Development, Application and Licensing of FPGA Based Safety Systems

Terrence C. Tuite [1], Jorge V. Carvajal[2]
[1] Westinghouse Electric Company, Pennsylvania, United States
(tuitetc@westinghouse.com)
[2] Westinghouse Electric Company, Pennsylvania, United States
(carvajjv@westinghouse.com)

Abstract

Westinghouse has developed the Advanced Logic System® (ALS®) platform. The ALS platform was recently approved by the US NRC. In addition, ALS was successfully installed and declared operational as a Thermocouple/Core Cooling Monitor upgrade at the Wolf Creek Generating Station. The ALS has also been installed at the AP1000 Sanmen and Haiyang unit sites as the Diverse Actuation System. The ALS platform is based on FPGA technology. FPGA safety system designs are simpler than comparable CPU based system designs in that they do not require an Operating System or instruction set. The ALS platform provides inherent diversity in redundant cores and diverse core designs. In addition, the ALS provides extensive self-testing and diagnostics which allows for extension of plant surveillance intervals.

1. Introduction

The ALS platform is a logic based platform which does not utilize a microprocessor or software for operation, but instead relies on simple hardware architecture. The logic is implemented using Field Programmable Gate Array (FPGA) technology. The ALS platform is nuclear safety related (Class 1E). It is important to note that in the ALS platform, the use of an FPGA, and associated development processes were approved by the NRC under Docket 50 482, Amendment 181 to License No. NPF 42 [1] for use in a main steam feedwater isolation system (MSFIS) application at the Wolf Creek Generating Station. The resulting safety evaluation report (SER) [2] included guidance on the use of the ALS platform in future applications.

The ALS platform was resubmitted under letter dated July 29, 2010, ADAMS Accession No. ML102160471, [3], which included the ALS platform Topical Report 6002-00301 [4]. This new submittal documented the enhancements to the ALS platform since the original ALS platform approval based on the guidance provided by the original SER [2]. The enhancements enable the ALS platform to be generically approved for use in a variety of Class 1E safety applications. These enhancements include incorporation of new hardware components (i.e., analog input board, analog output board, and communication board), incorporation of new features (redundant Reliable ALS Bus [RAB], new ALS Service Unit [ASU] interface, and online setpoint adjustment), and enhancements to the design process in the area of Independent Verification and Validation (IV&V). This topical report was approved by the NRC in July of 2013 per SER [5].

2. Background

The increasing recognition of the efficiency, economic advantages and environmental benefits of nuclear power has prompted a renewed interest in nuclear plant license extensions and the accompanying upgrading and maintenance of their Instrumentation and Control (I&C) systems.

New technologies are being applied to nuclear I&C systems to address this need, including FPGA (Field Programmable Gate Array)-based systems. These hardware-based systems provide high reliability and deterministic behavior by eliminating weaknesses of software-based systems, such as the asynchronous behavior of operating systems.

Westinghouse has developed and qualified the ALS Platform, an FPGA-based platform for nuclear I&C safety systems. The ALS platform is intended to be the basis for future Westinghouse Class 1E and other systems requiring inherent diversity. The ALS platform supports easy and reliable implementation of both Class 1E and non-1E systems.

3. History

In late 2003, Wolf Creek Nuclear Generating Station had a need to replace some of their safety-related I&C systems due to reliability and obsolescence issues. Based on this need and the fact that no viable solutions existed in the market place (i.e., current digital safety system offerings are CPU based designs that require an Operating System or instruction set and; therefore, are susceptible to Software Common Cause Failures [SWCCF]), Wolf Creek began working towards a new approach. In early 2004, Wolf Creek partnered with CS Innovations on a new approach to replacing safety related I&C systems. As a result of this partnership, the ALS architecture was proposed as a general safety platform to target the U.S. Nuclear Power Plant (NPP) Safety Related I&C System upgrade market.

The ALS platform is designed as a universal safety system platform. The ALS provides advanced diagnostics and testability features which improve the plant I&C personnel's ability to perform surveillance testing as well as diagnose failure detection should they occur. System integrity is greatly increased over the existing systems by eliminating single point vulnerabilities with the ability to identify and address any failure within the system without causing plant transient. The reliability of the system increases due to the simplicity of the ALS architecture and incorporation of repeatable advanced design processes for system development. Issues associated with future obsolescence are solved by incorporating a common platform across multiple applications. In addition to solving the above issues, the ALS platform provides benefits in the area of common spares and common training for station personnel. These benefits are realized by the ability of the ALS platform to be installed as a common platform which all safety related I&C systems can be based upon.

