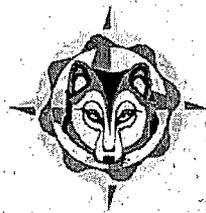


Enclosure VIII to GC 08-0024

CS Innovations Report 6002-00026, "ALS Platform Overview," Rev. 1

MAIN STEAM & FEEDWATER ISOLATION SYSTEM (MSFIS) CONTROLS REPLACEMENT



VENDOR SUBMITTAL APPROVAL

Name/Description	Document #/Rev	Date Submitted	Vendor Name	Comments
ALS Platform Overview	6002-00026 Rev. 1	7/29/2008	CS Innovations	Approval of the ALS Platform Overview 6002-00026 is based on-going reviews of draft revisions of the document. Final approval is based on the released Revision 1.

Approver Signature	Approval Date
	7/30/2008

Wolf Creek Nuclear Operating Corporation

PO Box 411
1550 Oxen Lane, NE
Burlington, KS 66839

Non-Proprietary



6002-00026
ALS Platform Overview

Revision 1
July 29, 2008

CS Innovations, LLC
Scottsdale, AZ

CS INNOVATIONS NON-PROPRIETARY INFORMATION

This document is the property of and contains information owned by CS Innovations, LLC.

© 2008 CS Innovations, LLC
All Rights Reserved

**CS Innovations, LLC**

9150 E Del Camino, Suite 110

Scottsdale, AZ, 85258

(623) 505-1055 Phone

(623) 505-1055 Fax

6002-00026 - ALS Platform Overview**Revision 1****July 29, 2008****APPROVALS**

Function	Name and Title	Signature and Date
Author	Sten Sogaard Design Manager	
Reviewer	Steen Sorensen President	
Approved	Steen Sorensen President	

RECORD OF CHANGES

Revision	Date	Description of changes	Made by
PRE-A	July 2008	Conversion from previous ALS L1 Spec to new CSI format. Removed board requirement specifications, and split it up in separate and independent documents.	Steen Sorensen
1	July 29 th 2008	Changed content of document to Non-Proprietary	Sten Sogaard

OPEN ITEMS

Item	Description	Status

Table of Content

1	Introduction	7
1.1	Purpose and Scope	7
1.2	Overview	7
1.3	Patent Pending Technology.....	7
1.4	References.....	8
1.5	Acronyms, Units of Measure and Designations.....	9
1.6	ALS Hardware Components and Definitions.....	10
2	ALS Platform Overview	11
2.1	ALS History	11
2.2	Characteristics of the ALS	12
2.3	ALS Architecture Overview.....	13
2.3.1	ALS Hardware	13
2.3.2	ALS Boards	14
2.4	ALS Operation.....	17
2.5	ALS Technology based on Solid State	18
2.5.1	FPGA Devices.....	18
2.5.2	Non-Volatile Memory (NVM)	20
2.5.3	Input / Output.....	20
2.6	Standards Compliance.....	21
2.6.1	Class 1E Safety Classification	21
2.6.2	Quality Assurance	21
2.6.3	RoHS Compliance.....	21
2.6.4	IPC Standards Compliance.....	21
3	ALS Boards.....	22
3.1	Core Logic Board (CLB).....	22
3.2	Service and Test Board (STB).....	23
3.3	Input Boards (IPB)	24
3.4	Output Boards (OPB).....	25
3.5	Communication Board (COM).....	26
3.6	Power Supply Board (PSU)	26
4	Environmental ALS Platform Qualifications	27
4.1	Temperature.....	27
4.2	Radiated Emissions	27
4.3	Conducted Emissions	27
4.4	Radiated Susceptibility.....	27
4.5	Conducted Susceptibility.....	27
4.6	Surge.....	28
4.7	Seismic.....	28
5	ALS Rack Mechanics.....	29
5.1	Rack Mechanics.....	29
5.2	ALS Slot and Card Configuration.....	29
5.3	ALS Rack Materials	29
5.4	ALS Front-Panel.....	29

5.4.1	System LEDs.....	30
5.4.2	Board Latches	30
5.5	ALS Rear-Panel.....	31
5.6	Cable Harnesses.....	32
5.7	ALS Boards	32
6	ALS Power Management	33
6.1	ALS Ground Domains	33
6.1.1	5V Power Domain	34
6.1.2	3V Power Domain	34
6.1.3	2.5V Power Domain	34
7	ALS Modes and States	35
7.1	ALS System Modes	35
7.1.1	ALS System Mode versus Local System Mode	36
7.2	Classification of Failures	37
7.3	Alarm Generation	38
7.4	ALS Test Mode	38
8	ALS Communication	39
8.1	ALS Bus Facts	39
8.2	ALS Bus Protocol.....	40
8.3	ALS Bus Failure Detection and Mitigation	41
8.3.1	ALS Bus Failure Mode Error Analysis.....	41
8.3.2	ALS Bus Failure Detection	42
8.4	ALS Bus Physical Layer.....	42
9	ALS Service Unit (ASU)	43
9.1	Configuration Report.....	43
10	SetPoint Configuration	44
10.1	SetPoint Definition	44
10.2	Configuration Integrity.....	44
11	Redundancy.....	45
11.1	Redundancy.....	45
11.2	BIST	45
11.3	Inherent Self-test.....	45

Table of Tables

Table 1: ALS Board Types.....	14
Table 2: Comparison between SRAM, FLASH and FUSE based FPGAs	19
Table 3: ALS System Modes	36
Table 4: Simple ALS Bus FMEA.....	41

Table of Figures

Figure 1: ALS Rack.....	13
Figure 2: Generic ALS Board.....	14
Figure 3: Generic ALS Architecture.....	15
Figure 4: Generic versus Custom Front Plate	30
Figure 5: ALS Rack Rear View (WolfCreek MSFIS Application).....	31
Figure 6: Male Phoenix Field-Connector	31
Figure 7: Generic ALS Board with ALS Bus Connector. The front panel width will vary	32
Figure 8: ALS Platform Power Domains.....	34
Figure 9: ALS System Mode.....	35

1

Introduction

1.1 Purpose and Scope

This document provides an overview of the Advanced Logic System (ALS). It is intended to be a non-proprietary overview of the ALS Platform and does not contain sensitive or proprietary information. The content is extracted from the ALS document suite, including 6000-00000, 6000-00102, 6000-00103, 6000-00104, 6000-00105, 6000-00106, and 6000-00107.

The purpose of this document is to provide an overview and general understanding of the ALS platform and how it can be used in a wide range of Nuclear Power Plant safety related I&C applications.

1.2 Overview

The document is organized in the following chapters:

- 1) Chapter 2: ALS Platform Overview – General background information about the ALS Platform and its history
- 2) Chapter 3: ALS Boards – Description of the different types of ALS Boards available
- 3) Chapter 4: Environmental Qualifications – Describes EMI, Surge, Seismic and Temperature capabilities
- 4) Chapter 5: ALS Rack Mechanics – General Description of how the ALS Platform is constructed
- 5) Chapter 6: ALS Power Management – ALS Power Domains
- 6) Chapter 7: ALS Mode and States – Operational states of the ALS Platform
- 7) Chapter 8: ALS Communication – Description of how ALS Boards communicate
- 8) Chapter 9: ALS Service Unit – Service and test support equipment
- 9) Chapter 10: SetPoint Configuration – ALS Configuration capabilities
- 10) Chapter 11: Redundancy – ALS Redundancy strategy

1.3 Patent Pending Technology

The ALS Platform is a CS Innovations invention with multiple patents pending. The patents focus on key aspects of the platform ranging from the overall platform architecture to details associated with diagnostics and methods used to ensure high integrity in solid state circuits and FPGAs.

1.4 References

- [1] 9000-00000 – CS Innovations Quality Manual, CS Innovations
- [2] NUREG 1.180 – Guidelines for Evaluating Electromagnetic and Radio Frequency Interference in Safety-Related Instrumentation and Control Systems
- [3] IEEE 344-1975 – Recommended Practice for Seismic Qualification of Class 1E Equipment
- [4] EPRI TR-102323 – Guidelines for Electromagnetic Interference Testing of Power Plant Equipment
- [5] IPC-A-610D – Acceptability of Electronics Assemblies
- [6] IPC-A-620 – Requirements and Acceptance for Cable and Wire Harness Assemblies
- [7] IPC-6012B – Qualification and Performance Specification for Rigid Printed Boards
- [8] IEEE 420-2001 – IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations

1.5 Acronyms, Units of Measure and Designations

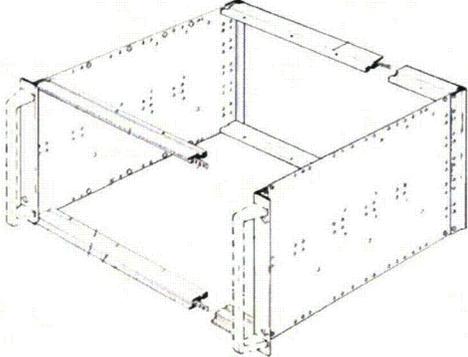
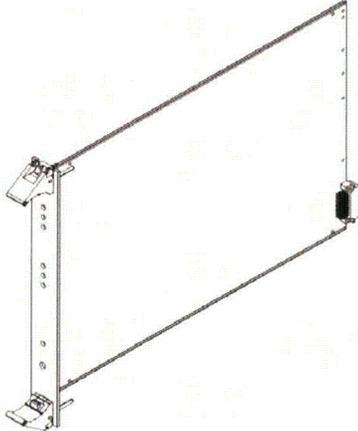
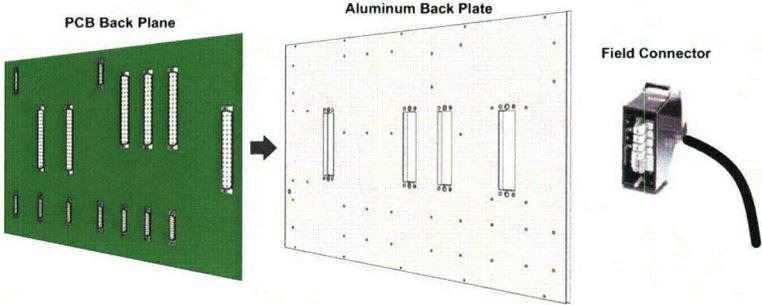
The following table defines pertinent acronyms used in this document.

Acronym	Definition
ALS	Advanced Logic System – CS Innovations hardware architecture platform
ASU	ALS Service Unit
ATE	ALS Test Equipment – reference the complete test harness, including the ATU
ATU	ALS Test Unit – independent test unit, which provides stimuli and tests ALS Racks
BIST	Built In Self Test includes dedicated logic for failure detection
BoardID	Unique ID assigned to each board related to the physical position in the Rack
CLB	Core Logic Board
CRC	Cyclic redundancy check (CRC) is used to produce a <u>checksum</u> – a small, fixed number of bits – against a block of data, such as a packet of network traffic or a block of information. The checksum is used to detect errors after transmission or storage.
EIA-485	Industry standard differential signaling protocol (formerly RS-485)
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
ESFAS	Engineered Safety Features Actuation System
FCO	Full Capability Operation (System Mode)
FPGA	Field Programmable Gate Array
Half-duplex	A half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously). Once a device begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.
IPB	Input Board
I&C	Instrumentation and Control which may refer to both engineers and technicians
MCB	Main Control Board
MSFIS	Main Steam and Feedwater Isolation System
NVM	Non-Volatile Memory also known as Flash Memory technology
PSU	Power Supply Unit (ALS Board based power supply)
RAB	Reliable ALS Bus
RCO	Reduced Capability Operation (System Mode)
RFI	Radio Frequency Interference
RPS	Reactor Protection System
RTL	Register Transfer Level refers to coding style utilized for the ALS design
STB	Service & Test Board
TAB	Test ALS Bus
TVS	Transient Voltage Suppressor (Zener diode)

The following table defines pertinent units and measurements used in this document.

Unit	Definition
6U	6 Rack Units (1U = 1.75" / 44.45mm), common unit of measure used in 19" cabinets.
6HP	6 Hole Pitch (1HP=0.2" / 5.08mm), common unit of measure used in 19" cabinets.

1.6 ALS Hardware Components and Definitions

<p>ALS Rack / Chassis / Platform Rack / Sub-Rack</p>	<p>A 19" cabinet mountable sub-rack. The ALS Rack is 6U tall and 16" deep. (1U=1.75"). Cables connect to the rear of the ALS rack and ALS boards are inserted from the front. The 19" mountable sub-rack is an industry standard form factor.</p> 
<p>ALS Board / ALS Card / ALS Module</p>	<p>A daughter card assembly which can be inserted into the ALS Rack. The ALS board includes printed circuit board, back plane connectors and front plate with injector/ejector latches. The ALS boards will have different front panel with depending on the type of board, but will generally be between 6HP and 12HP. (1HP=0.2").</p> 
<p>Back Plane / Back Plane Assembly</p>	<p>The back plane assembly is mounted as the rear wall of the ALS rack and serves to interconnect the ALS boards and to connect the ALS rack with power and field signals.</p> 

2

ALS Platform Overview

The Advanced Logic System (ALS) is a new approach to safety critical control systems. The ALS is a universal platform which targets safety critical control systems, where reliability and integrity are of the highest importance. The ALS is a logic based platform which does not utilize a microprocessor or software for operation, but instead relies on a simple hardware architecture.

