER, where appropriate.

3. Conclusion

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

The control system architecture for the ACR-1000 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 distributed control system (functionally partitioned for improved reliability), and modern information and status displays applied 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] IEC 61131-3, “Programmable controllers - Part 3: programming languages”, Edition 2.0, May 2003.

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

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

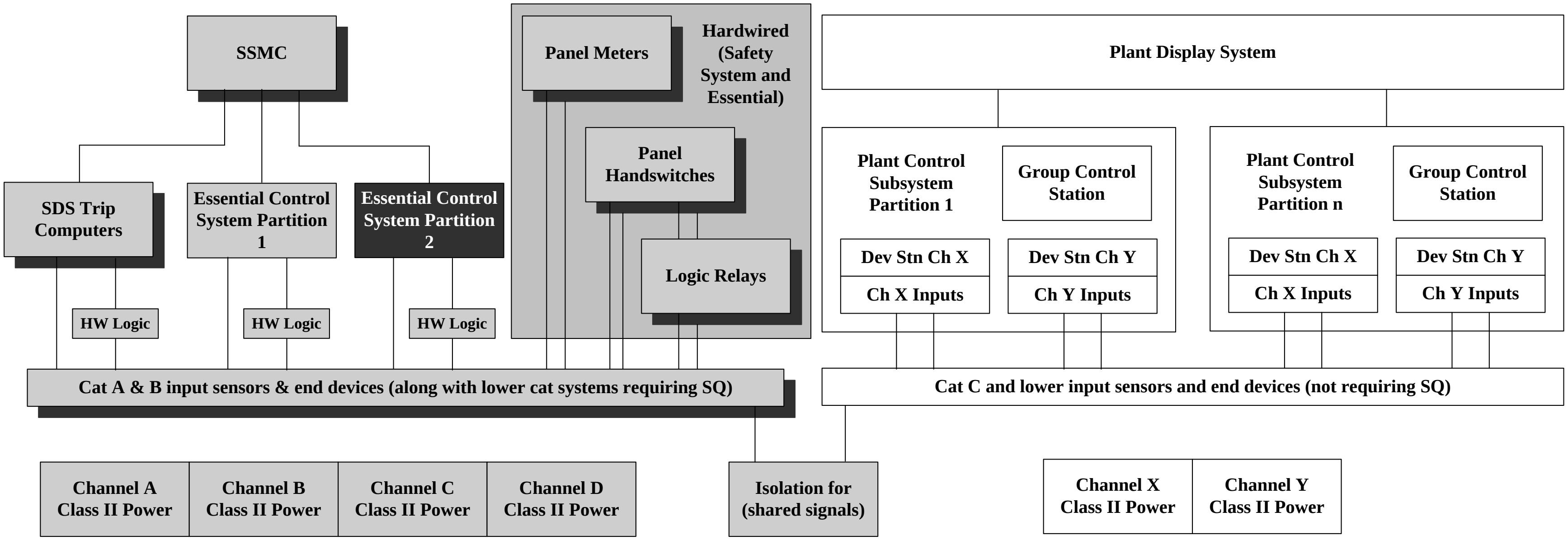

Figure 1 - Overview of the I&C Architecture in the ACR-1000 Plant Design

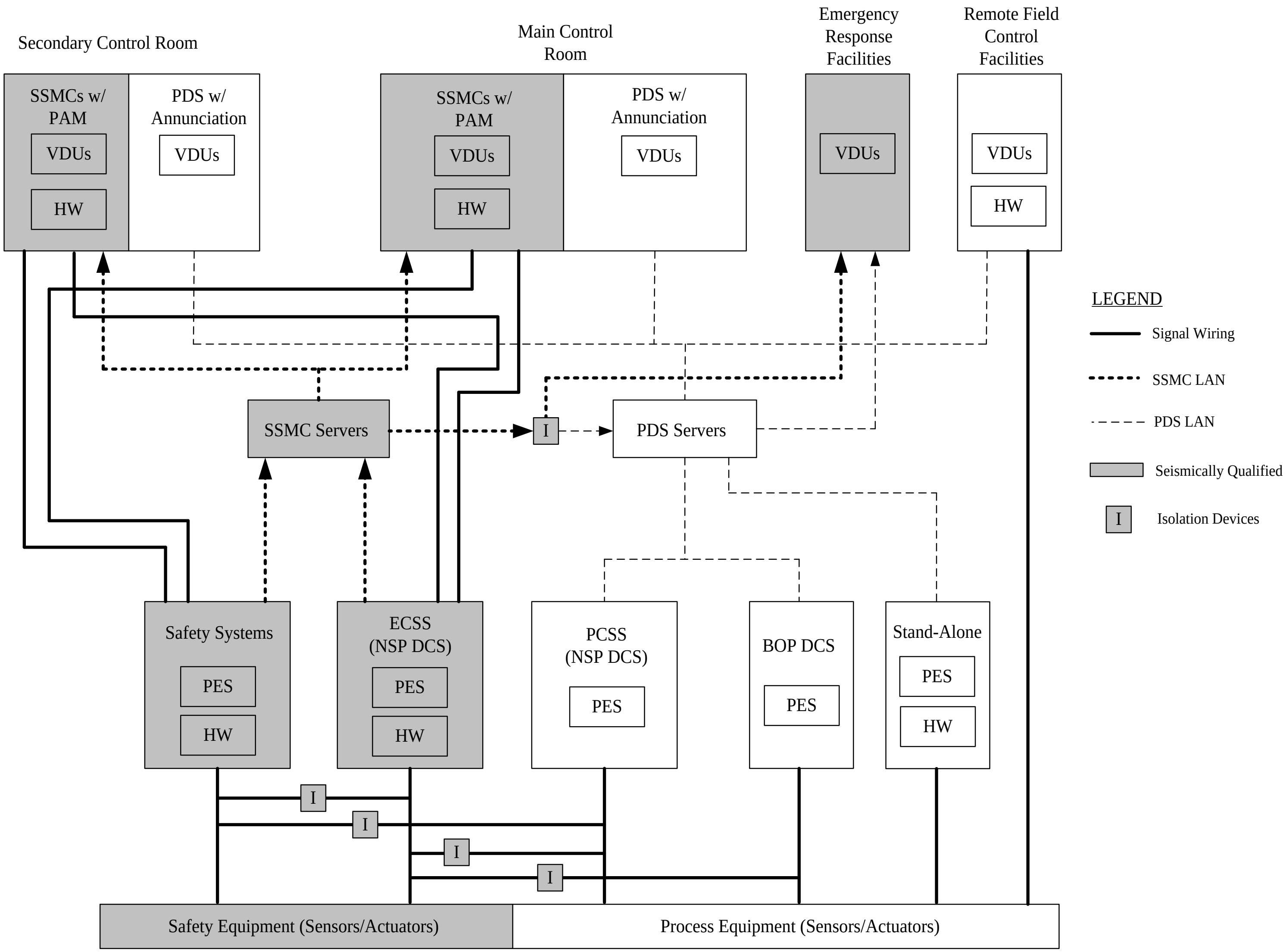

Figure 2 - Overview of the Control Platforms of the ACR-1000 Plant Design

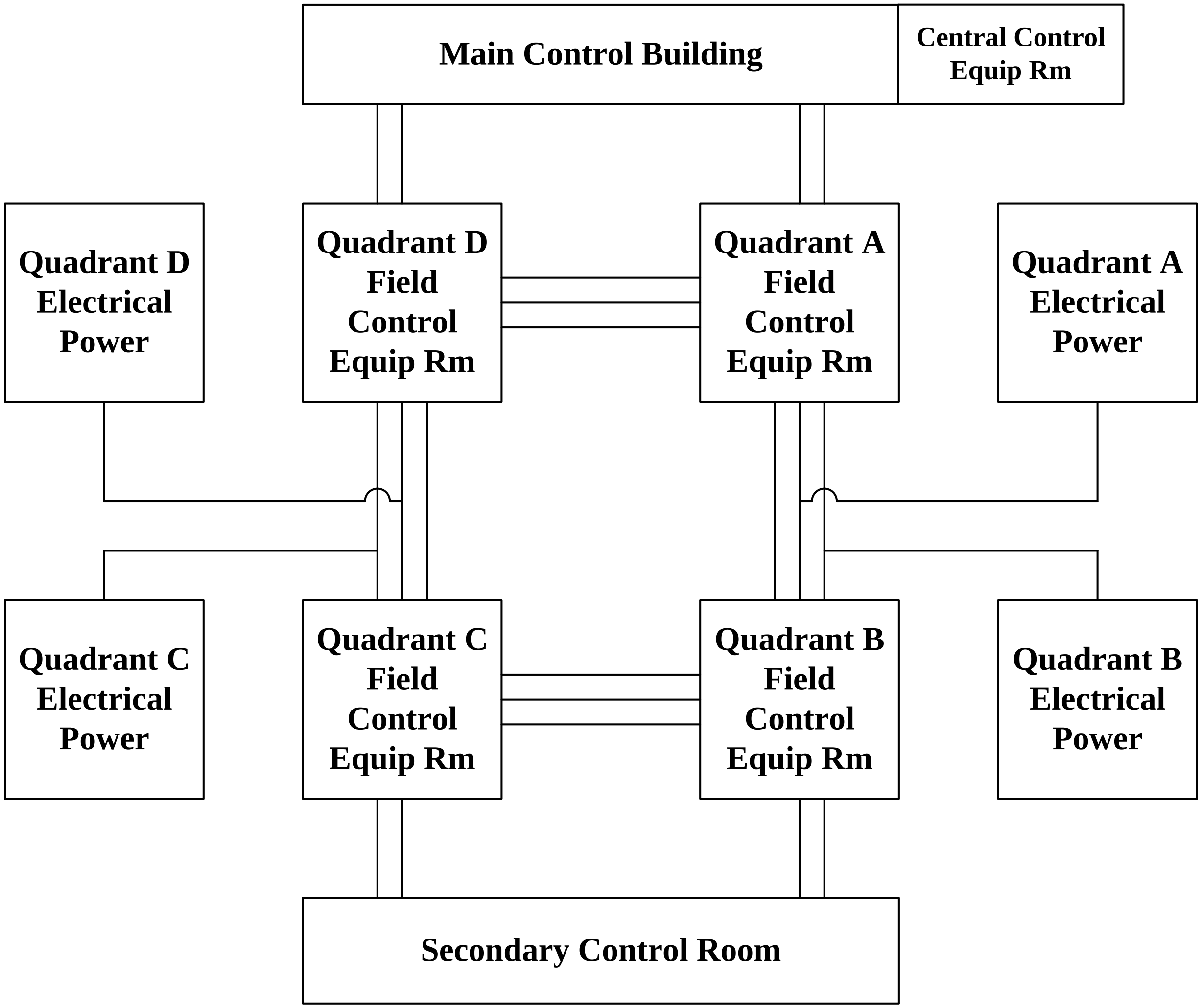
Main Control Building
Central Control Equip Rm
Quadrant D Electrical Power
Quadrant D Field Control Equip Rm
Quadrant A Field Control Equip Rm
Quadrant A Electrical Power
Quadrant C Electrical Power
Quadrant C Field Control Equip Rm
Quadrant B Field Control Equip Rm
Quadrant B Electrical Power
Secondary Control Room

Figure 3 - Simplified Layout of the Field Control Equipment Rooms in the ACR-1000 Plant Design