The ALS platform has been fully designed, built, and tested. The ALS platform meets or exceeds all of the mild Environmental, Seismic and EMC qualification testing requirements. This high level of environmental robustness ensures the ALS can be installed in all of the environments that existing nuclear power plant safety related I&C systems currently reside.

4. Technical Description

The ALS is a universal platform which targets nuclear safety critical applications, where reliability and integrity are of the utmost importance. The ALS is a logic based platform which does not utilize a microprocessor or software for operation, but instead relies on simplified hardware architecture and adherence to proven design methodology.

The ALS platform is designed to be at the appropriate level of complexity to achieve high reliability and integrity as well as allow enough flexibility to target multiple nuclear safety critical applications within a nuclear power plant. Redundancy and embedded self-test capability ensure integrity of the installed ALS system by detecting and announcing faults. Diagnostics and testing capabilities are designed into the ALS platform to ensure there is a systematic approach to maintaining and testing the system. A generic ALS platform chassis is illustrated in Figure 1.

The ALS is a modular platform where generic modules, referred to as ALS boards, can be combined in various configurations to solve a wide variety of nuclear safety applications. This also provides scalability allowing for a single system upgrade up to a full set of safety system upgrades using the same ALS platform. An available configuration is one that implements an inherent diversity within the FPGA platform design such that the safety analysis required by BTP 7-19 [6] is normally not necessary. This feature is discussed later in this report in subsection 5.2.

A safety application implemented using the ALS platform typically consists of one or more ALS chassis and peripheral equipment consisting of Cabinets, Power Supplies, Control Panels, Assembly Panels and ALS Service Units (ASU). The Assembly Panels incorporate field terminal blocks, fuse holders, switches, and other application specific hardware.

The ALS platform supports a wide range of field Input/Output (I/O) types, such as digital inputs, analog current and voltage inputs, Resistance Temperature Detector (RTD) and Thermocouple (TC) inputs, as well as contact and relay outputs. The ALS platform also supports communication datalinks.

The ALS chassis is an industry standard 19" chassis and can be mounted in a wide variety of existing 19" cabinets. Each chassis contains a number of boards which is dependent on the particular safety application as well as the type of boards that are installed into the chassis. Multiple ALS chassis can be connected together through an expansion bus if more boards are needed for a particular application (see Figure 1 for a typical ALS chassis populated with boards). The ALS internal bus system architecture allows for up to 60 boards to be connected in up to six different locally connected chassis (one main chassis and 5 Expansion Chassis connected within the same cabinet).

An ALS chassis may be powered from the Class 1E power source to a redundant pair of current-sharing external power supplies. The external power supplies ensure a stable ALS chassis voltage of 48V. Additional power supplies may be needed to power field I/O based on the particular application.

Figure 1 ALS Chassis Populated with Eight Boards.

4.1 ALS Boards and Features

The ALS platform is based on a combination of generic ALS boards, which allow for predefined configuration settings, and dedicated ALS boards, where the FPGA logic is configured for a specific application. Examples of such ALS boards are listed in the Table 1.

Table 1 ALS board types and features

Type	Name	Channels	Description	Use
ALS-102	Logic Board	6 DI, 4DO, 2 Comm	FPGA Based Logic Board	Performs application specific safety functions and controls the primary system functions.
ALS-302	Digital Input	32	Contact Input Board	Perform signal conditioning, sensing and filtering of field input signals.
ALS-311	Analog Input	8	TC / RTD Input Board	
ALS-321	Analog Input	8	Voltage / Current Input Board	
ALS-402	Digital Output	16	Solid State Contact Board	Responsible for controlling and conditioning of field output signals.
ALS-421	Analog Output	8	Voltage/Current Board	

Type	Name	Channels	Description	Use
ALS-601	Communications	8	EIA-422/485 Comm. Board	Provides secure communication links to external systems.
RAB	Reliable ALS Bus	-	Safety related communication buses	The two RAB busses are each implemented as independent and separate busses that are used for safety system function communication between ALS boards.
TAB	Test ALS Bus	-	Maintenance communication bus	TAB is used to transfer monitoring, diagnostics, test and calibration information.
ASU	ALS Service Unit	-	Connection to advanced features of the ALS system	ASU provides plant personnel access to features of the ALS system such as system diagnostics, post-trip analysis, monitoring real-time operation and calibration and maintenance operations.