The ALS platform incorporates advanced features to allow for diagnostics, testability, and modularity. 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 safety critical applications within a given plant. Diagnostics and testing capabilities are designed into the ALS platform to ensure there is a systematic approach to maintaining and testing the system.

2.1 ALS History

United States Nuclear Power Plants (USNPPs) have been facing significant challenges with replacing their existing safety related I&C systems. The original manufacturers of the existing equipment are in most cases either out of business or no longer support the product lines. The USNPPs have been faced with two approaches to replacing their safety related I&C systems 1) Reverse engineer the existing system and maintain the system as obsolescence and failures occur. 2) Replace the system with a Commercial-Off-The-Shelf system (COTS). Both of these approaches have a number of issues to contend with. The reverse engineered approach is a short term fix for a long term problem. This approach offers no benefit from advancements in the areas of system integrity, diagnostics, and testability. The COTS approach is typically a much more complex system, as it was designed for more complex industrial control applications. Since the COTS target is complex commercial controls systems the COTS platforms are rapidly advancing. This situation significantly shortens the obsolescence cycle of the product and creates issues with configuration control of the installed systems.

In late 2003 Wolf Creek Nuclear Generating Station was faced with the situation described above. Wolf Creek had an immediate need to replace one of the RPS/ESFAS 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, 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, by CS Innovations, as a general control platform to target the USNPPs Safety Related I&C System retrofit market.

The ALS is designed as a universal control system platform, but specifically targets Class 1E Reactor Protection Systems (RPS) and Engineered Safety Features Actuations Systems (ESFAS). The ALS architecture solves the issues associated with both the reverse engineered and COTS approaches described above. The ALS provides advanced diagnostics and testability features which improve the plant I&C personnel's ability to perform surveillance testing and well as diagnose failures should they occur. System integrity is greatly increased over the exiting 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 incorporating a repeatable advanced design process for system development. Issues associated with future obsolescence are solved by incorporating a simplified board level design and maintaining proven logic in an abstracted form in the event the underlying hardware is required to be updated in the future. This eliminates the issue of essentially starting from scratch with each update. In addition to solving the above issues, the ALS provides benefits in the area of common spares and common training for station personnel. These benefits are realized by the ability of the ALS 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, tested. This included all environmental qualification testing. The ALS meets and exceeds all areas within the EMI/RFI and seismic testing. This high level of environmental robustness ensures the ALS can be installed in all of the environments the existing safety related I&C systems reside.

CS Innovations has incorporated a very robust design, build, and test process. This process is constructed to be highly repeatable and allows CS Innovations to design, build, test and install safety related I&C applications based on the ALS Platform.

2.2 Characteristics of the ALS

Integrity through dedicated Failure Detection and Isolation

The ALS incorporates advanced failure detection and isolation techniques. The operation of the system is deterministic in nature and allows the system to monitor itself for validation of the desired function. The ALS implements advanced failure detection and mitigation in the active path, to avoid unintended plant events, and in the passive path to ensure inoperable systems cannot remain undetected. Undetected failures could cause an unintended plant event or prevent the system from performing its intended safety function, the ALS advanced failure detections prevents this situation. The ALS platform is based on autonomous boards working together. The system utilizes advanced logic to perform distributed control where no single failure will result in an erroneous plant event while maintaining the ability to perform the intended safety function.

Reliability

Reliability is one of the key aspects of a safety critical control system. The ALS incorporates several characteristics to achieve a high level of reliability. The ALS is both an analog and digital platform based on solid-state devices, such as opto-couplers, FPGAs, line drivers, and FET power transistors. The ALS utilizes proven FPGA technology to support a higher-level of integration. The higher level of integration removes discrete logic components and reduces overall system hardware requirements, i.e. fewer racks, boards, and relays. Reducing the complexity of the system has several benefits with regards to reliability and availability. A simpler system directly translates into increased reliability by incorporating fewer components. Another benefit is lower power dissipation which increases the overall system life and ensures a high level of system availability.

The ALS does not utilize a microprocessor and therefore has no software component for the operation of the system. The concern for software common mode failures is eliminated by incorporating a full hardware system which only uses proven design practices and methodologies for implementation of the hardware.

Advanced Diagnostics

The ALS supports advanced diagnostics features, such as LiveView and BlackBox using the ALS Service Unit (ASU). The ASU is a dedicated piece of test equipment which can be connected to the ALS rack during diagnostics or testing by plant personnel. LiveView is a non-intrusive diagnostics tool which allows plant personnel to access detailed status and configuration information of the system while the system is online. The BlackBox function provides post event analysis information about the system to plant personnel for evaluation of the event after it has occurred.

Universal Platform

The ALS is highly customizable to support a wide variety of safety system applications. The ALS architecture is scalable allowing for a single system upgrade up to full set of safety system upgrades using the same ALS platform. The system can be upgraded to support additional requirements which are added to the application after it has been deployed in the field. The ALS technology platform supports many additional features compared to the older relay, ECL or TTL systems, including increased testability, advanced diagnostics, increased integrity and reliability.

Maintainability

Long term maintainability is an important piece of the ALS Platform. Component obsolescence is a challenge to all electronics, especially if the components are one of a kind with only a single source. The obsolescence mitigation strategy for the ALS platform is to use industry standard components with a wide customer base. This helps ensuring availability of the components and increases the likelihood of second sources being available. Furthermore the FPGA logic is described at an abstracted level with allows for easy retargeting in the event the underlying hardware is required to be updated in the future.

Common Spare Parts

The ALS Platform is designed to allow for common spare parts between different ALS systems. This plays an important role in the long term maintainability of the platform and eases training and logistics requirements for the plant personnel.

2.3 ALS Architecture Overview

2.3.1 ALS Hardware

An application implemented using the ALS platform typically consists of one or more ALS racks and an assembly panel which incorporates terminal blocks, fuse holders and other field interface hardware.

The ALS rack is an industry standard 19" sub-rack and can be mounted in a wide variety of existing 19" cabinets.

The ALS boards are designed to a CS Innovations proprietary standard for size and shape of the board. This proprietary standard ensures only ALS boards will fit into the ALS rack, which is critical for ensuring the integrity of the safety system.

Each rack contains a number of boards which is dependant on the particular safety application as well as the type of boards that are fitted into the rack. An ALS rack will typically contain 6-14 boards.

A number of ALS racks can be chained together through an expansion bus if more boards are needed for a specific application. The internal bus system architecture allows for up to 62 boards to be connected in up to six different racks. Generally the racks must be located within 50 feet of one another.

Figure 1 shows a typical ALS rack configuration with the following parts:

- (#1) Sub-rack mountable in a 19" rack
- (#2) Core Logic Board
- (#3) Service and Test Board
- (#4 - #9) A number of IO-boards (up to 12)
- (#10) power supply boards
- (#11) Application name-plate
- Customized back panel and (#12) back plate w/ interconnects for cabling

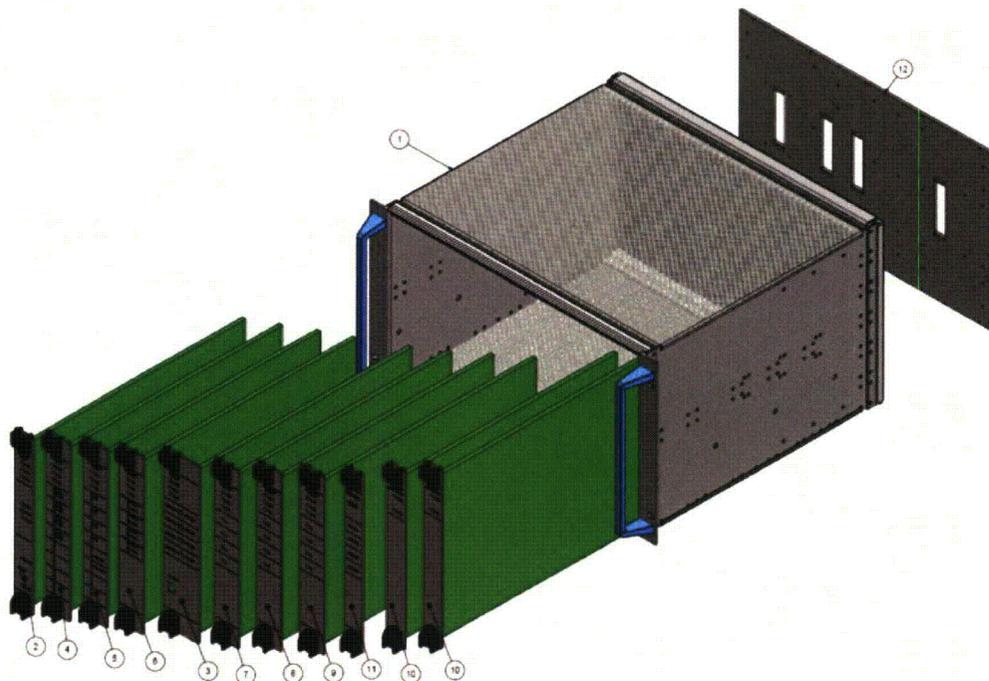


Figure 1: ALS Rack

An ALS rack may be powered directly from the Class 1E power source to a redundant pair of current-sharing internal power supply boards (DC-DC converters). The power supply boards ensure a stable internal ALS rack voltage of 5V. Each power supply board is capable of supplying the ALS rack with sufficient power to continue un-interrupted operation should one of the power supply boards fail.

2.3.2 ALS Boards

The ALS Platform is based on a combination of generic ALS boards; which can be retargeted either directly or after a simple configuration, and dedicated ALS boards; where the FPGA logic has been configured for a specific application. Examples of such ALS boards are listed below:

Table 1: ALS Board Types

Board Type	Configuration	Description
Core Logic Board (CLB)	Dedicated Board ¹	Responsible for control related activities and primary communication in the system. See Section 3.1.
Input Board (IPB)	Generic Configurable ²	Responsible for conditioning, sensing and filtering of field input signals. See Section 3.2.
Output Board (OPB)	Generic Configurable ²	Responsible for controlling and conditioning of field output signals. See Section 3.3.
Service & Test Board (STB)	Generic Configurable ²	Provides diagnostics and monitoring capability to the ALS platform. See Section 3.4.
Communication Board (COM)	Generic Configurable ²	Provides secure communication links to external systems. See Section 3.5.
Power Supply Unit (PSU)	Generic ³	Generates supply voltages from external power source. See Section 3.6.

- 1) FPGA is configured with application specific logic.
- 2) Generic board, with configuration capability. Note: precautions to avoid incorrect configurations. .
- 3) Generic board without configuration capability.

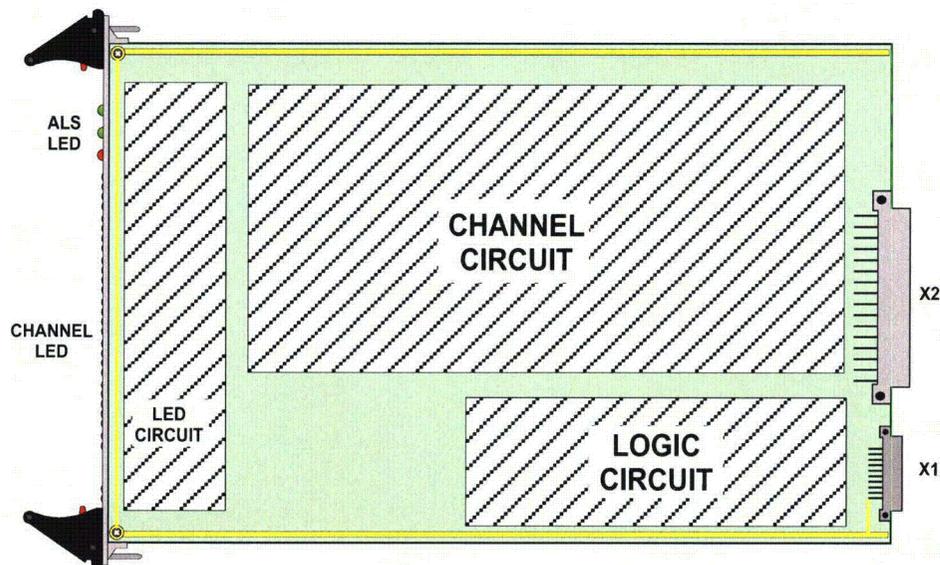


Figure 2: Generic ALS Board

Figure 2 shows a typical FPGA based ALS board. The Logic Circuit includes the voltage conditioning, FPGA and bus communication circuits. Generally all FPGA based ALS boards have identical components in the logic circuit area. The Channel Circuit area will vary with board type, this is the area where input channel conditioning or output drive channels are located.

Communication RAB/TAB - Board communication is supported using two different types of independent serial data structures;

- RAB: Reliable ALS Bus
- TAB: Test ALS Bus

The RAB is used for all data transfers between ALS boards during normal system operation, and the TAB is used for integrity monitoring, diagnostics and test information. Figure 3 below illustrates a generic ALS architecture with a total of 9 boards (simple ALS systems will have fewer boards and not include all board types). The boards communicate over the ALS Back Plane using RAB and TAB busses. The CLB is master on the RAB and the STB is master on the TAB. The RAB/TAB bus architecture is a simple differential EIA-485, point-to-point, master-slave communication protocol with a CS Innovation proprietary communication protocol and standard cyclic redundancy checks (CRC) protection to ensure the integrity of the communicated information between two boards. There will normally only be one TAB bus, but there may be multiple RAB busses if additional redundancy is required. Chapter 8 describes the ALS Communication in more detail.

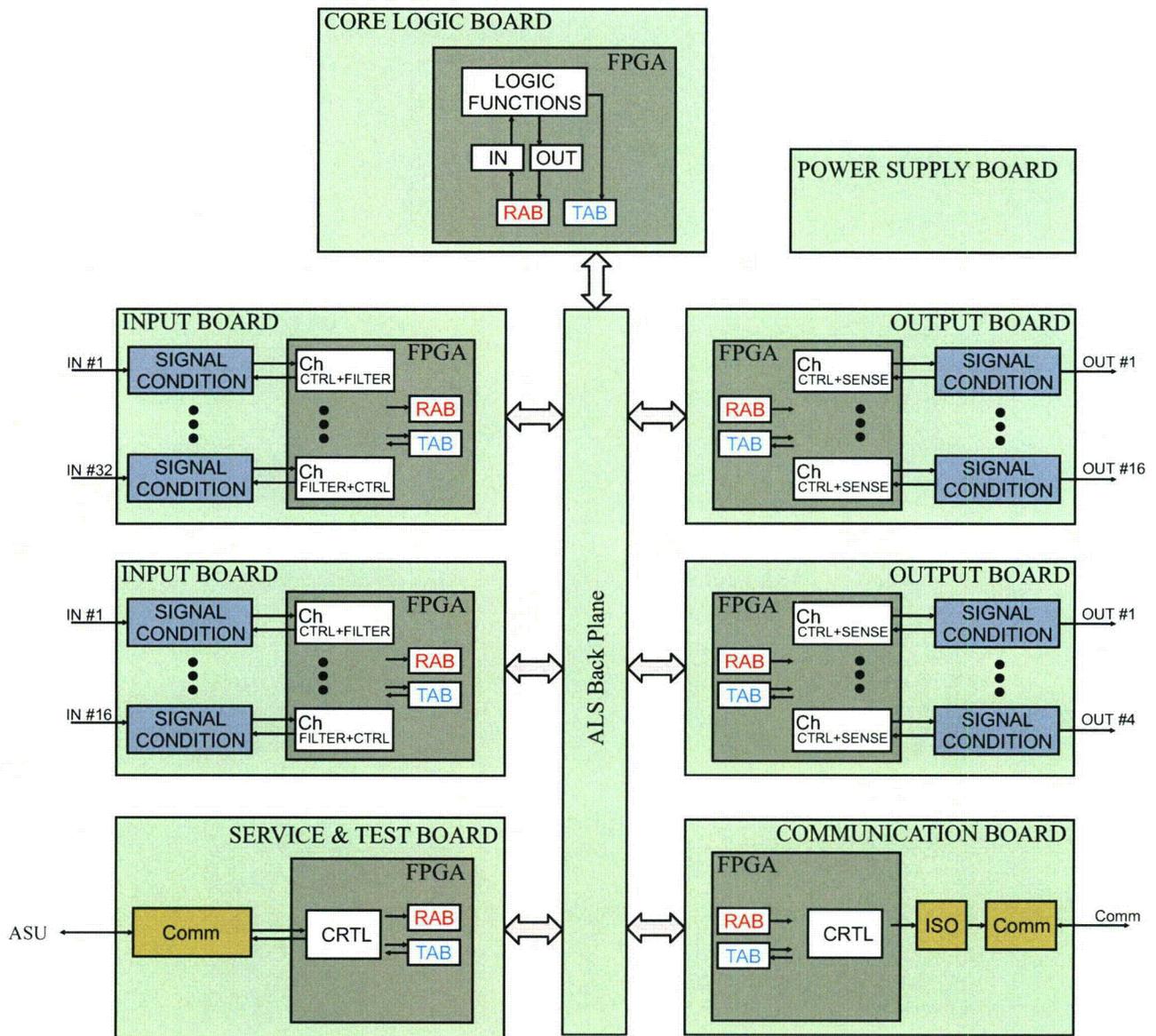


Figure 3: Generic ALS Architecture

Note: Figure 3 is an example only. A minimum system may only include a CLB, IPB, OPB, STB and PSU, a total of 6 boards. More complex systems may include multiple CLBs, IPBs OPBs, COMs, STBs and PSUs in order to provide redundancy.

Common Components/Design – Component reuse and circuit design reuse is a key aspect of the ALS platform design. This improves long term reliability and maintainability, but also gives the ALS boards a common look and feel. Generally the ALS board utilizes the following standard components:

- FPGA – handles all communications, control and integrity activities, and self-test functions
- Voltage regulators and monitors – ensures stable local board voltages
- Local oscillator – ensures a stable local timing reference
- Non-Volatile Memory (NVM) – stores all configuration information
- EIA-485 – differential communication transceiver used for serial communication links.
- In addition to the components above, all IO boards incorporate dedicated IO channels which typically include opto-coupler, TVS, and MOV devices for isolation and protection

Configurable Boards – The ALS Boards have a dedicated FLASH devices to store application specific SetPoints. The SetPoint configuration is stored in an external Non-Volatile Memory (NVM) and local copies are maintained / utilized within the FPGA. The configuration memory is particularly important for I/O boards, where the configuration memory allows for board reuse and common spare parts. Precautions have been made in the ALS platform to ensure that an incorrectly configured I/O board cannot cause unintended plant event if inserted into a rack.

System Mode – The ALS Platform utilizes a System Mode concept to control and indicate the overall capability of the ALS system. The System Mode is communicated between all boards within the rack as a part of the integrity information passed between the boards, it also provides easy to interpret diagnostics information to the plant personnel. The System Mode will during operation be in one of the following four modes; Full Capability Operation (FCO), Reduced Capability Operation (RCO), HALT mode, or (RESET) mode.

- FCO – Full Capability Operation: The ALS platform is operating in a normal mode of operation, and is ready to perform the intended safety function. All circuits are 100% functional and operational. Input channels are updated and evaluated and are in accordance with expected values. Output channels are controlled in the manner for which they are intended, all feed-back information is as expected, and the Core Logic is fully functional.
- RCO – Reduced Capability Operation: The ALS platform has detected one or more problems and indicates that it operates in reduced mode of operation. The failures have been isolated to prevent the failures from propagating through the system and causing unintended plant events. The ALS rack may perform specific actions depending of the location of failure, based on customer requirements. These actions include:
 - Entering a partial trip condition
 - Enter a failsafe condition
 - Performing a trip
 - Provide detailed status indication (operability indication to control room)

The system continues to perform as specified and all unaffected circuits will continue to perform their function. Input channels are updated and evaluated. Output channels are controlled in the way they were intended. The Core Logic is fully functional. The ALS platform alarm is active to show that maintenance is required.

- HALT mode indicates that a serious failure has been detected in the ALS platform and that it has entered a failsafe state. In this mode the ALS is inoperable and not capable of performing the intended safety function. The actual failsafe condition of outputs is configurable using SetPoints. All operations will stop and the system (i.e. all boards) enters a fail-safe state. Input boards continue as usual, except they do not respond to RAB requests. The front-panel LEDs continue to be updated. Output boards are placed in a fail-safe state, where all outputs will enter their configured fail safe mode which can be: “Fail-as-is” or “Fail-as-defined”. All RAB Communication has seized when the ALS is in HALT. The HALT mode is also the power up condition of the ALS platform .
- RESET mode is a transitory state which is only entered when the CLB’s reset switch is toggled. The RESET mode informs all ALS boards that the system will attempt to enter FCO mode and resume full operation. If failures persist the ALS platform will automatically degrade its System Mode to the proper level.

More details about the System Mode can be found in chapter 7.

Redundancy – All critical logic modules within the FPGAs are implemented with redundancy. The logic module redundancy is established such that it provides error detection and mitigation to the rest of the system.

2.4 ALS Operation

Signal flow in the ALS rack is simple and straight forward. This section outlines the basic principles of ALS operation. Refer to the generic ALS architecture shown in Figure 3. The actual number and type of input and output boards/channels is dependent on the particular application system requirements. The fundamental ALS operation remains the same regardless of the application specific aspects.

The ALS operation is accomplished by a fundamental cycle with three phases, the cycle is explained below:

- (1) **Sampling Field Inputs** – On a given input board there will be a number of input channels each responsible for conditioning, sensing, filtering, and sampling the field inputs. In the event an input channel changes due to a field input change (i.e. contact transition from open to close) the signal conditioning circuit will detect this transition and change state. Each channel is described with state information and integrity information. If a channel fails self-test it will be marked as invalid in the integrity information. The CLB retrieves the state and integrity information during the regular polling of data from the input board.
- (2) **Performing Logic Decisions** – Input state and integrity information are retrieved from the input boards and are stored in the input register bank in the CLB. When all input data is present the application specific Core Logic circuit within the CLB will perform its logic function. Based on the current state of the system, input states and integrity information, the CLB will determine a new output state for all outputs. The application specific logic functions consist of timers, random logic gates, FSMs, 2/4-voters, etc. The decision making process is instantaneous. All system level integrity and data checks are performed during this phase of operation.
The results of the application specific logic circuit are stored in an output register bank within the CLB FPGA and from there the information is transmitted to the output boards.
- (3) **Driving Field Outputs** – The output boards receive information from the CLB. The digital circuits will immediately drive the signal conditioning circuit and perform the intended output function.

The cycle above, (1) Sampling Field Inputs (2) Performing Logic Decisions (3) Driving Field Outputs, repeats every System Frame.

2.5 ALS Technology based on Solid State

The ALS is a hardware-based architecture which utilizes a minimal set of hardware to implement a system with high reliability and integrity. The system incorporates self-test capability for detection and mitigation of the effects of failures within or external to the system. This section describes the hardware technologies utilized in the ALS. This section also lists the characteristics for each technology and provides comparisons to alternate technologies. In the discussion which follows the ALS boards are split into 3 sections:

INPUT/OUTPUT (SOLID STATE I/O):

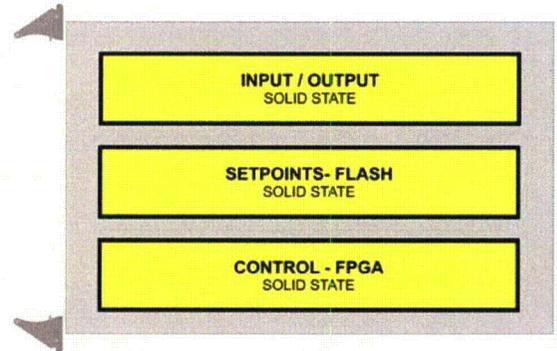
Input/Output channels.

CONTROL (FPGA):

The control logic in each ALS board is implemented in a FPGA using synchronous clocked Moore Finite State Machines.

SETPOINTS (NVM FLASH):

Settings such as input channel filter constants are stored in a NVM.



2.5.1 FPGA Devices

The key component in the ALS design is an FPGA. An FPGA is a semiconductor device containing programmable logic components and programmable interconnects. The programmable logic components can be programmed to duplicate the functionality of basic logic gates such as AND, OR, XOR, NOT. These logic components can be combined into more complex combinational functions such as decoders or simple math functions. In most FPGAs, these programmable logic components (or logic blocks, in FPGA parlance) also include a simple memory element in the form of a flip-flop. Many FPGAs also include dedicated memory blocks which can be combined to form more complex memories.

A hierarchy of programmable interconnects allows the logic blocks of an FPGA to be interconnected as needed by the system designer, somewhat like an on-chip programmable breadboard. These logic blocks and interconnects can be programmed after the manufacturing process by the customer/designer (hence the term "field programmable", i.e. programmable in the field) so that the FPGA can perform whatever logical function is required.

The logic design is based on schematic capture and/or VHDL code for the FPGA implementation. Schematic capture tools have been utilized for many years in the electronics design industry and have reached a mature state. VHDL was originally developed at the request of the US Department of Defense in order to document the behavior of the ASICs that supplier companies were including in equipment. That is to say, VHDL was developed as an alternative to huge, complex manuals which were subject to implementation-specific details. VHDL implementation offers the capability of simulating system behavior in a deterministic and iterative manner using simple test benches. Register Transfer Level (RTL) descriptions are a method of capturing the behavior of a digital circuit.