The ALS platform includes a number of ALS boards where the I/O board(s) functions are fixed slaves to the ALS-102 CLB which contains the specific application logic capable of performing very specific safety critical function. All ALS boards are identified by a three digit ALS number where the first digit defines the board type and they have all been defined in the previous table. Figure 2 is an illustration of a generic ALS platform architecture and the base architecture showing the relationship between input boards, logic boards, output boards and communication boards. The actual number and type of boards will depend on the specific application configured.

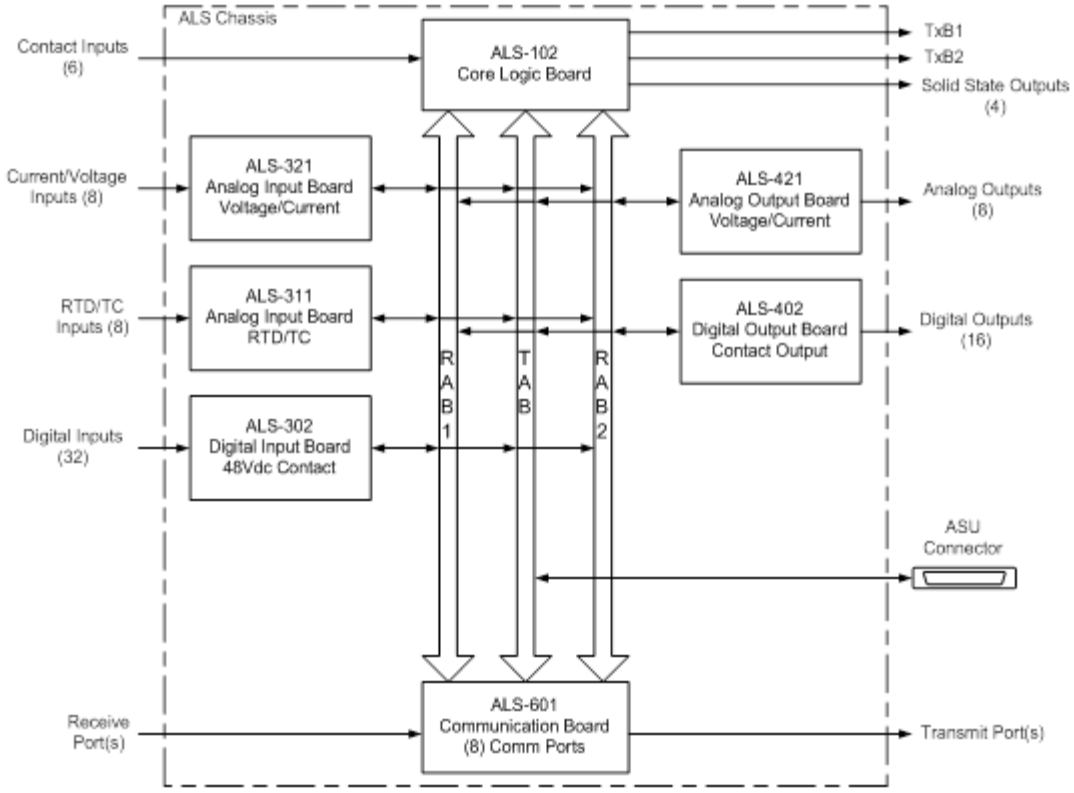

Figure 2 Generic ALS Platform Architecture Overview.

5. Benefits

5.1 Application Flexibility

The ALS platform is the first FPGA-based Safety System with U.S. NRC approval. The ALS platform has been designed as a universal safety system platform consisting of the ALS chassis and associated ALS boards that can be combined in various configurations to implement a variety of nuclear safety applications.