Dedicated test-benches and test systems are developed to test the final logic circuits. Faults can be injected in a controlled environment and verify proper error detection and expected response. A test plan with regression test suites utilizing well-defined golden test vectors is incorporated in the overall testing of the FPGA design.

Several families of FPGAs are available today. The table below identifies the high-level characteristics of the three major types of FPGAs:

Table 2: Comparison between SRAM, FLASH and FUSE based FPGAs

Description	SRAM	FLASH	FUSE
Typical use-case	Commercial, High Volume	Military & Space	Military & Space
Technology	Standard CMOS (typical deep-submicron)	CMOS with FLASH technology	Special FUSE technology many additional process steps
Prone to SEU (Single Event Upset)	Very sensitive to SEU. SRAM devices prone to neutron induced configuration errors	Insensitive to SEU. Immune to neutrons	Immune to SEU. Immune to neutrons
Prone to SEL (Latchup)	Very susceptible	Less susceptible	Less susceptible
Configuration Integrity (Bit flipping)	Susceptible	Leakage issue	Fuse defects, electron migration, weak oxide
Configuration Retention time	Until loss of power (20-50 years)	20-50 years (Temp < 70°C)	Indefinite
Device Configuration Lock (Intruders capability to change content)	Transferred at startup (Possible to modify setup)	FlashLock (Impossible)	FuseLock (Impossible)
Security (Read-back of content)	Transferred at startup (None)	FlashLock (Impossible)	FuseLock (Impossible)
Development friendliness	Fast and easy	Optimal	Slow and difficult

The ALS utilizes a FLASH-based FPGA type. The FLASH-based FPGA provides the best characteristics for the applications targeted by ALS. The SRAM-based FPGAs are prone to SEU and SEL which is a critical characteristic which makes this type of FPGA not viable for the applications for which the ALS is targeted.

The FLASH-based and FUSE-based FPGAs are similar type devices. Each of the two types has particular failure mechanisms. The ALS technology is designed to detect and isolate the failure mechanisms of each if they occur. This is done by implementing redundancy, where the control logic is duplicated into two independent logic modules which are continuously monitored. If a mismatch is detected between the redundant modules the failing ALS board will be isolated from the remaining system.

Radiation-hard FPGA options are available but are not typically required for the ALS target applications.

2.5.1.1 FPGA Technology – FPGA vs. ASIC

The ALS system is based on using FPGAs to implement the control functions. An alternative to FPGAs are ASICs (Application Specific Integrated Circuits). ASICs are typically used for complex digital devices such as processors, graphics controllers, or for very high volume consumer products where the high NRE (Non-Recurring Engineering) costs but low unit prices are favorable compared to the low NRE but high unit cost FPGAs. Due to the widespread use of ASICs in consumer products, where there are constant pressures to decrease cost and increase speed and processing power, the ASICs are constantly evolving. Unit price reductions are done by reducing the size of the transistors used in the ASIC. The size of the transistors in ASIC verbiage is referred to as "Technology" (examples "0.35um Technology" or "90nm Technology"). The dimension refers to the width of the gate in the transistors. The ASIC foundries are typically geared towards specific Technologies, and are required to undergo rebuilding or major renovations when changing "Technology". This constant upgrading of the foundries poses another obstacle for low volume, long life applications like the ALS where future designs might be forced into a new Technology because of availability of compatible foundries. For an ASIC to change technology it must undergo the same design and validation flow it underwent when it was originally design and will incur similar NRE costs. Every time the technology is reduced it causes the NRE costs to increase and at the same time increases the minimum yearly volume for ASICs to be a viable solution. This trend has made the market more favorable for FPGA based designs which has slowly moved into low and medium volume products. FPGAs are built in the same foundries as the ASICs and are subjected to the same design, validation and production costs as the ASICs. But, since a single FPGA device can be used by many customers, the FPGA vendors are able to achieve yearly volume in millions of unit quantities. Using

ASICs for a low volume application like the ALS system will result in a limited test-base where fundamental IC design issues such as thin oxide-layers, bad metallization or chemical residues can be difficult to detect.

The ability to leverage the design, validation, and quality control performed by the FPGA vendors has made FPGAs popular in end products such as military, space, and aerospace products. The FPGAs used in ALS are manufactured by Actel. Actel has focused on the military/space/aerospace product segment where high reliability, robust QA processes and procedures, and long product cycles are important.

2.5.1.2 Solid-State Technology Issues

Radiation Effects such as ionizing radiation can cause unwanted effects in semiconductor devices. Energetic protons, neutrons, heavy ions, and alpha particles can strike sensitive regions of the transistor, causing various failures, or Single Event Effects (SEE), such as:

- Single Event Upsets (SEUs) which occur when high-energy ionizing particles, such as heavy ions, alpha particles or protons, irradiate a circuit or pass through an integrated circuit causing a disruption in the system logic (CMOS memory element changes content).
- Single Event Latch-Up (SEL) which is a condition that causes loss of device functionality due to a single-event-induced high current state (occasional short circuit between power and ground). A SEL may or may not cause permanent device damage, but requires power strobing of the device to resume normal device operations.

SRAM cells are susceptible to neutron-induced errors where they change state in an unpredictable and uncontrollable way. Since SRAM cells are used to control the configuration of SRAM-based FPGA, a neutron-induced error could result in an unpredictable change in functionality of an SRAM-based FPGA and result in complete system failure. Independent and comprehensive reports from industry neutron-effects experts iRoC Technologies, determines that SRAM-based devices are susceptible to functional failure when exposed to neutron radiation. Failure rates are significant even when exposed to the naturally-occurring background neutron radiation present at ground level. On the contrary, the fuse and Flash based FPGAs are immune to the effects of neutron radiation.

Because of the incompatible characteristics described above, SRAM-based FPGAs are not utilized in the ALS.

2.5.2 Non-Volatile Memory (NVM)

The ALS boards have an on-board SetPoint memory where local settings are stored. Examples of such settings are *Input Channel Filter Setting* and *Input Channel Normally Open / Normally Close*. The SetPoint memory eliminates the need for using DIP switches or a Jumper Array to select these settings.

Storing the SetPoint information in a NVM memory offers several advantages over a DIP switch solution. The NVM contents are protected with a CRC checksum, which will detect and alert if any changes to the information has occurred. The DIP switch solution does not have this protection and could be accidentally modified during board installation or maintenance.

The ALS implements a high level of integrity for the data stored in the NVM. The ALS boards are designed to read out the NVM contents only at power-up. After power-up the ALS boards hold an internal copy of SetPoint settings within the FPGA. While the ALS is running the NVM contents will be tested at regular intervals to ensure there are no data integrity issues. If a data integrity issue is found, the ALS will actuate the plant alarm system to indicate an ALS board requires maintenance. In this case the ALS remains fully functional until the next power cycle.

2.5.3 Input / Output

The input and output channels are all designed for high reliability and integrity. The ALS is almost exclusively designed from solid state components. Solid state components have a very long life; however surge voltages, high temperatures, mishandling, overstressing, or manufacturing defects can reduce this life expectancy. The ALS channels are designed with the primary goal of avoiding such situations by building in margins in the design itself and providing early detection and mitigation capabilities for such problems. The ALS design also focuses on the power consumption and power loss of the system, which has been minimized in all components to ensure that all solid state components remain at low temperatures.

2.5.3.1 Input Channels

The input channels on the ALS boards are based on isolated solid-state devices. The input channels include self-test capability which continuously verifies all components within the channel are operational. During self-test, all components in the channel are tested to ensure full functionality. High isolation is maintained by utilizing opto-isolators. The input channels are protected against ESD and surge voltages using Transient Voltage Suppressors (TVS). The opto-isolators are used in a way which maximizes the life expectancy of the device.

2.5.3.2 Output Channels

The output channels, similar to the input channels, are based on isolated solid-state devices. Using solid-state devices vs. electro-mechanical relays offers several advantages particularly when long life and the ability to handle inductive loads is required. Output channels also include self-test capability and for some channel types provides redundancy and other specialized test features to ensure the channel is operational. The output channels are protected against ESD and surge voltages using Metal Oxide Varistors (MOV).

2.6 Standards Compliance

2.6.1 Class 1E Safety Classification

The ALS Platform is designed and implemented to meet all requirements of a Class 1E Safety System, reference IEEE 420-2001.

2.6.2 Quality Assurance

The ALS Platform is designed and manufactured under CS Innovations' Quality Assurance Program, Reference 9000-00000.

2.6.3 RoHS Compliance

Because the reliability properties of lead free is still unknown the ALS Platform is not design to be lead free or RoHS compliant. The ALS Platform will transition to RoHS once the reliability has been proven.

2.6.4 IPC Standards Compliance

The ALS Platform has been designed and manufactured to meet the following requirements:

- IPC-A-610D Class III requirements.
- IPC-6012B Class III requirements.
- IPC-A-620 Class III requirements.

3

ALS Boards

This chapter describes the 6 primary board types available in the ALS Platform

- 1) CLB – Core Logic Board
- 2) IPB – Input Board
- 3) OPB – Output Board
- 4) STB – Service and Test Board
- 5) COM – Communication Board
- 6) PSU – Power Supply

3.1 Core Logic Board (CLB)

The CLB contains all the application specific core logic circuits, which define and control the operation of a given system. The CLB controls all sequencing within the ALS system. The CLB issues requests to input boards to provide field input information as required, makes decisions based on received inputs, and commands the output boards to drive a specific output state to the field devices. The CLB is the primary decision making board in the ALS system, it has no direct field input or output capability except for the directly coupled alarm output. An ALS system will typically contain a single CLB, but may have two if redundancy is needed.

Core Logic – The core logic is customizable based on the requirements of a given application and can contain any type of digital building blocks which can be generated from a NAND2 device, such as AND/OR/XOR-gates, Flip Flops (D, JK, SR). These building blocks can then be combined to form more complex logic such as, counters, timers, multiplexers, comparators or Finite State Machines (FSMs).

The core logic is implemented in the FPGA and the typical size of the core logic module is less than 5K gates (NAND2).

SetPoint Configuration – The CLB has a dedicated FLASH device to store application specific SetPoints used by the design. The SetPoint configuration is stored in an external Non-Volatile Memory (NVM) and local copies are maintained / utilized within the FPGA. Typically only parameters which are requested by the customer to be adjustable are included in the SetPoint configuration, otherwise they will be hardcoded.

Examples of such configuration SetPoints are: sequencer delays, time constants and trigger-points.

RAB Communication – The CLB is a RAB master and is the initiator of all communication on a RAB bus. All communication performed on a RAB bus is performed in a predetermined sequence also known as a System Frame. During the System Frame all inputs are acquired, all new outputs are determined and written to output boards. During operation the System Frame is repeated at a fixed rate (typically 10ms).

The inherent architecture (protocol and implementation) detects any RAB communication failure. The CLB maintains a status of all RAB communication, when communication does fail, due to a CRC failure, loss of packet or similar defect, the system will retry the transmission 1 time. An unsuccessful retry will result in the failing board being removed from the list of active boards and the system alarm being actuated. When a board has been removed from the list of active board no further accesses will be attempted without acknowledgement by plant personnel. Data (or the lack thereof) from the failing communication will be isolated (not used) and will not cause any further effects.

TAB Communication – The CLB is a slave on the TAB and will respond with the requested diagnostic and integrity information. The information is collected in a non-intrusive manner and does not affect the on-going operation of the system.

Examples of diagnostics from the CLB are inputs and outputs to the core logic module, as well as any internal node that is of interest to a certain application (e.g. states in a state machine or the count of a counter).

System Mode – The CLB maintains the System Mode which is used to control the run capability of the ALS system, and to provide easy to interpret diagnostics information to plant personnel.

Alarm – The CLB has a dedicated and independent alarm circuit to control and generate an isolated alarm output. Two types of failures can cause the alarm to be actuated:

- Application related failures – The Core Logic within the CLB can be configured to generate alarms if inputs to the ALS are invalid. Examples of such failures are redundant inputs not being consistent or valve position indicators indicating both open and close.
- System related failures – caused by failures within the ALS circuitry such as failures on the RAB bus, supply voltages out of specified range or blown fuses, device or circuit failures.

Note: a redundant Alarm circuit similar to the CLB alarm circuit is located on the STB.

3.2 Service and Test Board (STB)

The STB provides several advanced on-line and off-line maintenance features such as; integrity monitoring and diagnostics.

The monitoring and diagnostic capabilities support fast system installation and post-installation test during the installation phase, accurate troubleshooting in the event a failure or an unintended plant event occurred during normal operation, as well as general I&C maintenance during outages and while the system is on-line.

Diagnostics – The two key features provided by the STB are LiveView and BlackBox:

- **LiveView** – is a run-time diagnostics feature which provides a live-view of all important signals within the ALS. Signals include information transferred between input/output boards and the CLB (on the RAB), as well as important internal Core Logic signals and health information for all the boards in the ALS rack. The LiveView feature is available while the system is both on-line and off-line and provides the real-time information with 100uS resolution.
- **BlackBox** – is a run-time logging and post-event off-line diagnostics feature which provides the plant personnel with information about the sequence of events in the past. The BlackBox circuit continuously records information transmitted on the RAB. When a change in the system occurs the information is stored into an NVM, which allows for high resolution analysis of pre-event conditions, event sequence and post events. In a typical ALS rack application the BlackBox information is stored for the previous 18 months of operation up to and including the most recent information.