The ALS platform can be utilized as the foundation for multiple safety-related I&C applications such as:

- Diesel Load Sequencers
- Post Accident Monitoring
- Reactor Protection Systems
- Diverse Protection Systems

5.2 Diversity

The ALS platform inherently provides diversity attributes integrated within the ALS platform. The ALS platform uses key design attributes which provide a foundation that licensees may use in their Diversity and Defense in Depth (D3) analysis to construct reliable safety systems, because the design concepts have been specifically constructed to mitigate the likelihood of Software Common Cause Failures (SWCCF). As such, a licensee could demonstrate its use of the ALS platform's key attributes to justify the elimination of a diverse actuation system for some plant-applications. These design attributes provide two levels of diversity features. 1) Core Diversity; is the fundamental level of diversity which can be used in applications. 2) Embedded Design Diversity; adds additional design diversity and is intended for those applications in which a diverse backup does not exist (i.e., Diesel Load Sequencer [DLS] application). This section provides further explanation of these diversity levels.

The ALS platform incorporates two levels of diversity: Core Diversity and Embedded Design Diversity. The first level, Core Diversity, is implemented for each of the FPGAs on all of the ALS boards. Each of the FPGA images contains two sets of redundant logic, called a core. The diversity between the two cores is achieved by changing the logic implementation during the synthesis and Place & Route process. The synthesis process utilizes the hardware descriptive language (HDL), which is a formal specification of the configuration of the hardware circuits to be implemented in the FPGA. The synthesis of the HDL is performed using one type of hierarchical structure and finite state machine (FSM) encoding for the first set of logic in the core and a second type of hierarchical structure and FSM encoding for the second set of logic in the core. The logic for each of the two cores then undergoes the place and route process, and is then tested to validate proper operation. An independent V&V team verifies and validates the design for correctness and proper performance of the safety function. This results in a design that provides an FPGA image with two cores for redundancy checking as well as diversity.

The second level of diversity, Embedded Design Diversity, implements additional design diversity. This development process results in the production of two diverse FPGA images, A and B, which implement the same functionality in a diverse manner.

Therefore, the inherent diversity attributes of the ALS platform provides a manageable means for the licensee to address SWCCF associated with nuclear I&C safety system upgrade projects. The implementation of both Core Diversity and Embedded Design Diversity results in a Core A chassis subsystem and a Core B chassis subsystem that are comprised of the same ALS hardware modules; therefore, providing the same look and feel from both a maintenance and operations perspective. Additionally, common set of spare boards are provided and can be programmed/configured as either a Core A or Core B board. The Human Machine Interfaces to both Core A&B subsystems are identical. The implementation of the two Cores A&B designs allows for application configurations to mitigate SWCCF associated with I&C safety system upgrades without having to implement a separate Diverse Actuation System (DAS).

5.3 ALS Longevity and Support

The Westinghouse ALS platform is intended to be the basis for future Westinghouse Class 1E and other systems requiring inherent diversity. The ALS platform supports both Class 1E and non-1E applications. The ALS platform also has the added advantage of being employed in the AP1000™ Nuclear Power Plant I&C system design for the Diverse Actuation System (DAS) application.

5.4 Quality Assurance

NRC review of the ALS platform quality assurance program has determined that it conforms to 10 CFR Part 50, Appendix B, and 10 CFR Part 21 for nuclear industry safety related work.

5.5 Regulatory Compliance

The ALS platform is compliant to the following codes, standards and regulations as specified:

- IEEE-603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- IEEE 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- DI&C-ISG-04, Interim Staff Guidance 04: Highly Integrated Control Rooms – Communications Issues
- BTP 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- BTP 7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems
- Regulatory Guide 1.152, Criteria for use of Computers in Safety Systems of Nuclear Power Plants
- DI&C ISG-06, Interim Staff Guidance 06: Digital I&C Licensing Process

6. Experience

Westinghouse ALS Installations

- 2009: Installed and operational at the Wolf Creek site, United States
  Main Steam and Feedwater Isolation system (MSFIS) Controls

- 2014: Installed and operational at the Wolf Creek site, United States
  Thermocouple/Core Cooling Monitor (TC/CCM) System

- 2014: Installed in AP1000 Plants, Sanmen 1 and Haiyang 1 in China
  Diverse Actuation System (DAS)

- Future ALS installations
  Process Protection System (PPS) will be installed in Diablo Canyon 1 and 2, in United States
  Diverse Actuation System (DAS) will be installed in all AP-1000 Plants Sanmen 2 and Haiyang 2, in China

Diverse Actuation System (DAS) will be installed in Vogtle 3 and 4, Summer 2 and 3 in United States

6.1 Wolf Creek Main Steam and Feedwater Isolation system Controls Experience

MSFIS was designed as a safety related replacement system for the Wolf Creek Generating Station Site and successfully installed in 2009. Figure 3 shows the high level logical overview. The MSFIS receives discrete (ON/OFF) signals in the form of contact states from two separate systems/locations, which are the manual inputs from the Main Control Board (MCB) and automatic inputs from the Solid State Protection System (SSPS)/ Engineered Safety Features Actuation System (ESFAS). The actuation system consists of two redundant, independent and separated actuation trains to control the valves.

- MSFIS Channel I (Separation Group 1) – also referred to as train A.
- MSFIS Channel IV (Separation Group 4) – also referred to as train B.

Each Separation Group is installed in a separate cabinet, and both separation groups actuate the same Main Steam Isolation Valve (MSIV) and Main Feedwater Isolation Valve (MFIV).

MSFIS receive inputs from a variety of locations: operator inputs from the Main Control Board (MCB) switches, ESFAS actuation signals from ESFAS/SSPS and valve feed-back from valve position switches. The input signals are signal conditioned using the ALS-301 boards.

Locally on the rack front-panel provide the operator with access to a place the valve in BYPASS mode. The rack provides local LED-indication of all input/output signals on the ALS-rack front-panel, as well as remote indication (to MCB) of STATUS and ALARM and BYPASS indication (to SSPS).

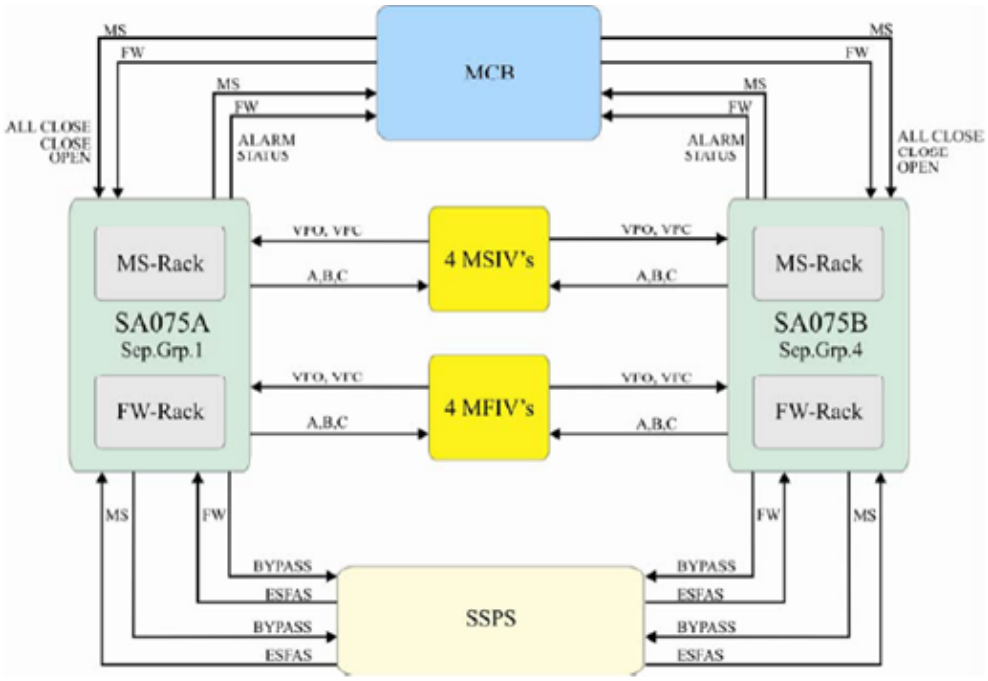

Figure 3 MSFIS block diagram.

6.2 Wolf Greek Thermocouple and Core Cooling Monitor System Experience

The Thermocouple Core Cooling Monitoring (TC/CCM) system was designed to be a fit, form and functional replacement of the existing TC/CCM system at the Wolf Creek Generating Station site. As such the TC/CCCM system was installed in the existing cabinet while employing the existing field cabling. This system was successfully installed in April of 2014.