The STB gathers information and records it for either real-time retrieval or retrieval at a later time. The information recorded by the STB is retrieved by plant personnel using the ALS Service Unit (ASU).

The diagnostics features are implemented in a **passive and non-intrusive** manner and do not affect ALS system performance. All communication (information gathering) is (a) performed on the TAB, and does therefore not interfere with I/O information flowing on the RAB and (b) the STB only retrieves information from the other boards. It does not write to or attempt to control other boards. The hardware implementation prevents any interference from the TAB to the system operation.

TAB Communication – The STB is master on the TAB and initiates all requests on the bus.

Communication on the TAB is controlled and synchronized to a System Frame. During each System Frame all boards within the system will be accessed one or more times. Information gathered on the TAB is made available to the BlackBox recorder and ASU interface (should the ASU be connected).

RAB Communication – The STB is slave on the RAB and will respond with the information when the CLB requests it.

Alarm – The STB includes an ALARM output which is normally wired in series with the alarm output from the CLB. Similarly to the CLB the STB will generate an alarm if failures are detected with the ALS platform.

ASU Interface – The STB provides an access port, which allows the ASU to attach to the ALS rack. The ASU is not attached during normal operation. It is only attached and utilized by plant personnel for maintenance and troubleshooting activities. The alarm circuit is actuated immediately when an ASU is plugged into the ALS rack.

An ALS system typically contains one STB. The ALS system will operate without the board; however the absence of the board will remove the advanced diagnostics features provided by the board.

SetPoint Configuration – The STB has a dedicated FLASH device to store application specific SetPoints used by the design. The SetPoint configuration is stored in an external Non-Volatile Memory (NVM) and local copies are maintained / utilized in the FPGA.

3.3 Input Boards (IPB)

IPBs are responsible for conditioning, sensing, filtering, and sampling field inputs. IPBs are typically dedicated to a specific input type, such as 24V or 48V digital inputs, 4-20mA analog inputs, 0-10v analog inputs, or thermo-couple inputs.

The IPB provides a front panel indication which shows the status of a particular input using an LED. The ALS design allows for both generic IPB front-panels as well as customized front panels where each channel LED is marked with a descriptive text such as sensor ID.

An ALS rack may require multiple IPBs to support a particular application. The number of IPBs in the ALS rack is related to the number of channels and/or the type of field inputs required. A particular IPB can provide a number of input channels – typically between 4 and 32 channels. The input channel itself can be simple with minimal circuitry to measure a digital signal, or can contain more complex feedback measuring and test circuitry to ensure channel integrity.

Input Channels – An input channel consists of two key circuits – the analog signal conditioning circuit and a digital circuit.

- The analog circuit is responsible for converting analog voltages or currents into digital representation and is also referred to as signal conditioning circuitry.
- The digital portion of the channel is located in the FPGA and performs all channel control, sample & hold, integrity checks, self-testing, and digital filtering functions. All digital channel circuits, RAB communication, and channel integrity are implemented with redundant logic within the FPGA. The redundancy and self test circuits ensures the detection of any single failure on the board is isolated from the rest of the ALS rack in a controlled manner.

Generally all input channels are galvanic isolated from the ALS logic and can withstand 1500V_{AC}. The input channels may also be individually isolated or isolated into groups with common reference.

SetPoint Configuration – The IPB has a dedicated FLASH device to store application specific SetPoints used by the design. The SetPoint configuration is stored in an external Non-Volatile Memory (NVM) and local copies are maintained / utilized in the FPGA. The amount of SetPoint information stored is between 0-80 bytes. The input conditioning configuration such as filter time and normal open/normal close configuration is stored in the SetPoint memory.

RAB/TAB Communications – The IPB's are slave devices on the RAB and TAB busses and will respond as required by the masters. The IPB's will automatically acquire the input condition and make it available on the busses. Integrity information is provided with each input channel and allows the CLB to mitigate failures on channel basis. The IPB's expects to be accessed in every System Frame, if the IPB detects no access for a duration of time it will automatically time-out and enter HALT.

Integrity – The IPB's maintains integrity information for all input channels which are passed to the CLB together with channel data. Other failures will cause the IPB to either enter RCO mode to HALT mode depending on the severity. The IPB can detect communication failures on the RAB or TAB and is responsible for isolating the board from further communication on the RAB until the failure(s) has been removed.

3.4 Output Boards (OPB)

OPBs are responsible for controlling and conditioning actuators, indicators, relays and field output devices. OPBs are typically dedicated to a specific output type, such as 24-48VDC digital outputs, relay outputs capable of switching 125VAC analog signals, high inductive solenoid loads, or resistive devices.

OPBs are named according to the type of signal conditioning they provide: ALS-4xx where 'xx' designates the output type and number of channels available. The OPB provides a front panel indication which shows the status of a particular output with an LED. The ALS design allows for both generic OPB front-panel indications as well as customized front panel indications by mapping the LED indication to application specific field outputs.

An ALS rack may require multiple OPBs to support a particular application. The number of OPBs in the ALS rack is related to the number of outputs and/or the type of field devices the ALS rack is interfaced to. A particular OPB can provide a number of output channels – typically between 1 and 16 channels. The output channel itself can be simple with minimal circuitry to switch a relay, or it can be more complex such as a FET driver channel with feedback measuring and test circuitry to ensure channel integrity.

Output Channels – An output channel consists of two key circuits – a digital circuit and the analog signal conditioning circuit.

- The analog circuit is responsible for signal conditioning from digital 3.3V control voltage levels into the desired output function, (i.e. switching to an analog voltage, switching a relay or solid-state-contact or a high-power FET transistor). The analog circuit is responsible for all integrity sensing and feedback loops, which provide information about the state of the output circuit.
- The digital portion of the channel is located in the FPGA and performs all channel control, integrity checks, self-testing and any necessary digital filtering. All digital channel circuits, RAB communication, and channel integrity are implemented with redundant logic within the FPGA. The redundancy ensures, in the event of a device failure, the failure is detected and the board is isolated from the rest of the ALS rack.

Note: ALS has the capability of driving field devices directly from the rack without the use of interposing relays. This is accomplished with the use of well protected FET transistor devices and a specific isolation scheme.

Output channels are divided up into groups – typically one to four groups. Each group uses a common ground and provides galvanic isolation from the other groups, as well as the digital portions of the board. The galvanic isolation typically withstands a minimum 1500Vac. Channels and/or groups of channels can typically be configured to perform the intended function (Normally Open/Normally Closed or Fail Safe modes).

RAB/TAB Communications – The OPB communicates over the RAB and the TAB as requested. The OPB is a slave device on the both the RAB and the TAB. All OPBs are slave devices with limited intelligence. The OPBs are dedicated to driving or actuating a field output every time a request is made, and the on-board intelligence is limited to the capability of the integrity monitor or redundancy scheme to decide if a failure has been detected. The OPB does not have the capability of broadcasting the failure to the rest of the ALS rack. The CLB will detect the failure and handle all broadcast responsibilities. The OPB can detect communication failures on the RAB or TAB and is responsible for isolating the board from further communication on the RAB until the failure(s) has been removed.

SetPoint Configuration – The OPB has a dedicated FLASH device to store application specific SetPoints used by the design. The SetPoint configuration is stored in an external Non-Volatile Memory (NVM) and local copies are maintained / utilized in the FPGA. The amount of SetPoint information stored is between 0-80 bytes.

Channels and/or groups of channels can typically be configured to perform the intended function (Normally Open/Normally Closed or filter time constants). This application specific information is stored in the board NVM.

Integrity – The OPB incorporates a FailSafe feature which allows the OPB to autonomously assume a predefined FailSafe state upon a system failure. The fail safe state for a particular OPB is defined during the system design cycle. There are three states for each of the independent channels of a board. The states are; 1) Fail-As-Is, 2) Fail-As-Defined-Open, 3) Fail-As-Defined-Closed.

3.5 Communication Board (COM)

The COM provides a reliable communication link in and out of a ALS Rack. The COM may be used to establish an isolated and reliable communication link between two ALS systems. This may be used in larger ALS systems where an input conditioning ALS rack may be placed close to the source of the signals. This is common practice when the inputs are analog signals such a thermocouples. The input conditioning ALS rack may then communicate the digitized data over a communication link to a processing cabinet where the actual decision making and output generation takes place.

The communication boards may also be configured for **One-Way Communication** which may be used for communicating detailed status and configuration information to non-safety equipment. This may be plant computers or plant historians. By implementing the communication link as an isolated one-way link a Class 1E barrier may be maintained.

RAB/TAB Communications – The COM is a slave device on the both the RAB and the TAB and will only communicates over the RAB and the TAB as requested.

Communications Link – The behavior of the communication link will depend on its configuration.

- 1) It may be configured to repeat all RAB and TAB communication on the Comm Link.
- 2) It may selectively collect data transmitted on the RAB and TAB and send at regular interval.
- 3) It may received data directly from the CLB and only send it when directed by the CLB.

The communication links are isolated from ALS logic and capable of 1500V_{AC}. The communication board may include multiple communication links. The communication links will typically be: EIA-232, EIA-422 or EIA-485 type connections.

SetPoint Configuration – The COM has a dedicated FLASH device to store application specific SetPoints used by the design. The SetPoint configuration is stored in an external Non-Volatile Memory (NVM) and local copies are maintained / utilized in the FPGA.

3.6 Power Supply Board (PSU)

The PSU's are used to generate a regulated local supply to be used by all ALS boards in the rack. The PSU can be connected directly to a Class 1E power source. A redundant pair of PSUs are utilized in ALS racks to provide load sharing and redundancy, which ensures a stable internal rack voltage both long term but also in the event of a single power supply failure. Each of the PSUs are capable of supplying the ALS rack with sufficient power to continue uninterrupted operation should the other PSU fail.

The PSU is hot-swappable and can be replaced while the system is operational. The PSU contains built in diagnostics to detect an under-voltage. The PSU provides an energized NO contact to indicate the failure to the rest of the ALS rack.

The PSUs may also be used to generate other voltages such as 24V or 48V to be used to drive external components such as fan-out relays or breaker trip coils.

4

Environmental ALS Platform Qualifications

This chapter describes the environmental capabilities of the ALS Platform and which requirements it has been designed to meet. The basis for setting the Environmental Qualification requirements was the guidance provided in EPRI TR-102323 Rev 2 and the requirements listed in NUREG RG 1.180.

4.1 Temperature

The ALS Platform is designed to operate in a mild environment, such as control rooms or electrical equipment rooms, with an operational temperature of 0°C to 50°C and relative humidity: 20 to 80% (Non-condensing)
Storage Temperature conditions is: -10°C to 60°C. Relative Humidity: 20 to 80% (Non-condensing).

4.2 Radiated Emissions

The ALS Platform was qualified to the following MIL-STD-461E tests.

Test	Description	Item
RE101	Radiated emissions (Low Frequency)	System (Rack)
RE102	Radiated emissions (High Frequency)	System

4.3 Conducted Emissions

The ALS Platform was qualified to the following MIL-STD-461E tests.

Test	Description	Item
CE101	Conducted emissions (Low Frequency)	Power leads
CE102	Conducted emissions (High Frequency)	Power leads

4.4 Radiated Susceptibility

The ALS Platform was qualified to be able to withstand the following MIL-STD-461E and IEC-61000 tests.

Test	Description	Item
RS101	Radiated Susceptibility (Low Frequency)	System (Rack)
IEC 61000-4-3	Radiated immunity (High Frequency)	System
IEC 61000-4-6	Radiated immunity (High Frequency)	Power / Signal leads
IEC 61000-4-8	Radiated immunity (High Frequency)	System
IEC 61000-4-9	Pulse magnetic field immunity	System
IEC 61000-4-10	Damped oscillatory magnetic field immunity	System

4.5 Conducted Susceptibility

The ALS Platform was qualified to be able to withstand the following MIL-STD-461E and IEC-61000 tests.

Test	Description	Item
CS101	Conducted Susceptibility (Low Frequency)	Power Lead Lines

4.6 Surge

The ALS Platform was qualified to be able to withstand the following IEC-61000 tests.

Test	Description	Item
IEC61000-4-2	Electrostatic Discharge (ESD) Immunity	Case & Cables
IEC61000-4-4	Electrical Fast Transient Immunity (EFT/B)	Power / Signal leads
IEC61000-4-5	Surge Immunity	Power leads
IEC61000-4-12	Ring Wave immunity	Power / Signal leads
IEC61000-4-16	Conducted, common-mode immunity	

4.7 Seismic

The ALS Platform was qualified to handle seismic events according to IEEE 344-1975. The ALS Platform remained operational during and after all seismic tests.

5

ALS Rack Mechanics

5.1 Rack Mechanics

The ALS Platform is based on 19" (482.6mm) Sub-Racks, 6U (266mm) tall and 400mm deep. The sub-racks are an industry standard products following IEC 60297-3-101. For easy insertion and ejection the ALS Boards are configured with IEC 60297-3-102 style injector/ejector handles and IEC 60297-3-103 style card guides.

The combination of Injector/Ejector handles, card guides and general rack mechanics ensures ESD safe insertion of ALS boards.

The ALS rack is fully enclosed with perforated top and bottom panels. All 6 sides of the rack is electrically connected and grounded to chassis ground. Chassis ground is provided through a single earthing lug on the back of the ALS rack. The ALS Platform rack is IP20 rated against foreign objects and water.

Connectors – All cable harnesses are securely attached to the rear of the ALS rack using industrial grade plug connectors.

Weight – A fully configured ALS Platform rack will typically weigh less than 20kg.

Cooling – The ALS Platform is designed to rely on natural convection in the cabinet and with no internal fans.

5.2 ALS Slot and Card Configuration

The ALS rack has the capacity to support 14 boards maximum, assuming each ALS board is 6 HP wide (1.2"). Component height and front plate indication requirements may require that certain types of ALS board to be wider.

Each opening in the ALS rack which can accommodate an ALS board is referred to as an ALS Slot. The ALS Slots are not designed to be interchangeable; the combination of back plane connectors, their locations and optional keying ensures that only the correct type of ALS board can be inserted into a given slot. In addition to this the ALS logic will also verify that the inserted board contains proper configuration before allowing it to become an active part of the system.

Unused slots in the ALS rack are covered with generic filler plates to maintain an IP20 rating.

5.3 ALS Rack Materials

The ALS rack is implemented in a lightweight and durable construction, suitable for rugged environments and long life expectancy. The ALS rack is made from aluminum alloys with a combination of alodine or anodized finishes.

The side plates are made from solid aluminum with a yellow alodine finish.

The top and bottom covers are made from perforated aluminum with a yellow alodine finish.

The rear plate is made from solid aluminum with anodized finish. The rear plate will typically be customized for each application to provide an optimal combination of cable connectors.

5.4 ALS Front-Panel

All ALS boards are design with a generic front plate, this front plate is application independent and can be reused across many designs. To aid I&C technicians and to improve general serviceability the front plate may be modified with application specific designators. This includes adding description labels to input and output channels matching the equipment or component tagging nomenclature used at the particular plant.

To ensure long term durability and readability all text are engraved and painted black. Figure 4 shows how ALS board front plates can be customized to provide application specific information directly on the front plate.

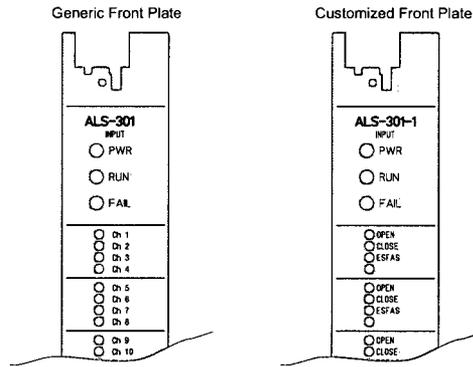


Figure 4: Generic versus Custom Front Plate

5.4.1 System LEDs

All ALS boards include 3 common system LEDs. The System LED's are located identically on all ALS boards and are used for easy diagnostics of the system.

The ALS System LEDs are the following:

System LED	Indication Type	Colors	Style	Description
PWR	Board power indicator	Green	Solid	The board is powered – Both latches are locked
		Yellow	Solid	The board is powered – One latch is locked
		Off	Solid	None of the latches have been locked
RUN	Board running indicator	Green	Blink 1Hz	The board is running in FCO mode
		Yellow	Blink 1Hz	The board is running in RCO mode
		Off	Solid	The board has stopped execution and is in HALT mode
FAIL	Board fail indicator	Red	Solid	The board has experienced and detected a failure
		Off	Solid	The board has not detected any failures

5.4.2 Board Latches

Boards are fastened and secured to the rack using dedicated ergonomically injector/ejector handles, referred to as board latches.

One latch is located on the top and another is located on the bottom of the front-plate to secure the board in the rack.

The latches are IEC 60297-3-102 compatible board latches used for supporting hot-swapping of board while providing ESD precautions and alignment pins. The latches includes a microswitch which allows the ALS board to enter a safe state before the board is ejected.

Latch State	Board State	PWR LED Indication
Both OPEN (not inserted in rack)	Board without power	Off
Both OPEN (inserted in rack)	Board will be powered, but in HALT mode	Off
One OPEN, One CLOSED	Board will be operational	Yellow
Both CLOSED	Board will be operational	Green

5.5 ALS Rear-Panel

The ALS rear-panel is made with 4mm Anodized Aluminum. The text is engraved with a black or blue background as shown in the table below. Figure 5 shows the rear side of ALS rack showing Cable Connectors and labels.

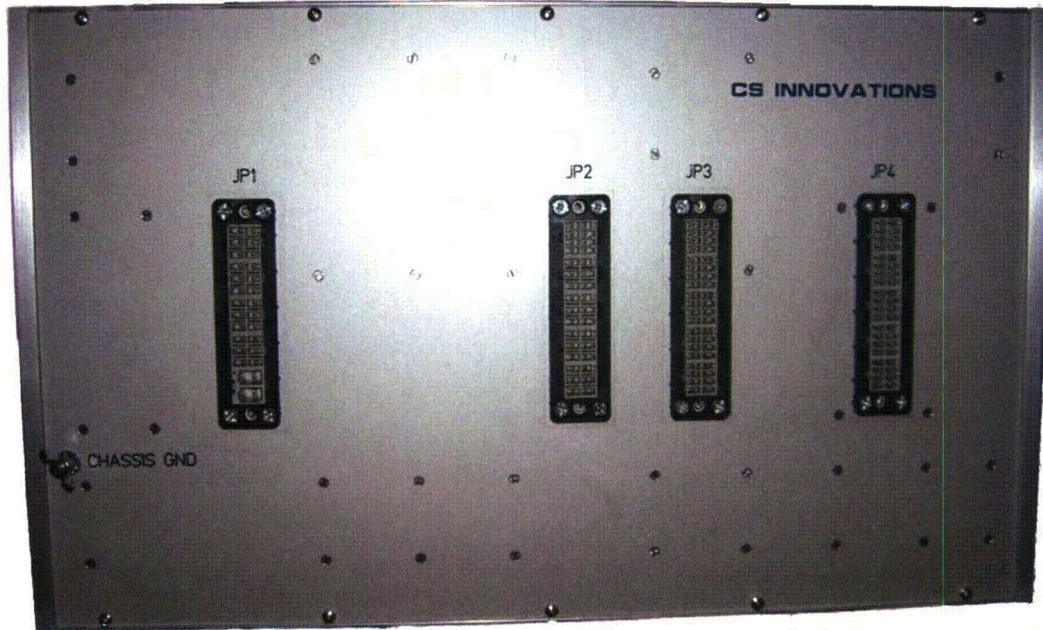


Figure 5: ALS Rack Rear View (WolfCreek MSFIS Application)

All permanent rack connections are made using cable harnesses connecting to the back panel. The connectors used by the ALS Platform are Phoenix Contact Variocon style connectors. The Variocon connectors are modular connectors where each module can be selected to provide an optimal combination of voltage/current capability and connector density. The Variocon connector shells can accommodate between 2-5 modules where each module includes between 2 and 8 connections.

Positions	Picture Female	Picture Male	UL Nom.
2			600V / 20A 6kV Surge AWG 10-30
6			250V / 10A 2.5kV Surge AWG 14-30
8			300V / 10A 2.5kV Surge AWG 14-30



Figure 6: Male Phoenix Field-Connector

The Earthing connection (Chassis Ground) is located in lower-left corner of the rear-panel.

5.6 Cable Harnesses

Cable harnesses are built to specifications and will vary from application to application.



5.7 ALS Boards

ALS boards are designed to fit directly into an ALS platform rack. The ALS boards connects to the back plane using DIN41612 style connectors. All components, switches and LEDs are mounted directly on the printed circuit board (PCB) which allows for easy removal of the front plate.

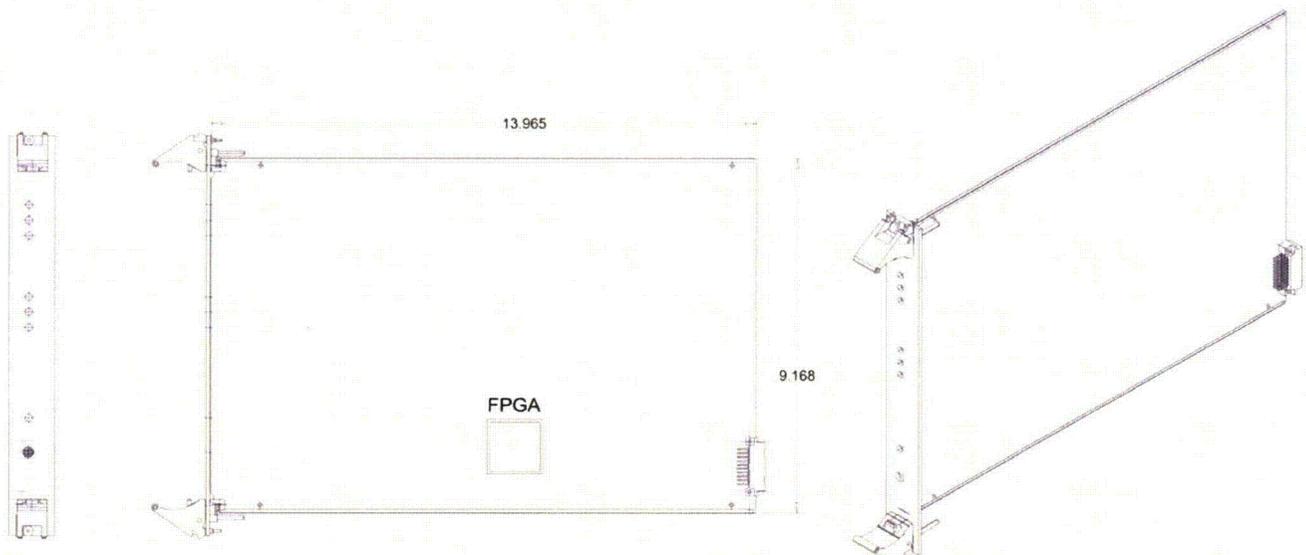


Figure 7: Generic ALS Board with ALS Bus Connector. The front panel width will vary

The intelligence on each board is located in the FPGA. The FPGA contains the communication controllers (RAB and TAB), registers, NVM interface and all other auxiliary logic as well as board specific logic (input channel logic). All ALS boards use the same FPGA, however each of the FPGAs contain a different board build functionality.

A key design goal for the ALS platform was to reduce the number of different components used on the ALS boards by striving to reuse sub-circuits. This reduces the part number count used in the ALS platform and helps to mitigate obsolescence issues. All common sub-circuits are located identical on all ALS boards.

6

ALS Power Management

The ALS power management architecture is based on a two-step conversion approach to supply circuits with power:

- Centralized power is fed to the ALS platform rack where a DC/DC or AC/DC converter generates a stable 5V ALS rack power from the available cabinet power. Typically the cabinet power will be a Class 1E 125V power feed.
 - Input: 125Vdc plant (90Vdc-150Vdc)
 - Output: 5Vdc ALS supply voltage (Common 5V for all boards in the ALS rack)
- Distributed (local) DC-DC voltage regulation and filtering on each ALS board is used to generate the required stable voltages for the digital domains:
 - Input: 5Vdc ALS supply voltage
 - Output: 5Vdc (Filtered / Regulated)
 - Output: 3Vdc (Filtered / Regulated)
 - Output: 2.5Vdc (Filtered / Regulated)

Figure 8 shows a typical ALS platform with the different voltage domains.

6.1 ALS Ground Domains

The ALS has three fundamental types of ground domains:

- Chassis Ground – referred to as CGND
- Digital Ground – referred to as DGND, used for ALS Logic circuits
- Isolated Field Ground – An ALS rack may have many individually isolated field ground domains.

Chassis ground (CGND) is the overall cabinet earth ground. Chassis ground is typically supplied to the cabinet from a plant grounding system using heavy gauge copper wires to a distribution point within the cabinet. The ALS Platform rack are grounded directly to this ground distribution point.

All conductive parts of the ALS rack (chassis) are connected to CGND to provide effective EMI characteristics.

Furthermore, all board card guides are connected to CGND to ensure early grounding of PCB boards while boards are being inserted by CSI or I&C technicians.

Digital ground (DGND) is a local ALS ground reference generated by the central 5V DC-DC converters on the redundant power supply boards within the rack.

All digital ALS circuits (FPGA's bus communication devices, 3V/2.5V-voltage regulators, etc.) are referenced to DGND.

Isolated Ground is used for field signal condition circuits. The isolated ground is usually supplied by the field input or output device and enters the ALS rack together with the field signals. Examples of isolated ground references are:

- Digital field input boards with isolated channel power
- Field output drive channels with high-power isolated drive circuits

6.1.1 5V Power Domain

The 5V board supply voltage is supplied to each ALS board through the ALS Bus backplane connector and is described in the following sections.

Filtering – Upon entry onto the ALS board the 5V is fused, filtered and overvoltage protected. The fuse ensures that catastrophic failures on a ALS board cannot disrupt the rack power. The filtering is done to avoid noise propagating from the ALS back-plane (transients, etc) to the board itself and also to avoid noise coming from the the ALS board to the ALS back-plane.

Each ALS board provides it's own protection circuit to ensure no damage is caused to any of the on-board components in the case of transients coming from the back-plane.

Supervisor – The 5V voltage supervisor is utilized by the FPGA to provide direct monitoring capability of the 5V supply voltage.

6.1.2 3V Power Domain

The 3V domain is primarily utilized to power the FPGA I/O-ring and associated components.

Supervisor – The 3V voltage supervisor is utilized by the FPGA to provide direct monitoring capability of the 3V supply voltage.

6.1.3 2.5V Power Domain

The 2.5V domain is dedicated to provide a stable FPGA core voltage.

Supervisor – The 2.5V voltage supervisor is utilized for Power-On Reset of the FPGA logic.

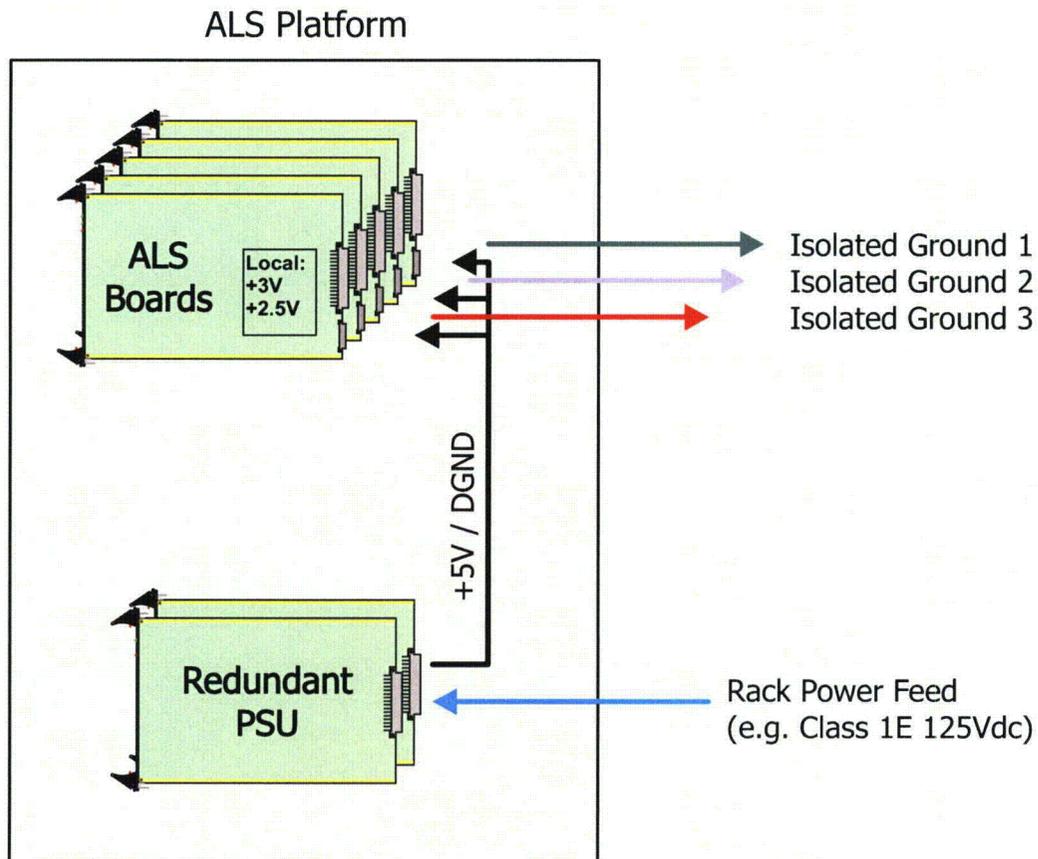


Figure 8: ALS Platform Power Domains

7

ALS Modes and States

This chapter describes the ALS Modes and States and includes the following concepts: ALS System Mode, Classification of Failures, Alarm Generation and ALS Test Mode.

7.1 ALS System Modes

The Core Logic Board (CLB) maintains the ALS platform's "System Mode", which defines the operational state of the ALS system. The System Mode can be "FCO", "RCO", "HALT" or "RESET". Figure 9 and Table 3 define the 4 System Modes.

FCO, RCO and HALT are the 3 primary modes of operation. FCO is the ideal situation which indicates no errors are present within the system, RCO indicates that non-vital error(s) have occurred, the ALS will disregard information from the failing units but otherwise continue to perform its function, HALT means a serious error has occurred and all functions have stopped in the rack. RESET is a transitory state only entered when plant personnel toggle the reset switch on the CLB front panel in order to clear all latched errors. The classification of failures (non-vital and vital) can be found in section 7.2.

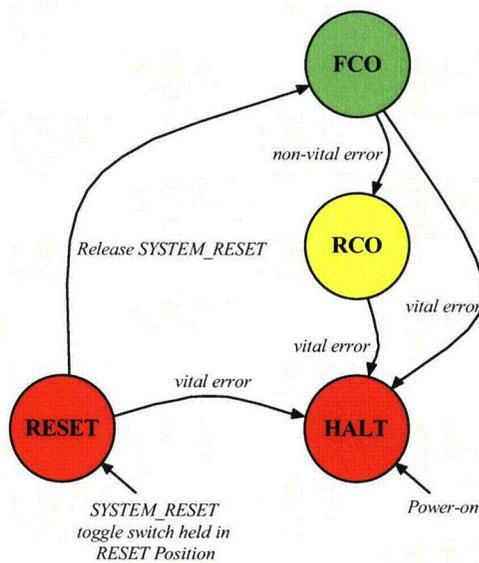


Figure 9: ALS System Mode

Table 3: ALS System Modes

SYSTEM MODE	DESCRIPTION
FCO	<p>Full Capability Operation (FCO) mode: FCO is the normal mode of operation for the ALS rack. It indicates that all circuits are 100% functional and that the ALS rack is ready to perform the intended safety function.</p> <ul style="list-style-type: none"> ▪ Input channels are continuously updated, and BIST values are in accordance with expected values. ▪ Output channels are controlled in the manner in which they were intended, and BIST values are as expected. ▪ Core Logic circuit is fully functional.
RCO	<p>Reduced Capability Operation (RCO) mode: The ALS rack operates in RCO mode when one or more failures have been detected within the ALS system. The failures have been isolated and all other functions continue to perform their intended function. The failures can be simple channel related failures with one or more individual failing channels. The failures can also represent a more complex set of failures have occurred on a particular ALS board and the entire board has been removed from operation. The failed functions or boards are not longer used by the CLB to determine the desired output state. If an ALS board is removed from the ALS rack, after two failed accesses the CLB will enter RCO mode and stop accessing the board.</p>
HALT	<p>HALT mode indicates the ALS rack is inoperable and not capable of performing the safety function. Vital failures have occurred and the ALS rack is forced into HALT mode. The rack will also enter HALT at power-up or when CLB is initially inserted in the rack. All operation is halted and all boards within the ALS system are forced to a FailSafe state:</p> <ul style="list-style-type: none"> ▪ All input channels are updated. BIST engines continue to monitor the channel circuitry. ▪ All output channels are placed in a FailSafe state, where all outputs are either force to 'Fail-as-is' or 'Fail-as-defined' – depending on their SetPoint configuration. BIST engines continue to monitor channel circuitry. ▪ Core Logic circuit is in HALT mode. <p>HALT is also referred to as the FailSafe state.</p>
RESET	<p>RESET mode indicates manual action is being taken by the plant personnel to confirm (and clear) existing alarm conditions in order to (re-)start the system in a normal mode of operation. The ALS rack is inoperable and not capable of performing the safety function while in RESET mode. All operations will stop and the system (i.e. all boards) is forced to a FailSafe state:</p> <ul style="list-style-type: none"> ▪ All input channels are updated. BIST engines continue to monitor the channel circuitry. ▪ All output channels are placed in FailSafe state, where all outputs are either force to 'Fail-as-is' or 'Fail-as-defined' – depending on their SetPoint configuration. BIST engines continue to monitor channel circuitry. ▪ Core Logic circuit is in RESET mode.

7.1.1 ALS System Mode versus Local System Mode

The ALS platform provides two levels of System Modes; The top level is the Global System mode distributed by the CLB to the ALS slave board during each RAB access, at a lower level all ALS boards maintains a Local System Mode. The Local System Mode will ideally track the ALS System Mode, but it allows the individual boards to autonomously enter RCO or HALT as soon as the failure is discovered. As soon as the detected failure has been transmitted to the CLB, the CLB will adjust the system mode accordingly.

System Mode Facts:

- System Mode is the global mode of operation for the entire ALS system (ALS system refers to all boards within a rack controlled by the CLB).
- System Mode is based solely on 'ALS System Integrity' information, such as device operation, power supply operation, redundancy checks and is 100% independent of the application related core logic circuits.
- The System Mode is based on integrity information retrieved from all ALS boards in the system during the process of communicating I/O-data between ALS I/O-boards and the CLB using the RAB bus.
- System Mode will initially be HALT mode when the system powers up or when the CLB board is inserted into the rack.
- The System Mode 'master-copy' is physically located in a register within the integrity monitor module in the CLB. Local replicas of the System Mode are maintained by each ALS-board within the slave integrity monitor module.
- System Mode is communicated to all ALS boards in the system during transactions on the RAB.

Important note:
 The System Mode is an indicator of the health of the ALS hardware platform. If BIST engines have detected an issue in non-vital circuits the system is forced into a reduced capability mode of operation (RCO), and if BIST engines detect issues related to vital circuitry the system is forced into HALT mode. Whether the system can perform its safety related function or not is not related to the System Mode, but instead related to application specific circuits located within the Core Logic circuits
 Example: WCGS MSFIS system has a alarm linked directly to the System Mode, and has independent STATUS signals to provide indication of the capability of the system to perform its intended safety function.

7.2 Classification of Failures

This section defines the failure states used in the CLB decision process to determine the System Mode of operation. The ALS boards are also capable of monitoring the local System Mode from board integrity. The terms are used to define the class of failures a system will observe:

Class of Failure	Description
Fatal	Fatal failures refer to a severe type of failure, which compromises the control function of the system, and the concept of SYSTEM_MODE is no longer valid. The most obvious fatal failure is the complete loss of input power to the ALS rack – the result is loss of all system functionality and status indication.
Vital	Vital failures refer to the class of errors which affect the overall system and possibly degrade the performance to a degree, where the overall system performance and integrity is compromised. The occurrence of one or more vital failures will result in loss of ALS integrity and maintenance is required immediately. The system will immediately enter HALT mode, if a vital error is detected and boards will enter the predefined FailSafe state.
Non-vital	Non-vital failures refer to the class of errors, which do not affect the overall system performance or integrity of the system. Following one or more non-vital failures, the ALS platform is still operable and the integrity of the system has not been compromised, but requires maintenance to operate as specified. The system will immediately enter RCO mode, if a non-vital error is detected.
Undetectable	Undetectable failures refer to the class of errors; which do not affect the overall system performance or general integrity of the system. Examples of undetectable failures are LED related circuit failures (wiring, failed LED, driver). The rack front-panel provides wrong indication, but the system will perform the function as specified.

7.3 Alarm Generation

The dedicated alarm generation/indication from ALS rack is implemented using redundant Solid State Relays (SSR). The alarm is designed to be CLOSED during normal operation and OPEN to indicate a failure.

There are two sources for alarm within an ALS rack:

- Application related alarms, which is associated to the application logic
- System related alarms, which is generated in the integrity monitor circuits protecting the integrity of the board.

The alarm generation circuit is located on 2 independent boards:

- CLB (ALS-101 boards)
- STB (ALS-201 boards)

The alarm connections points are independent, but can be wired together in series on the back-panel.

7.4 ALS Test Mode

TESTMODE is a special feature available to CS Innovations engineering teams to allow access to test circuits within the ALS platform. TESTMODE is a special mode which basically provides access to otherwise hidden and inaccessible registers in the ALS boards, without actually probing or forcing external voltages onto boards.

Access to TESTMODE is restricted and requires a specific set of conditions to be valid in order for a board to enter TESTMODE. This ensures no faulty signals or defects on the board can cause sensitive information to change without notice in the background.

TESTMODE is only active when explicitly enabled from an external device using special tools (ATU) provided by CS Innovations. Standard PCs are not able to establish connections to an ALS board. A series of "checks" as well as the proprietary TAB protocol ensures that a ALS board will never enter TESTMODE when in a ALS Rack.

8

ALS Communication

The ALS architecture is based on reliable and high integrity communication between boards. The bus architecture is a unique feature to the ALS platform with an advanced fault detection and mitigation strategy designed not only to provide reliable communication of information, but also to detect and handle faulty components in the communication link itself.

The dedicated and efficient bus implementation is achieved using industry standard differential EIA-485 hardware, a dedicated, simple and efficient communication protocol and a small optimized embedded controller implemented using redundancy.

Two separate and independent communication busses are implemented:

- **Reliable ALS Bus (RAB)** – is the primary communication bus within the ALS platform. The RAB is dedicated to transfer safety related signal information between the boards, i.e. IPBs → CLB and CLB → OPBs. The RAB is the primary bus used for communication during normal operation (not in HALT mode). The RAB data always includes:
 - DATA – The actual I/O-information
 - INTEGRITY – The associated health information to a DATA I/O-point.
- **Test ALS Bus (TAB)** – is the secondary communication bus within the ALS platform. The TAB is dedicated to transfer run-time diagnostics information to the STB in the background without affecting the main system operation, as well as off-line test and configuration tasks with the ATU. During normal operation the TAB interface supports the diagnostics and LiveView features, where the STB collects integrity information from all ALS boards in the system and stores the information in the BlackBox or transfers the information to an ASU (if attached). While off-line the TAB is the only interface, where CS Innovations test equipment (ATU) has access to write configuration (SetPoint) information to the board NVMs. TAB communications are performed asynchronously in the background without affecting RAB communication.

The RAB and the TAB interfaces utilize equivalent design and implementation, as well a similar protocol and packet format, see section 8.2.

The RAB and TAB interfaces are the only means of communication between ALS boards and all information shared between boards is transferred using these two interfaces.

All transfers over the busses are validated for integrity utilizing checksums. If the checksum does not match the expected, then the data packet is not utilized.

ALS bus communication is handled by simple, dedicated communication circuits on each board (section 8.4) in conjunction with digital circuits within the FPGA device.

8.1 ALS Bus Facts

Dedicated Bus Topology:

- Linear bus topology with all devices connected to a low-speed differential EIA-485 wire-pair. The back-plane provides the main wire-pair with a terminator at each end. All nodes (ALS-boards) are connected to the linear bus thru back plane connectors.
- Master-slave protocol with 1 master and many slaves on each bus:
- Access scheme:
 - a. RAB transactions with I/O data are point-to-point communication initiated by the master, with slaves responding with valid data when requested. Response is immediate.
- Half-duplex communication protocol between two devices. The bus provides for communication in both directions, but only one direction at a time (not simultaneously).

Reliability and High Integrity:

- Two-way communication, which utilizes a request-and-response protocol for transactions meaning all communication is acknowledged (except Broadcasts).
- The packet payload (I/O-data information) is protected by cyclic redundancy check (CRC). Packets are ignored, if the CRC is invalid, which again leads to the payload being discarded and the information not used.
- Integrity information collected in the I/O-channels is transferred along with I/O-data. This enables the CLB to make decisions based on valid information and take appropriate action only if invalid channel information is available. If boards become un-available (due to board removal or vital failures) then data and the integrity gets invalidated within the CLB.
- High noise immunity due to dedicated EIA-485 differential wire-pair, implemented with short wire length and high drive capability.

Fault Isolation:

- Bus protocol avoids bus contention, can detect unintended bus contention, and will isolate boards with failing devices.
- Instant detection of communication failure (invalid data) and communication loss (indicating a failing unit).
- Spoof-proof communication ensures instantaneous detection of interference from invalid or failing boards.

Advanced, Deterministic Protocol:

- Guaranteed response time which allows the system to have deterministic reaction time for any input state changes.
- Guaranteed response time enable detection of lost or failing devices.
- Guaranteed packet synchronization, with instant detection of synchronization loss.

8.2 ALS Bus Protocol

This section specifies the ALS Bus (RAB and TAB) protocol. The protocol is a set of rules that governs communications between devices (ALS boards). These rules include guidelines that regulate the network characteristics such as access method, fault detection, fault isolation, physical topology, physical layer, and speed of data transfers. All CRC calculations will be based on a CCITT standard polynomial.

A RAB master (CLB) requests accesses to the slaves in a round robin fashion at a fixed rate determined by the RAB System Frame Timing. The RAB master will read information from all appropriate input boards and write information to all appropriate outputs boards once every ALS System Frame.

8.3 ALS Bus Failure Detection and Mitigation

This section describes the general detection of ALS bus failures and the actions taken to ensure high system reliability. In normal operation the ALS platform will detect any failure on the ALS bus (RAB or TAB). In addition to being able to detect any failure, care is taken in defining the protocol to ensure that a secondary failure cannot occur as a result of a primary bus failure. Having multiple layers of error detection and mitigation techniques results in a highly reliable bus where all failures or errors will be detected and handled appropriately.

8.3.1 ALS Bus Failure Mode Error Analysis

The following RAB communication failures can be detected and isolated – see the simple FMEA in Table 4.

Table 4: Simple ALS Bus FMEA

Causes	Failure Mechanism	Detection Mechanism	Mitigation
Hardware	Defective crystal or loss of synchronization	SYNC detector (On ALS board)	RETRY then FAILSAFE
	FPGA device defect: <ul style="list-style-type: none"> ▪ Defective flash cell ▪ Logic gate failure ▪ I/O pad defect ▪ Clock or voltage distribution ▪ Redundant channel disagrees with primary channel 	Redundant bus circuit (within FPGA)	RETRY then FAILSAFE
	External circuitry defect: <ul style="list-style-type: none"> ▪ Defective EIA-485 driver ▪ Bus-termination circuit ▪ Loose connector ▪ Bad soldering ▪ Broken wire or Tin whisker 	CRC-check and implicit encoding of information	RETRY then FAILSAFE
External System	Spoofing by defective ALS board	CRC check and implicit encoding of information	RETRY then FAILSAFE
	Induced noise on communication line	CRC check and implicit encoding of information	RETRY then FAILSAFE
Packet error	Read or Write transaction failed: <ul style="list-style-type: none"> ▪ CRC received on ALS bus does not compare to calculated CRC ▪ Incomplete transmission ▪ No response from slave 	CRC check and implicit encoding of information Note: Received data is not used.	RETRY then FAILSAFE
	Read or Write requests to undefined ALS slave addresses	Action will only occur on slave address match and CRC OK	FAILSAFE

TAB failures will be detected and mitigated in a similar fashion. The only exception is that the TAB will not force the board into HALT Mode, but instead will detect the failure and ensure no valid response is issued. A failure of the TAB interface is not considered vital to the ALS rack, even though it is an essential part of the system. TAB communication failures will only affect debugging and diagnostics. This approach allows the system keep running as long as possible, while still preserving point-to-point integrity.

8.3.2 ALS Bus Failure Detection

Both the RAB and TAB interfaces provide a layered failure detection scheme. This layered failure detection scheme is designed to detect any possible failure that can occur on the communication bus, the communication devices, or the communication logic circuits within the FPGA.

Four detection schemes are responsible for detecting a communication failure:

- Redundancy failure detection
- Synchronization failure detection
- CRC failure detection
- Protocol failure detection

Note: Detection and reaction of Redundancy and Synchronization failures are instantaneous

Detection of CRC or Protocol failures will likely not be instantaneous (payload data will be transferred before the CRC is calculated) but the reaction will be instantaneous. The Rx will not allow the data to propagate

8.4 ALS Bus Physical Layer

The physical layer for ALS Bus (RAB and TAB) is implemented with standard EIA-485 devices.

EIA-485 specifies a 2-wire, bidirectional, differential line, half-duplex data transmission, multipoint communication standard. Up to 32 transmitters and 32 receivers may be interconnected in any combination, including one driver and multiple receivers (multi-drop), or one receiver and multiple drivers.

9

ALS Service Unit (ASU)

The ALS Service Unit (ASU) is the primary tool used when accessing a particular ALS system in operation. The ASU provides plant personnel access to advanced features of the ALS system such as system diagnostics, post-trip analysis, monitoring real-time operation, and initiating various run-time tests. The advanced diagnostics capabilities enable fast and efficient system setup and troubleshooting. The ASU is a standard laptop running the dedicated ASU software application. It is connected to the ALS-201 STB board of an ALS rack through a USB connection.

The main features of the ASU are:

- **State Information:** Features monitoring of real-time operation, including all I/O signals as well as detailed status information from internal debugging registers. The advanced monitoring capabilities enable fast system diagnostics and troubleshooting.
- **System and Board Information:** Provides detailed information about the static parameters of an ALS system, including board FPGA programming, board build information, and board set-point configurations.
- **Black Box:** The ASU facilitates retrieving and presenting the black box information, thereby enabling plant personnel to inspect the ALS system's reaction to a past event. This feature significantly helps reduce the time it takes to pinpoint the cause of problem situations.
- **Testing:** Various surveillance tests can be initiated using the ASU.

The ASU operation is passive and non-intrusive, i.e. it cannot modify the system configuration, nor can it override any of the safety-related functionality within the ALS. All communication initiated by the ASU takes place on the TAB bus. No RAB interruption can occur, effectively leaving the safety operations of the ALS system unaffected.

9.1 Configuration Report

The ASU can generate a configuration report for the ALS system. This configuration report includes:

Build Information – similar to information written on labels on the board and the PCB silk-screen. It is stored in the NVM for more reliable traceability, and it offers an efficient way to retrieve information. This information is static and only programmed once by CS Innovations personnel. The Build Information will typically include: Board Serial Number, Board Part Number, Board Revision Number, Build Date, FPGA Part Number, and FPGA Revision Number.

SetPoint Configuration – The application specific configuration of the ALS boards. It is stored in the NVM to enhance reliability and robustness as well as to have a more reliable traceability, and it offers an efficient way to retrieve information about a board configuration using the ASU. The set-point information is configured by CS Innovations during board dedication for use in a particular application. The set-point configuration is static in nature, and it is only supposed to be programmed once by CS Innovations personnel. However, the set-point configuration can be modified using the ALS Test Equipment if changes to the system application parameters if desired. The ASU can retrieve the SetPoint Configuration, but cannot modify the SetPoints.

10

SetPoint Configuration

The ALS platform has the capability of configuring each board to support application specific functions. The configuration is facilitated with the use of a non-volatile memory (NVM) device attached to the FPGA device, and a small sequencer within the FPGA to read information stored in the NVM and place it in local registers within the FPGA.

SetPoint information is local to a board. Individual ALS boards have their own configuration memory where information local to the board is stored. SetPoint information consists of local settings, such as channel setup, sequencer setup, timing setup, build information, etc.

SetPoint configuration is stored in the NVM using the ATU and the TAB bus.

10.1 SetPoint Definition

ALS defines SetPoints as local values related to an ALS board, which can be either set or cleared, activated or de-activated, enabled or disabled, a trip value, a timing value.

Examples of SetPoints are:

- Channel Enable/Disable
- Channel NO/NC Type
- Channel Filter Timing
- Temperature Trip Values
- Timing Delays (used in timers / sequencers)
- FAIL_AS_DEFINED (Mode and State values)
- BoardID
- SetPoint Build information

10.2 Configuration Integrity

The traditional approach to set-point implementation on PCBs has been the use of jumpers, DIP-switches or 0Ω resistors.

The ALS approach to maintain set-points is to store them as bits in a non-volatile memory device (a serial-FLASH device), also referred to as the SetPoints FLASH or the SetPoint NVM.

Information stored in the SetPoint NVM is protected by CRC Redundancy which ensures instant detection of failures in the NVM.

11 Redundancy

The ALS Platform uses a combination implementation and test strategies in order to maintain its **high integrity** status. These strategies are covered by the pending ALS Patents. This chapter describes the 3 primary implementation and test strategies:

- Redundancy
- Built In Self Test (BIST)
- Inherent Self-Test

The testing will typically be performed automatically by the ALS system without the need for interaction by plant personnel and may replace the need for regular surveillance testing at the plant.

11.1 Redundancy

All ALS FPGAs are all implemented with redundant digital logic. This is to protect the ALS board against a type of failure which can potentially occur over time as a result of manufacturing defects, radiation damage or flash cell charge degradation. This section exclusively focuses on how the redundancy is implemented internal to the ALS FPGAs. Other levels of redundancy such as the redundant input or outputs, or application level redundancy are not covered in this section. Difference between the redundant circuits will cause the ALS to take appropriate action. The redundancy implementation will detect any deviation between the redundant circuits before a possible erroneous signal can propagate to the remainder of the system.

11.2 BIST

The Built In Self Test (BIST) is used for exercising all critical functions within a board. This is done to ensure that latent failures cannot build up in the system and make the system inoperable without the knowledge of plant personnel. The BIST will typically apply input stimuli on the inputs to a sub-circuit and validate the correct response on the output.

11.3 Inherent Self-test

Inherent Self-test is a method for implementing high integrity directly into the logic circuits by constructing it in a way that latent STUCK-AT or OPEN failures will be instantly detected. An example of inherent self-testing is a serial communication link with CRC protection.