The TC/CCM provides a margin to saturation meter as well as caution and alarm alerts to the Master Control Board (MCB). A serial datalink is provided to the Plant Computer System (PCS). The saturation meter, caution and alarm alerts as well as the data contained in the serial datalink is based on the monitored core temperatures and pressures.

The TC/CCM provides information to the plant operators regarding the adequacy of reactor core cooling during normal shutdown conditions, abnormal events and postulated accidents. The basic inputs and outputs of the TC/CCM system are shown in Figure 4. Figure 5 shows the Train A and Train B displays as installed at the Wolf Creek site.

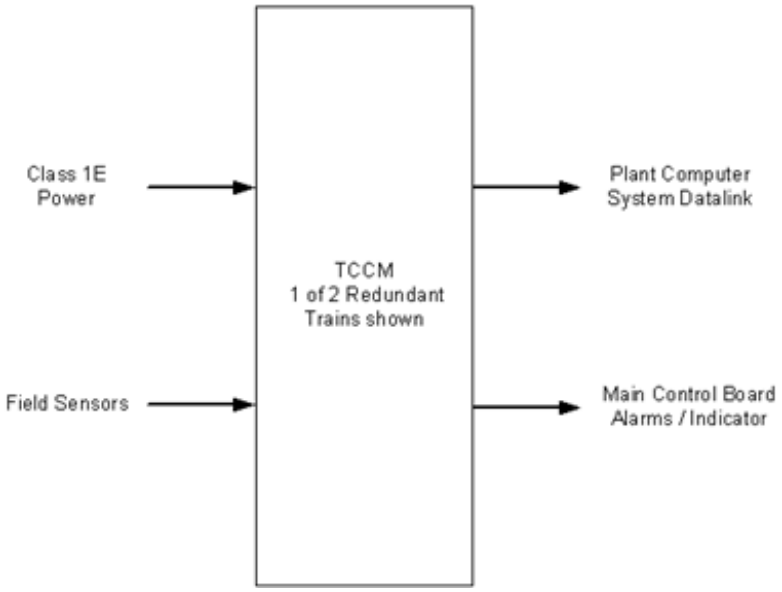

Figure 4 TC/CCM High Level Diagram (One Train Shown).

Figure 5 TC/CCM Train A and Train B installed.

6.3 AP1000 Diverse Actuation System Experience

The Diverse Actuation System (DAS) that is required for operation of the AP1000™ Nuclear Power Plant and is based on the ALS platform.

The DAS is a non-safety related system that provides a diverse backup to the Protection and Safety Monitoring System (PMS) in case of an unlikely Common-Cause Failure (CCF) of the PMS. This backup is included to support the aggressive AP1000 risk goals by reducing the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated CCF in PMS.

The DAS provides an alternate means of initiating a reactor trip and actuating selected engineered safety features, and provides plant information to the operator.

The PMS is designed and qualified to prevent CCFs. However, in the low probability case of a CCF occurring, the DAS provides diverse protection.

The DAS accepts inputs from non-Class 1E power, field sensors and manual system level commands; and provides outputs to field components, control room indicators and plant and computer alarm systems as shown in Figure 6, "DAS High Level Inputs and Outputs."

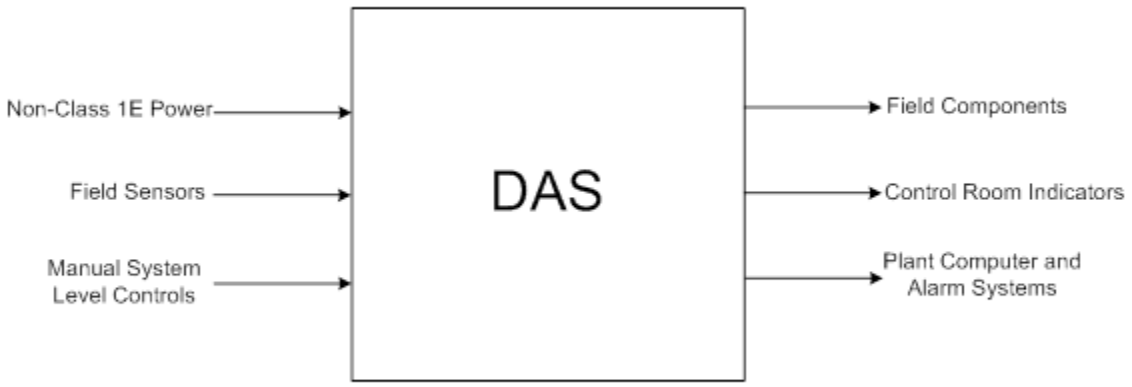

Figure 6 DAS High Level Inputs and Outputs

6.4 Diablo Canyon Process Protection System Upgrade Experience

The scope of this project is the replacement of the Eagle 21 Process Protection System (E21 PPS) equipment for Diablo Canyon Power Plant Units 1 and 2. The project replaces the Westinghouse Eagle 21 protection sets currently housed in Protection Racks 1 – 16 in the Cable Spreading Room. The Eagle 21 was installed in 1994 to replace the original analog Westinghouse 7100 PPS.

Figure 7 shows the proposed PPS replacement system utilizing the software-based Triconex Tricon processor to implement those safety functions where existing safety analysis has determined that diverse and independent automatic mitigating functions are available to mitigate the effects of postulated Common Cause Failure (CCF) concurrent with FSAR Chapter 15 events. For the safety functions where existing analyses credit manual mitigative action under 30 minutes, automatic protective functions will be performed in the diverse safety-related Westinghouse ALS utilizing ALS Core A/B inherent design diversity. These safety functions include the following and are shown per Figure 7:

- Low reactor coolant flow mitigation of loss of reactor coolant flow due to a locked rotor;
- Low Pressurizer Pressure mitigation of RCS depressurization, steam line break and Loss of Coolant Accident (LOCA); and
- High Containment pressure mitigation of steam line break and LOCA.
- Additional, the ALS processes all RTD inputs and provides a 4-20mA signal to the Tricon subsystem.

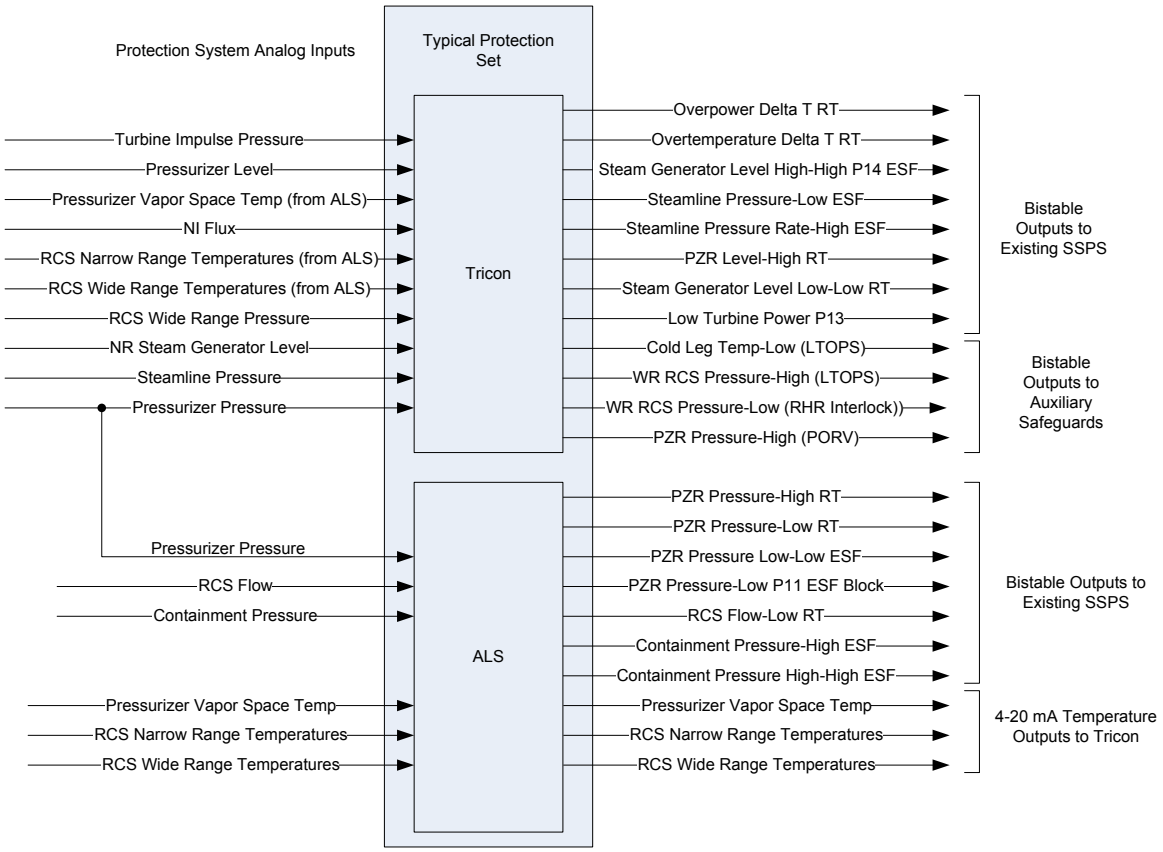

Figure 7 Typical PPS Safety Functions

6.5 Diesel Load Sequencer Experience

Westinghouse has performed significant work in the area of the Diesel Load Sequencer (DLS) application. The ALS platform is the platform of choice for the replacement for a DLS application due to the inherent diversity attributes of the platform.

The function of the DLS is to provide controlled loading of the Emergency Diesel Generator(s) (EDGs) during a station blackout (Loss of Offsite Power [LOOP]) in the presence or absence of an event that requires a Safety Injection (SI) actuation.
Plants typically have two EDGs (i.e., two trains), each of which has an associated DLS.
A DLS typically has multiple SI and multiple undervoltage (UV) inputs that are combined via coincidence logic to actuate the SI Sequencer (SIS) or Blackout Sequencer (BOS) (i.e., load equipment, primarily pumps, onto the EDG) as required. Some DLSs perform a loadshed function and some actually start the EDGs. The DLS is fundamentally a "black box" function that has no functional diversity. Therefore, diversity considerations are limited to those internal to the DLS "black box".

A Diversity Strategy is required for the DLS applications because there is no diverse backup for the sequencer application, and manual action before 30 minutes, cannot be credited; therefore utilize both levels of the ALS platform diversity attributes, including Core Diversity and Embedded Design Diversity resulting in a Core A (Train A)/Core B (Train B) design configuration which adequately mitigates the likelihood of SWCCFs.

6.6 Operational Experience

Although the ALS installation base is limited, there has not been a reported failure of the ALS hardware since installation at the Wolf Creek nuclear power station for either the MSFIS or the TC/CMM installation. The ALS platform has also been installed and energized in multiple AP1000 DAS applications without a reportable failure and is currently being used for site integration testing activities.

The hardware design of the ALS platform is simple and robust and employs a common design across all of the ALS boards.

7. Summary and Conclusion

The ALS platform provides key diversity attributes inherent within the product that can be used to address diversity issues associated with digital protection system upgrades.

Because of the uniqueness of the ALS digital platform design (FPGA based rather than processor based), a generic description of the Defense-in-Depth and Diversity (D3) design concept for the ALS platform design can be used in plant specific applications providing a foundation that licensees can use in their D3 analysis to construct reliable safety systems, because the design concepts have been specifically constructed to mitigate the likelihood of SWCCF. As such, a licensee could demonstrate

its use of the ALS platform's key attributes to justify the elimination of a diverse actuation system for certain plant-applications.

8. References

[1] MSFIS application of the ALS Platform in Docket 50-482, amendment 181 to License No. NPF-42, U.S. Nuclear Regulatory Commission.

[2] USNRC Safety Evaluation Report, March 31, 2009, "Wolf Creek Generating Station – Issuance of Amendment RE: Modification of the Main Steam and Feedwater Isolation System Controls (TAC NO. MD4839)," ML# 090610317.

[3] "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated July 29, 2010 (Non-proprietary - ML102160471).

[4] 6002-00301, Rev. 4, "Advanced Logic System Topical Report," Westinghouse Electric Company LLC.

[5] USNRC Safety Evaluation Report, July 16, 2013, "U.S. Nuclear Regulatory Commission Approval Letter for Topical Report 6002-00301, "Advance Logic System Topical Report" (TAC NO. ME4454)," ML# 13071A061.

[6] BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission.