ALS™

CS Innovations
A Westinghouse Electric Company

Westinghouse Non-Proprietary Class 3

6002-00301-NP
Advanced Logic System Topical Report

Revision 2
November 10, 2011

APPROVALS

Function	Name and Title	Signature and Date
Author	Steve Seaman Manager, ALS Platform Engineering	10-Nov-11
Approved	John Porter Director, Safety I&C Upgrades and Development	10-Nov-11

WESTINGHOUSE NON-PROPRIETARY CLASS 3

PRINTED COPIES ARE UNCONTROLLED

Table of Contents

Acronyms and Trademarks 11

References..... 13

1 Introduction 16

1.1 Objective 16

1.2 Scope 16

1.3 ALS Background 17

2 ALS Platform Technical Description 18

2.1 ALS Platform Overview 18

2.1.1 ALS Boards 20

2.1.2 Generic ALS Core Logic Boards (ALS-1xx) 21

2.1.3 Generic ALS Input Boards (ALS-3xx) 22

2.1.4 Generic ALS Output Boards (ALS-4xx) 22

2.1.5 Common Components/Design 23

2.2 Standard ALS Boards 26

2.2.1 ALS-102 Core Logic Board 26

2.2.2 ALS-302 Digital Input Board (48Vdc contact inputs) 28

2.2.3 ALS-311 Analog Input Board (RTD/Thermocouple) 29

2.2.4 ALS-321 Analog Input Board (Voltage/Current) 31

2.2.5 ALS-402 Digital Output Board (Contact Output) 33

2.2.6 Deleted 35

2.2.7 ALS-421 Analog Output Board 35

2.2.8 ALS-601 Communication Board 37

2.3 ALS Internal Communications 39

2.3.1 Reliable ALS Bus (RAB) 41

2.3.2 Test ALS Bus (TAB) 42

2.3.3 ALS Bus Failure Detection and Mitigation 42

2.3.4 ALS Internal Communication Acceptance 43

2.4 Board Operation Modes 44

2.5 ALS Chassis 46

2.5.1 Chassis Mechanics 48

2.5.2 ALS Slot and Card Configuration 48

2.5.3 ALS Boards 48

2.5.4 ALS Front Plate 49

2.5.5 Board Latches 49

2.5.6 Front Panel LEDs 50

2.5.7 ALS Backpanel Assembly 50

2.5.8 Expansion Chassis 51

2.6 Cabinet and Peripherals 52

2.6.1 Cabinet 53

2.6.2 Power Supply and Distribution 53

2.6.3 ALS Service Unit (ASU) 54

2.6.4 Control Panel 55

2.6.5 Assembly Panel 56

2.7 Response Time 56

2.8 ALS System Accuracy 57

2.9 Human Factors Considerations 58

3 Diagnostics and Maintenance 59

3.1 ALS Diagnostics and Fault Indications 59

3.1.1 ALS Platform Diagnostics 59

3.1.2 Application Diagnostics 63

3.1.3 Preferred Failure Mode for Abnormal and Unexpected Inputs 63

3.1.4 ALS Alarm Reset 63

3.2 ALS Platform Maintenance Features 63

3.3 Maintenance Terminology 64

3.4 Calibration of ALS Input and Output Boards 65

3.5 Test of Digital Output Boards 66

3.6 Maintenance of Set Points 67

4 Equipment Qualification 69

4.1 Environmental Qualification 69

4.1.1 Temperature/Humidity 69

4.2 Seismic 71

4.2.1 Pre-Seismic Inspection and Operability Check 71

4.2.2 Resonance Search Test 71

4.2.3 Qualification Seismic Tests 71

4.2.4 Post-Seismic Baseline Test and Operability Check 73

4.3 Electromagnetic Compatibility (EMC) Testing 73

4.3.1 EMC Emissions 74

4.3.2 EMC Susceptibility 74

4.3.3 Surge Withstand Capability 75

4.3.4 Electro-Static Discharge (ESD) 75

4.3.5 Deleted 76

4.4 Deleted 76

5 ALS Platform Communications 77

5.1 Intra-Divisional Communication 77

5.2 Inter-Divisional Safety-to-Safety Communication 78

5.3 Inter-Divisional Safety-to-Non-Safety Communication 79

5.3.1 Broadcasting Information to Non-Safety Devices Using ALS-601 79

5.3.2 Broadcasting Information to Non-Safety Devices Using TxB Busses 80

5.3.3 Communication with Non-Safety Devices Using the TAB Bus 80

5.4 Multidivisional Control, Display and Management 81

5.4.1 Multidivisional Control in Multiple Safety Divisions 81

6 Life Cycle Management Process 97

6.1 Development Process 97

6.1.1 Planning Stage 97

6.1.2 Development Stage 97

6.1.3 Manufacturing Stage 97
6.1.4 System Test Stage 97
6.1.5 Installation/Operation Phase 98
6.2 Life Cycle Planning Documentation 98
6.3 Verification and Validation 98
6.3.1 Field Programmable Gate Array V&V 98
6.3.2 Board V&V 98
6.3.3 System V&V 98
7 Reliability.... 99
7.1 Failure Modes and Effects Analysis (FMEA) 99
7.2 Reliability and Availability 99
8 Security...... 100
8.1 ALS Platform Security Overview 100
8.2 Life Cycle Security 101
8.2.1 Planning Activity 101
8.2.2 Development and Manufacturing Activities 101
8.2.3 System Test, Installation, and Maintenance Activities 101
8.3 ALS Platform Security Methods and Features 101
9 Diversity...... 102
9.1 Implementation of Diversity to Address Common Cause Failure 102
9.2 NUREG/CR-6303 Diversity Evaluation 103
9.3 Typical Applications of Diversity 103
9.3.1 Diversity within the ALS FPGA 103
9.3.2 Diversity Between Chassis 103
9.3.3 Diversity Within Separation Groups 104
10 Quality Assurance 105
11 Training...... 106
12 Regulatory Compliance 107
12.1 Review of ALS Platform Compliance to IEEE-603 Requirements 107
12.1.1 IEEE 603-1991 Clause 4 – Safety System Designation 107
12.1.2 IEEE 603-1991 Clause 5.1 – Single-Failure Criterion 108
12.1.3 IEEE 603-1991 Clause 5.2 – Completion of Protective Action 108
12.1.4 IEEE 603-1991 Clause 5.3 – Quality 109
12.1.5 IEEE 603-1991 Clause 5.4 – Equipment Qualification 109
12.1.6 IEEE 603-1991 Clause 5.5 – System Integrity 110
12.1.7 IEEE 603-1991 Clause 5.6 – Independence 110
12.1.8 IEEE 603-1991 Clause 5.7 – Capability for Test and Calibration 112
12.1.9 IEEE 603-1991 Clause 5.8 – Information Displays 113
12.1.10 IEEE 603-1991 Clause 5.9 – Control of Access 115
12.1.11 IEEE 603-1991 Clause 5.10 – Repair 115
12.1.12 IEEE 603-1991 Clause 5.11 – Identification 116
12.1.13 IEEE 603-1991 Clause 5.12 – Auxiliary Features 116
12.1.14 IEEE 603-1991 Clause 5.13 – Multi-Unit Stations 117
12.1.15 IEEE 603-1991 Clause 5.14 – Human Factors Considerations 117

12.1.16 IEEE 603-1991 Clause 5.15 – Reliability 117
12.1.17 IEEE 603-1991 Clause 6.1 – Automatic Controls 118
12.1.18 IEEE 603-1991 Clause 6.2 – Manual Control 118
12.1.19 IEEE 603-1991 Clause 6.3 – Interaction between Sense of Command Features and Other Systems 119
12.1.20 IEEE 603-1991 Clause 6.4 – Derivation of System Inputs 119
12.1.21 IEEE 603-1991 Clause 6.5 – Capability for Testing and Calibration 120
12.1.22 IEEE 603-1991 Clause 6.6 – Operating Bypasses 120
12.1.23 IEEE 603-1991 Clause 6.7 – Maintenance Bypass 120
12.1.24 IEEE 603-1991 Clause 6.8 – Setpoints 121
12.1.25 IEEE 603-1991 Clause 7.1 – Automatic Control 121
12.1.26 IEEE 603-1991 Clause 7.2 – Manual Control 121
12.1.27 IEEE 603-1991 Clause 7.3 – Completion of Protective Action 122
12.1.28 IEEE 603-1991 Clause 7.4 – Operating Bypasses 122
12.1.29 IEEE 603-1991 Clause 7.5 – Maintenance Bypass 122
12.1.30 IEEE 603-1991 Clause 8 – Power Source Requirements 122
12.2 IEEE-7-4.3.2 Compliance 123
12.2.1 IEEE 7-4.3.2 Clause 4 – Safety System Design Basis 123
12.2.2 IEEE 7-4.3.2 Clause 5.1 – Single-Failure Criterion 123
12.2.3 IEEE 7-4.3.2 Clause 5.2 – Completion of Protective Action 123
12.2.4 IEEE 7-4.3.2 Clause 5.3 – Quality 123
12.2.5 IEEE 7-4.3.2 Clause 5.3.1 – Software Development 123
12.2.6 IEEE 7-4.3.2 Clause 5.3.1.1 – Software Quality Metrics 124
12.2.7 IEEE 7-4.3.2 Clause 5.3.2 – Software Tools 124
12.2.8 IEEE 7-4.3.2 Clause 5.3.3 – V&V 124
12.2.9 IEEE 7-4.3.2 Clause 5.3.4 – Independent V&V Requirements 124
12.2.10 IEEE 7-4.3.2 Clause 5.3.5 – Software Configuration Management 124
12.2.11 IEEE 7-4.3.2 Clause 5.3.6 – Software Project Risk Management 125
12.2.12 IEEE 7-4.3.2 Clause 5.4 – Equipment Qualification 125
12.2.13 IEEE 7-4.3.2 Clause 5.5 – System Integrity 126
12.2.14 IEEE 7-4.3.2 Clause 5.6 – Independence 127
12.2.15 IEEE 7-4.3.2 Clause 5.7 – Capability for Test and Calibration 127
12.2.16 IEEE 7-4.3.2 Clause 5.8 – Information Displays 127
12.2.17 IEEE 7-4.3.2 Clause 5.9 – Control of Access 127
12.2.18 IEEE 7-4.3.2 Clause 5.10 – Repair 127
12.2.19 IEEE 7-4.3.2 Clause 5.11 – Identification 127
12.2.20 IEEE 7-4.3.2 Clause 5.12 – Auxiliary Features 127
12.2.21 IEEE 7-4.3.2 Clause 5.13 – Multi-Unit Stations 128
12.2.22 IEEE 7-4.3.2 Clause 5.14 – Human Factors Considerations 128
12.2.23 IEEE 7-4.3.2 Clause 5.15 – Reliability 128
12.2.24 IEEE 7-4.3.2 Clause 6 – Sense and Command Features 128
12.2.25 IEEE 7-4.3.2 Clause 7 – Execute Features 128
12.2.26 IEEE 7-4.3.2 Clause 8 – Power Source Requirements 128
12.3 DI&C ISG-04 Highly-Integrated Control Rooms- Communications Issues 129

12.4 BTP 7-14, R5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems 129
12.5 BTP 7-19, Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems and ISG-02, Diversity and Defense-in-Depth Issues 129
12.6 RG 1.152, Revision 3 (Draft), Criteria for Use of Computers in Safety Systems of Nuclear Power Plants..130
12.7 ISG-06, Digital I&C Licensing Process 131
Appendix A Reactor Protection System (RPS)/Engineered Safety Features Actuation System (ESFAS) Application...137
Appendix B Train Diverse Application...144
Appendix C Dual Train Application 146

List of Figures

Figure 2-1: ALS Chassis Populated with Eight Boards 19
Figure 2-2: Generic ALS Platform Architecture Overview 21
Figure 2-3: Generic ALS Board 24
Figure 2-4: ALS-102 with 6 Input Channels, 2 Comm Channels and 4 Output Channels 27
Figure 2-5: ALS-302 with 32 Input Channels 29
Figure 2-6: ALS-311 with 8 Channels Split Into Individually Isolated Blocks 30
Figure 2-7: ALS-311 Board Configurations 30
Figure 2-8: ALS-321 with 8 Channels Split Into Individually Isolated Blocks 32
Figure 2-9: ALS-321 Board Configurations 32
Figure 2-10: ALS-402 with 16 Contacts Split Into 2 Groups with Reinforced Isolation 34
Figure 2-11: Illustration of ALS-402 Channel Design and Use 35
Figure 2-12: Deleted 35
Figure 2-13: ALS-421 8 Channel Analog Output Board 36
Figure 2-14: ALS-601 with 8 Independent Channels 38
Figure 2-15: Illustration of ALS-601 Channel Design and Use 38
Figure 2-16: ALS Platform Bus Architecture 40
Figure 2-17: RAB Transactions 41
Figure 2-18: ALS Board Modes 45
Figure 2-19: Typical ALS Chassis Populated with 8 ALS Boards 47
Figure 2-20: Generic ALS Board with ALS Bus Connector 49
Figure 2-21: Generic vs. Custom Front Plate 49
Figure 2-22: [ ]^{a,c,e} Connector 51
Figure 2-23: Backplane Connector Assembly 51
Figure 2-24: Example Uses of Expansion Chassis 52
Figure 2-25: ALS Cabinet 53
Figure 2-26: Typical ALS Platform 48Vdc Power Distribution 54
Figure 2-27: ALS Platform Response Time Contributors 56
Figure 2-28: ALS System Accuracy 57
Figure 3-1: ALS Platform Self-Testing 60
Figure 3-2: Maintenace Modes for Analog Input/Output Channel 65
Figure 3-3: Maintenance Modes for a Digital Output Channel 66
Figure 3-4: Maintenance Modes for a Set Point 67
Figure 4-1: Generic Temperature Profile 70
Figure 4-2: Deleted 71
Figure 4-3: SSE RRS, Horizontal Direction, 5% Damping 72
Figure 5-1: Safety to Safety Interdivisional Communications 78
Figure 5-2: Communication between ALS and a safety QDS (left) and non-safety ASU (right) 80
Figure 5-3: Control and Maintenance from Central Computer 81
Figure 9-1: FPGA with Redundant Cores 102
Figure 9-2: Diversity within the ALS FPGA 103
Figure 9-3: Diversity Between Chassis 104
Figure 9-4: Diversity within Separation Groups 104
Figure A-1: [ ]^{a,c,e} 138

Figure A-2: [ ]a,c,e 139
Figure A-3: [ ]a,c,e 141
Figure A-4: [ ]a,c,e 142
Figure B-1: [ ]a,c,e 145
Figure C-1: [ ]a,c,e 148

List of Tables

Table 2-1: ALS Board Types 20
Table 2-2: NVM Content.....25
Table 2-3: ALS Board LED Indicators 50
Table 3-1: Self-testing ALS Platform Intervals.....61
Table 3-2: Class of Failure Description 62
Table 4-1: Normal and Abnormal Operating Environments per WCAP-8587, Rev. 6-A.....70
Table 4-2: Seismic Test Runs for the ALS Platform.....72
Table 4-3: EMC Emissions Tests and their Frequency Ranges.....74
Table 4-4: EMC Susceptibility Tests, Excluding Surge Withstand Tests 75
Table 4-5: IEC 61000-4 Test Methods 75
Table 4-6: ESD Test 76
Table 5-1: Inter-divisional Safety-to-Non-Safety Communication 79
Table 5-2: ALS ISG-04 Compliance Matrix – Interdivisional Communications 83
Table 5-3: ALS ISG-04 Compliance Matrix – Multidivisional Communications.....92
Table 12-1: Document Map – ISG06, Revision 44.....131
Table C-1: [Typical Dual Train Safety System Applications]^{a,c,e}.....146

Acronyms and Trademarks

Term	**Definition**
ADC	Analog-to-Digital Converter
ALS	Advanced Logic System
ASU	ALS Service Unit
BIST	Built-in-self-test
CCITT	International Telegraph and Telephone Consultative
CDI	Commercial Dedication Item
CGND	Chassis Ground
CLB	Core Logic Board
CJC	Cold Junction Compensation
CJT	Cold Junction Temperature
COM	Communication Board
COTS	Commercial-off-the-shelf
CFR	Code of Federal Regulations
CRC	Cyclic Redundancy Check
D3	Defense-in-Depth and Diversity
D/A	Digital to Analog
DGND	Digital Ground
DLL	Dynamic Link Library
EFT	Electrical Fast Transient
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FCO	Full Capability Operation
FET	Field Effect Transistor
FIFO	First-in, First-out
FMEA	Failure Modes and Effects Analysis
FPD	Flat Panel Display
FPGA	Field Programmable Gate Array
FRAM	Ferromagnetic Random Access Memory
FSM	Finite State Machine
FSV	Full Scale Value
HDL	Hardware Descriptive Language
HSI	Human-System Interface
I&C	Instrumentation and Control
I/O	Input/Output
IDI	Isolated Development Infrastructure
IPB	Input Board
IV&V	Independent Verification and Validation

LED	Light Emitting Diode
LSELS	Load Shedder and Emergency Load Sequencer
MCB	Main Control Board
MSFIS	Main Steam Feedwater Isolation System
MTBF	Mean Time Between Failure
NC	Normally Closed
NIST	National Institute of Standards and Technology
NO	Normally Open
NRC	Nuclear Regulatory Commission
NVM	Non-volatile Memory
OBE	Operating Basis Earthquake
OPB	Output Board
OS	Operating System
PAMS	Post-Accident Monitoring System
PC	Process Computer
PCB	Printed Circuit Board
PWR	Pressurized Water Reactor
QDS	Qualified Display System
RAB	Reliable Advanced Logic System (ALS) Bus
RCO	Reduced Capability Operation
RRS	Required Response Spectra
RT	Reactor Trip
RTD	Resistance Temperature Detector
RTOS	Real-time Operating System
RVLIS	Reactor Vessel Level Indicating System
Rx	Receiver
SPST	Single Pole Single Throw
SSE	Safe Shutdown Earthquake
SSPS	Solid State Protection System
SSR	Solid State Relay
SWCCF	Software Common Cause Failure
TAB	Test Advanced Logic System (ALS) Bus
TC	Thermocouple
TC/CCM	Thermocouple/Core Cooling Monitor
TVS	Transient Voltage Suppressor
Tx	Transmitter
QA	Quality Assurance
UART	Universal Asynchronous Receiver Transmitter
V&V	Verification and Validation
VL	Voter Logic
WCGS	Wolf Creek Generating Station

References

Following is a list of references used throughout this document:

1. NRC Regulations Title 10, Code of Federal Regulations, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," U.S. Nuclear Regulatory Commission.
2. MSFIS application of the ALS Platform in Docket 50-482, amendment 181 to License No. NPF-42, U.S. Nuclear Regulatory Commission.
3. BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," U. S. Nuclear Regulatory Commission.
4. IEEE 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
5. [ ]^{a,c,e}
6. NRC Regulations Title 10, Code of Federal Regulations, Part 50, Section 55a, "Codes and Standards," U.S. Nuclear Regulatory Commission.
7. IEEE Standard 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
8. NRC Regulations Title 10, Code of Federal Regulations, Part 50, Section 36, "Technical Specifications," U.S. Nuclear Regulatory Commission.
9. [ ]^{a,c,e}
10. WCAP-8587 Rev. 6-A, "Methodology for Qualifying (Westinghouse) WRD Supplied NSSS Safety Related Electrical Equipment," Westinghouse Electric Company LLC.
11. RG 1.89, Rev. 1, "Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, June 1984.
12. NRC Regulations Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Requirements for Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
13. IEEE 323-2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
14. IEEE 344-1987, "Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
15. RG 1.100, Rev. 2, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," U.S. Nuclear Regulatory Commission
16. RG 1.180, Rev. 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," U. S. Nuclear Regulatory Commission.
17. MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," U.S. Department of Defense, August 1999.
18. Electrical Power Research Institute (EPRI) Topical Report (TR) EPRI TR-102323, Rev.1, "Guidelines for Electromagnetic Interference Testing in Power Plants.
19. IEC 61000-4-3-2006, "Electromagnetic Compatibility: Testing and Measurement Techniques – Radiated, Radio-frequency, Electromagnetic Field Immunity Test," International Electrotechnical Commission.
20. Electrical Power Research Institute (EPRI) Topical Report (TR) EPRI TR-102323, Rev.3, "Guidelines for Electromagnetic Interference Testing in Power Plants.
21. IEC 61000-4-2-2009, "Electromagnetic Compatibility: Testing and Measurement Techniques – Electrostatic Discharge Immunity Test," International Electrotechnical Commission.
22. IEC 61000-6-2-1999, "Electromagnetic Compatibility: Generic Standards - Immunity for Industrial Environments," International Electrotechnical Commission.
23. IEC 61000-6-4-1997, "Electromagnetic Compatibility: Generic Standards – Emission Standard for Industrial Environments," International Electrotechnical Commission.
24. [ ]^{a,c,e}
25. RG 5.71, Rev. 3, "Cyber Security Programs for Nuclear Facilities," U. S. Nuclear Regulatory Commission.

26. RG 1.152, Rev. 3 (draft), "Criteria for use of Computers in Safety Systems of Nuclear Power Plants," U. S. Nuclear Regulatory Commission.
27. [ ]^{a,c,e}
28. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," U. S. Nuclear Regulatory Commission.
29. Wolf Creek Generating Station CFR Part 50, Appendix B audit of CS Innovations, September 10-13, 2007, Wolf Creek Nuclear Operating Corporation (WCNOC) audit report RON NO: 20205-01.
30. WES-2007-191, "Westinghouse Quality Assurance Audit Report of CS Innovations, LLC," Westinghouse Electric Company LLC, November 10, 2008.
31. NUREG 0800, Chapter 7, "Instrumentation and Controls - Overview of Review Process," U. S. Nuclear Regulatory Commission.
32. IEEE 379-2000, "Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," Institute of Electrical and Electronics Engineers.
33. IEEE 627-1980, "Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
34. RG 1.75, Rev. 3, "Criteria for Independence of Electrical Safety Systems," U. S. Nuclear Regulatory Commission.
35. IEEE 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers.
36. IEEE 338-1987, "Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers.
37. RG 1.22-1972, Rev. 0, "Periodic Testing of Protection System Actuation Functions," U. S. Nuclear Regulatory Commission.
38. RG 1.118, Rev. 3, "Periodic Testing of Electric Power and Protection Systems," U. S. Nuclear Regulatory Commission.
39. NUREG 0800, Rev. 5, Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions," U. S. Nuclear Regulatory Commission.
40. RG 1.47, Rev. 0, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," U. S. Nuclear Regulatory Commission.
41. IEEE 497-1981, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
42. IEEE 420-1982, "Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
43. IEEE 494-1974 (R1990), "Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
44. NUREG 0800, Rev. 5, Branch Technical Position 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," U. S. Nuclear Regulatory Commission.
45. IEEE 308-1980, "Standard Criteria for Class 1E Power Generating Stations," Institute of Electrical and Electronics Engineers.
46. IEEE 1023-1988, "Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and other Nuclear Facilities," Institute of Electrical and Electronics Engineers.
47. IEEE 352-1987, "Guideline for General Principles of Reliability Analysis of Nuclear Power Generating Safety Systems," Institute of Electrical and Electronics Engineers.
48. IEEE 577-1976, "Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities," Institute of Electrical and Electronics Engineers.
49. [ ]^{a,c,e}
50. RG 1.62, Rev. 0, "Manual Initiation of Protection Action," U. S. Nuclear Regulatory Commission.
51. ISA Standard S67.04 1987, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."
52. RG 1.105, Revision 3, "Instrument Setpoints for Safety Systems," U. S. Nuclear Regulatory Commission.
53. NUREG 0800, Rev. 5, Branch Technical Position 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints," U. S. Nuclear Regulatory Commission.
54. Regulatory Issue Summary 2006-17, "NRC Staff Position on the Requirements of 10 CFR 50.36, 'Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels.

55. NUREG 0800, Branch Technical Position 7-3, “Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service U. S. Nuclear Regulatory Commission.
56. IEEE/EIA Standard 12207.0-1996, “Guide for Information Technology Software Life Cycle Processes.”
57. [ ]^{a,c,e}
58. IEEE 1012-1998, “Standard for Software Verification and Validation,” Institute of Electrical and Electronics Engineers.
59. RG 1.97-1990, Rev. 2, “Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Environs Conditions During and Following an Accident,” U. S. Nuclear Regulatory Commission.
60. Interim Staff Guidance 4 - Task Working Group #4: Highly Integrated Control Rooms – Communications Issues (HICRc), 2007, U. S. Nuclear Regulatory Commission.
61. IEEE 1042 1987, “Guide to Software Configuration Management,” Institute of Electrical and Electronics Engineers.
62. IEEE 828-1990, “Standard for Software Configuration Management Plans,” Institute of Electrical and Electronics Engineers.
63. RG 1.169-1997, “Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants,” U. S. Nuclear Regulatory Commission.
64. IEEE 1540-2001, “IEEE Standard for Life Cycle Processes & Risk Management,” Institute of Electrical and Electronics Engineers.
65. EPRI TR 106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications”
66. EPRI TR 107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants”
67. Branch Technical Position 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” U. S. Nuclear Regulatory Commission.
68. Interim Staff Guidance 6 – Task Working Group #6: Digital I&C Licensing Process” (draft), 2010, U. S. Nuclear Regulatory Commission.
69. MIL-HDBK-217F (December 1974), “Military Handbook – Reliability Prediction of Electronic Equipment.”
70. USNRC Safety Evaluation Report, March 31, 2009, “Wolf Creek Generating Station – Issuance of Amendment RE: Modification of the Main Steam and Feedwater Isolation System Controls (TAC NO. MD4839),” ML# 090610317.
71. WCAP-8892-A, “Westinghouse 7300 Series Process Control System Noise Tests,” Westinghouse Electric Company LLC.
72. CENPD-255-A, Rev. 3, “Class 1E Qualification, Qualification of Class 1E Electrical Equipment.”
73. IEEE 323-1974, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers.

1 Introduction

1.1 Objective

This report describes the Advanced Logic System (ALS) platform with the intent to obtain U.S. Nuclear Regulatory Commission (NRC) review and generic approval for use of the platform in nuclear safety related instrumentation and control (I&C) applications, and to identify the bounding conditions under which this approval is to be granted.

The ALS platform is a logic based platform which does not utilize a microprocessor or software for operation, but instead relies on a simple hardware architecture. The logic is implemented using field programmable gate array (FPGA) technology. The ALS platform is nuclear safety related (Class 1E) and has been developed by CS Innovations, a 10 CFR Part 50, Appendix B (Reference 1) supplier, and wholly owned subsidiary of Westinghouse Electric Company.

It is important to note that in the ALS platform, the use of an FPGA, and CS Innovations development processes were approved by the NRC under Docket 50-482, Amendment 181 to License No. NPF-42 (Reference 2) for use in a main steam feedwater isolation system (MSFIS) application at the Wolf Creek Generating Station. The resulting safety evaluation report (SER) (Reference 70) included guidance on the use of the ALS platform in future applications. This report documents enhancements to the platform that have occurred since that approval and the enhancements are based on the guidance provided by the SER. The enhancements enable the ALS platform to be generically approved for use in a variety of Class 1E safety applications. These enhancements include incorporation of new hardware components (i.e., analog input board, analog output board, and communication board), incorporation of new features (redundant Reliable ALS Bus [RAB], new ALS Service Unit [ASU] interface, online setpoint adjustment, and external power supply), enhancements to the design process in the area of independent verification and validation (IV&V), and the use of independent design teams for the development of diverse FPGA cores.

1.2 Scope

The scope of this report is limited to the ALS platform, which consists of the following components:

- ALS-102 Core Logic Board
- ALS-302 Digital Input Board (Contact Input)
- ALS-311 Analog Input Board (RTD and Thermocouple)
- ALS-321 Analog Input Board (Voltage/Current)
- ALS-402 Digital Output Board (Contact Output)
- ALS-421 Analog Output Board (Voltage/Current)
- ALS-601 Communications Board
- ALS chassis and backplane and backpanel

The ALS platform does not include the cabinet and peripheral devices. These components may be a part of a complete ALS safety system and are discussed in Section 2.6 to the extent necessary to ensure the acceptability of the ALS platform, but are otherwise outside the scope of this report. These peripheral components include the Cabinet (which houses the ALS chassis), Control Panel, ASU, Assembly Panel (which contains application specific switches, indicators, terminal blocks, fuse holders, relays, unique/stand-alone signal processing devices, etc.) and Power Supply System (which consists of external redundant power supplies, filters, and associated distribution breakers).

The report provides a detailed discussion of the ALS platform (including hardware, communication, reliability, and FPGA development tools) and associated processes, including design, qualification, configuration management, and IV&V.

The document is organized in the following sections:

1) Section 2: ALS Technical Description – Describes the ALS platform, architecture, input boards, output boards, core logic board, communication board, internal communications, chassis and diagnostics. This section also describes the cabinet and peripheral components that are required to support the ALS platform in a typical safety system application.
2) Section 3: Diagnostics and Maintenance – Describes how the ALS platform is designed to support periodic surveillance testing, safety channel calibration and maintenance.
3) Section 4: Equipment Qualification – Describes Environmental, Seismic and Electromagnetic Compatibility (EMC) qualifications.
4) Section 5: ALS Platform Communications – Describes hardwired inputs and outputs and the ALS communication data links.
5) Section 6: Life Cycle Management Process – Describes the FPGA life cycle design process and configuration management process.
6) Section 7: Reliability – Describes the reliability of the ALS platform.
7) Section 8: Security – Describes the physical and platform security features to prevent unauthorized access and unintended functions.
8) Section 9: Diversity – Describes the ALS internal diversity strategy.
9) Section 10: Quality Assurance – Describes compliance to 10CFR50 Appendix B.
10) Section 11: Training – Describes assimilation of the ALS platform into the plant.
11) Section 12: Regulatory Compliance – Describes compliance to IEEE-603, IEEE-7-4.3.2, and Interim Staff Guidance documents.
12) Appendix A: Reactor Protection System (RPS) Application
13) Appendix B: Train Diverse Application
14) Appendix C: Dual Train Application

1.3 ALS Background

In late 2003, Wolf Creek Nuclear Generating Station had a need to replace the 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 as a general safety platform to target the U.S. Nuclear Power Plant (NPP) Safety Related I&C System market.

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

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

2 ALS Platform Technical Description

2.1 ALS Platform Overview

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

The ALS platform is designed to be at the appropriate level of complexity to achieve high reliability and integrity as well as allow enough flexibility to target multiple nuclear safety critical applications within a nuclear power plant. Redundancy and embedded self-test capability ensure integrity of the installed ALS system by detecting and announcing faults. Diagnostics and testing capabilities are designed into the ALS platform to ensure there is a systematic approach to maintaining and testing the system. A generic ALS platform is illustrated in Figure 2-1.

The ALS is a modular platform where generic modules, referred to as ALS boards, can be combined in various configurations to solve a wide variety of nuclear safety applications. This also provides scalability allowing for a single system upgrade up to a full set of safety system upgrades using the same ALS platform. An available configuration is one that implements an inherent diversity within the FPGA platform design such that the safety analysis required by BTP 7-19 (Reference 3) is normally not necessary. This feature is discussed later in this report.

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

The ALS platform supports a wide range of field input/output (IO) types, such as digital inputs, analog current and voltage inputs, resistance temperature detector (RTD) and thermocouple (TC) inputs, as well as contact and relay outputs.

The ALS chassis is an industry standard 19" chassis and can be mounted in a wide variety of existing 19" cabinets. The ALS boards are designed to a proprietary standard for size and shape of the board. Each chassis contains a number of boards which is dependent on the particular safety application as well as the type of boards that are installed into the chassis. Multiple ALS chassis can be connected together through an expansion bus if more boards are needed for a particular application (see Figure 2-1 for a typical ALS chassis populated with boards). The ALS internal bus system architecture allows for up to 60 boards to be connected in up to six different locally connected chassis (one main chassis and 5 Expansion Chassis connected within the same cabinet).

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

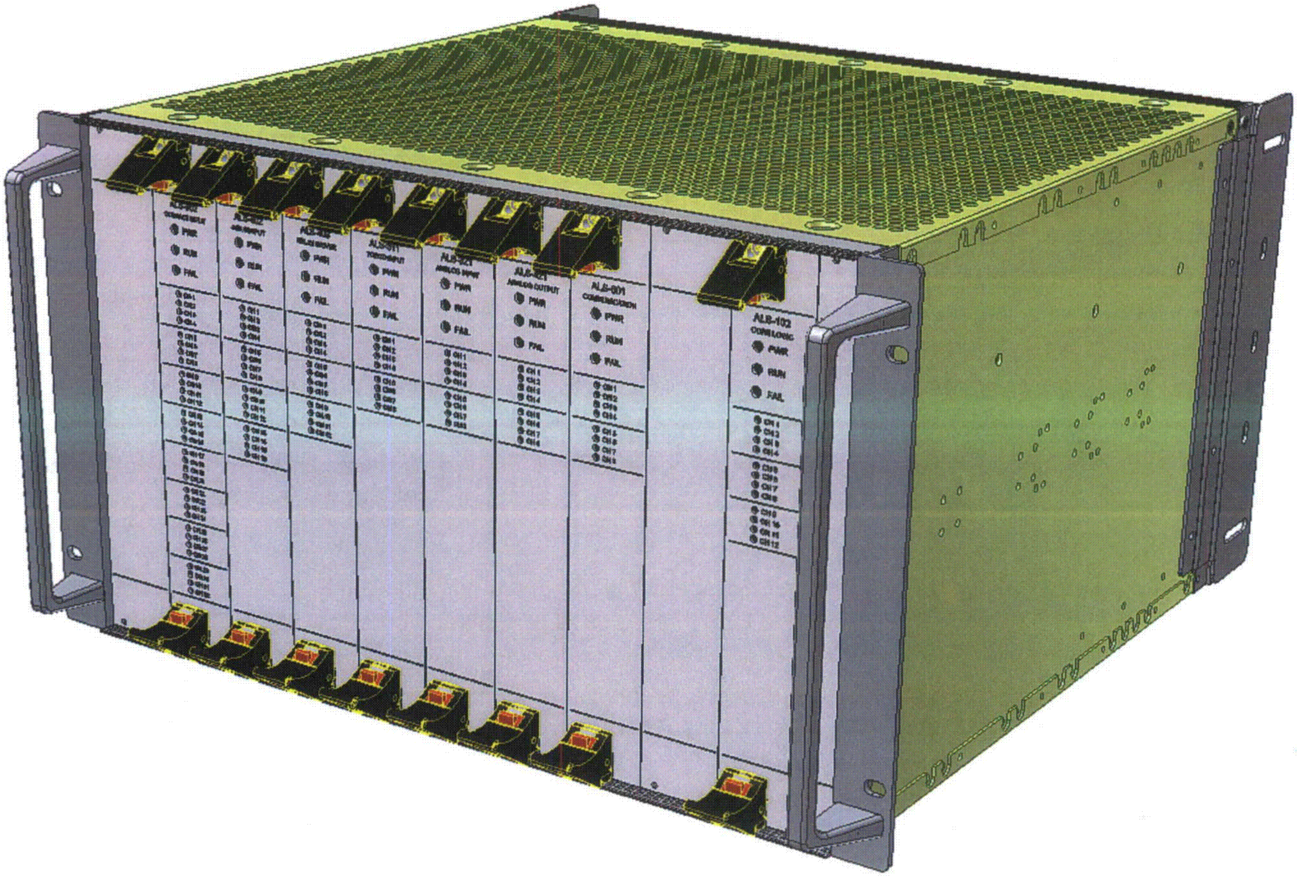

Figure 2-1: ALS Chassis Populated with Eight Boards

2.1.1 ALS Boards

The ALS platform is based on a combination of generic ALS boards, which allow for predefined configuration settings, and dedicated ALS boards, where the field programmable gate array (FPGA) logic is configured for a specific application. Examples of such ALS boards are listed in the Table 2-1: ALS Board Types.

Table 2-1: ALS Board Types

Type	Description	Acronym	Board Nomenclature	Use
ALS-1xx	Core Logic Board	CLB	ALS-102	Performs application specific safety functions and controls the primary system functions.
ALS-3xx	Input Boards	IPB	ALS-302 ALS-311 ALS-321	Perform signal conditioning, sensing and filtering of field input signals.
ALS-4xx	Output Boards	OPB	ALS-402 ALS-421	Responsible for controlling and conditioning of field output signals.
ALS-6xx	Communications Board	COM	ALS-601	Provides secure communication links to external systems.

The ALS platform includes a number of ALS boards capable of performing different but very specific safety critical functions. All ALS boards are identified by a three digit ALS number where the first digit defines the board type and they have all been defined in the previous table.

Figure 2-2 is an illustration of a generic ALS platform architecture and the base architecture showing the relationship between input boards, logic boards, output boards and communication boards. The actual number and type of boards will depend on the specific application configured.

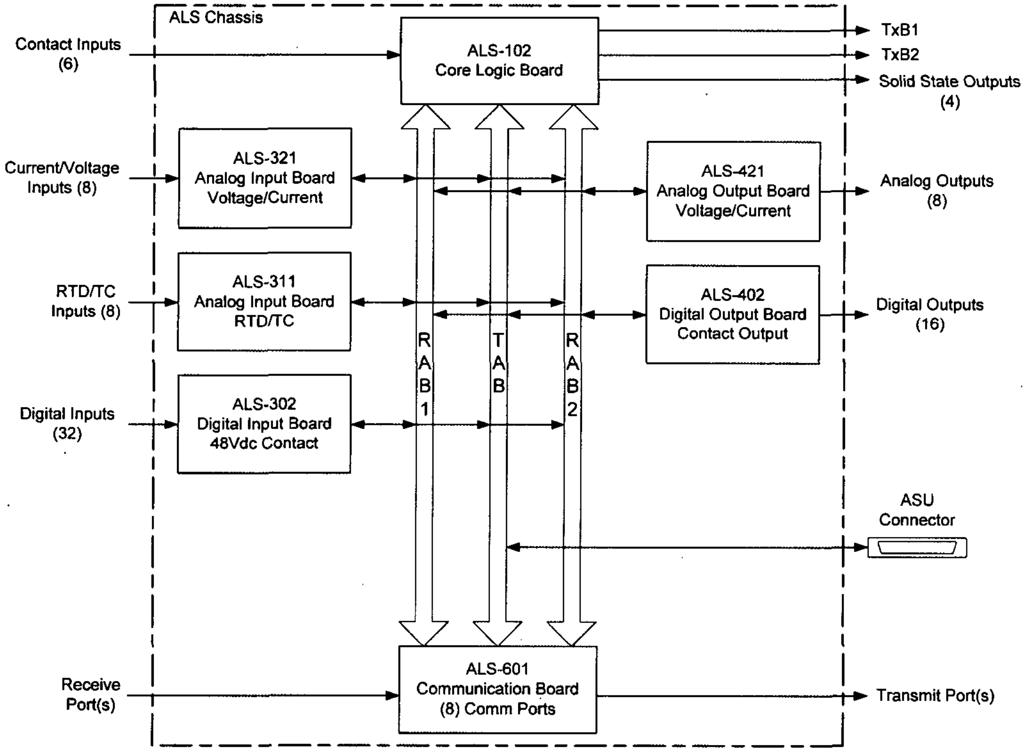
ALS Chassis
Contact Inputs (6)
ALS-102 Core Logic Board
TxB1
TxB2
Solid State Outputs (4)
Current/Voltage Inputs (8)
ALS-321 Analog Input Board Voltage/Current
ALS-421 Analog Output Board Voltage/Current
Analog Outputs (8)
RTD/TC Inputs (8)
ALS-311 Analog Input Board RTD/TC
ALS-402 Digital Output Board Contact Output
Digital Outputs (16)
Digital Inputs (32)
ALS-302 Digital Input Board 48Vdc Contact
RAB1
TAB
RAB2
ASU Connector
Receive Port(s)
ALS-601 Communication Board (8) Comm Ports
Transmit Port(s)

Figure 2-2: Generic ALS Platform Architecture Overview

2.1.2 Generic ALS Core Logic Boards (ALS-1xx)

The Core Logic Board (CLB) contains all the application specific logic circuits, which define and control the operation of a given system. The core logic board 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.

A part of the FPGA logic in the CLB is customizable based on the requirements of a given application, and is customized for each customer and for each application. The overall functionality of the desired system is specified by the customers, and from this specification CS Innovations creates an application specific logic specification describing the detailed functionality of the CLB.

The application specific logic can contain any type of digital building blocks which can be generated from a 2-input NAND-gate, 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 phrase 'Core Logic Board' or 'CLB' is used throughout this report to identify the main board that performs the dedicated application specific functions. Currently, the only CLB type board available in the ALS platform is the ALS-102.

The CLB, such as the ALS-102 board is based on a generic ALS board, that is configured with application specific logic, i.e., the FPGA is configured with application specific logic to make the system (e.g., a process protection system or a sequencer system). The application specific logic is implemented in the FPGA and is typically small (less than 5K gates [2-input NAND-gate equivalent] for simple applications such as sequencers or mainstream feed water isolation systems), but is significantly more complex in the event of analog and temperature calculations.

The core logic boards typically have a set of locally connected I/Os such as dedicated inputs, outputs or communication channels. These dedicated I/Os are deployed for tightly coupled system functions, such as system reset (clear alarm) inputs or alarm indication outputs.

2.1.3 Generic ALS Input Boards (ALS-3xx)

Input Boards are standard boards responsible for sensor sampling, signal conditioning, filtering and performing analog-to-digital conversion (ADC) of field input signals. Input Boards are typically dedicated to a specific input type, such as digital 24V or 48V contact sensing, 4-20mA analog inputs, 0-10V analog inputs, RTD inputs, or TC inputs.

The input channels on the ALS Input Boards are based on solid-state devices. The input channels include self-test capability which continuously verifies vital components within the channel are operational. During self-test, vital components in the channel are tested to ensure full safety functionally. High isolation between the channels and the ALS logic is maintained by utilizing galvanic isolators. Depending on the board type, the channels may be individually isolated or located on a common isolation domain. The input channels are protected against electrostatic discharge (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.

The Input Boards provide front panel light-emitting diode (LED) indicators which show the status of a particular input signal. The ALS design allows for both generic Input Board front-panels as well as customized front panels where each channel LED is marked with a descriptive text such as sensor tag number.

An ALS chassis may require multiple Input Boards to support a particular application. The number of Input Boards in the ALS chassis is related to the number of channels and/or the type of field inputs required. A particular Input Board 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.

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 partially located in the channel section and partially in the FPGA logic, and performs all channel control, sample & hold, integrity checks, self-testing, and digital filtering functions. All digital channel circuits, bus communication, and channel integrity are implemented with redundant logic within the FPGA. The redundancy and self test circuits ensure 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 more than 1500Vrms.

2.1.4 Generic ALS Output Boards (ALS-4xx)

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

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

The Output Boards provide a front panel LED indicators which show the status of a particular output. The ALS design allows for both generic Output Board front-panel indications as well as customized front panel indications by mapping the LED indication to application specific field outputs.

An ALS chassis may require multiple Output Boards to support a particular application. The number of Output Boards in the ALS chassis is related to the number of outputs and/or the type of field devices interfacing with the ALS chassis. A particular Output Board 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 field effect transistor (FET) driver channel with feedback measuring and test circuitry to ensure channel integrity.

An output channel consists of two key circuits – a digital circuit and an 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., converting to an analog voltage, switching a relay or solid-state-contact or a high-power FET transistor). The analog circuit performs 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, bus communication, and channel integrity are implemented with redundant logic within the FPGA. The redundancy ensures, in the event of a gate failure, the failure is detected and the board is isolated from the rest of the ALS chassis.

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

All output boards have galvanic isolation between the channels and the ALS logic, and can withstand a minimum of 1500Vrms. Depending on the board type, the output boards can have individually isolated channels, or they can be located on a common isolation domain.

Digital output channels can be configured to drive its output to a predefined state in case of board failures or lack of communication with the CLB. The predefined states are determined during the system level design of a given application. These predefined states are Open, Closed or As Is.

2.1.5 Common Components/Design

All FPGA based ALS boards have been designed similarly and, with the exception of the channel circuit, have identically designed circuits. This section specifies the design of these common circuits and will be referenced from the individual ALS board's design specification.

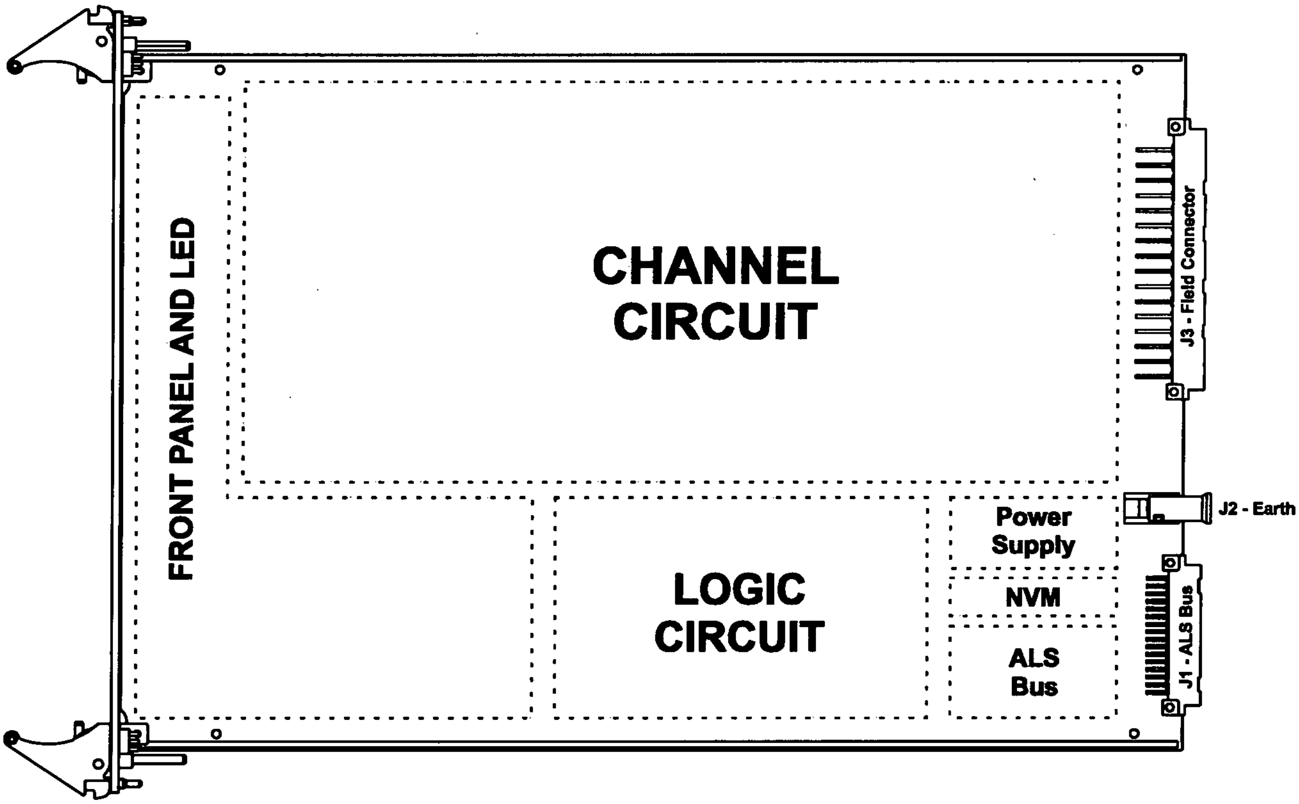

Figure 2-3: Generic ALS Board

Figure 2-3 shows a generic standard layout of an ALS board. The layout of the typical ALS circuit board consists of the following major circuit groups:

- **Logic Circuit** – includes the FPGA device and the local oscillator
- **Non Volatile Memory** (NVM) – includes the NVM device used for storing configuration information
- **Power Supply** – includes power supplies and under voltage detection circuits
- **ALS Bus** – includes the physical hardware drivers used to for communication between boards
- **Front Panel and LED** – includes the front panel LED indicators and the associated mechanical parts
- **Back Panel Connectors** – includes the connection points to mate a ALS board with the back plane in the ALS chassis

Circuits, which vary between board types:

- **Channel Circuit** – includes all analog, digital, protection and isolation circuits used in the I/O channels

Component reuse and circuit design reuse is a key aspect of the efficiency of the ALS platform design. This improves long-term reliability and maintainability, but also gives the ALS boards a common look and feel. Generally, ALS board designs utilize the following standard components: FPGA device, oscillator, NVM, EIA-485 bus communication drivers, connectors, power supplies and regulators, surge suppression devices, as well as the mechanical components.

2.1.5.1 Logic Circuits / FPGA

The central component in the logic circuit is the FPGA. The FPGA used is flash based. The FPGA handles all control, communications, test and integrity activities. The control function varies between board types. Input boards provide input channel control circuits, output boards have output channels, and the core logic boards provide the application specific control logic circuits, as described in Section 2.1.1.

[

]a,c,e

FPGA circuits are implemented using modern style design methodologies, based on a solid design process, using only simple, yet highly reliable design techniques, [ ]a,c,e , exhaustive testing using advanced test environments, and independent verification and validation by experienced independent teams.

2.1.5.2 Non-Volatile Memory Device

The ALS Boards have a dedicated NVM memory device to store application specific SetPoints. The SetPoint configuration is stored in an external NVM. The NVM [ ]a,c,e device with a +60 year retention time. Table 2-2: NVM Content outlines the general content of the NVM, the typical type of content, as well as the possibility of changing the information online for an operational application.

Table 2-2: NVM Content

NVM Information Type	Description	Online Update
Board Information	Board serial-number, part-number, revision number, etc	Not Possible
Configuration information	Channel Configuration (such as filter time, NO/NC contacts, channel enable/disable, FailSafe settings, etc.)	Not possible
Calibration Information	Channel Calibration Coefficients (ALS-3xx and ALS-4xx) Set Point and Trip Values (ALS-1xx)	YES
Channel Control	Bypass, Override, and Calibration Control registers	YES

Board information is used for maintenance purposes only. [ ]a,c,e Board information can be retrieved when necessary.

Configuration information 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 such as keyed connectors to ensure that an incorrectly configured I/O board will not cause an unintended plant event if inserted into a chassis.

Calibration information is mainly used for analog boards with a need for configurable tables to perform the conversion from resistance to temperature, or from a voltage measured on a certain thermocouple to a temperature. Further, the same calibration information is used to store trip values or table values needed on a core logic board.

Channel control information is stored within the NVM, and is used to control the operation of the FPGA to prevent access to certain features.

2.1.5.3 Power Supply

ALS boards are designed with local voltage regulators and monitors to ensure stable and reliable local board voltages. The boards are designed to accept a redundant pair of 48V power feeds to power its internal circuits. The 48V feeds are diode auctioneered and fuse protected and down converted on the ALS board to the voltage domains needed for its logic circuitry. The ALS board uses +3.3V as its general logic supply and +1.5V for the FPGA core supply. The ALS board is equipped with two voltage supervisors used to reset the FPGA logic. The voltage supervisors monitor the +3.3V and +1.5V domains to ensure voltages level are adequate for reliable operation of the FPGA logic and channel circuits.

2.1.5.4 ALS Bus

The ALS bus circuits are the physical layer that implements the Reliable ALS Bus (RAB) and Test ALS bus (TAB) communication. The busses are described in detail in Section 2.3.

2.1.5.5 Front Panel and LED

The LEDs are used for indicating the board and channel status as discussed in [ ]^{a,c,e} The front panel circuit is used to detect the state of the front panel latches. When both latches are open the board will be OFF.

2.1.5.6 Back Panel Connectors

ALS boards presently have 3 back panel connectors. J1 connects the ALS board to other ALS boards and provides power to the ALS board. J2 is a low impedance connection to earth ground used for electromagnetic interference/radio frequency interference (EMI/RFI) and surge purposes. J3 connects the ALS board to other field cabling through the back panel. Connection usage could vary from this in future designs.

2.1.5.7 Channel Circuits

The channel circuit is board dependent. Section 2.2 describes the channel circuits in detail.

2.2 Standard ALS Boards

This section provides a general description of the ALS boards.

2.2.1 ALS-102 Core Logic Board

The ALS-102 is a versatile high-reliability, high-integrity, and highly-integrated design that is typically referred to as the Core Logic Board (CLB) (see Figure 2-4).

The CLB 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 2-input NAND-gate, such as AND/OR/XOR-gates, Flip Flops (D, JK, SR), etc. These building blocks can then be combined into more complex logic circuits such as counters, timers, multiplexers, comparators, lead/lag functions, or FSMs.

The application specific logic within the CLB would normally contain circuits to perform safety functions, such as:

- **Thermocouple/Core Cooling Monitoring system (TC/CCM)**: logic to calculate average temperature, quadrant temperature, T_{SAT}, etc.
- **Diesel Sequencer**: The counter and comparator circuit that makeup the sequencer function.
- **Voter / Solid State Protection System (SSPS)**: The 2-out-of-4 voter circuits.
- **Process Protection System**: decision circuits, which compare pressure, temperature, level and flow measurements with their respective trip-value-SetPoints to generate a trip, T_{AVG} calculations, etc.

The ALS-102 CLB performs all of the application specific algorithms and/or logic functions which define and control the operation of a given safety related system. The CLB controls all sequencing within the ALS system. The CLB issues requests to the input boards to provide field input information as required, executes the application specific algorithm and/or logic functions, and commands the output boards to drive a specific output state to the field devices.

The Core Logic Board has a dedicated NVM device to store application specific SetPoints used by the design, such as comparator setpoints, tuning constants, gain, offset, etc. The end user can only adjust parameters allowed by the design. The algorithm and/or control logic is deterministic in execution and cannot be changed. Examples of such configuration SetPoints located in the ALS-102 NVM are: sequencer delays, time constants and trigger-points.

The ALS-102 CLB also has the capability to accommodate 6 contact input channels, 4 solid-state output channels and 2 transmit-only EIA-422 communication channels. All input, output and communication channels are isolated from the ALS logic and can withstand 1500Vrms.

The ALS-102 board is the only board in the ALS platform portfolio that is customized for every new application. The logic core is customized to perform the desired safety function, such as a sequencer function, coincidence logic voter function, process protection function, or whichever function is required per the customer's system requirements. The board will, for each application, be implemented following the CS Innovations development process under the 10CFR50 Appendix B program.

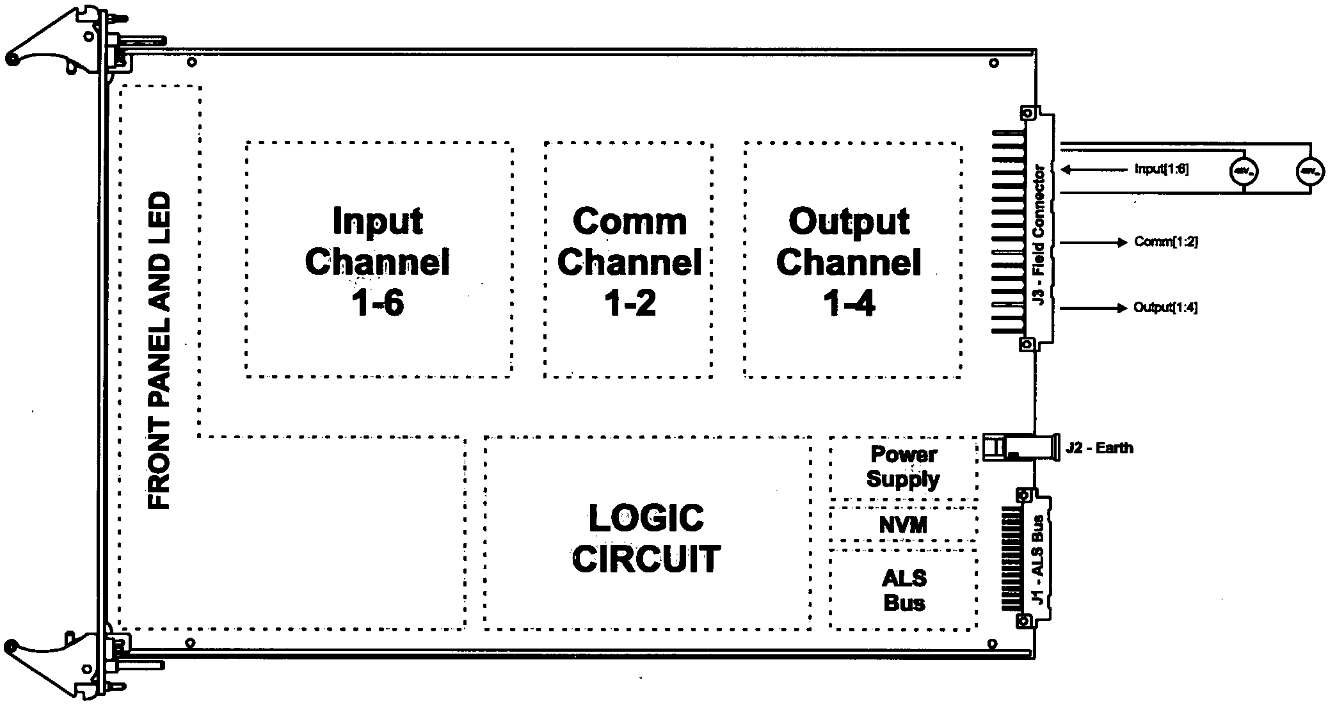

Figure 2-4: ALS-102 with 6 Input Channels, 2 Comm Channels and 4 Output Channels

2.2.1.1 ALS-102 Input Channels

The contact input channels are intended to be used for system related inputs. Examples of such inputs are:

1) Toggle switch for acknowledging and/or clearing Alarms
2) Detecting the state of maintenance key switch, i.e., COMM keyswitch
3) Door Alarm

4) Power Supply Health
5) Function Bypass Toggle Switches

2.2.1.2 ALS-102 Output Channels

The four output channels are single pole de-energize to actuate type outputs. These output channels are typically used for alarm, trouble or status indication. Internal dedicated and independent alarm circuits control and generate alarm output signals based on operability and integrity of the system.

The output channels are implemented with redundant and failsafe logic which ensure that all credible logic and board failures will cause the output channels to open.

2.2.1.3 ALS-102 Communication Channels

The two unidirectional (transmit only) communication channels (TxB1 and TxB2) on the ALS-102, [ ]^{a,c,e}. These channels can be used to send internal state and diagnostics data from the ALS chassis to local or remote safety equipment. For example, in a typical safety system application, one channel on the ALS-102 CLB will continuously transmit data to the ALS Service Unit (ASU) via one of the communication channels bus. The data stream includes information such as contact input/output states, analog input/output states, internal state (including counter values, analog computed values, etc.), board and system integrity, and application specific operational data. The second channel may, in the same application, continuously transmit data to a Qualified Display System (QDS) mounted on a main control board, or to a non-safety system(s) (such as the plant computer), as required by the specific application. The exact data content will be specified in the application specific logic specification for the particular application.

The dedicated communication channels on the ALS-102 board have the following characteristics:

- Independent, dedicated, serial, uni-directional (no handshake) EIA-422 communication channels.
- Simple universal asynchronous receiver transmitter (UART) based (proprietary) protocol with standard baud rates.
- The 2 communication links are typically used for sending state information to a local display unit (the ASU) and sending information to a remote plant computer / data logger.
- The content transmitted on the 2 communication channels is application specific. Typical information includes application/system level type information, such as temperature measurements, calculated T_{AVG} temperatures, pressure measurements, contact state information, health and integrity information etc.

2.2.2 ALS-302 Digital Input Board (48Vdc contact inputs)

The ALS-302 board is a versatile high-reliability, high-integrity, optically-isolated 32-channel contact input board (see Figure 2-5).

The board provides simultaneous monitoring of 32 independent field contacts. All inputs are galvanic isolated from the ALS logic, and are further divided into two galvanic isolation groups with high isolation between the groups.

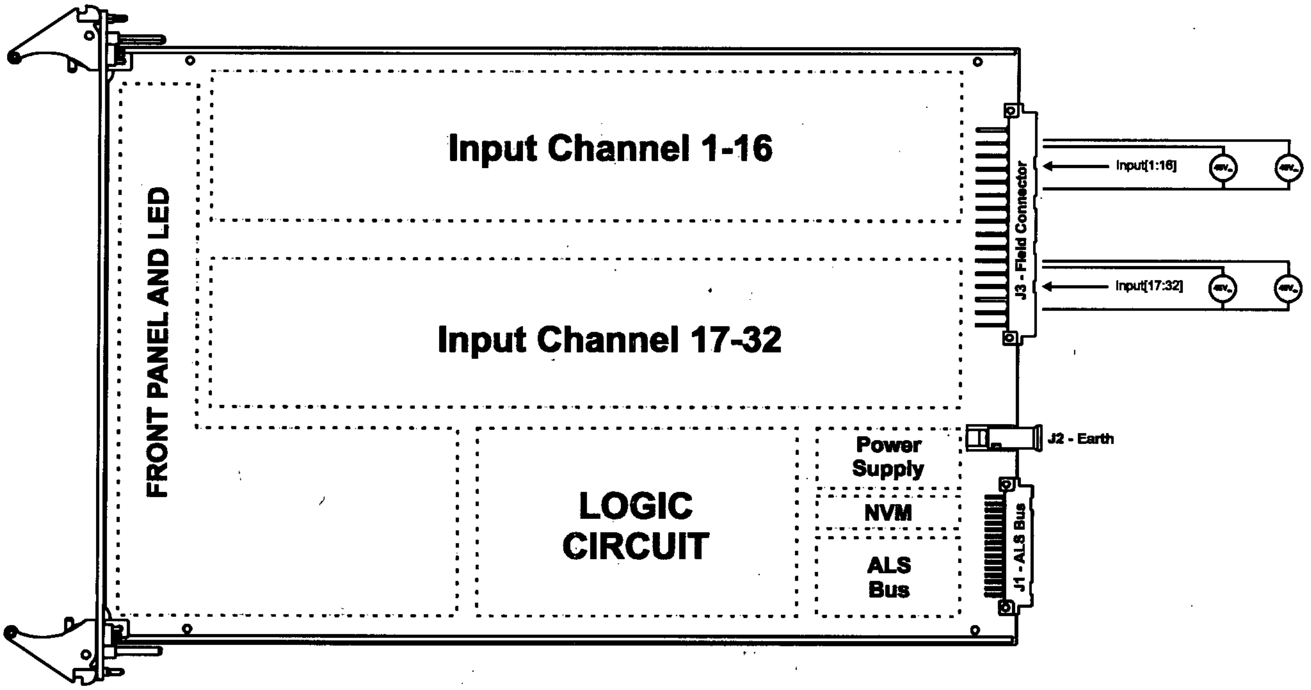

Figure 2-5: ALS-302 with 32 Input Channels

The target application for the board is remote contact sensing of discrete field contacts, and the board may be used over a wide range of application apparatus with different channel and wiring configurations.

The function of the ALS-302 board is to detect the state (open/closed) of a remote set of contacts and make the state information available on the RAB bus interface. The state information detected also includes integrity information indicating the integrity status of the channels. The state of the remote contacts is detected by wetting the contacts and attempting to drive a current through them. Each input channel contains an analog surge suppression circuit and an analog filter circuit implemented discretely, as well as a digital filter and sample-and-hold circuit implemented within the FPGA. The channel information detected is communicated onto the RAB, where upon request, it can be provided to the ALS-102 Core Logic Board.

The ALS-302 has self-test capabilities to ensure detection of single-point (and most multi-point) failures in the channels, the FPGA logic circuits, the configuration NVM and power management logic. The input channels employ automated internal self-test circuits to validate the integrity of each channel [ ]^{a,c,e}.

2.2.2.1 Channel Configuration Options

The following parameters can be configured for each individual channel:

- ENABLED or DISABLED.
- Normally Open (NO) or Normally Closed (NC).
- Channel response time (depending on the filtering required).

2.2.3 ALS-311 Analog Input Board (RTD/Thermocouple)

The ALS-311 is a high-integrity, 8-channel temperature sensor board used in the ALS platform (see Figure 2-6). Each temperature channel can be individually configured for 3-wire RTD, 4-wire RTD, or TC operation.

The ALS-311 is presently compatible with the following temperature sensor types:

RTDs: Pt100, Pt200.
Thermocouples: J, K, N, E, T, R, S.

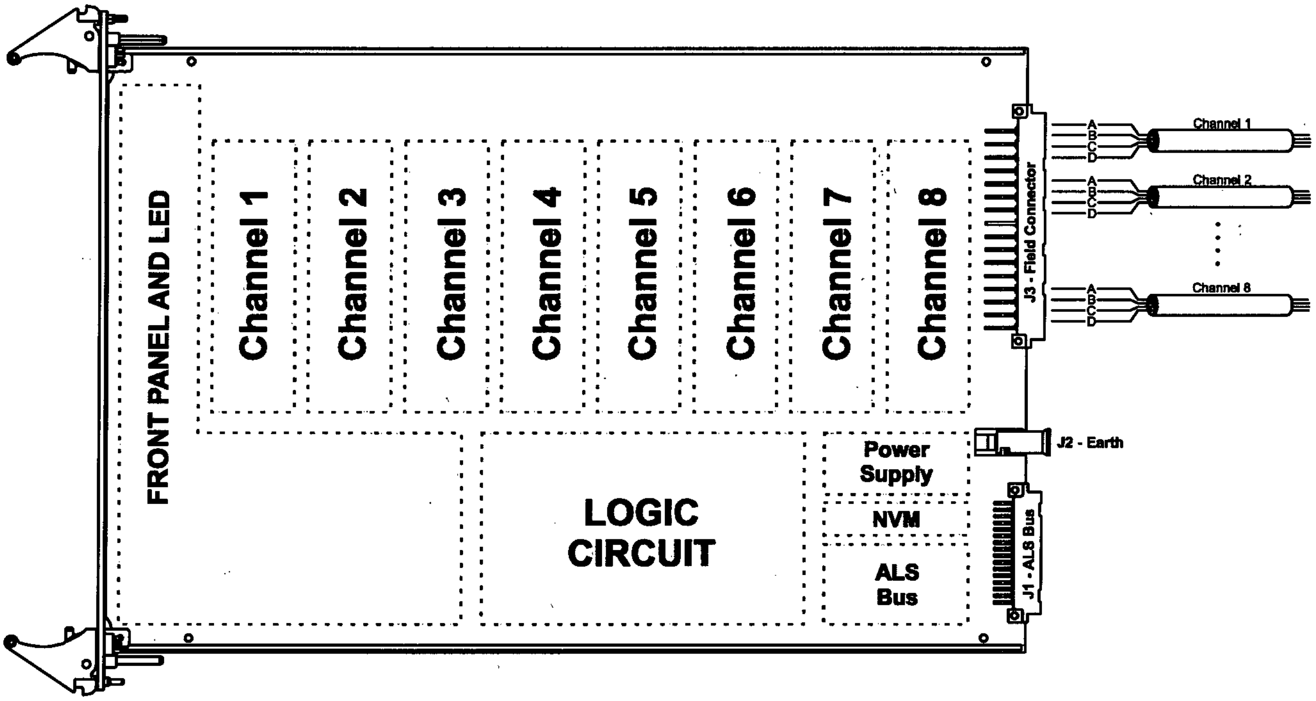

Figure 2-6: ALS-311 with 8 Channels Split Into Individually Isolated Blocks

Each of the 8 channels on the ALS-311 board can be configured as illustrated in Figure 2-7.

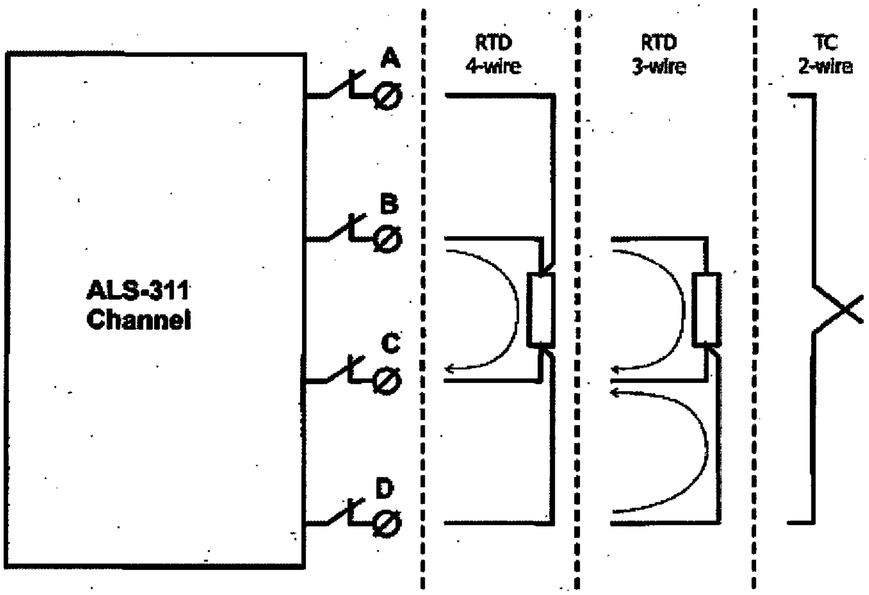

Figure 2-7: ALS-311 Board Configurations

The temperature inputs are converted into digital values representing the temperatures and are made available on the RAB bus together with integrity information for each channel. The board senses voltage (for thermocouples) or impedance (for RTDs) and uses an analog-to-digital converter and linearization constants specific to the type of thermocouple or RTD configuration to convert the raw sensor data into highly accurate digital temperature readings. The information is made available on the RAB bus, where upon request, it can be provided to the ALS Core Logic Board.

The ALS-311 may be used over a wide range of applications with different channel and wiring configurations.

The ALS-311 supports automatic cold junction compensation (CJC) of thermocouple sensors using a common cold junction temperature (CJT). The CJT is written to the ALS-311 by the CLB and can originate from another RTD channel on the board itself, from a RTD on another ALS-311, or from a combination of multiple temperature inputs. If needed by the application it is possible to implement complex CJT selection criteria in the CLB, such as voting and/or averaging between multiple RTD inputs.

[

]a,c,e

2.2.3.1 Channel Configuration Options

The following parameters can be configured for each individual channels:

- Each channel can be ENABLED or DISABLED. .
- Configurable channel type: 2-wire TC, 3-wire RTD, 4-wire RTD
- Linearization parameters used by TC or RTD channels
- Refresh Rate

2.2.4 ALS-321 Analog Input Board (Voltage/Current)

The ALS-321 is a high-integrity, 8-channel analog input board used in the ALS platform (see Figure 2-8). Each input channel can be individually configured for voltage or current input operation.

The ALS-321 channels can operate in the following standard modes:

- Current mode: [4 to 20mA], [0 to 20mA], [10 to 50mA] or [0 to 50mA]
- Voltage mode: [0 to 5V], [-5 to +5V], [0 to 10V], or [-10 to +10V]

Process instrument loop power is provided by external loop power supplies from a cabinet-mounted or remote power-supply. The board may be used over a wide range of applications with different channel and wiring configurations.

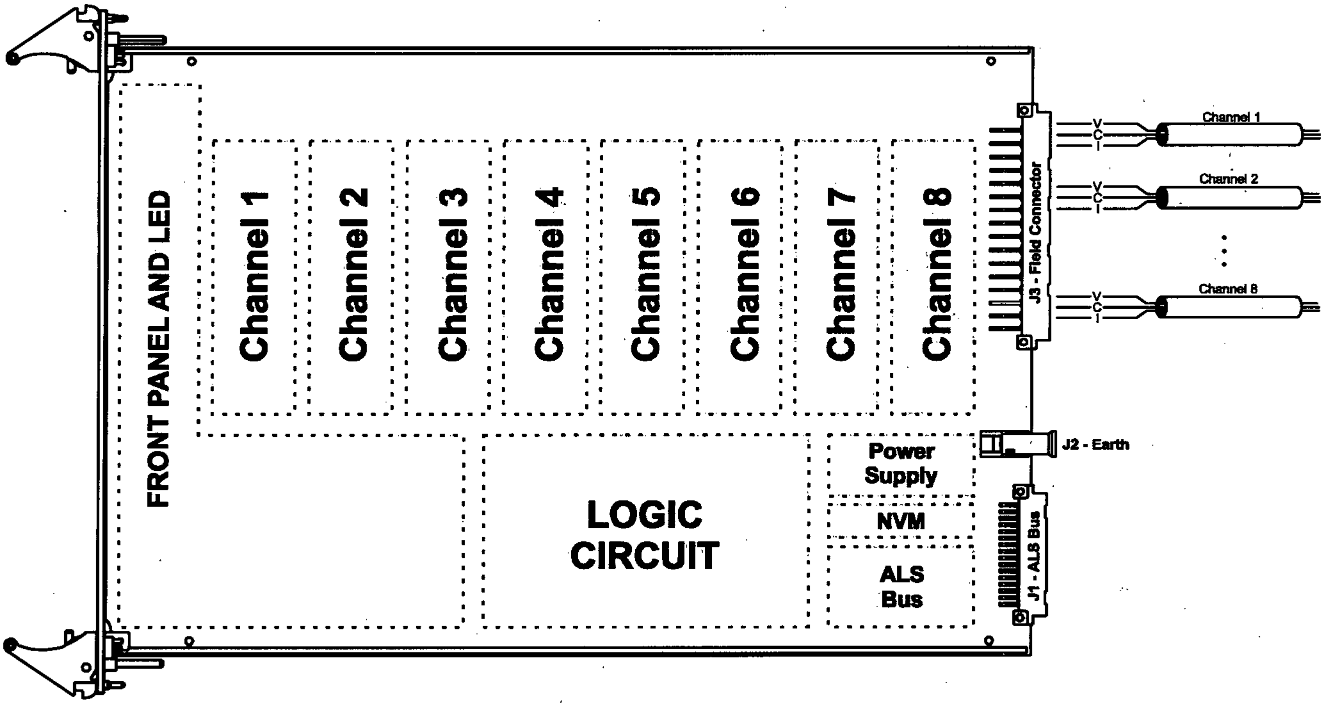

Figure 2-8: ALS-321 with 8 Channels Split Into Individually Isolated Blocks

Each of the 8 channels on the ALS-321 board can be configured as shown in Figure 2-9.

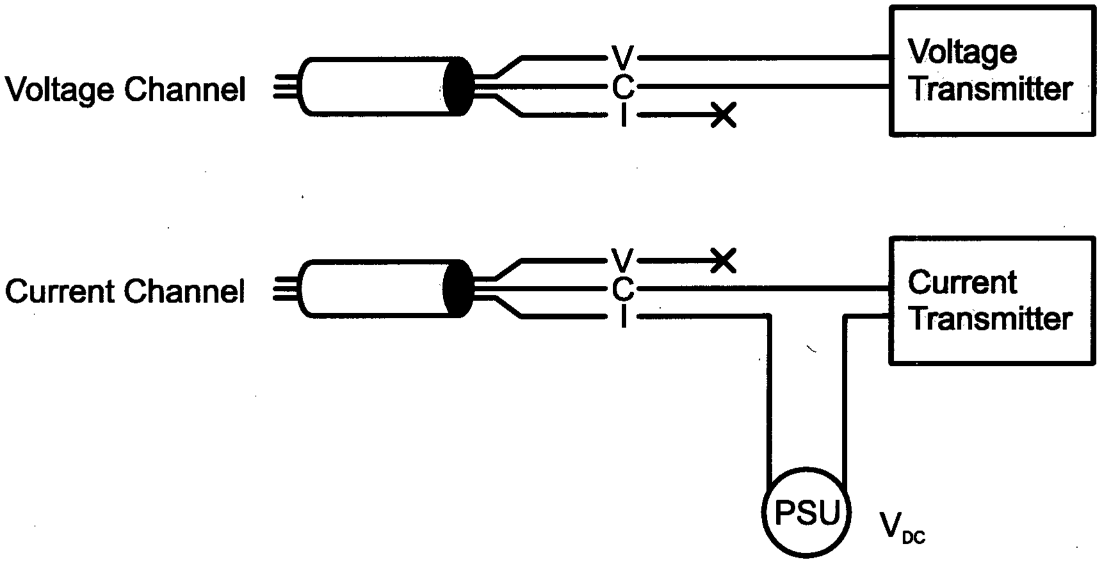

Figure 2-9: ALS-321 Board Configurations

The analog inputs are converted into digital values representing the current or voltage level and are made available on the RAB together with integrity information for each channel. This board senses voltage from an external voltage source/transmitter or current from an externally wetted and controlled current source/transmitter, and uses an analog-to-digital converter to convert the raw sensor data into highly accurate digital readings. The information is made available on the RAB, where it is provided to the Core Logic Board upon request.

[

]^{a,c,e}

All channels are surge protected and have an analog low pass filtering circuit.

[

]^{a,c,e}

The ALS-321 includes 8 independently isolated analog input channels. The characteristics of the individual channels are:

- Each channel can be configured to be either voltage or current mode
- A failure in one channel will not affect other channels
- The calibration of one channel will not affect other channels
- Each channel is independently (and individually) calibrated.
- Each channel supports out-of-range detection, as well as automatic recovery from an overload condition
- Each channel performs a self-test to ensure integrity

2.2.4.1 Channel Configuration Options

The following parameters can be configured for each individual channel:

- Each channel can be ENABLED or DISABLED.
- Channel mode: Voltage or Current w/Internal Dropping, Current w/External Dropping.
- Channel range: [4 to 20mA], [0 to 20mA], [0 to 10V], etc.
- Out-of-Range Limits
- Refresh Rate

2.2.5 ALS-402 Digital Output Board (Contact Output)

The ALS-402 board is a versatile high-reliability, high-integrity, 16-channel optically-isolated solid state output board which utilizes solid-state relays (SSR) to open and close contacts on the field-side (see Figure 2-10). Each channel can switch AC or DC signals up to 150V and 1A maximum voltage and current levels.

Output channels are isolated from the ALS logic domain with optical-isolators capable of withstanding at least 1500V (RMS). Furthermore, all 16 output channels are individually isolated and are divided into 2 groups of 8 channels with isolation.

The target application for the board is contact switching to drive/control both resistive and low inductive field loads at low-to-medium power levels, using standard typical/nominal voltages of 24Vdc, 48Vdc, 125Vdc or 120Vac, with continuous currents up to 1A, from sources outside the ALS. Further, the board is also intended to provide the ALS platform with dry-contact capability with generic use. The board may be used over a wide range of applications with different channel and wiring configurations.

Each of the ALS-402 output channels acts as a single pole single throw (SPST) contact capable of switching up to 125Vdc or 120Vac with a 1 Amp load current. Each channel is individually isolated to 300Vrms. The channels are furthermore located in two groups of 8 channels with 1500Vrms isolation between the two banks.

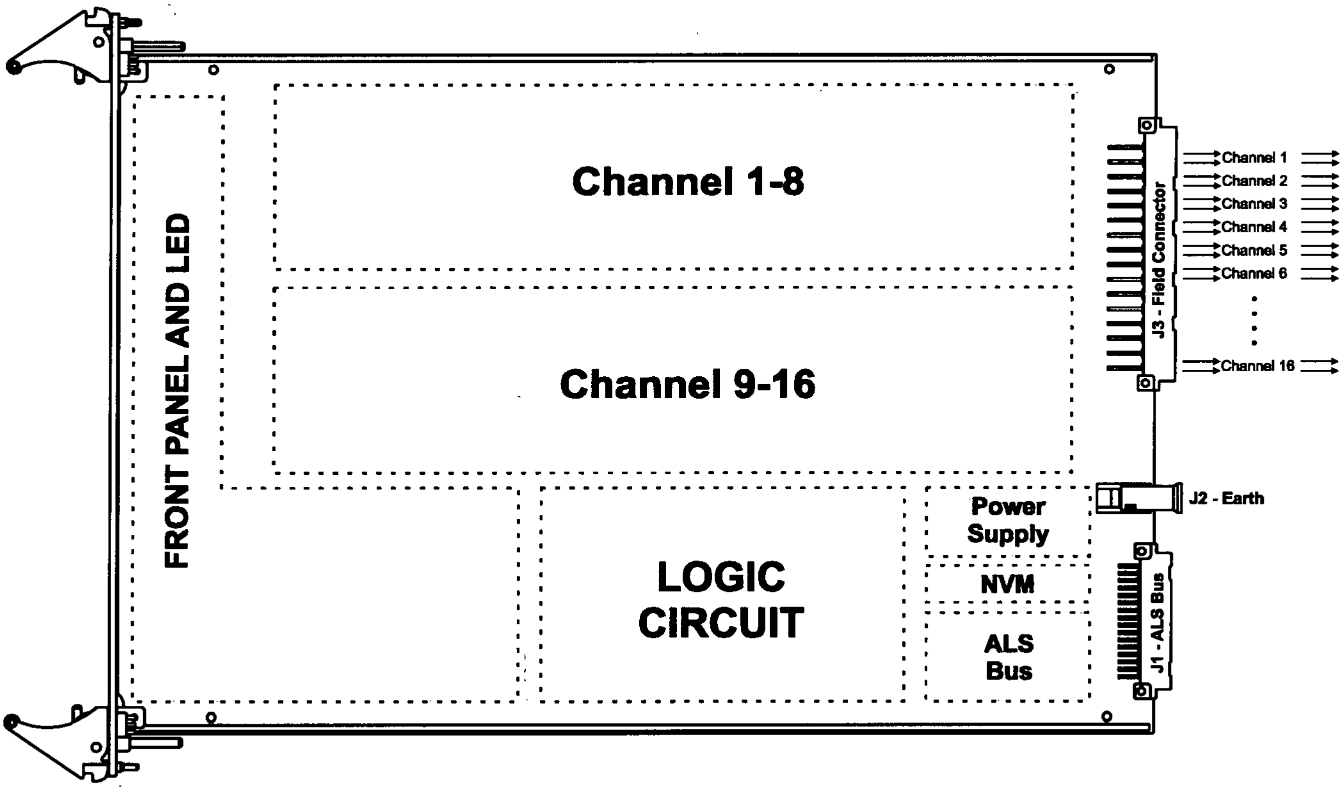

Figure 2-10: ALS-402 with 16 Contacts Split Into 2 Groups with Reinforced Isolation

An ALS-402 conducts self testing to ensure channel output integrity. [

]^{a,c,e} The ALS-402 channels also include field continuity testing allowing the channel to detect continuity in the field wiring on a de-energized contact.

This integrity data is fed back to the Core Logic Board embedded in the RAB response packets. Figure 2-11 illustrates a single ALS-402 channel with the FPGA controlling the state of the contact through an isolation barrier. The feedback from the channel control signal are used by the FPGA to verity that the drive signal arrived in the channel, the continuity detection feedback provides a feedback from the field side of the channel to verify continuity to the load and power supply when the contact is de-energized.

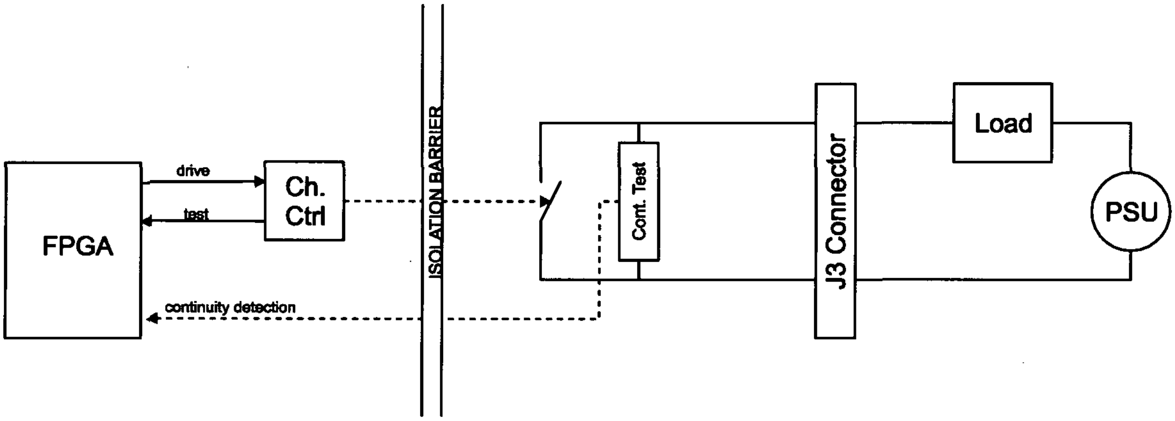

Figure 2-11: Illustration of ALS-402 Channel Design and Use

The primary mission of the ALS-402 board is to receive RAB request packets with channel output state information, and to then use this information to control the SSR output channel states (either OPEN or CLOSED). The secondary mission is to provide integrity information on RAB response packets back to the master to indicate if the integrity of the channels has been compromised.

The board includes self-test capabilities to ensure detection of single-point (and most multi-point) failures in the channels, the FPGA logic circuits, the Configuration NVM, and power management logic. Each channel performs a self-test to ensure integrity and failure in one channel will not affect other channels.

2.2.5.1 Channel Configuration Options

The following parameters can be configured for each individual channel:

- Channel Enable
- Continuity Test Enable
- Channel Bypass Enable (allow bypass)
- Channel Override Enable (allow override)

2.2.6 Deleted

Figure 2-12: Deleted

2.2.7 ALS-421 Analog Output Board

The ALS-421 is a high-integrity, 8-channel analog output board used in the ALS platform (see Figure 2-13). Each output channel can be individually configured for voltage or current output operation.

The ALS-421 channels can operate in the following standard modes:

- Current mode: [4 to 20mA] or [0 to 20mA].
- Voltage mode: [0 to 5V], [0 to 10V], [-5 to 5V] or [-10 to 10V].

The ALS-421 channels receive the digital channel value and state information from the Core Logic Board via the RAB bus. The channel performs the digital-to-analog conversion and drives the output channel to the specified voltage or current (depending on the configuration).

The 8 channels are wetted from an isolated on-board power supply capable of withstanding 1500Vrms. The 8 output channels are independent, but located on a common isolation domain.

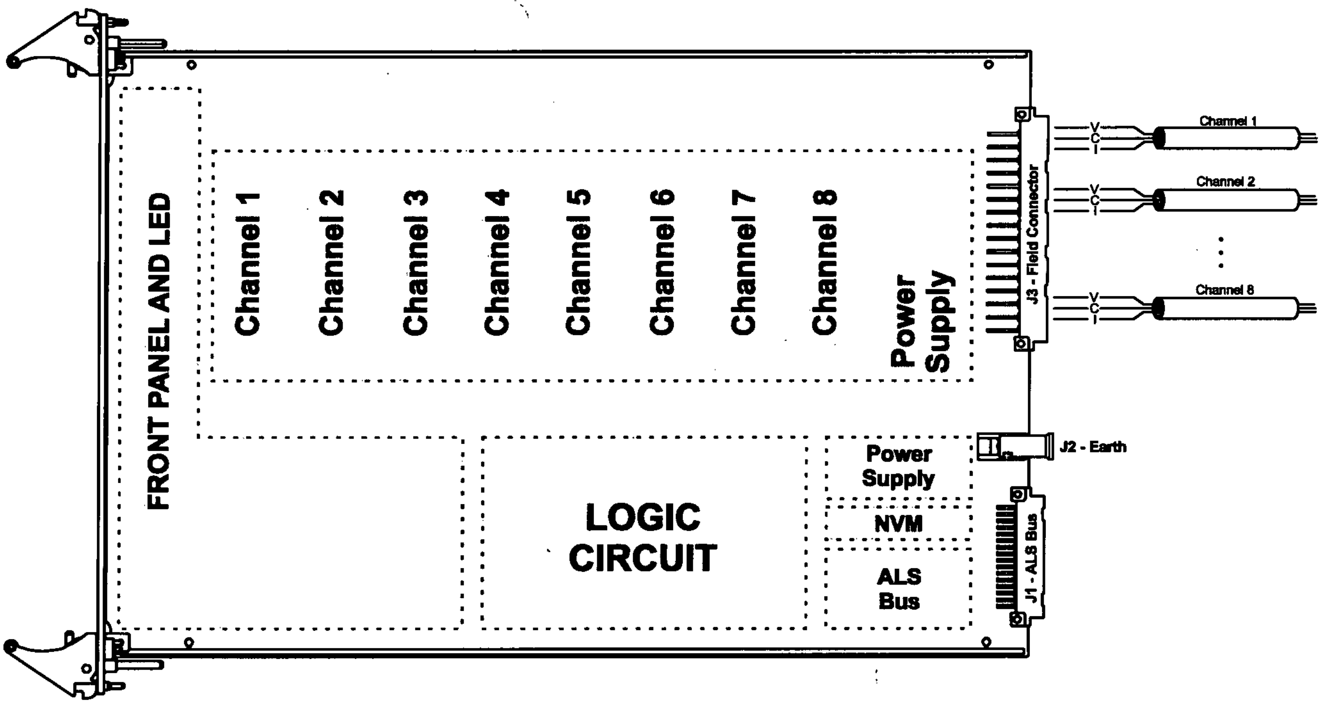

Figure 2-13: ALS-421 8 Channel Analog Output Board

The board may be used over a wide range of applications with different channel and wiring configurations.

[

]^{a,c,e}

All channels are surge protected, short circuit protected and over-voltage protected to prevent permanent damage.

[

]^{a,c,e}

The ALS-421 includes 8 independent analog output channels. The characteristics of the individual channels are:

- Each channel can be configured to be either voltage or current mode
- A failure in one channel will not affect other channels
- The calibration of one channel will not affect other channels
- Each channel is independently (and individually) calibrated with OFFSET and SPAN.
- Each channel support out-of-range detection, as well as automatic recovery from an overload condition

- Each channel performs a self-test to ensure integrity

The ALS-421 channels conduct self testing to ensure channel output integrity. [

]a,c,e Failures in the channels will be provided back to the Core Logic Board in the RAB response packets.

2.2.7.1 Channel Configuration Options

The following parameters can be configured for each individual channels:

- Each channel can be ENABLED or DISABLED
- Channel mode: Voltage or Current
- Channel range: [4 to 20mA], [0 to 20mA], [0 to 10V], etc.

2.2.8 ALS-601 Communication Board

The ALS-601 board is a versatile high-reliability communications board with 8 independent and isolated channels capable of EIA-422 communications (see Figure 2-14). This board provides reliable data transmission and is capable of supporting unidirectional, differential signaling with terminated, point-to-point transmission lines.

The target application for the board is providing highly-reliable communications links between ALS racks, communication to/from other vendor's equipment, communications to a plant computer, and data-logging equipment.

The mission of the ALS-601 board is to receive RAB request packets with data and transmit these packets through the isolated communication channels, and similar on the receive side, to receive packets thru the communication channel and make the information available to the RAB.

As an example, one ALS chassis may be used to collect process measurements from multiple sensors (such as RTDs, thermocouples, pressure, level and flow sensors) and multiplex the data to a second ALS chassis that executes the safety algorithm (calculation of average temperature, comparison to set points, etc.).

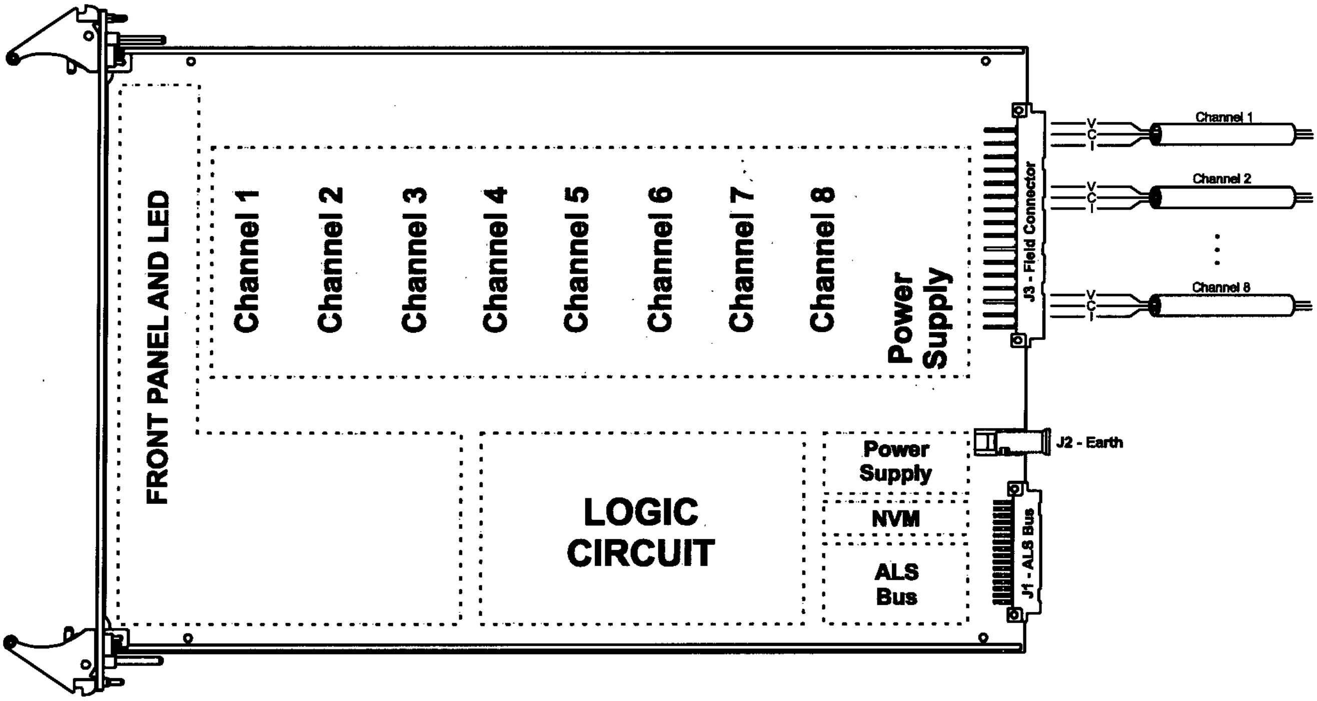

Figure 2-14: ALS-601 with 8 Independent Channels

The ALS-601 board contains 8 independent communication channels. Each channel implements a uni-directional (simplex) EIA-422 communication link.

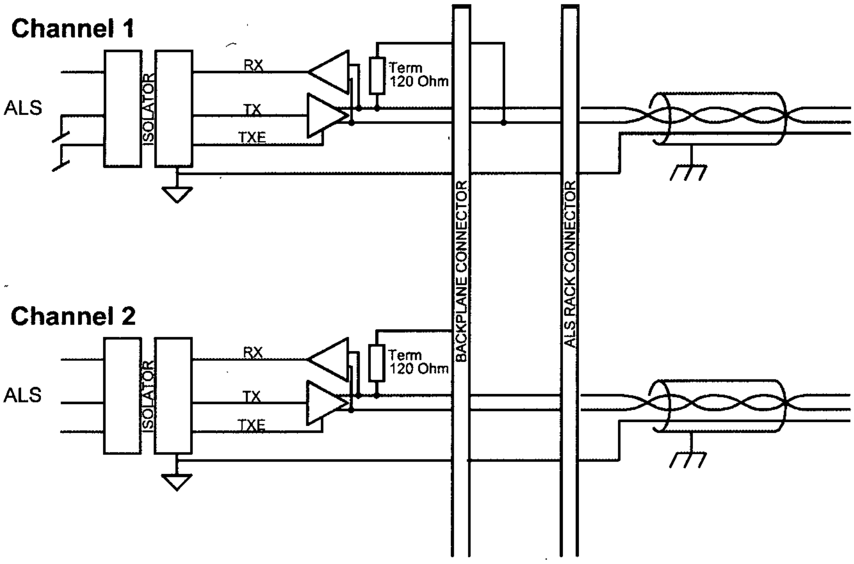

Figure 2-15: Illustration of ALS-601 Channel Design and Use

Figure 2-15 illustrates ALS-601 channels 1 and 2 in two possible configurations:

- EIA-422 Rx: Channel 1 is used for receiving EIA-422 communication. The termination resistor is used and the transmitter part of the transceiver is disabled.
- EIA-422 Tx: Channel 2 is used for transmitting EIA-422 communication. The termination resistor is not used. The receiver is used for continuous self-testing.

Each communication channels on the ALS-601 has the following high-level feature set:

- Uni-directional EIA-422 (act as either a receiver or a transmitter)
- Data are transmitted using the standard UART encoding styles: 8n1, 8o1, 8e1, 8n2.
- The channels support the following standard baud rates: 4800, 9600, 19200, 34800, 57600, 115200, 230400, 460800, and 921600 baud
- A termination option for adding a 120Ω termination resistor across the two differential lines.

The ALS-601 channels support two modes of operation (Byte Mode and Packet Mode):

- **Byte Mode** – Treats each byte as an individual byte of information with no overall synchronization or checksum.
- **Packet Mode** – Data is grouped into small packets with header and checksum. Packet Mode is preferred when the ALS-601 is used to transfer data to another ALS rack.

Self-test detects any reasonably identifiable faults within any component in the ALS domain, including the channel domain, defective soldering or electronic component including the isolation devices and transceivers. A failure in one channel will not affect other channels.

[ ]^{a,c,e}

Each channel has a dedicated buffer [ ]^{a,c,e} to store incoming or outgoing information.

The ALS-601 board does not support higher level protocol features, such as automatic re-transmission in case of data error.

2.2.8.1 Channel Configuration Options

The following parameters can be configured for each individual channel:

- Each channel can be ENABLED or DISABLED
- Each channel can be Receive or Transmit
- Baud Rate
- UART encoding style
- Communication Mode (i.e., Byte Mode or Packet Mode)

The ALS-601 board does not require any pre or post installation calibration.

2.3 ALS Internal Communications

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 logic controller implemented using redundancy.

Communication is performed using two separate and independent serial communication data bus structures;

- Reliable ALS Bus (RAB) – The RAB is the safety path used for all data transfers between ALS boards during normal system operation
- Test ALS Bus (TAB) – The TAB is the communication path used to retrieve integrity and diagnostics, as well as to perform test and calibration

The ALS architecture includes two redundant RAB busses. The RABs are exclusively used to move critical data between the boards, such as input state data and output state data. The RABs are only used by the CLB during normal processing. The redundant structure ensures that an ALS system can continue operation unaffected if one bus fails.

The TAB bus is only used for moving non-control related data between the boards and the ALS Service Unit (ASU) and includes; diagnostics, configuration, calibration and test data. The TAB bus has been designed to be non-intrusive in the sense that it cannot interfere with the regular processing of the RAB bus.

[

]^{a,c,e}

Figure 2-16 illustrates the bus architecture used for internal communication within the ALS platform, as well as the connection between the ALS and the ASU using the TAB bus.

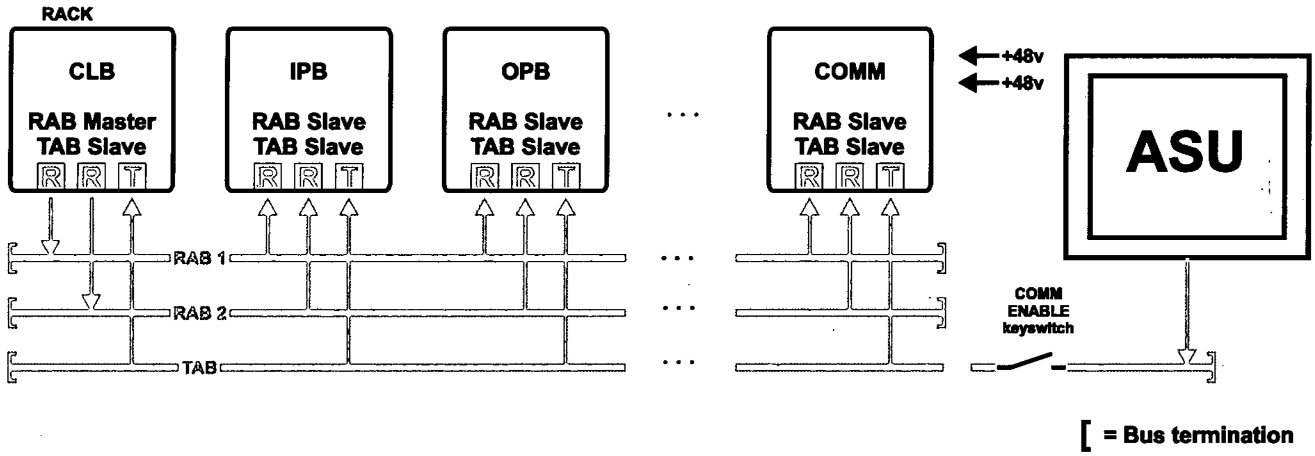

Figure 2-16: ALS Platform Bus Architecture

The boards communicate over the ALS Backplane using RAB and TAB busses. The Core Logic Board is bus master on the RAB and the ASU is bus master on the TAB when it is connected to the ALS chassis.

A fully configured ALS rack consists of a CLB, and a number of ALS input (IPB), output (OPB) and/or Communication (COMM) slave boards, as shown in Figure 2-16. The CLB uses both available RABs as redundant communication links to the RAB slaves. The core logic board is bus master (on each RAB bus). The bus master is the initiator of all communications to the multiple slaves on each bus.

The RAB bus structure is based on a standard EIA-485 interface. EIA-485 specifies a 2-wire, bidirectional, differential line, half-duplex data transmission, multipoint communication standard. [

]^{a,c,e} The access scheme is point-to-point transactions based communication initiated by the master, with slaves responding with valid data when requested. All communication is based on an EIA-485 half-duplex communication protocol between two devices. The bus provides for communication in both directions, but only one direction at a time (not simultaneously). This provides high noise immunity due to dedicated EIA-485 differential wire-pair, implemented with short wire length and high drive capability.

The TAB bus is nearly identical to the RAB bus. It is based on the same standard EIA-485 interface with 2-wire differential signaling. [

]^{a,c,e}

2.3.1 Reliable ALS Bus (RAB)

The two RAB busses are each implemented as independent and separate busses that are used for safety system function communication between ALS boards. The two RAB busses are redundant to each other and the information transferred on RAB1 is the same as RAB2. A failure of RAB1 will, therefore, not prevent the system from performing its safety function using RAB2.

Architecture of the RAB is a CS Innovations proprietary master-slave communication protocol, using simple differential EIA-485 point-to-point communication. It employs standard cyclic redundancy checks (CRCs) protection to ensure the integrity of the communicated information between two boards.

All RAB communications utilize a request-response protocol where the master will send a request and the appropriate slave will provide a response. All requests are initiated by the Core Logic Board by sending a fixed-length packet to an ALS slave board. Upon reception, the slave board responds by sending a packet back to the Core Logic Board. The packet sent by the Core Logic Board to the slave board is referred to as the 'request' packet and the response packet is referred to as the 'response' packet. Together, this process is referred to as a RAB transaction as illustrated in Figure 2-17.

a,c,e

Figure 2-17: RAB Transactions

[

]^{a,c,e} The RAB master will read information from all appropriate input boards and write information to all appropriate outputs boards once every ALS Bus Frame.

The ALS Bus Frame cycle time is fixed for a given application and does not change once the system has been implemented. [

]^{a,c,e}

The content of a RAB packet is 'data' with the actual safety I/O information, as well as the associated 'integrity' information with health information associated to the data information from the analog or digital channels, as well as board health information.

2.3.2 Test ALS Bus (TAB)

The TAB Architecture is a CS Innovations proprietary master-slave communication protocol, using simple differential EIA-485 point-to-point communications. It employs standard cyclic redundancy checks (CRC) protection to ensure the integrity of the communicated information.

The TAB is used to transfer monitoring, diagnostics, test and calibration information.

Examples of diagnostics information from the ALS-102 Core Logic Board 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, the count of a counter or the value of a temperature sensor).

[

]^{a,c,e} It is only active when the ALS system is connected to the ASU.

[

]^{a,c,e}

The information is collected in a non-intrusive manner and does not affect the on-going operation of the system (or the RAB busses).

2.3.3 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 detects any failure on the ALS busses (RAB or TAB). In addition to being able to detect any failure, care was 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.

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.

2.3.3.1 ALS Bus Failure Detection

Four detection schemes are responsible for detecting any communication failure within the ALS platform:

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

Detection of failures and the successive reaction to the detection are instantaneous. This is key to the reliability and integrity of the platform, since it prevents failures to propagate from board to board.

The following failures related to the ALS bus communication path can be detected:

[ ] a,c,e

[ ]^{a,c,e}

Integrity information collected in the I/O channels is transferred along with I/O data. This enables the Core Logic Board to make decisions based on valid information and take appropriate action only if valid channel information is available. If boards become unavailable (due to board removal or failures) then data and the integrity is invalidated within the core logic board.

The inherent architecture (protocol and implementation) detects any RAB communication failure. The ALS Core Logic Board maintains the status of all RAB communication.

The logic on the ALS boards will timeout if there are no valid RAB transactions time-out. If both redundant RABs time out the board will enter its fail-safe state. If the timed out board is an ALS output board the output channels will be driven to the predefined safe state.

TAB failures are detected and mitigated in a similar fashion. [ ]^{a,c,e} 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 to continue running as long as possible, while still preserving point-to-point integrity.

2.3.3.2 ALS Bus Failure Mitigation

Fault Isolation:

- Prevent the propagation of defective data
- Prevent the use of defective data
- The packet payload 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.

2.3.4 ALS Internal Communication Acceptance

As previously described, internal communications within the ALS platform architecture are limited to serial data transfers through the RAB and TAB busses. The first of two buses are the Reliable ALS Bus (RAB) that is used for the safety signal path. The RAB is comprised of two buses for reliability (RAB1 and RAB2). The second bus is the Test ALS Bus (TAB) that is used for diagnostics and test data. Each bus follows a master-slave protocol. The Core Logic Board is the bus master of the RAB, and the ASU is the bus master of the TAB.

In Docket 50-482, Amendment 181 to License No. NPF-42 (Reference 2), as written in the SER (ML # 090610317) (Reference 70), the NRC determined that communications independence is provided by the inclusion of two separately controlled buses (RAB and TAB), as described by the ALS system design. Communications independence exists, because 1) the RAB segregates the operational safety signal path from the TAB that provides the maintenance and troubleshooting diagnostic signal path; 2) independent digital logic circuits in the form of separate finite state machines implement the bus logic; and 3) operation of the TAB does not affect operation of the RAB.

Each bus protocol is based on the EIA-485 differential standard. ALS boards are connected using the application specific Backplane Assembly of each chassis. Each bus is half-duplex and, therefore, does not allow simultaneous data transmission and reception. The serial communication protocol for each bus utilizes cyclic redundancy checks (CRCs) to ensure the integrity of a data transfers between boards.

Each bus follows a master-slave protocol, with a Core Logic Board always being the RAB bus master, and the ASU always being the TAB bus master. The half-duplex communications allows for only one active transmitter at any point in time as controlled by the bus master. Each bus master (Core Logic Board or ASU) controls its serial data bus resource (RAB or TAB) that is shared among boards, so that two boards cannot simultaneously access a bus. The master controls the bus, and the slaves only communicate when requested and enabled. [ ]a,c,e When a board is declared as failed, it triggers the bus master's alarm status output and is indicated as failed on the ASU.

Each slave board can detect communication failure on the RAB or TAB, and can isolate itself from further communications on the RAB until the communication failure is corrected. Each RAB slave implements a communication watchdog time-out and "HALT" function for RAB communications. This watchdog function detects a condition where the slave board has not successfully been polled for a prescribed interval.

The proprietary communication protocol that is used for the TAB is similar, but not identical, to the protocol used for the RAB. The ASU does have the capability to write to or attempt to otherwise configure slave boards, but any action of this nature is under the control of the Core Logic Board to assure that no damage can be done to the system by the ASU.

In Docket 50-482, Amendment 181 to License No. NPF-42, as written in the SER, the NRC determined that the application of the RAB and TAB buses provide for error detection to preclude the use of invalid data in accordance with the guidance of IEEE 7-4.3.2-2003 (Reference 4). In addition, the NRC determined that the communications protocol provided by the ALS platform provides deterministic point-to-point communications in accordance with IEEE 7-4.3.2-2003 (Reference 4).

2.4 Board Operation Modes

The state of an ALS system is specified by the operational mode of each of the boards operating in a decentralized fashion.

The ALS boards utilize a simple board mode concept to control the startup and operational state of an ALS board. During operation, the board mode is in one of the following three modes: Board operation is in Startup (STARTUP), Normal (OK), or HALT (HALT) mode.

Figure 2-18 shows the transitions between states.

a,c,e

Figure 2-18: ALS Board Modes

a,c,e

a,c,e

2.5 ALS Chassis

The ALS chassis houses the ALS Backplane and printed circuit boards (PCBs), and provides the mounting structure for installation into a cabinet. The ALS chassis is an industrial standard 19" sub-rack designed to install into industry-standard 19-inch cabinets. Figure 2-19 shows a typical ALS chassis, with ALS boards, back-plane and back-panels.

The major system components of the ALS chassis are:

- ALS Boards: Control, input or output boards mounted into the rack by their front-plate
- Backplane Assembly: A backplane PCB mounted onto an aluminum backplate
- Chassis: 19" Sub-Rack Chassis, 6U tall (266mm), 400mm deep

Figure 2-19 below shows the front panel view of a typical ALS chassis populated with 8 ALS boards and 2 filler panels. Various types of boards can be configured in the ALS chassis depending on application specific requirements.

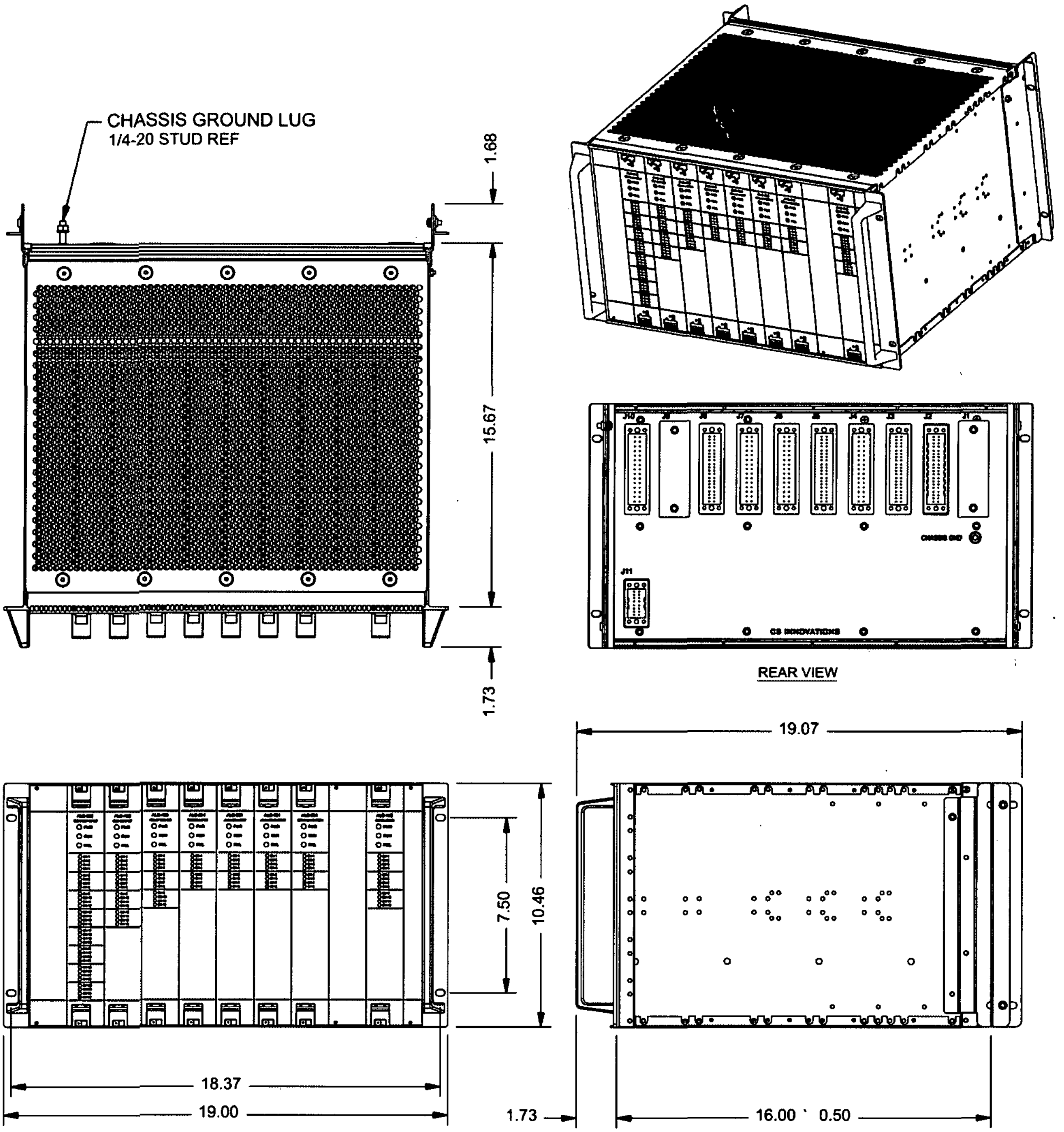

Figure 2-19: Typical ALS Chassis Populated with 8 ALS Boards

2.5.1 Chassis Mechanics

The ALS is based on a 19" (482.6mm) Chassis width, 6U (266mm) height and 400mm deep. The ALS chassis is implemented in a lightweight and durable construction, suitable for rugged environments and long-life expectancy.

For easy installation and replacement, the ALS Boards are configured with injector/ejector handles located on the top and bottom of the ALS board front panel.

The ALS chassis is designed to rely on natural convection in the cabinet, with no internal fans. The chassis has fully enclosed front/back/sides, and has perforated top and bottom panels to allow bottom-to-top airflow. This construction gives the ALS chassis an IP20 rating against foreign objects and water.

All 6 sides of the chassis are electrically connected and grounded to chassis ground. Chassis ground is provided through a single earthing lug on the back of the ALS chassis.

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

A fully configured ALS platform chassis will typically weigh less than 20kg.

2.5.2 ALS Slot and Card Configuration

The ALS boards will have a different front panel depending on the type of board, and will generally be between 6HP and 12HP (1 HP = 0.2 inches). Component height and front plate indication requirements may necessitate that certain types of ALS boards are wider than 12HP.

Each opening in the ALS chassis that can accommodate an ALS board is referred to as an ALS Slot. The ALS Slots are not designed to be interchangeable; the backplane connectors are keyed to ensure that only the correct type of ALS board can be inserted into a given slot. In addition, the ALS logic also verifies that the inserted board contains the proper configuration settings 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.

2.5.3 ALS Boards

ALS boards are designed to fit directly into an ALS chassis. The ALS board is a printed circuit board assembly, which includes printed circuit board, backplane connectors and front plate with injector/ejector latches (see Figure 2-20).

The ALS boards connect to the backplane [$]^{a,c,c}$. All components, switches and LEDs are mounted directly on the printed circuit board (PCB) which allows for easy removal of the front plate.

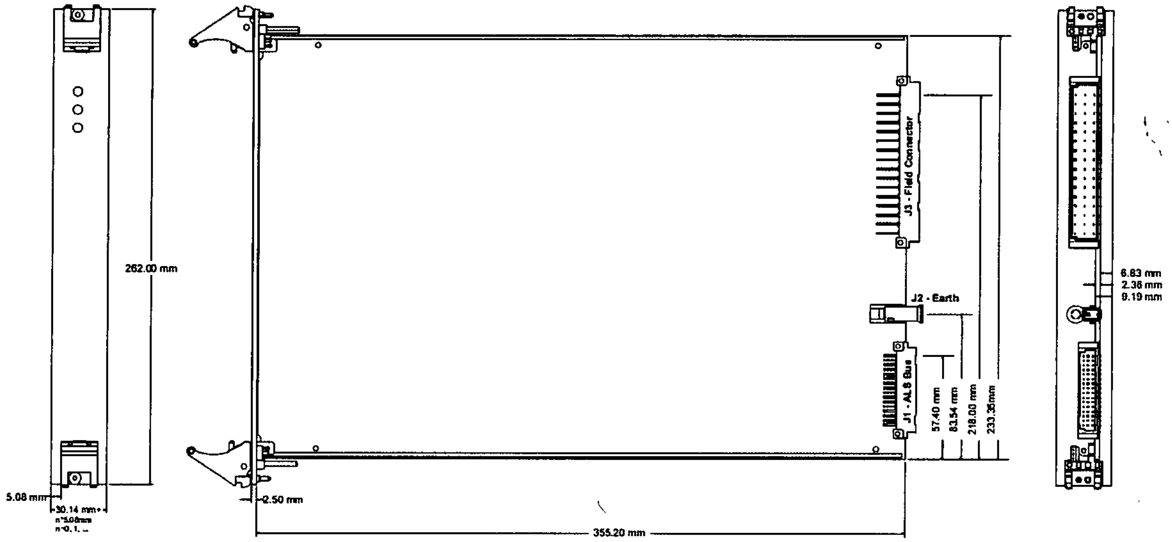

Figure 2-20: Generic ALS Board with ALS Bus Connector

2.5.4 ALS Front Plate

All ALS boards are designed 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 2-21 shows how ALS board front plates can be customized to provide application specific information directly on the front plate.

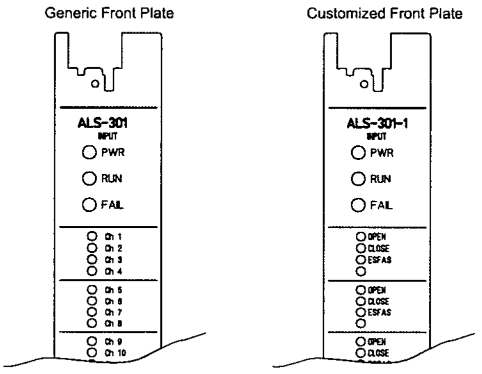

Figure 2-21: Generic vs. Custom Front Plate

2.5.5 Board Latches

Boards are fastened and secured to the chassis using dedicated ergonomic 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 and they secure the board in the chassis.

The latches include micro-switches which ensures that the board is in a safe state before it is ejected from its slot.

2.5.6 Front Panel LEDs

Two types of local indications are provided on the front plates of all ALS boards: 1) Board Indication LEDs and, 2) Channel Indication LEDs.

2.5.6.1 Board Indication

ALS boards include three common board LED indicators located on the top of the front-plate. The board indicators provide easy local indication of the state of the board. Table 2-3 describes and defines the LEDs and their indications.

Table 2-3: ALS Board LED Indicators

a,c,e

2.5.6.2 Channel Indication

ALS boards include a channel specific LED, which typically provides state indication, but more importantly, always provide local indication of the channel integrity and as well as calibration or test.

2.5.7 ALS Backpanel Assembly

The backpanel assembly consists of a solid aluminum backplate with a PCB backplane mounted directly onto it. The backpanel assembly is an application specific item which is designed to accommodate the ALS Boards and field interconnects needed for the application to which it is being installed. Although there are several specific ALS plant applications, the backpanel design and assembly methods are similar.

The backplate provides the interconnection mechanism between installed boards and provides the interface between the ALS chassis and the other ALS safety system components. [

]^{a,c,e}

All permanent chassis connections are made using cable harnesses connecting to the backpanel. [

]^{a,c,e}

The 'Earthing connection' (Chassis Ground) is located in lower-left corner of the rear-panel. The connection is tied to a common earth ground point within the cabinet.

a,c,e

Figure 2-22: [ ]^{a,c,e} Connector	**Figure 2-23: Backplane Connector Assembly**

The exact wire allocation of the backplate connectors and the location these connectors are application specific and will be specified for each application. It is also here that any application special cabling or isolation requirements will be addressed.

2.5.8 Expansion Chassis

The ALS Expansion Chassis provides the capability to accommodate additional input/output boards to meet application specific requirements. The RAB and TAB busses from the main ALS chassis are extended to the ALS Expansion Chassis so that the input/output boards in the Expansion Chassis can communicate to the ALS Core Logic Board in the main chassis as illustrated in Figure 2-24. Further, the cable between ALS chassis will contain +48Vdc and ALS ground.

Up to five ALS Expansion Chassis can be connected to one ALS Main Chassis.

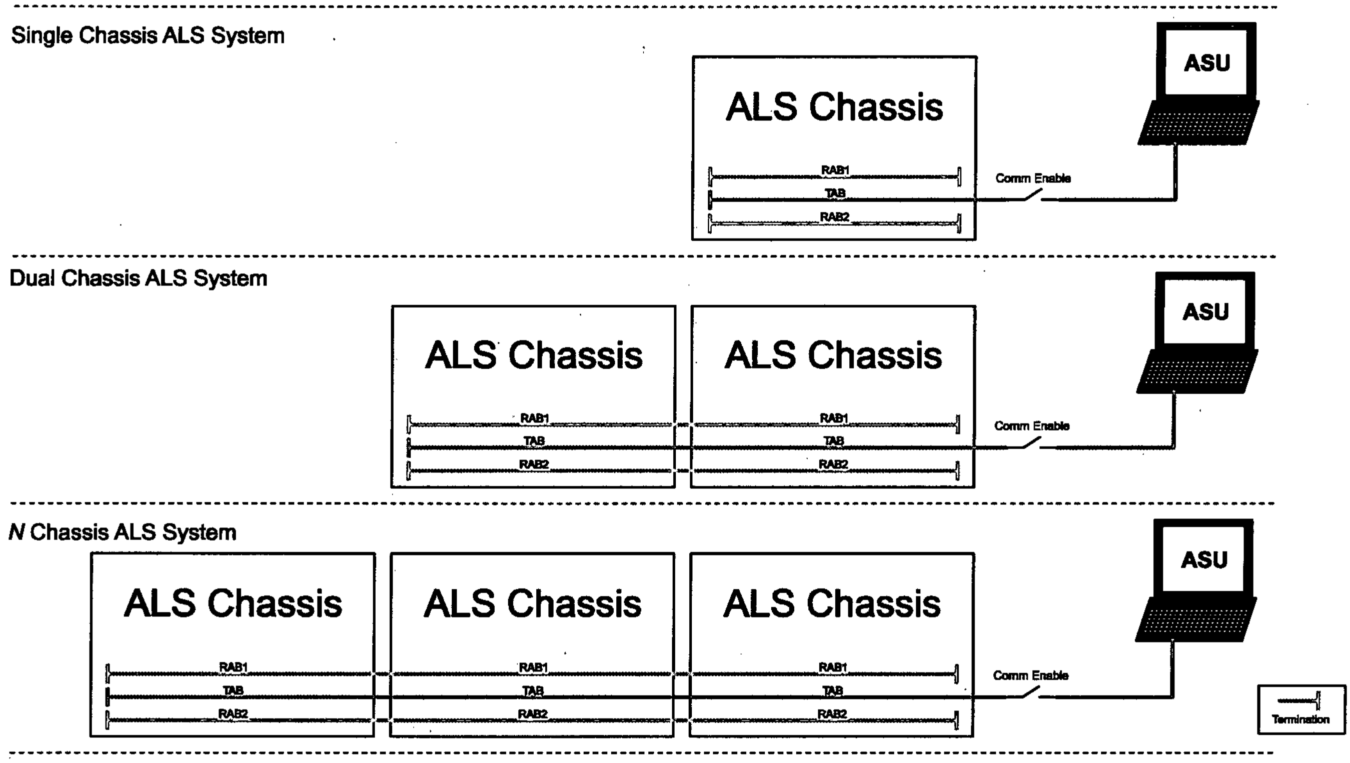

Figure 2-24: Example Uses of Expansion Chassis

2.6 Cabinet and Peripherals

Cabinets and peripheral devices are required to support the ALS platform and application and to comply with applicable safety system codes and standards (see Figure 2-25). The following peripheral components are typically used in conjunction with an ALS chassis to accomplish a safety system application:

- **Cabinet**: Houses the ALS chassis and other peripheral components.
- **Power Supplies**: Convert the incoming ac or dc vital bus power to dc power used by the ALS chassis and other peripheral components such as interposing relays, etc.
- **ALS Service Unit (ASU)**: Used to perform diagnostics, test, calibration and maintenance of the ALS chassis.
- **ALS Chassis**: Populated with ALS Boards.
- **Control Panel**: Houses the key switches and connectors that facilitate test, calibration and maintenance of the ALS chassis, as well as lamps and other indicators.
- **Assembly Panel**: Houses application specific components, such as terminal blocks, interposing relays, fuse holders and isolators/repeaters.

NOTE: An installed ALS system may consist of none, one, or more of each of the peripheral components previously described.

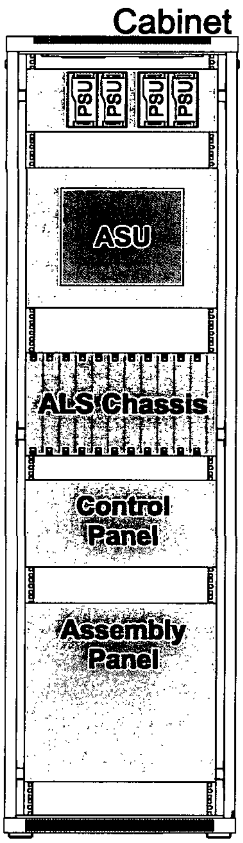

Figure 2-25: ALS Cabinet

2.6.1 Cabinet

ALS safety systems can be provided as new installations or as replacements for existing installations. Typically, project specific requirements will state whether a new cabinet is to be provided, or the existing cabinet is to be utilized to house the replacement ALS system. If a new cabinet is required, the ALS system is packaged in a one-bay cabinet that has been seismically, EMI, and ESD qualified for safety system applications. If an existing cabinet is used, the cabinet is modified as required to comply with site specific seismic, EMI and ESD requirements. Seismic qualification can be performed by analysis or actual testing.

Cabinet door handles with integral key locks can be used to limit access to cabinet internals. Door switches monitor the status of each door and initiate an alarm if the door is opened.

ALS safety systems typically do not require forced air cooling due to the low heat dissipation. Natural convection via the lower and upper door louvers provides sufficient cabinet ventilation. The cabinet has the capability to support the addition of forced air cooling if necessary to satisfy application specific requirements.

Internal cabinet wires and cables are application specific and will be designed according to the application requirements.

2.6.2 Power Supply and Distribution

The ALS chassis is powered via the Backplane Assembly from an external dual-redundant power supply system. The power supplies are typically mounted in the same cabinet as the ALS chassis.

Each ALS safety system cabinet contains two qualified, independent ac/dc power supplies. Each power supply is capable of providing 150% of the cabinet load, and operates in a redundant configuration. The cabinet load consists of all ALS platform components and peripheral devices.

In a typical safety system application, each separation group (division) is powered from an independent Class 1E vital bus source. Within the division, the Class 1E vital bus supplies power to each cabinet. The cabinet power supplies can accept source voltages in the range of 100-240Vac, or 90-300Vdc. If required by the application, each of the redundant power supplies in the cabinet can be powered separately by separate Class 1E sources. The output of the redundant cabinet power supplies is 48Vdc.

The individual cabinet power supplies are hot swappable and capable of being replaced while the system is operational without interruption of power to the ALS chassis or other safety system components. Cabinet mounted diode auctioneering is provided for other cabinet loads if necessary to satisfy application specific requirements.

Inside the cabinet, an AC Line Filter is used to reduce incoming noise and suppress conducted emissions and conducted susceptibility. In addition to the power supplies and AC Line Filter, the power distribution system consists of breakers and terminal blocks as necessary to satisfy application specific requirements.

Power supply failures (loss of output voltage) and opening of distribution breakers are alarmed.

The 48Vdc from the redundant cabinet power supplies is fed to the ALS chassis, where they are diode auctioneered to provide a single local 48Vdc supply. Each ALS board contains dc/dc converters that generate stable local board power. All ALS boards are fused, filtered and over-voltage protected on the incoming cabinet 48Vdc supply voltage. The fuse ensures that local failures on an ALS board cannot disrupt the chassis power. The filtering is done to avoid noise propagating from the ALS backplane (transients, etc) to the board itself and also to avoid noise coming from the ALS board to the ALS backplane.

Figure 2-26 depicts a typical power distribution used to power the ALS platform with redundant 48Vdc. Some applications may have a redundant cabinet power feed, in which case the Surge Protection, Breaker and Line Filter will be replicated.

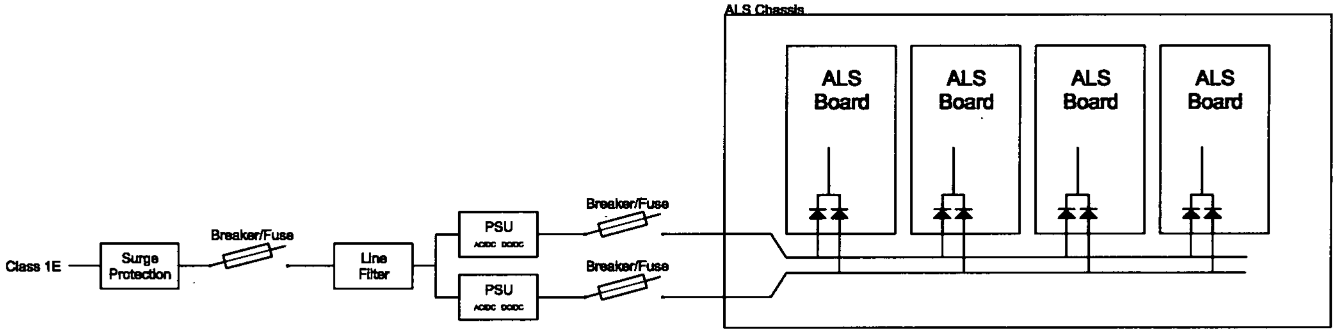

Figure 2-26: Typical ALS Platform 48Vdc Power Distribution

2.6.3 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, initiating various run-time tests, and performing test, calibration and maintenance operations.

The ASU can be a permanently attached device as shown in Figure 2-25, or it can be a removable laptop brought to the system and temporarily connected.

The ASU can only communicate with the ALS platform when the COMM Enable keyswitch has been activated on the Control Panel.

If the ASU used in the particular application is qualified as safety the TAB bus may be directly connected to the ALS platform (through the COMM Enable key switch), if it is non-safety the TAB bus must be isolated as described in [ ]^{a,c,e}

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 debugging registers. The advanced monitoring capabilities enable fast system diagnostics and troubleshooting.
- **System and Board Information** – Provides detailed information about the configuration of an ALS system, including board FPGA programming, board build information, and board configuration.
- **Blackbox** – The ASU may include a blackbox functionality where all events of an ALS system are recorded. This allows plant personnel to inspect the ALS system's reaction to a past event. The blackbox helps reduce the time it takes to pinpoint the cause of a series of events.
- **Test** – Application specific periodic surveillance tests can be implemented to be performed through the ASU. Based on the needs of the application features may be implemented in the CLB that allows surveillance testing to be performed and/or monitored through the ASU.
- **Calibration** – The ASU is used to readout and change application SetPoints and channel calibration coefficients. The CLB holds the application SetPoints and according to the application, it will allow the ASU to modify these SetPoints. The ASU is also used during input/output channel calibration where it is used for selecting the board and board channel to be calibrated and to change calibration coefficients based on the readings received on a external calibrator. This calibrator will typically be an industry standard process calibrator traceable to a National Institute of Standards and Technology (NIST) standard.

The ASU operation is passive and non-intrusive, i.e., it can only modify the safety system tunable parameters stored in NVM for which it is designed (i.e., input/output calibration coefficients, setpoints and tuning constants). It is not possible to modify the safety channel algorithm. All communications initiated by the ASU takes place on the TAB bus. No RAB bus interruption can occur, effectively leaving the safety operations of the ALS system unaffected.

2.6.4 Control Panel

The Control Panel is accessible from the front of the cabinet and is equipped with switches, status indicators and test points as required by the specific application. The switches are used for application specific functions such as bypass of a partial reactor trip channel, test initiation and control, and manual actuations to support the application specific requirements. Control Panel devices are typically connected to input and output channels on the ALS boards.

In addition to the application specific components, the Control Panel contains two standard components that interface with the ALS chassis:

- **COMM ENABLE** key switch allows two-way communications between the ALS chassis and the ASU via the TAB bus.
- The **CLEAR_ALARM** switch is used to force the ALS chassis to reset the ALARM circuits. This is utilized when the initiating condition of an alarm is removed and the chassis is reset to clear the alarm indicator.

Furthermore, if the ASU is not the fixed mounted style, but instead a laptop style test unit, the Control Panel will contain an ASU CONNECTOR to provide a connection point for the ASU.

2.6.5 Assembly Panel

Depending on the safety system application, one or more Assembly Panels may be mounted inside the Cabinet. These application specific Assembly Panels are equipped with peripheral devices such as terminal blocks, fuse holders, relays, fiber optic modems, isolator modules and other field interface hardware.

The Assembly Panels allow for application specific cabling of signals from the ALS chassis to an Assembly Panel which then allows for the connection to the field wiring. They also allow for the application specific cabling and distribution of system power within the cabinets.

Field Cable Terminal Blocks provide termination points for field cables, disconnection points, test injection and monitoring points for incoming and outgoing signals.

All peripheral devices are typically mounted on the Assembly Panel, and are qualified to the same criteria as the base safety system.

2.7 Response Time

The accident analysis of design basis events at nuclear power plants includes a determination of how soon the protective actions are needed to mitigate the design basis events. The basis for this is contained in 10 CFR 50.55a, "Codes and Standards," of 10 CFR, "Domestic Licensing of Production and Utilization Facilities" (Reference 6). This states that “protection systems must meet the requirements stated in IEEE Std. 603-1991, ‘Criteria for Safety Systems for Nuclear Power Generating Stations,’ and the correction sheet dated January 30, 1995." In addition, 10 CFR 50.36(c)(1)(ii)(A) (Reference 8) requires inclusion in the technical specifications the limiting safety systems settings for nuclear reactors, those settings "so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded." Once the total time required for a protective action is determined, licensees allocate portions of that time to portions of the protective system (i.e., the time required for the sensors to respond to changes in plant conditions, time required for the actuation logic, and the time required for the breaker to open, valve to close or a pump to start).

For replacement applications, the licensee provides the response time requirements for the safety functions to be performed by the ALS platform. This is typically the same response time as the system being replaced. For new applications, the response time is provided as part of the functional requirements for the safety system. The safety system design specification then incorporates the response time requirements to assure that the system is designed to meet the required response time. A system test plan (which is developed for each system) specifies how to conduct the response time test to measure worst case response time for that system. The response time test is typically conducted several times (as specified in the test procedure) and the maximum measured response time must be less than the required response time specified by the requirements documents. This process provides verification that the response time of a given system is below the threshold established by safety system functional requirements per IEEE 603 (Reference 7).

In the ALS platform the system response time is generally defined by 3 components; Input Delay, Logic Delay and Output Delay as illustrated in Figure 2-27.

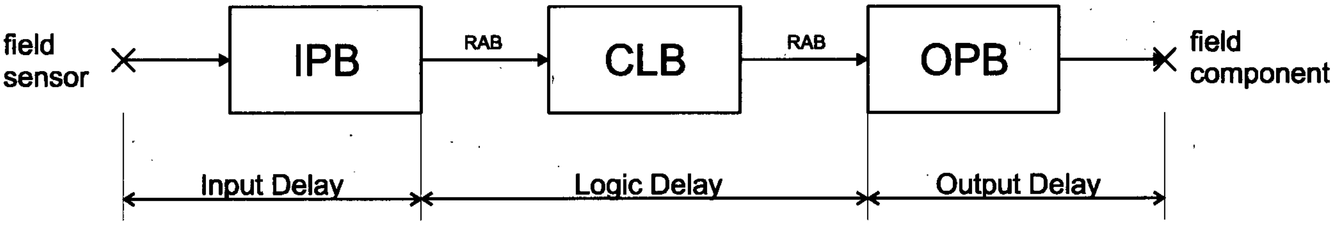

Figure 2-27: ALS Platform Response Time Contributors

The input delay (response time) is defined as the time it takes for a sensor value to change until the response is available to read on the RAB bus. On analog boards the response time is measured as the time from an input step change until the detected value has reached halfway to the new value (50%). The input delay will vary with the type of input board, and the configuration of that input boards. An example of this is the digital input board ALS-302. The response of the ALS-302 is primarily determined by the digital filter setting of the channel [ ]^{a,c,e}. See Section 2.2.2 for additional information. Analog boards can be configured to sample the input data at different rates, [ ]^{a,c,e}. When making application specific ALS systems the board configurations are defined according to the needs of the application. In general it is desirable to allow as much filtering as possible in the input board to filter out noise [ ]^{a,c,e}

The logic delay (response time) is defined as the time it takes from the RAB data being available on the input board until the associated RAB data has been written to the output board. The two contributors of this delay are the ALS Bus Frame period and the logic processing delay. [ ]^{a,c,e}

The output delay (response time) is defined as the time it takes from a RAB command being received by the output board until the output channel has changed state. On analog output boards the response time is defined as the time it takes for a step change on the RAB bus until the output channel to reach halfway to the final value. This output delay will vary with board type.

A typical response time of an ALS system is around [ ]^{a,c,e}, which is well within typical safety system response time requirements. Shorter response times can be provided if required by the application.

2.8 ALS System Accuracy

The overall accuracy of the ALS system can be split into three major components: Input Accuracy, Logic Accuracy, and Output Accuracy. The following section will present these components one at a time. The worst case scenario is if both the input and output are analog, as shown in Figure 2-28.

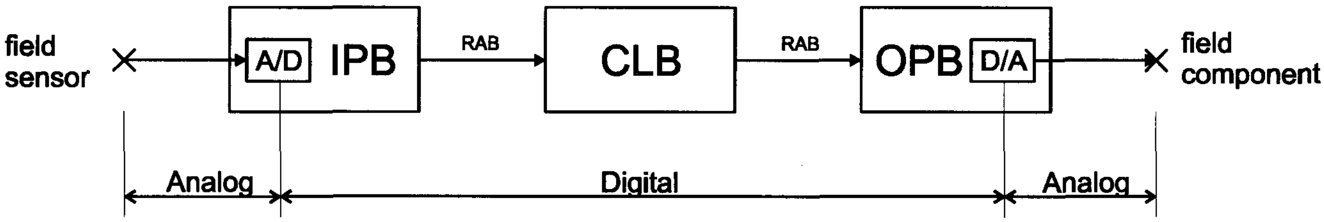

Figure 2-28: ALS System Accuracy

The input accuracy is determined by the input channel on the ALS board. An analog input channel will in general consist of an analog input conditioning circuit and an analog to digital (A/D) converter. There will be no additional loss of accuracy after the data has been converter to digital representation. Most ALS analog input boards are specified [ ]^{a,c,e}.

The digital accuracy of the ALS platform is 20-bit when processing analog values. Because the values are digital there will be no additional loss of accuracy during processing. This inaccuracy component is referred to as quantization noise [ ]a,c,e

The output accuracy is determined by the output channel on the ALS board. An analog output channel will in general consist of a digital to analog (D/A) converter and an output conditioning circuit. The ALS analog output board (ALS-421) is specified [ ]a,c,e.

In the example illustrated in Figure 2-28, the worst case combined accuracy [ ]a,c,e.

2.9 Human Factors Considerations

The following human factors concepts are considered at the initial stages and throughout the design process during development of the ALS platform:

- Simple Architecture – The ALS platform has a simple design in order to enhance operation and maintenance. As discussed earlier, one of the problems with modern processor based systems is the increase in complexity that is necessary to maintain reliability and resolve diversity issues. The ALS platform utilizes a simple architecture with fewer boards and components, resulting in higher reliability and a longer mean time between failure (MTBF).
- Hot swappable boards – ALS boards are hot swappable. This capability eliminates the need to shutdown the entire system to replace a board.
- Board Indications – ALS board indications are designed to be straightforward to minimize the chance of misinterpretation. Failures are clearly indicated by the behavior of front plate LEDs.
- Pre-configured boards – ALS board FPGA cores are configured prior to shipment and cannot be altered by the licensee or any of its employees. This approach strengthens cyber security defenses and improves configuration control of ALS safety systems.
- ESD – The ALS platform is extremely resistant to ESD as discussed in the section on EMC Qualification. This hardening eliminates the need for ESD protection during maintenance.
- Self-test – The ALS platform has extensive self-test features built into the platform. This provides for a simpler and faster identification of issues and their resolution.

During the audit of the ALS MSFIS application, the NRC staff reviewed the customer design requirements documents, the ALS system design specification, individual ALS board specifications, and the methods used for design. This review concluded that human factors were considered at the initial stages and throughout the design process and, therefore, the MSFIS design and design methods meet the requirements of IEEE 603-1991 Clause 5.14 (Reference 7).

3 Diagnostics and Maintenance

This chapter presents a high-level description of the ALS platform diagnostics and maintenance features. The ALS platform is designed for long-term reliability and maintainability. The ALS platform includes several features for diagnostic and maintenance of the platform, which are described within this section.

3.1 ALS Diagnostics and Fault Indications

The ALS platform incorporates advanced failure detection and isolation techniques. The operation of the system is deterministic in nature and allows the system to monitor itself in order to validate its functional performance. The ALS platform implements advanced failure detection and mitigation in the active path to avoid unintended plant events, and in the passive path to ensure inoperable systems do not remain undetected. The ALS platform's advanced failure detections were developed to prevent this type of scenario from occurring. The ALS platform is based on autonomous boards working together. The system utilizes logic to perform distributed control where no single failure results in an erroneous plant event while maintaining the ability to perform its intended safety functions.

3.1.1 ALS Platform Diagnostics

The ALS platform incorporates self-diagnostic features that provide a means to detect and alarm any significant failure within the platform. Details of the ALS Board self-diagnostic features are described in the hardware specification associated with each board. ALS platform fault detection and self-diagnostics are described in the ALS Platform Specification.

The self-diagnostic features are integral to the platform (i.e., not added-on), and are, therefore, subject to the same high quality design development and independent verification and validation (IV&V) processes as the rest of the platform. The self-diagnostic features are functional during all modes of ALS platform operation, including power-up, operation, and test.

3.1.1.1 System Self-Diagnostics

The ALS platform is designed to support the elimination of manual periodic surveillance testing of an installed ALS safety system. In typical safety system applications the ALS platform is operating at steady state where it is monitoring plant conditions to initiate reactor trip or engineered safety feature (ESF) actuations. To verify operability, it is necessary to test these static commands on a regular basis. Historically this has been done with periodic surveillance testing which involves plant personnel placing the system into a bypassed or partial tripped state and then testing the critical functions. The ALS platform is designed to eliminate the need for periodic surveillance testing with a combination of redundancy and self-testing which automatically and transparently verifies critical system functions.

This document summarizes the concepts and provisions that are available to support relaxation of periodic surveillance testing requirements. The actual justifications to relax periodic testing requirements would be included in the application specific submittal.

The ALS platform self-test strategy is based on four simple and effective steps:

- **Detect:** The ALS platform detects failures in its circuits or connected field devices by running background tests on a regular interval, and by redundancy.

- **Mitigate:** The circuits causing the failure are isolated before the failure is allowed to propagate from an ALS board to another and from the ALS system to other systems.
- **Announce:** The detected failure is announced using the ALS chassis alarm which typically ties into a power plant's main control board alarm. Other application specific indicators may also be added to the system to give a more detailed status indication to the control room, such as indicating in which function the failure occurred and provide indication as to whether the system remains operable.
- **React:** The failure is announced using the system alarm and by other application specific means. The ALS safety system may also be designed so that a failure in a sub-circuit causes the system to enter a specific state, such as a partial trip or bypass.

The critical functions for a particular application are defined in the functional requirements and become key requirements when specifying the application specific ALS safety system. Generally, a critical function is the system's ability to drive its output channels to a predefined state when a specified set of input events occur, such as digital inputs being activated or an analog input going beyond a threshold.

3.1.1.2 ALS Platform Self-Testing

Self-testing of the ALS platform can be divided into segments as shown in Figure 3-1. The following sections describe the self-test strategy for each of these segments. Figure 3-1 depicts a full safety path from the field input through the CLB to the field output.

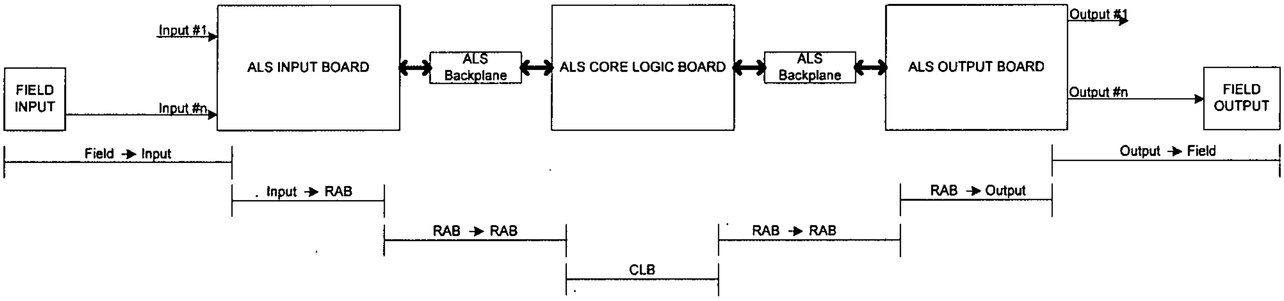

Figure 3-1: ALS Platform Self-Testing

Field→Input: The capability of testing the connection to a field input is determined by the specific application (or equipment) and the particular ALS input board. If the field input supports self-test, the ALS board determines the integrity of the wiring and performs an application specific action in case of failure (i.e., preferred failure mode). A simple example of this is a 4-20mA current loop where a wire break is detected, appropriate response generated and annunciated accordingly. Another example is a 0-10V input where the self-test, for an ALS-321 input board, uses the on-board independent high precision reference to detect a problem with the calibration of the A/D.

Input→RAB: The generic ALS input boards are designed to automatically detect circuit failures between the input channels and the ALS RAB bus. This is performed with a combination of redundancy and self-test. The digital input channels typically include a self-test circuit where the channels are disconnected from the field input and tested. These tests are done in a way that the test time has a very minimal affect on the response time of the system. This minimal time is included in the calculation of response time. Such self-tests normally occur [ ]^{a,c,e}, see Table 3-1. Logic inside the FPGAs on the input boards are protected with the standard ALS dual-core redundancy as well as internal Build-In-Self-Test (BIST) engines.

RAB→RAB: The ALS RAB bus communication is protected using redundancy, timeout detectors, CRC checksum protected communication protocols and by the way the data packets are constructed. Any error on the ALS RAB bus is immediately detected and handled appropriately. The failure detection mechanism for the ALS RAB bus is contained on the ALS boards connected to the bus. This ensures that any one ALS board cannot cause an undetected failure. If the Core Logic Board fails the ALS slave boards detect a timeout event and enter their pre-determined fail-safe mode. If an ALS slave board fails, the Core Logic Board detects the failure and performs the predetermined action. The ALS RAB bus implementation and protocol inherently ensure that no 'frozen data' failures can occur in the ALS system without detection.

Core Logic Board: The logic function is application specific. The Core Logic Board is based on state machines and other basic building blocks. A self-test strategy is designed specifically to ensure no undetected failures exist in the critical functions. The FPGA logic inside the Core Logic Board is protected by the standard dual-core redundancy.

RAB→Output: The generic ALS output boards are designed to automatically detect circuit failures between the ALS RAB bus and the output channel. This is performed with a combination of redundancy and self-test.

Output→Field: The capability of testing the connection to a field device is determined by the specific application (or equipment) and the particular ALS output board. If the field device supports self-test, the ALS board determines the integrity of the wiring and component and performs an application specific action in case of failure. The field testing may be a combination of wire-break, current/voltage level detection and component integrity.

Table 3-1: Self-testing ALS Platform Intervals

a,c,e

Failures related to the FPGA, the busses, and the analog channels are detected, and the effects are mitigated and managed according to the particular application specifications.

3.1.1.3 System Self-Diagnostics

Board failures are separated into four categories: fatal, vital, non-vital, and undetectable. Table 3-2 defines the class of failure used in Board mode of operation. The front plate of each ALS board includes three standard LEDs to indicate the failure category:

- **PWR** – The PWR LED indicates the availability of power to the board. It incorporates the status of the latch micro switches.
- **RUN** – The RUN LED indicates whether the board is operating, or is HALT'ed.
- **FAIL** – The FAIL LED indicates the overall integrity of the board.

Table 3-2: Class of Failure Description

Class of Failure	Description	RUN	FAIL
Fatal	Fatal failures refer to a severe type of failure which compromises the control function of an ALS system. The most fatal failure is the complete loss of input power to the ALS rack. The result is a loss of all ALS board functionality and status indication.	off	off
Vital	Vital failures refer to the class of errors which compromises the integrity and operation of an ALS board. The occurrence of a vital failure will result in immediate loss of the ALS board and human intervention is required to clear the failure. The ALS board will immediately enter the HALT mode, if a vital error is detected. During HALT the ALS board will, if possible, drive its outputs to its predetermined failsafe state.	off	red
Non-vital	Non-vital failures refer to the class of errors which do not affect the overall ALS board performance or integrity. Following one or more non-vital failures, the ALS board is still operable and its integrity has not been compromised, but requires maintenance to operate as specified.	green	red
Undetectable	Undetectable failures refer to the class of errors which do not affect overall ALS board performance or its general integrity. Examples of undetectable failures are LED related circuit failures (wiring, failed LED, driver, etc.). The front-panel provides a wrong indication, but the ALS board will perform the function as specified.	green	unknown

NOTE: A board in "HALT" mode does not mean the ALS platform or the System is inoperable or incapable of performing the intended safety function, but it means that the particular board which has entered the HALT mode is incapable of normal operation and has entered the pre-defined fail-safe state.

NOTE: A green RUN LED and a blank FAIL LED indicates the ALS board performs as specified and all circuits are 100 percent functional and operational, input channels are updated, evaluated, and are in accordance with expected values; output channels are controlled in the manner for which they are intended such that the feedback information received is as expected; and the logic is functional.

3.1.2 Application Diagnostics

Application diagnostics are determined during the safety system design phase. For a reactor trip system application, an example of an application diagnostic is a mismatch check that compares the trip demand (output of the coincidence logic) to a feedback signal derived from auxiliary contacts mounted on the reactor trip circuit breaker. A mismatch occurs if the trip demand signal does not agree with the breaker open signal. For an engineered safety features actuation system (ESFAS) application, an example of an application diagnostic is a check of the continuity through the relay coil that controls the field component. In a main steam feedwater isolation system (MSFIS), an example is the valve position indicator. If the valve position indicator does not correspond with the state the valve is driven to, an application alarm will be issued.

Since these diagnostics are a function of the specific application, they are not described in further detail in this report.

3.1.3 Preferred Failure Mode for Abnormal and Unexpected Inputs

The ALS Input Boards, Core Logic Board and Output Boards are designed with configurability through NVM device programming. The configuration data establishes the specific values for available standard board settings that are required by the system application of the board. The configuration data includes the preferred failure mode for a specific function. The preferred failure mode is the default state of an input or output signal when a failure is detected by the platform or application diagnostics. For each specific safety system application, the ALS system is designed to operate in a known and predictable manner when subjected to unexpected inputs.

3.1.4 ALS Alarm Reset

The CLEAR_ALARM is a manually operated switch located on the Control Panel. If the CLEAR ALARM is enabled, all ALS boards clear all latched alarms in order for the system to resume normal operation, if the alarm condition is no longer present.

The system will remain fully operational while the reset switch is toggled. This means all input channels are updated, and the self-testing continues to monitor the channel circuitry. Further, all outputs are continuously driven according to the application logic specification.

3.2 ALS Platform Maintenance Features

This section presents description of the ALS platform maintenance features. The ALS platform provides for periodic maintenance of an operational system in order to support surveillance testing requirements while the plant is online. The maintenance features includes; analog channel calibration and process set point modification.

The online maintenance features are either: 1) Standard features built into the ALS input and output boards, or 2) Maintenance features which are application specific and built into the CLB.

The ALS platform is designed to support periodic surveillance testing, channel calibration and maintenance on a particular channel, while retaining the capability to accomplish its intended safety functions on the remaining channels. The channel under calibration will enter a pre-determined trip or bypass, based on the plant specific requirements.

This design approach results in the following safeguards and features:

- Only the desired channel of interest is placed in trip or bypass.

- All other safety channels in the same ALS chassis remain on-line and functional (i.e., able to perform their intended safety function).
- All calibration and testing is done through the test ALS bus (TAB), which does not interface with the reliable ALS bus (RAB). This is to ensure there is no data corruption or result in an unintended function.
- Simulated test signals can be injected and monitored at the field terminal blocks. This provides traceability to NIST standards.
- The system can be tested and maintained with the plant on-line.
- Complies with overlap test requirements of RG 1.118 (Reference 38) and IEEE-338 (Reference 36) because channel is tested from field input to field output.
- Complies with Bypass & Inoperable Status Indication requirements of RG 1.47 (Reference 40), because the ALS system immediately generates an alarm when the TAB bus is accessed from the ALS Service Unit (ASU).
- Normal safety signal path is tested (i.e., no alternate or substitution paths).
- Post change surveillance tests can be performed to validate any changes.
- Printouts of "as-found" and "as-left" data are possible via the ASU laptop or qualified display system (QDS).
- A range check is performed in the ASU to guard against out-of-range entries by test personnel.
- Input and output channel calibrations are independent from one another.
- Calibration of one channel on a board does not affect adjacent channels on the same board [

  ]^{a,c,e}.

Application specific surveillance testing requirements are supported by the ALS platform and are determined during application development. Customer input is communicated in their requirements specification or purchase order.

3.3 Maintenance Terminology

The following describes the maintenance terminology used for the ALS platform. In this section, a channel is referred to as an individual input or output of a particular board, used to sense or drive a single field signal.

ALS maintenance terminology:

1) BYPASS
   a. The ability to bypass analog inputs or outputs (I/Os) as a part of calibration.
   b. The ability to bypass an output to ensure it does not change state. Only possible if allowed by the particular board configuration.
   c. The ability to bypass application specific functions within the CLB logic according to the requirements of the application.
   d. When an input channel is placed in Bypass, the channel data reported on the RAB is frozen at the last value it detected before the Bypass was engaged.

i. The CLB is always aware that the data is frozen and generates an ALARM when it sees any data being frozen.

ii. The actual value detected by the input can be read from the TAB bus.

2) OVERRIDE

a. The ability to override analog outputs as a part of a calibration check. The channel must first be placed in Bypass.

b. The ability to override digital outputs to allow for output channel testing or field component testing. Only possible if allowed by the particular board configuration.

3) CALIBRATION

a. The ability to calibrate analog I/O channels to compensate for drift within the ALS platform or drift external to the ALS platform.

b. The ability to calibrate SetPoint parameters (i.e., trip points, time delays, etc.) in the CLB.

The calibration coefficients of a channel can only be changed when the channel is placed in CALIBRATION mode.

A maintenance mode is assigned to each input channel, output channel and SetPoint parameter, and is used to manage changeable parameters, and to notify dependent logic about the validity of the channel or parameter. The maintenance mode of each channel or parameter is independent.

3.4 Calibration of ALS Input and Output Boards

The calibration of an analog input/output channel is performed using the ASU and calibrated external test equipment. The ASU is used to select the channel to be calibrated and place that particular channel in BYPASS mode before the external test equipment is connected to the channel wiring on test points located on the field terminal blocks.

Each analog input/output channel shall be in [ ]^{a,c,e} maintenance modes of operation as illustrated by Figure 3-2. [

]^{a,c,e}

[ ] a,c,e

Figure 3-2: Maintenace Modes for Analog Input/Output Channel

[ ] a,c,e

[

]

a,c,e

3.5 Test of Digital Output Boards

The following ALS boards with digital output channels do not require any type of calibration. Any deviation from the nominal or specified operation will be deemed a failure. This is detected by either the board self test or during system surveillance testing.

- ALS-102 – Core Logic Board
- ALS-402 – Digital Output Board
- ALS-601 – Communication Board

Any deviation from the nominal or specified operation of these boards will be deemed a failure. This is detected by either the board self test or during system surveillance testing.

The digital output boards, will in some cases, still make use of the maintenance modes. An example of this is the ALS-402 Digital Output Board, which can be configured to allow for a particular output being placed in BYPASS mode, [ ]a,c,e. When a digital output channel is placed in BYPASS mode it will notify the CLB that it will no longer accept data from the RAB bus. In BYPASS mode the output channel state is frozen. [

]a,c,e

Each digital channel output will always be in [ ]a,c,e maintenance modes of operation as shown in Figure 3-3. [

]a,c,e

[

]

a,c,e

Figure 3-3: Maintenance Modes for a Digital Output Channel

[

]

a,c,e

a,c,e

3.6 Maintenance of Set Points

This section describes the maintenance features implemented in the CLB to allow for changing Set Points.

The Set Point values are protected by the same mechanism in the field programmable gate array (FPGA) logic that is used to store calibration coefficients in the analog board. Each Set Point may be modified in the same way that a single analog channel may be changed. This allows similar FPGA logic to be used to protect calibration coefficients and Set Points.

NOTE: *When creating a system specification for a specific application, it will be determined which Set Points are necessary.*

Each Set Point will always be in [ ]^{a,c,e} of operation as shown in Figure 3-4. [

]^{a,c,e}

a,c,e

Figure 3-4: Maintenance Modes for a Set Point

a,c,e

The maintenance mode for each individual Set Point may be used by the CLB logic to place outputs in a bypassed or tripped state.

4 Equipment Qualification

This section of the topical report details the qualification of the ALS platform hardware and associated equipment described in Section 2.

The objectives of the ALS platform hardware qualification are 1) to demonstrate that the ALS platform hardware will perform its intended safety functions during and after abnormal service conditions of temperature, humidity, power source, radiation, and seismic and 2) to verify that the test methods meet all applicable standards and regulatory guidance requirements.

The ALS test program for equipment qualification includes the following:

- Environmental Qualification: Temperature, humidity, power source voltage and power source frequency tests verify that the ALS hardware will operate in a mild environment.

- Seismic Qualification: Seismic tests verify the structural integrity and operability of the ALS platform during and after a design basis seismic event.

- EMC Qualification: Emissions, susceptibility, electrical fast transient (EFT), surge, and electrostatic discharge (ESD) tests verify the operability of the ALS platform in the presence of external noise sources and electrostatic discharges while also verifying that the ALS platform will not impact similarly tested equipment.

The testing on the ALS platform is contained in CS Innovations document [ ]^{a,c,e}.

4.1 Environmental Qualification

The ALS platform is qualified for Class 1E installation in a mild environment per WCAP-8587, Revision 6-A, (Reference 10) and IEEE Standard 323-1974 (Reference 73), which was endorsed by Regulatory Guide 1.89 (Reference 11).

Criteria for environmental qualifications of safety related equipment are provided in 10 CFR Part 50, Appendix A, "General Design Criterion (GDC) 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases" (Reference 12). Additionally, 10 CFR 50.55a (h) (Reference 6) incorporates IEEE Standard 603-1991 (Reference 7), which addresses both system-level design issues and quality criteria for qualifying devices. Section 5.4 of IEEE Standard 603-1998 states that it is used in conjunction with the equipment qualification requirements for safety systems, IEEE Standard 323-2003 (Reference 13).

To comply with the requirements of GDC 4, 10 CFR 50.49, and IEEE 603-1991, it must be demonstrated through environmental qualification that instrumentation and control (I&C) systems meet design-basis and performance requirements when the equipment is exposed to normal and adverse environments.

4.1.1 Temperature/Humidity

Mild environment is defined as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." The ALS is located in a mild environment area in the nuclear power plant. WCAP-8587, Revision 6-A, outlines normal and abnormal operating environments, as shown in Table 4-1.

Table 4-1: Normal and Abnormal Operating Environments per WCAP-8587, Rev. 6-A

a,c,e

During qualification testing, since the ALS platform is not tested inside a cabinet, heat rise is accounted for by adding 20°F to the parameters identified above. To provide additional margin, the two cycles indicated above are repeated, consisting of 2 normal cycles and 2 abnormal cycles. An additional low temperature cycle is added after the four original cycles per CENPD-255, Revision 3 (Reference 72). Figure 4-1 shows the generic environmental profile.

a,c,e

Figure 4-1: Generic Temperature Profile

The ALS platform performance criterion that is demonstrated during environmental testing includes on-demand actuation, no spurious trips, and performance to the timing and accuracy requirements specified as part of the design. The input voltage and frequency are also varied in accordance with the requirements in Clause 4 of IEEE Standard 603-1991, including the margin specified in Clause 6.3.1.6 in IEEE Standard 323-2003.

Figure 4-2: Deleted

4.2 Seismic

The ALS platform is qualified for Seismic Category 1 events per IEEE Standard 344-1987 (Reference 14), which is endorsed by Regulatory Guide 1.100 Revision 2 (Reference 15) and WCAP-8587 Revision 6-A.

Clause 4 of IEEE Standard 344-1987 states that the seismic qualification of Class 1E equipment should demonstrate an equipment's ability to perform its safety function during and after the time it is subjected to the forces resulting from one safe shutdown earthquake (SSE). In addition, the equipment must withstand the effects of a number of operating basis earthquakes (OBEs) prior to the application of an SSE as noted in WCAP-8587 Revision 6-A.

To demonstrate that the ALS platform functions during a seismic event, the test specimen is subjected to a series of seismic simulation tests using a tri-axial seismic simulator shake table. These tests include resonance search tests, five OBEs, and an SSE in accordance with IEEE Standard 344-1987.

The test specimen consists of the ALS platform mounted in a fixture to simulate the actual in-service configurations. The fixture is then mounted to a tri-axial seismic simulator table such that the principal axes of the specimens are collinear with the input excitations of the test table. Accelerometers are also mounted to the test table and the test specimen to record the in-equipment acceleration levels.

Pre-seismic baseline testing, seismic monitoring, and post-seismic baseline test data supports the ability of the equipment to operate during and after a seismic event. The acceptance criterion for the seismic testing includes no loss of safety function, no spurious actuations, and performance within the vital accuracy and timing requirements. Additionally, the equipment must not experience structural failures, such as broken or loose parts that could become a missile hazard.

4.2.1 Pre-Seismic Inspection and Operability Check

The ALS test specimen is examined upon arrival at the test facility to verify that no damage has occurred during shipping and handling. A baseline functional test to verify the operability of the equipment is conducted prior to testing.

4.2.2 Resonance Search Test

The ALS test specimen is subjected to a resonance search test consisting of a single-axis sine sweep in each of the three orthogonal axes. Sine sweeps are performed from 1 Hz to 100 Hz at a sweep rate of one octave per minute. The results of these tests demonstrate any resonance below 100 Hz in each of the three orthogonal axes and can be used to relax the enveloping of the required response spectra (RRS) as noted in Clause 7.6.3.1 of IEEE Standard 344-1987.

4.2.3 Qualification Seismic Tests

The ALS platform is Class 1E and designated Seismic Category 1. It is designed and qualified to withstand the cumulative effects of a minimum of five (5) OBEs followed by one (1) SSE without loss of safety function or physical integrity.

Table 4-2 lists the seismic test runs for the ALS platform.

Table 4-2: Seismic Test Runs for the ALS Platform

a,c,e

[

]a,c,e

a,c,e

Figure 4-3: SSE RRS, Horizontal Direction, 5% Damping

The ALS platform must operate during and after each seismic event. Operation is defined by the following capabilities:

1. The ALS platform demonstrates no spurious actuations of safety functions
2. The ALS platform actuates all safety functions on command
3. The ALS platform operates all safety functions within the required accuracy specifications
4. The ALS platform executes all safety functions within the required time responses

4.2.4 Post-Seismic Baseline Test and Operability Check

The ALS test specimen operation during and after the seismic test is recorded for verification and comparison after testing. The test specimen is also visually examined at the conclusion of the seismic test to verify the operability and structural integrity of the test specimen. A baseline test conducted on the test specimen after completing the seismic testing further verifies that the test specimen was not impacted by the seismic events by comparison with the initial baseline test results.

For each application specific project, an evaluation will need to be performed to determine that the ALS platform qualifications exceed the specific plant's seismic requirements.

4.3 Electromagnetic Compatibility (EMC) Testing

The ALS platform is qualified for electromagnetic compatibility per Regulatory Guide 1.180 Revision 1 (Reference 16). The specific test methods found in MIL-STD-461E (Reference 17) and the IEC 61000 series that have been endorsed by Regulatory Guide 1.180 are applied to the ALS platform. These tests are reasonable methods of evaluating the effects of conducted and radiated electromagnetic interference (EMI), radiofrequency interference (RFI), and power surges on safety related I&C systems as noted in Regulatory Guide 1.180.

Regulatory Guide 1.180 also mentions in the discussion section that both Regulatory Guide 1.180 and EPRI TR-102323 Revision 1 (Reference 18) present acceptable means for demonstrating EMC, and that the licensee or applicant has the freedom to choose either method. It should be noted that for some types of testing, the maximum acceptable limits for emissions or susceptibility are different and, therefore, it is possible that tested equipment may meet the requirements of one test, and not meet the requirements of the equivalent test from the other document. For the purposes of the ALS platform, Regulatory Guide 1.180 serves as the qualification basis and any tests from EPRI TR-102323 are considered optional and above the requirements.

Position 3 in Regulatory Guide 1.180 states that there should be no mixing and matching of test methods for emissions testing. Position 4 in Regulatory Guide 1.180 similarly states that there should be no mixing and matching of test methods for susceptibility testing. To be in accordance with these two positions, the approach taken to qualify the ALS platform includes applying the MIL-STD-461E set of tests for emissions testing, and the IEC 61000 series set of tests for susceptibility and surge testing. Position 6 requests further testing to MIL-STD-461E test RS103 to cover the 1 GHz to 10 GHz range when using the IEC 61000 series for susceptibility, rather than extending the test range of IEC 61000-4-3 (Reference 19) up to 10 GHz.

Before and after every qualification test, an operability check on the test specimen is used to verify equipment operation before continuing with testing. A baseline test is performed before and after the entire set of EMC testing to verify that the operation of the test specimen is not affected.

EMC testing of the ALS includes the following:

- EMC Pre-Test Inspection and Baseline Testing
- Qualification Level EMC Emissions Testing
- Qualification Level EMC Susceptibility Testing
- Qualification Level EMC Surge Withstand Capability Testing
- EMC Post-Test Inspection and Baseline Testing

The ALS platform must operate during and after each EMC test unless otherwise noted in the sections that follow. Operation is defined by the following capabilities:

1. The ALS platform demonstrates no spurious actuations of safety functions
2. The ALS platform actuates all safety functions on command
3. The ALS platform operates all safety functions within the required accuracy specifications
4. The ALS platform executes all safety functions within the required time responses

4.3.1 EMC Emissions

The objective of EMC emissions testing is to reasonably ensure that the ALS platform will not interfere with the function or operation of other power plant equipment. As with the other qualification testing, the test setup for EMC tests consists of an ALS rack without the benefit of a shielded cabinet.

Both conducted and radiated emissions testing are performed on the ALS in accordance with MIL-STD-461E test methods. These tests measure the conducted and radiated electric field emissions, as well as the radiated magnetic field emissions from the enclosure and cables of the ALS test specimen. The acceptance criterion for all emissions testing consists of meeting the levels specified by Regulatory Guide 1.180 for each individual test. The EMC emissions tests and their frequency ranges are listed in Table 4-3

Table 4-3: EMC Emissions Tests and their Frequency Ranges

a,c,e

The ALS platform is also designed to meet the optional test levels for MIL-STD-461E test RE102 found in EPRI TR-102323 Rev 3 (Reference 20). These levels are more stringent than those specified in Regulatory Guide 1.180 and are intended to help protect against impacts from portable transceiver devices. Adherence to the EPRI TR-102323 levels is considered optional and is compared for information only.

4.3.2 EMC Susceptibility

The objective of EMC susceptibility testing is to reasonably ensure that the ALS platform will function and operate as designed when installed in the industrial electromagnetic environment of a power plant.

Both conducted and radiated susceptibility testing are performed on the ALS platform in accordance with the IEC 61000-4 test methods. In addition to IEC susceptibility tests, the MIL-STD-461E susceptibility test RS103 is performed to extend the test range up to 10 GHz as proposed in Position 6 of the Regulatory Guide 1.180. Table 4-4 lists the EMC susceptibility tests, excluding surge withstand tests.

Table 4-4: EMC Susceptibility Tests, Excluding Surge Withstand Tests

a,c,e

EMC Test	Description	Range
IEC 61000-4-3	Radiated electric field susceptibility	26 MHz to 1 GHz
IEC 61000-4-6	Disturbances induced by radio-frequency fields conducted susceptibility	150 kHz to 80 MHz
IEC 61000-4-8	Radiated magnetic field susceptibility	50 Hz and 60 Hz
IEC 61000-4-9	Radiated magnetic field susceptibility	50/60 Hz to 50 kHz
IEC 61000-4-10	Radiated magnetic field susceptibility	100 kHz and 1 MHz
IEC 61000-4-13	Low-frequency conducted susceptibility	16 Hz to 2.4 kHz
IEC 61000-4-16	Common-mode conducted susceptibility	15 Hz to 150 kHz
RS103	Radiated electric field susceptibility	1 GHz to 10 GHz

4.3.3 Surge Withstand Capability

The objective of surge withstand testing is to verify the ability of the equipment to withstand high-energy over voltage conditions on power and interconnection lines.

Surge withstand testing is performed on the ALS platform in accordance with IEC 61000-4 test methods as listed Table 4-5 below.

Table 4-5: IEC 61000-4 Test Methods

a,c,e

EMC Test	Description	Range
IEC 61000-4-4	Electrical fast transient/ burst immunity	Power: Level 4 (4 kV) Signal: Level 4 (2 kV)
IEC 61000-4-5	Surge combination wave immunity	Power: Level 4 (4 kV) Signal: Level 3 (2 kV)
IEC 61000-4-12	Surge ring wave immunity	Power: Level 4 (4 kV) Signal: Level 3 (2 kV)

4.3.4 Electro-Static Discharge (ESD)

EPRI TR-102323 specifies IEC 61000-4-2 "ESD Withstand Testing" (Reference 21) as an optional test, because electrostatic discharge is not considered a common mode failure mechanism for safety related systems. An ESD test is not required by Regulatory Guide 1.180 and is therefore performed for information only.

The objective of ESD testing is to verify the ability of the ALS platform to withstand electrostatic discharges. Data from the testing is used to assess whether additional precautions, such as ESD wrist straps, are required when working in the same region as the equipment.

The ALS platform is designed to meet IEC 61000-4-2, level 4 (15 kV air discharge/8 kV contact discharge). The test is conducted at the locations most likely to come into human contact while the equipment is operational, including handles, rails, switches, lamps, and connectors.

Table 4-6: ESD Test

EMC Test	Description	Range
IEC 61000-4-2	Electrostatic discharge immunity test	Level 4 (15 kV air discharge, 8 kV contact discharge)

4.3.5 Deleted

4.4 Deleted

5 ALS Platform Communications

The ALS platform supports external data communication in a manner that meets regulatory requirements. The external communication interfaces consist of the following categories:

- Safety to safety communication data links within the same division
- Safety to safety communication data links between different divisions
- Safety to non-safety communication data links

These communication data links support the performance of the safety function, provide signals to control and indication functions, and support maintenance, testing and troubleshooting of the equipment.

Except for the TAB bus interface to the ASU, all external communication data links are one-way, point-to-point using qualified isolation devices, where required. The TAB bus is discussed in Section 5.3. The external communication channels do not utilize handshaking or acknowledgement. The ALS Platform utilizes a qualified isolation device when physical separation and electrical isolation between redundant portions of safety systems and/or between safety and non-safety systems is required.

5.1 Intra-Divisional Communication

For safety applications that require communication data links between multiple ALS chassis within a safety division, the ALS-601 Communications Board and the RAB bus are utilized. As an example, one ALS chassis within a safety division may perform the process signal acquisition and comparator function, and communicate the result to a second ALS chassis that performs the coincidence logic function (e.g., two-out-of-four logic). Isolation is not required for communication data links between multiple ALS Chassis within a safety division.

The RAB bus is the primary bus that connects boards within an ALS chassis. The RAB bus also connects to ALS expansion chassis to provide additional I/O capabilities. The RAB is described in detail in Section 2.3.1 and the connection scheme of connecting multiple ALS expansion chassis together is described in Section 2.5.8.

The ALS-601 Communications Board is utilized in the situation where intra-divisional communication is required between ALS chassis. Intra-divisional communication using the ALS-601 Communications Board is described in section 5.2, since the ALS platform handles intra-divisional and inter-divisional communications in a similar manner.

For safety applications that require communication data links between an ALS chassis and a fixed installed Qualified Display System (QDS) within the cabinet, one of the TxB communication channels from the CLB or the ALS-601 Communication Board can be used. A QDS is typically used for the following safety applications:

- Post Accident Monitoring System (PAMS) for RG 1.97 (Reference 59) compliance
- Reactor Vessel Level Indication System (RVLIS)
- Core Subcooling Margin Monitor (SMM)
- Inadequate Core Cooling Monitor (ICCM)
- Thermocouple Core Cooling Monitor (TCCM or CETM)

Isolation is not required for communication data links between an ALS chassis and a QDS within the same safety division. The QDS may also serve as the ASU for communication with the TAB bus. The TAB bus, which is used for test, calibration, and maintenance functions, may also be regarded as an intra-divisional communications bus; however, because the ASU may be non-safety, the TAB bus is covered in section 5.3.

5.2 Inter-Divisional Safety-to-Safety Communication

Inter-divisional communication is utilized within the ALS platform to implement voting where inputs from multiple safety divisions are required. An example of this voting: one ALS Chassis in Division I may perform the process signal acquisition and comparator function, and communicate the result to Train A and Train B ALS Chassis that receives comparator information from all four divisions and performs the coincidence logic function (e.g., two-out-of-four logic), as shown in Figure 5-1.

The ALS-601 Communications Board is utilized for the multiple safety division voting as described above. This application requires communication channels between ALS chassis located in different separation groups. In order to achieve electrical isolation and communication independence between separation groups, all inter-division communication between ALS chassis use isolated, point-to-point, one way serial communication. Where the transmit port is connected to receive port.

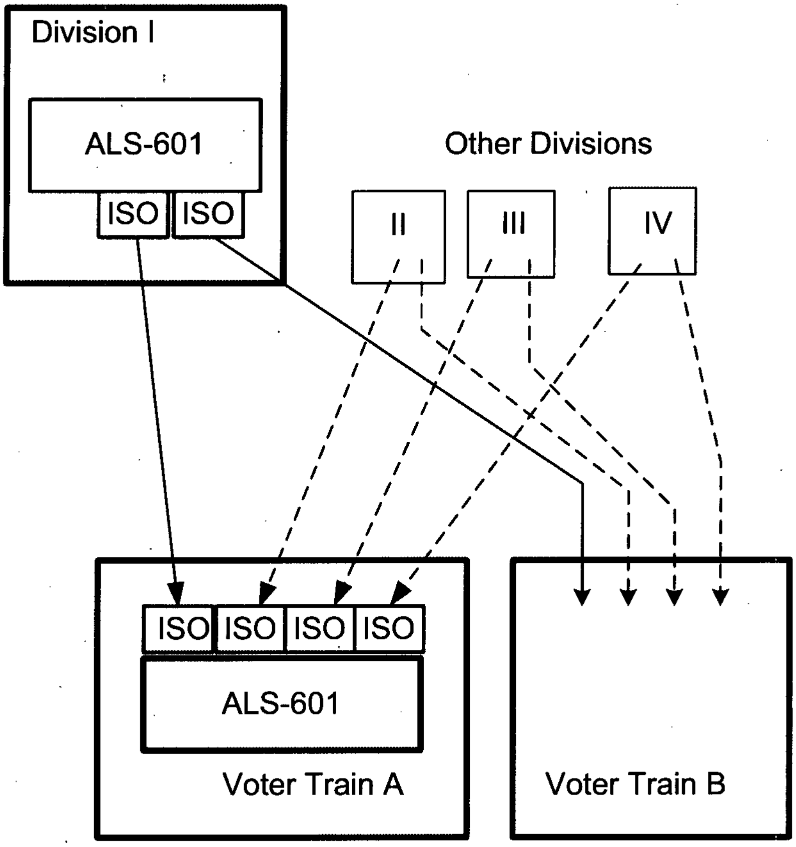

Figure 5-1: Safety to Safety Interdivisional Communications

The transmit channel of the transmitting ALS-601 Communication Board is connected to the receive channel of the receiving ALS-601 Communication board.

The Application Logic of the CLB in the transmitting ALS chassis will be configured to send data values at a fixed interval as predetermined by the application logic. No handshaking is incorporated for this data exchange with the receiver. The CLB will continue to transmit the predetermined values regardless of the condition and availability of the receiver. The condition of the transmit channel shall in no way affect the safety functions of the CLB in the transmitting division.

[

]a,c,e

Separation and independence of the communication function between safety divisions from the safety function processes is guaranteed by utilizing separate ALS boards (i.e., the ALS-102 CLB and the ALS-601 Communication Board) for each purpose, as well as the configuration of the ALS-601 Communication Board. This approach:

(1) Does not use common components for the safety function and communication function.

(2) Maintains functional and physical separation between CLB and ALS-601 Communication Board.

(3) Maintains electrical independence from the non-safety system.

5.3 Inter-Divisional Safety-to-Non-Safety Communication

Typical safety system applications require communication data links from the safety related ALS chassis to non-safety equipment. The ALS platform provides for three types of communication data links that can be used for this purpose, as shown in Table 5-1.

Table 5-1: Inter-divisional Safety-to-Non-Safety Communication

Communication bus	Typical Purpose / Use case	Type
ALS-601	Digital Indicators/recorders	Unidirectional
TxB	QDS, plant computer, or plant data highway	Unidirectional, Tx Only
TAB	ASU, QDS for test, diagnostics, maintenance and troubleshooting	Bidirectional

5.3.1 Broadcasting Information to Non-Safety Devices Using ALS-601

For communication data links to non-safety equipment the ALS-601 Communications Board is used in much the same manner as described above for communication data links between different separation groups. In order to achieve electrical isolation and communication independence between the safety related ALS Chassis and the non-safety equipment, qualified isolation devices are used in conjunction with point-to-point, one way serial communication (transmit port connected to receive port). The output port of the transmitting ALS-601 Communication Board is connected to the input port of the receiving equipment.

Information transmitted from the ALS-601 Communication Board cannot impact the safety functions performed by the CLB. Separation and independence of the communication data link between the safety functions and the non-safety system is guaranteed by using separate ALS boards (i.e. the ALS-102 CLB and the ALS-601 Communication Board) for each purpose, and the configuration of the ALS-601 board. This approach:

(1) Does not use common components for safety function and communication function.

(2) Maintains functional and physical separation between CLB and ALS-601 Communication Board.

(3) Maintains electrical independence from the non-safety system.

5.3.2 Broadcasting Information to Non-Safety Devices Using TxB Busses

The ALS platform contains two dedicated communication channels for broadcasting information to external safety and non-safety systems. The TxB1 and TxB2 communications channels are unidirectional, one way, communication data links. The TxB1 can be used for one way communication to the non-safety ASU or the safety QDS, as shown in Figure 5-2. The TxB2 can be used for one way communication to other non-safety equipment, such as the plant computer or main control room display.

The TxB busses have the same properties as described for the ALS-601 Communication Board, except for the location of the communication hardware. The communication hardware is located within the CLB FPGA, but is implemented with independent logic circuits. The communication logic circuit does not interact with the safety function logic circuit; rather it is non-intrusively monitoring the safety function logic circuit. A failure of the TxB communication circuit cannot prevent the performance of the safety function.

a,c,e

Figure 5-2: Communication between ALS and a safety QDS (left) and non-safety ASU (right)

5.3.3 Communication with Non-Safety Devices Using the TAB Bus

The TAB is a bidirectional communication data link used between the ALS chassis and the ASU for test, calibration and maintenance functions. The segregation of safety data on the RAB from test and maintenance information on the TAB, as described in Section 2.3.2, provides the communications independence as required by IEEE 7-4.3.2 (Reference 4) for communication between safety and non-safety computers.

The ALS chassis to ASU interface over the TAB is a bidirectional communications channel. The data link is operational only after the activation of the COMM ENABLE key switch on the local Control Panel. The COMM ENABLE key switch is provided as an input to the safety logic circuit located in the FPGA on the CLB. The ALS chassis generates an alarm status signal when an ASU-to-ALS chassis communication channel is enabled. The ALS chassis also indicates there is an active TAB communication channel on the front panel. The ASU is a laptop PC, or the ASU functionality can be within a QDS mounted within the cabinet to limit access. Both of these scenarios are shown above in Figure 5-2. In either case, it executes a software application with a proprietary data protocol to exchange data with the ALS Chassis.

The ASU sends data requests to the ALS chassis to obtain troubleshooting information. The ALS chassis provides test and diagnostics data back to the ASU and the ASU displays the test and diagnostic data. The ASU also provides data commands to the ALS chassis to support testing of its supported safety function.

[

]a,c,e

The ASU and its application are non-safety and shall be utilized in accordance with administrative controls. These administrative controls for the use of the ASU and the non-safety connection to the ALS chassis are application specific and plant specific.

The communication data links described maintain separation between safety and non-safety systems, and do not compromise the independence of redundant portions of the safety system when used in accordance with identified administrative controls.

5.4 Multidivisional Control, Display and Management

Section 3 of Interim Staff Guidance 04 (ISG-04) (Reference 60) provides guidance concerning multidivisional control, display, and maintenance. Specifically, the concerns related to a central computer or operator workstation controlling safety related equipment in multiple divisions simultaneously. Further, the concerns related to a central computer or operator workstation that can be used to program, modify and maintain safety related equipment in multiple divisions simultaneously.

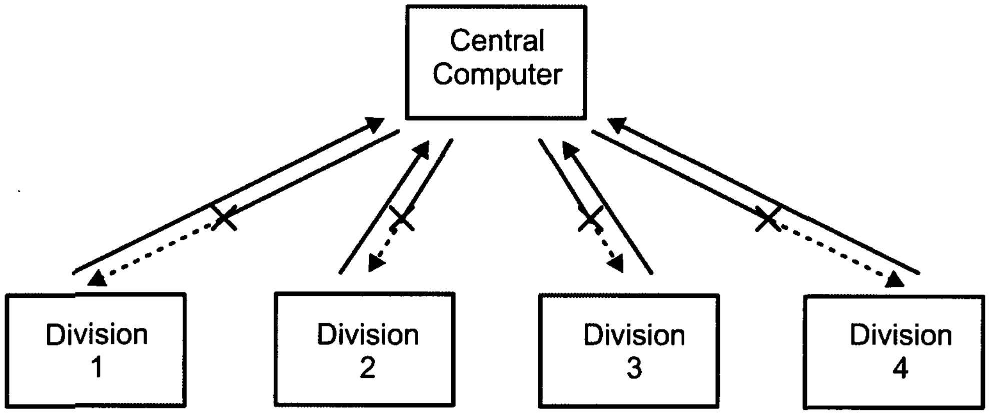

Figure 5-3: Control and Maintenance from Central Computer

5.4.1 Multidivisional Control in Multiple Safety Divisions

The ALS platform does not provide for any options to connect the ALS chassis to a central computer (or operator workstation). The ALS platform does not have a priority module type functionality built in, and can therefore not serve as a priority voter. The ALS platform has one option to receive information. This would be with the use of an ALS-601 communication link configured as an input. This would allow an ALS-601 chassis to receive information (safety related) and use it as needed. The support of this type of information input is application specific, and can only be tested on an application basis as part of the ALS-102 testing.

The ALS platform could provide information to (and only to) a central computer (or operator workstation), using the TxB busses or ALS-601 as described earlier.

5.4.1.1 Multidivisional Maintenance in multiple safety divisions

The ALS Platform does not provide for any options to connect the ALS chassis to a central computer (or operator workstation) that would be capable of programming, modifying or maintain the boards within the ALS chassis.

The TAB bus, is a point-to-point style bus, and does not support communication to chassis in multiple divisions simultaneously.

To reprogram or modify the FPGA image on an ALS board, the board must be removed from the chassis. The modification of the FPGA image cannot be accomplished by remotely connecting an operator workstation.

The NRC Task Working Group #4, "Highly Integrated Control Rooms – Communications Issues" has provided interim staff guidance on the review of communications issues. DI&C ISG-04 contains three sections: 1) Interdivisional Communications, 2) Command Prioritization, and 3) Multidivisional Control and Display Stations. Table 5-2 and Table 5-3 respectively provide details regarding ALS platform compliance to ISG-04 for interdivisional and multidivisional communications.

Table 5-2: ALS ISG-04 Compliance Matrix – Interdivisional Communications

a.c.e

a,c,e

a,c,e

a.c.e

a.c.e

a,c,e

a.c.e

a.c.e

a,c,e

Table 5-3: ALS ISG-04 Compliance Matrix – Multidivisional Communications

a,c,e

a,c,e

a.c.e

a.c.e

a.c.e

6 Life Cycle Management Process

The ALS platform development is structured to follow a traditional waterfall lifecycle that includes a top-down requirement and specification development, design implementation, and a bottoms-up verification and validation (V&V) effort at each level of integration. Prototyping activities and in-process quality assurance efforts are executed integral to the development stages. The NRC staff has reviewed the development process of the MSFIS application of the ALS platform in Docket 50-482, amendment 181 to License No. NPF-42 (Reference 2), as written in the USNRC Safety Evaluation Report (SER) (ML#090610317) (Reference 70), and determined that the process may be suitable for reference when developing new boards that comply with the ALS platform architecture, or when applying the ALS platform to other safety-related uses in nuclear power plants. The following summarizes the process.

6.1 Development Process

The lifecycle that is used for the development of ALS boards and systems is discussed in this section.

6.1.1 Planning Stage

The Planning Stage includes concept, planning, and requirements phases and is the initial step of the project lifecycle. As part of this planning, the project execution strategy is established, resources are identified, and organizational interfaces are defined. The major outputs of this phase are the planning documents for the project.

6.1.2 Development Stage

The Development Stage begins with collecting and analyzing the requirements. From the requirements, the detailed designs are completed, and then the designs are translated into the hardware. First article boards are built and a complete validation of the design is performed. This validation includes the verification and validation efforts as well as the equipment qualification testing. The outputs of this stage include the specifications, design drawings, design analyses, test plans, and test reports.

6.1.3 Manufacturing Stage

In the Manufacturing Stage, the production hardware is fabricated and tested, producing functional hardware ready to be integrated into the system. The outputs of this stage include the production hardware and the test documentation. These documents are project specific and thus created for each application.

6.1.4 System Test Stage

During the System Test Stage, the verified hardware components produced in the manufacturing stage are integrated into a completed system capable of performing the functions described in the requirement specifications. The system tests provide a complete verification of the system requirements. The output of this stage includes the test documentation. These documents are project specific and thus created for each application.

6.1.5 Installation/Operation Phase

This Installation Phase includes the factory testing, installation in the plant, and testing the completed system in the plant. After the system testing in the plant is completed, the operation of the equipment is done by the utility. The outputs of this stage include the hardware and test documentation. These documents are project specific and thus created for each application.

6.2 Life Cycle Planning Documentation

SRP BTP 7-14 contains documentation requirements that are required for a digital platform. ISG-06 is draft guidance that clarifies the documents that are required to enable the NRC to complete its review. A mapping of the documentation to the documents required by ISG-06 is included in Section 12.

6.3 Verification and Validation

V&V activities are performed in a bottoms-up fashion that progresses from the FPGA digital logic programming level, to the board level, and then to the system level. [

]^{a,c,e} The IV&V team is independent in management, schedule, and finance. The verification activities are summarized in the following sections.

6.3.1 Field Programmable Gate Array V&V

The field programmable gate array (FPGA) is subjected to in-process V&V activities that are integral to the development of the device. [

]^{a,c,e} The purpose of this verification is to validate that the design performs as intended.

In addition, the IV&V team is used to validate the design. The IV&V efforts are performed in parallel with the design, and the scope of the review covers the requirements through the final system testing. [

]^{a,c,e}

6.3.2 Board V&V

After the FPGA V&V is completed, the board is configured with a configuration-controlled version of the FPGA. The board is tested using a test fixture that has been developed to test the board's compliance against its requirements and specifications. [

]^{a,c,e}

6.3.3 System V&V

For each system, the boards are installed into an operational configuration. The system V&V utilizes a test fixture with external interface simulators to exercise the system against application-specific scenarios. [

]^{a,c,e}

7 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, field programmable gate arrays (FPGAs), line drivers, and 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, interconnects, 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 of this simplicity is lower heat dissipation, which increases the overall system life and ensures a high level of system availability. The ALS is designed using very conservative design guidelines ensuring that the boards and their components are operating in a safe area of operation where reliability is maximized.

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 mitigated by incorporating inherent ALS platform diversity using diversely configured FPGAs. This process only uses proven design practices and methodologies for implementation of the hardware.

7.1 Failure Modes and Effects Analysis (FMEA)

A failure modes and effects analysis (FMEA) is a procedure for analyzing potential hardware or programming failure modes within a system for determination of the effect of failures on the system. This information can then be used to assess the potential for an undetectable failure or a common mode failure. Each specific application of the ALS will have its own safety assessment containing a system level FMEA. For the ALS platform, the FMEA for each board is a part of the board's hardware design specification.

7.2 Reliability and Availability

The reliability and availability goals for each application will be based on requirements of the plant application. The analysis will demonstrate that the overall goals are satisfied. To support this analysis, each board in the ALS platform has a mean time between failure (MTBF) calculation that is documented in the board's hardware design specification.

8 Security

8.1 ALS Platform Security Overview

The ALS platform is based on a robust architecture and development process that in combination provide high assurance that a nuclear power plant safety control system based on the ALS platform cannot be compromised by security threats.

Document [ ]^{a,c,e}, establishes the approach for applying the security-related regulatory guidance, standards and CS Innovations processes throughout the ALS platform's life cycle to address security risks. The following CSI project life-cycle activities are addressed in the ALS Security Plan:

- Planning
- Development
- Manufacturing
- System Test, Installation and Maintenance

a,c,e

The NRC staff reviewed the security provisions of the MSFIS application of the ALS platform in Docket 50-482, amendment 181 to License No. NPF-42 and, as written in the SER (ML#090610317), and determined that cyber security considerations were satisfactorily addressed within the development. The approach to security is fundamentally the same as the approach that was reviewed and described in the SER with improvements, as defined in this document, to address developments in the regulatory environment.

8.2 Life Cycle Security

The following section discusses ALS development process and how security is addressed in each activity of a digital safety system life cycle to meet the intent of RG 1.152, Rev. 3, "Criteria for use of Computers in Safety Systems of Nuclear Power Plants" (Reference 26).

8.2.1 Planning Activity

The Planning Activity includes the concept and requirements activities listed in RG 1.152. [

]^{a,c,e}

8.2.2 Development and Manufacturing Activities

The Development Activity includes the design, manufacturing (implementation), and test activities.
[

]^{a,c,e}

8.2.3 System Test, Installation, and Maintenance Activities

Once an authorized purchase order or internal work order is received, the associated ALS platform components are removed from Class 1E storage and delivered to the requestor. If delivered to an internal requestor, the security of the component continues to be under the control of CS Innovations. If delivered to a plant licensee, the responsibility for security transitions from CS Innovations to the plant licensee at the installation activity.

ALS platform maintenance activities include modifications, migration, and replacement of ALS platform components. These types of maintenance activities use the same security methods used during the earlier portions of the life cycle. The exact methods employed depend on the type of activity and are application-specific.

8.3 ALS Platform Security Methods and Features

The ALS platform implements acceptable methods that can be used by licensees and applicants to assist in their licensing of a protection system. The methods address control over 1) physical and logical access and 2) data communication with other systems. The types of methods used include:

- ALS platform security features
- Test, maintenance, and calibration
- Communication
- Control of access

Details of the methods used are provided in the [ ]^{a,c,e}.

9 Diversity

The ALS platform uses key design attributes which are sufficient to eliminate the consideration of software common cause failure (SWCCF). These design attributes provide two levels of diversity features. 1) Core Diversity; is the fundamental level of diversity which can be used in simple applications. 2) Embedded Design Diversity; adds additional design diversity and is intended for more complex applications. This section provides further explanation of these diversity levels.

9.1 Implementation of Diversity to Address Common Cause Failure

The ALS platform incorporates two levels of diversity: Core Diversity and Embedded Design Diversity. The first level, Core Diversity, is implemented for each of the FPGAs on all of the ALS boards. Each of the FPGA images contains two sets of redundant hardware logic, called a core, as shown in Figure 9-1 below. The diversity between the two cores is achieved by changing the logic implementation during the synthesis and Place & Route process. The synthesis process utilizes the hardware descriptive language (HDL), which is a formal specification of the configuration of the hardware circuits to be implemented in the FPGA. The synthesis of the HDL is performed using one type of hierarchical structure, finite state machine (FSM) encoding, and state decoding for the first set of logic in the core and a second type of hierarchical structure, FSM encoding, and state decoding for the second set of logic in the core. The logic for each of the two cores then undergoes the place and route process, and is then tested to validate proper operation. [

]a,c,e This results in design that provides a FPGA image with two cores for redundancy as well as diversity.

[ ] a,c,e

Figure 9-1: FPGA with Redundant Cores

The second level of diversity, Embedded Design Diversity, implements additional design diversity. [

]a,c,e The final result is two diverse FPGA images, A and B, which implement the same functionality in a diverse manner.

The level of diversity employed for a particular application is determined by the complexity of the application. For simple systems, such as post-accident monitoring systems, only Core Diversity is required. For more complex systems, such as a system receiving sensor signals and making trip or actuation determinations, the additional level of Embedded Design Diversity shall be employed. Examples of how the diversity is implemented for various applications are shown in Section 9 and in the Appendices of this document.

9.2 NUREG/CR-6303 Diversity Evaluation

The ALS uses different techniques to provide diversity within the system. These implementations are described in the previous section. The evaluation examines each of the elements of diversity included in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems" (Reference 28). The details of this evaluation are included in [ ]^{a,c,e} (Reference 49). The evaluation concluded that sufficient diversity is provided, when both levels of diversity are employed, for complex applications, such as those for a system receiving sensor signals and making trip or actuation determinations.

9.3 Typical Applications of Diversity

As described above, the ALS Platform provides Core Diversity for simple systems, and Embedded Design Diversity can be added for more complex systems. The following illustrates typical applications of the two levels of diversity. Additional details on typical applications are provided in the appendices.

9.3.1 Diversity within the ALS FPGA

For simple systems, only Core Diversity is used. [

]^{a,c,e}

[ ]a,c,e

Figure 9-2: Diversity within the ALS FPGA

9.3.2 Diversity Between Chassis

For systems that require diversity between trains, both Core Diversity and Embedded Design Diversity is required. [

]^{a,c,e}

a,c,e

Figure 9-3: Diversity Between Chassis

9.3.3 Diversity Within Separation Groups

For systems that require the highest level of diversity, both Core Diversity and Embedded Design Diversity is required. [

]a,c,e

a,c,e

Figure 9-4: Diversity within Separation Groups

10 Quality Assurance

All work at CS Innovations is performed in accordance with the CS Innovations document [ ]^{a,c,e}, and all of the procedures referenced from this manual. The Quality Assurance (QA) program is based on 10 CFR Part 50, Appendix B. Several 10 CFR 50, Appendix B audits have been performed, as discussed below.

Wolf Creek Generating Station (WCGS) conducted a 10 CFR Part 50, Appendix B audit of CS Innovations on September 10-13, 2007, as noted in the Wolf Creek Nuclear Operating Corporation (WCNOC) audit report RON NO: 20205-01 (Reference 29). The scope of the WCGS audit was "to evaluate the effectiveness and proper implementation of an acceptable [Quality Assurance] QA Program for the supply of ALS Control Systems, including Engineering Design Analysis & Production of an FPGA Control and Signal Processing Application in support of nuclear safety-related work as it applies to 10 CFR Part 50, Appendix B, and 10 CFR Part 21 for the nuclear industry." The audit report was issued on November 21, 2007, and states that CS Innovations is a WCGS qualified supplier for the audited scope.

Westinghouse conducted an independent 10 CFR Part 50, Appendix B, audit of CS Innovations on October 25, 2007. The scope of the audit was "to evaluate the effectiveness and proper implementation of an acceptable QA Program for the supply of I&C Hardware and Engineering Design Services in support of nuclear safety-related work as it applies to 10 CFR Part 50, Appendix B, and 10 CFR Part 21 for the nuclear industry." Audit report WES-2007-191 (Reference 30) was issued on November 10, 2008, and states that CS Innovations is a Westinghouse qualified supplier for the audited scope.

Also, as part of the review of the Main Steam and Feedwater Isolation System (MSFIS) upgrade at WCGS, the NRC conducted a review of CS Innovations' QA program. The results of this review are documented in the SER (ML# 090610317) (Reference 70) documents the results of that review, and the NRC concluded that CS Innovations' QA plans exhibit the appropriate management, implementation, and resource characteristics, and that the use of the plan will result in high-quality outputs..

11 Training

The CS Innovations Quality Assurance Manual [ ]^{a,c,e} states "CS Innovations managers shall be responsible for the quality assurance/quality control indoctrination and training of personnel under their supervision. This program shall also include training in job-related requirements to assure that personnel are qualified in the principles, techniques and requirements of the activities being performed. All training sessions associated with activities affecting quality shall be documented as to Instructor, subject, attendees and date of attendance". Records retention will be maintained by CSI for in-house training. All staff participating in the ALS Platform project are required to complete the QA indoctrination training and all training required for their job function.

The required training is reviewed periodically by the functional managers. If a new project requires additional training, the new training requirement is added. All personnel complete the identified training prior to working on the applicable project task.

In addition to the training of CS Innovations personnel, future applications will require training to be provided to the customer. The scope of project-specific customer training depends upon how the customer will operate and maintain the system. The details of the application-specific training are documented in each project's Management Plan which becomes the project specific training plan. The ALS customer-training plan is tailored to meet the training needs for the customer's ALS platform. This training plan implements the training requirements for the operation and maintenance of the ALS platform. This plan has the utility designate the plant personnel that will become future ALS instructors and those that will only require ALS training.

There are several constraints for training related to a specific system. First, the Operations and Maintenance Manuals and supporting documentation for the specific ALS are completed and approved by the customer. These need to be available in time to support preparation of training material for the instructor training courses. Secondly, the instructors need to be ready to train the plant staff including the applicable managers in time to support installation and site acceptance testing. Risks to the success of the CSI training plan are eliminated by planning adequate time with margin for these considerations and any others that occur.

Reviews of the CSI training program will be conducted at periodic intervals. Training records for personnel will be retained in accordance with CSI procedures. In addition, CSI will retain records of the training program it delivers in accordance with requirements stipulated by the contract.

12 Regulatory Compliance

This section describes ALS platform's compliance to the requirements of:

- IEEE-603 (Reference 7)
- IEEE 7-4.3.2 (Reference 4)
- DI&C-ISG-04 (Reference 60)
- BTP 7-14 (Reference 67)
- BTP 7-19 (Reference 3)
- Regulatory Guide 1.152 (Reference 0)
- DI&C ISG-06 (Reference 68)

Table 12-1 in the ISG-06 discussion maps the ALS platform documentation to the submittal requirements of DI&C-ISG-06. It should be noted that some requirements are met at the platform level, and some requirements are met at the safety system application level. This report deals with the ALS platform only, thus compliance to system level requirements may not be demonstrable.

12.1 Review of ALS Platform Compliance to IEEE-603 Requirements

10 CFR Part 50.55a(h), "Protection and safety systems," approves the 1991 version of IEEE Standard 603 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet dated January 30, 1995, for incorporation by reference.

IEEE 603-1991 prescribes functional and design requirements for the power, instrumentation, and control portions of nuclear power generating station safety systems as a whole. For purposes of this report, the following discussion is limited to the ALS platform and its compliance with the requirements of the standard. Other components which may be a part of a complete ALS based safety system are discussed only to the extent necessary to ensure the acceptability of the ALS platform. The topics discussed in the following sections are presented in the same order as they appear in IEEE 603-1991.

12.1.1 IEEE 603-1991 Clause 4 – Safety System Designation

Clause 4 of IEEE 603-1991 states that a specific basis shall be established for the design of each safety system of a nuclear power generating station. The sub clauses of this requirement include the following:

Clause 4.1	Identification of the design basis events
Clause 4.2	Safety functions and corresponding protective actions
Clause 4.3	Permissive conditions for each operating bypass capability
Clause 4.4	Identification of variables monitored
Clause 4.5	Minimum criteria for manual initiation and control of protective actions
Clause 4.6	Identification of the minimum number and location of sensors
Clause 4.7	Range of transient and steady state conditions
Clause 4.8	Identification of conditions which may degrade performance
Clause 4.9	Methods to be used to determine reliability
Clause 4.10	Critical points in time after onset of a design basis event
Clause 4.11	Equipment protective provisions
Clause 4.12	Any other special design basis

SRP Chapter 7, Appendix 7.1 C (Reference 31), Section 4, "Safety System Designation," provides acceptance criteria for these requirements.

Evaluation of the design basis for an ALS safety system is application specific and is, therefore, outside the scope if this report.

In the case where the ALS platform is used as a direct replacement for an existing safety system application, it will usually have the same design basis as the existing system. For those replacement applications where a design bases is changing, the ALS platform will meet the new design bases. The bases for the design of the existing safety system, including accident analyses, as discussed in Clauses 4.1 through 4.8 and 4.10 through 4.12, are not expected to change simply by the use of the ALS platform. If, for any reason, this expectation is not fulfilled, an application specific evaluation is performed to demonstrate compliance with the requirements of Clause 4 of IEEE 603-1991.

Determination of ALS safety system reliability (Clause 4.9) requires an application specific reliability analysis and a system level Failure Modes and Effects Analyses (FMEA) as discussed in Section 7, "Reliability." The board level FMEA results are part of the board's hardware design specification. ALS platform diversity and defense in depth (Clause 4.12) is discussed in Section 9, "Diversity."

Evaluation of the need for Technical Specification changes is application specific and is, therefore, outside the scope if this report.

In the case where the ALS platform is used for a new safety system application (e.g., new plants), the design basis for the entire safety system must be established. This activity is outside the scope of this report.

12.1.2 IEEE 603-1991 Clause 5.1 – Single-Failure Criterion

Clause 5.1 of IEEE 603-1991 requires that the safety system satisfies the single failure criterion as defined by IEEE Standard 379-2000 (Reference 32). SRP Chapter 7, Appendix 7.1 C, Section 5.1, "Single Failure Criterion," provides acceptance criteria for the single failure criterion. This section states that the applicant/licensee analysis should confirm that the requirements of the single failure criterion are satisfied.

[

]^{a,c,e}

12.1.3 IEEE 603-1991 Clause 5.2 – Completion of Protective Action

Clause 5.2 of IEEE 603-1991 states that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion, and that deliberate operator action shall be required to return the safety systems to normal. SRP Chapter 7, Appendix 7.1 C, Section 5.2, "Completion of Protective Action," provides acceptance criteria for this requirement.

Completion of protective action is a functional requirement that is independent of the platform and that requires verification on an application specific basis.

[

]^{a,c,e}

[

]^{a,c,e}

12.1.4 IEEE 603-1991 Clause 5.3 – Quality

Clause 5.3 of IEEE 603-1991 requires that safety system components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. SRP Chapter 7, Appendix 7.1 C, Section 5.3, "Quality," provides acceptance criteria for the quality requirement. This acceptance criteria states that the quality assurance provisions of 10 CFR Part 50, Appendix B (Reference 1) apply to a safety system.

[

]^{a,c,e}

12.1.5 IEEE 603-1991 Clause 5.4 – Equipment Qualification

Clause 5.4 of IEEE 603-1991 requires that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis. SRP Chapter 7, Appendix 7.1 C, Section 5.4, "Equipment Qualification," provides acceptance criteria for IEEE 603-1991 Clause 5.4. This acceptance criteria states that the applicant/licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located as identified by Clauses 4.7 and 4.8 of the design basis. Clause 5.4 also states that qualification of Class 1E equipment be in accordance with the requirements of IEEE Standard 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 13) and IEEE Standard 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations" (Reference 33). Regulatory Guide 1.89, Revision 1, (Reference 11), endorses and provides guidance for compliance with IEEE 323-1974.

[

]^{a,c,e}

12.1.6 IEEE 603-1991 Clause 5.5 – System Integrity

Clause 5.5 of IEEE 603-1991 requires that safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1 C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity. This acceptance criteria states that the NRC staff should confirm that tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady state conditions of both the energy supply and the environment; that test shows that if the system does fail, it fails in a safe state, and that failures detected by self diagnostics should also place a protective function into a safe state.

[

]a,c,e

12.1.7 IEEE 603-1991 Clause 5.6 – Independence

Clause 5.6 of IEEE 603-1991 requires in part independence between 1) redundant portions of a safety system, 2) safety systems and the effects of design basis events, and 3) safety systems and other systems. SRP Chapter 7, Appendix 7.1 C, Section 5.6, "Independence," provides acceptance criteria for system integrity. This acceptance criteria states that three aspects of independence: 1) physical independence, 2) electrical independence, and 3) communications independence, should be addressed for each previously listed cases. Guidance for evaluation of physical and electrical independence is provided in Regulatory Guide 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems" (Reference 34), which endorses IEEE Standard 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 35). The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.

SRP Chapter 7, Appendix 7.1 C, Section 5.6, "Independence," provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non safety system, a logical or software malfunction of the non safety system must not be able to affect the functions of the safety system.

12.1.7.1 IEEE 603-1991 Clause 5.6.1 – Independence between Redundant Portions of a Safety System

Clause 5.6.1 of IEEE 603-1991 requires that redundant portions of a safety system provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. SRP Chapter 7, Appendix 7.1 C does not provide any additional acceptance criteria beyond that in clause 5.6.1.

[

]^{a,c,e}

12.1.7.2 IEEE 603-1991 Clause 5.6.2 – Independence between Safety Systems and Effects of Design Basis Event

Clause 5.6.2 of IEEE 603-1991 requires that the safety system equipment required to mitigate the consequences of a specific design basis event be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that equipment qualification in accordance with Clause 5.4 is one method that can be used to meet this requirement. SRP Chapter 7, Appendix 7.1 C does not provide any additional acceptance criteria beyond that in clause 5.6.2.

[

]^{a,c,e}

12.1.7.3 IEEE 603-1991 Clause 5.6.3 – Independence between Safety Systems and Other Systems

Clause 5.6.3 of IEEE 603-1991 requires that the safety systems be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. SRP Chapter 7, Appendix 7.1 C does not provide any additional acceptance criteria beyond that in Clause 5.6.3. Each of the sub clauses is addressed in the following paragraphs.

Clause 5.6.3.1, "Interconnected Equipment," of IEEE 603 requires that equipment used for both safety and non-safety functions, as well as the isolation devices used to affect a safety system boundary, be classified as part of the safety systems. Clause 5.6.3.1 further states that no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function, and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system.

[

]^{a,c,e}

[

]^{a,c,e}

Clause 5.6.3.2, "Equipment in Proximity," of IEEE 603 states that equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, will be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment, and that physical separation may be achieved by physical barriers or acceptable separation distance. Clause 5.6.3.2 further states that the separation of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 384-1992. Finally, Clause 5.6.3.2 states that the physical barriers used to affect a safety system boundary shall meet the requirements of 5.3, "Quality," 5.4, "Equipment Qualification" and 5.5, "System Integrity" for the applicable conditions specified in Clauses 4.7 and 4.8 of the design basis.

[

]^{a,c,e}

12.1.8 IEEE 603-1991 Clause 5.7 – Capability for Test and Calibration

Clause 5.7 of IEEE 603-1991 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Clause 5.7 further states that the testing of Class 1E systems shall be in accordance with the requirements of IEEE Standard 338-1987 (Reference 36). Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station; however, appropriate justification shall be provided; acceptable reliability of equipment operation shall be demonstrated; and the capability shall be provided while the generating station is shut down. SRP Chapter 7, Appendix 7.1 C, Section 5.7, "Capability for Test and Calibration," provides acceptance criteria for IEEE 603-1991 Clause 5.7. First, it states that guidance on periodic testing of the safety system is provided in Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions" (Reference 37), and in Regulatory Guide 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems" (Reference 38), that endorses IEEE Standard 338-1987. Section 5.7 acceptance criteria states that periodic testing should duplicate, as closely as practical, the overall performance required of the safety system, and that the test should confirm operability of both the automatic and manual circuitry. This capability should be provided to permit testing during power operation and that when this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Clause 5.7 further states that test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. SRP Chapter 7, Appendix 7.1 C, Clause 5.7 further states that for digital computer based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup. SRP BTP 7-17 (Reference 39) describes additional considerations in the evaluation of test provisions in digital computer based systems.

[

]a,c,e

12.1.9 IEEE 603-1991 Clause 5.8 – Information Displays

Clause 5.8 of IEEE 603-1991 has four sub clauses: 5.8.1, "Displays for Manually Controlled Actions;" 5.8.2, "System Status Indication;" 5.8.3, "Indication of Bypasses;" and 5.8.4, "Location." SRP Chapter 7, Appendix 7.1 C, Section 5.8, "Information Displays," provides acceptance criteria for IEEE 603-1991 Clause 5.8. This guidance states that the information displays for manually controlled actions should include confirmation that displays will be functional, and that safety system bypass and inoperable status indication should conform to the guidance of Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" (Reference 40).

12.1.9.1 IEEE 603-1991 Clause 5.8.1 –Displays for Manually Controlled Actions

Clause 5.8.1 states that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Standard 497-1981 (Reference 41). The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. SRP Chapter 7, Appendix 7.1 C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603-1991 Clause 5.8.1.

[

]a,c,e

12.1.9.2 IEEE 603-1991 Clause 5.8.2 – System Status Indication

Clause 5.8.2 states that display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status, and that this information shall include indication and identification of protective actions of the sense and command features and execute features. Clause 5.8.2 further states that the design shall minimize the possibility of ambiguous indications that could be confusing to the operator, and that the display instrumentation provided for safety system status indication need not be part of the safety systems. SRP Chapter 7, Appendix 7.1 C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603-1991 Clause 5.8.2.

[

]a,c,e

IEEE 603-1991, Clause 5.8.2. This is discussed in more detail in the USNRC SER (Adams ML090610317) (Reference 70).

[

]a,c,e

12.1.9.3 IEEE 603-1991 Clause 5.8.3 – Indication Bypass

Clause 5.8.3 states that if the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room. Clause 5.8.3 further states that this display instrumentation need not be part of the safety systems, that this indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable, and that the capability shall exist in the control room to manually activate this display indication. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603 Clause 5.8.3.

| [

]a,c,e

[

]a,c,e

12.1.9.4 IEEE 603-1991 Clause 5.8.4 – Location

Clause 5.8.4 states that information displays shall be located accessible to the operator and that information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions. SRP Chapter 7, Appendix 7.1 C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603 1991 Clause 5.8.4.

[

]a,c,e

12.1.10 IEEE 603-1991 Clause 5.9 – Control of Access

Clause 5.9 of IEEE 603-1991 requires that the safety system be designed to permit administrative control of access to the safety system equipment, and that these administrative controls be supported by provisions within the safety system, by provision in the generating station design, or by a combination thereof. SRP Chapter 7, Appendix 7.1 C, Section 5.9, "Control of Access," provides acceptance criteria for IEEE 603-1991 Clause 5.10. This acceptance criteria states that administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access, and that digital computer based systems need to consider controls over electronic access, including access via network connections and maintenance equipment, to safety system software and data.

[

]a,c,e

12.1.11 IEEE 603-1991 Clause 5.10 – Repair

Clause 5.10 of IEEE 603-1991 states that safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Chapter 7, Appendix 7.1 C, Section 5.10, "Repair" provides acceptance criteria for IEEE 603-1991 Clause 5.10. This acceptance criteria states that while digital safety systems may include self diagnostic capabilities to aid in troubleshooting, the use of self diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5 of IEEE 603-1991.

[

]^{a,c,e}

12.1.12 IEEE 603-1991 Clause 5.11 – Identification

Clause 5.11 of IEEE 603-1991 states that safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Standard 384-1992 (Reference 35) and IEEE Standard 420-1982 (Reference 42); that identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes; that identification of safety system equipment and its divisional assignment shall not require frequent use of reference material; and that the associated documentation shall be distinctly identified in accordance with the requirements of IEEE Standard 494-1974 (R1990) (Reference 43); however, components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification. SRP Chapter 7, Appendix 7.1 C, Section 5.11, "Identification," provides acceptance criteria for IEEE 603-1991 Clause 5.11. This acceptance criterion also identifies IEEE 384-1992 as guidance.

[

]^{a,c,e}

12.1.13 IEEE 603-1991 Clause 5.12 – Auxiliary Features

Clause 5.12 of IEEE 603-1991 states that auxiliary supporting features shall meet all requirements of this standard, and that auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions and are not isolated from the safety system shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. SRP Chapter 7, Appendix 7.1 C, Section 5.12, "Auxiliary Features," provides acceptance criteria for IEEE 603-1991 Clause 5.12. This acceptance criterion states SRP BTP 7-9 (Reference 44) provides specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

[

]^{a,c,e}

[

]^{a,c,e}

12.1.14 IEEE 603-1991 Clause 5.13 – Multi-Unit Stations

Clause 5.13 of IEEE 603-1991 states that the sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Clause 5.13 further states that guidance on the sharing of electrical power systems between units is contained in IEEE Standard 308-1980 (Reference 45), and that guidance on the application of the single failure criterion to shared systems is contained in IEEE Standard 379-2000 (Reference 32). SRP Chapter 7, Appendix 7.1 C, Section 5.13, "Multi Unit Stations," provides acceptance criteria for IEEE 603-1991 Clause 5.13. This acceptance criterion states that the shared user interfaces must be sufficient to support the operator needs for each of the shared units.

[

]^{a,c,e}

12.1.15 IEEE 603-1991 Clause 5.14 – Human Factors Considerations

Clause 5.14 of IEEE 603-1991 states that human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Standard 1023-1988 (Reference 46). SRP Chapter 7, Appendix 7.1 C, Section 5.14, "Human Factors Considerations," provides acceptance criteria for IEEE 603-1991 Clause 5.14, and states that safety system human factors design should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the UFSAR.

[

]^{a,c,e}

12.1.16 IEEE 603-1991 Clause 5.15 – Reliability

Clause 5.15 of IEEE 603-1991 states that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. Clause 5.15 further states that IEEE Standard 352-1987 (Reference 47) and IEEE Standard 577-1976 (Reference 48) provide guidance for reliability analysis. SRP Chapter 7, Appendix 7.1 C, Section 5.15, "Reliability," provides acceptance criteria for IEEE 603-1991 Clause 5.15. This acceptance criterion states that the applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed and that for computer systems, both hardware and software reliability should be analyzed. The acceptance criteria further states that software that complies with the quality criteria of IEEE 603-1991 Clause 5.3 and that is used in safety systems that provide measures for defense against common cause failures, as previously discussed for IEEE 603-1991 Clause 5.1, are considered by the NRC staff to comply with the fundamental reliability requirements of GDC 21 and IEEE 603-1991.

Appendix 7.1 C, Section 5.15, further states that the assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures, and that hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common cause failures, cascading failures, and undetected failures. SRP Chapter 7, Appendix 7.1 C, Section 5.15 also references SRP Chapter 7, Appendix 7.1 D, and points out that quantitative reliability goals are not sufficient as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems.

[

]^{a,c,e}

[

]^{a,c,e}

12.1.17 IEEE 603-1991 Clause 6.1 – Automatic Controls

Clause 6.1 of IEEE 603-1991 requires that means be provided to automatically initiate and control all protective actions except as justified in Clause 4.5. Clause 6.1 further requires that the safety system design be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4.5 following the onset of each design basis event. SRP Chapter 7, Appendix 7.1 C, Section 6.1, "Automatic Controls," provides acceptance criteria for IEEE 603-1991 Clause 6.1. The acceptance criterion states the automatic initiation should be precise and reliable, and the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. Section 6.1 also states that SRP BTP 7-12 (Reference 53) discusses considerations for the review of the process for establishing instrument setpoints.

[

]^{a,c,e}

12.1.18 IEEE 603-1991 Clause 6.2 – Manual Control

Clause 6.2 of IEEE 603-1991 requires that means be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions, and that the means minimize the number of discrete operator manipulations and depend on the operation of a minimum of equipment consistent with the constraints of Clause 5.6.1. Clause 6.2 further requires that means be provided in the control room to implement manual initiation and control of the protective actions identified in Clause 4.5 that have not been selected for automatic control under Clause 6.1 and that the displays provided for these actions meet the requirements of Clause

5.8.1. Finally, Clause 6.2 requires that means be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4.10, and that the information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls be appropriate for the time period within which the actions are required to be accomplished and the number of available qualified operators. The displays and controls are required to be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action. SRP Chapter 7, Appendix 7.1 C, Section 6.2, "Manual Control," provides acceptance criteria for IEEE 603-1991 Clause 6.2. This acceptance criterion states that features for manual initiation of protective action should conform to Regulatory Guide 1.62, "Manual Initiation of Protection Action" (Reference 50), and will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

[

]^{a,c,e}

12.1.19 IEEE 603-1991 Clause 6.3 – Interaction between Sense of Command Features and Other Systems

Clause 6.3 of IEEE 603-1991 requires that, if a single credible event can both cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to failure from the same single event or equipment not subject to failure caused by the same single credible event be provided. SRP Chapter 7, Appendix 7.1 C, Section 6.3, "Interaction between the Sense and Command Features and Other Systems," provides acceptance criteria for IEEE 603-1991 Clause 6.3. This acceptance criterion states that if the event of concern is a single failure of a sensing channel shared between control and protection functions, isolating the safety system from the sensing channel failure by providing additional redundancy or isolating the control system from the sensing channel failure by using data validation techniques to select a valid control input are approaches that have been previously accepted.

[

]^{a,c,e}

12.1.20 IEEE 603-1991 Clause 6.4 – Derivation of System Inputs

Clause 6.4 of IEEE 603-1991 states that, to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. SRP Chapter 7, Appendix 7.1 C, Section 6.4, "Derivation of System Inputs," provides acceptance criteria for IEEE 603-1991 Clause 6.4. This acceptance criterion states that if indirect parameters are used, the indirect parameter must be shown to be a valid representation of the desired direct parameter for all events, and that for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate, are consistent with the analysis provided in Chapter 15 of the UFSAR.

[

]^{a,c,e}

12.1.21 IEEE 603-1991 Clause 6.5 – Capability for Testing and Calibration

Clause 6.5 of IEEE 603-1991 requires that means be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. Clause 6.5 further requires that means be provided for assuring the operational availability of each sense and command feature required during the post accident period. SRP Chapter 7, Appendix 7.1 C, Section 6.5, "Capability for Testing and Calibration," provides acceptance criteria for IEEE 603-1991 Clause 6.5. This acceptance criterion confirms that the operational availability can be checked by varying the input to the sensor or by cross checking between redundant channels. The acceptance criteria also states that when only two channels of readout are provided, the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ must be stated. SRP Chapter 7, Appendix 7.1 C, Section 6.5 also states that SRP BTP 7-17 (Reference 39) concerning sensor check and surveillance test provisions for digital computer I&C systems.

[

]^{a,c,e}

12.1.22 IEEE 603-1991 Clause 6.6 – Operating Bypasses

Clause 6.6 of IEEE 603-1991 states that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). Clause 6.6 further states that if plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall either remove the appropriate active operating bypass, restore plant conditions so that permissive conditions once again exist, or initiate the appropriate safety function(s). SRP Chapter 7, Appendix 7.1 C, Section 6.6, "Operating Bypasses," provides acceptance criteria for IEEE 603-1991 Clause 6.6. This acceptance criterion states that the requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

[

]^{a,c,e}

12.1.23 IEEE 603-1991 Clause 6.7 – Maintenance Bypass

Clause 6.7 of IEEE 603-1991 states that the capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. Clause 6.7 further states that during such operation, the sense and command features shall continue to meet the requirements of Clauses 5.1 and 6.3, with the exception that one out of two portions of the sense and command features are not required to meet Clauses 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (i.e., that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significant detrimental effect on the overall sense and command features availability). SRP Chapter 7, Appendix 7.1 C, Section 6.7, "Maintenance Bypass," provides acceptance criteria for IEEE 603-1991 Clause 6.7. This acceptance criterion states that provisions for this bypass need to be consistent with the required actions of the plant Technical Specifications.

[

]^{a,c,e}

[

]a,c,e

12.1.24 IEEE 603-1991 Clause 6.8 – Setpoints

Clause 6.8 of IEEE 603-1991 states that the allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint shall be determined using a documented methodology with reference to ISA Standard S67.04 1987 (Reference 51). .Clause 6.8 further states that where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide a positive means of ensuring that the more restrictive setpoint is used when required, and that the devices used to prevent improper use of less restrictive setpoints shall be a part of the sense and command features. SRP Chapter 7, Appendix 7.1 C, Section 6.8, "Setpoints," provides acceptance criteria for IEEE 603-1991 Clause 6.8. This acceptance criteria states that the setpoint analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system, and should confirm that an adequate margin exists between setpoints and safety limits, and that additional guidance on establishment of instrument setpoints can be found in Regulatory Guide 1.105, Revision 3, "Instrument Setpoints for Safety Systems" (Reference 52), and SRP BTP 7-12 (Reference 53), and in Regulatory Issue Summary 2006-17, "NRC Staff Position on the Requirements of 10 CFR 50.36, 'Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels" (Reference 54). SRP Chapter 7, Appendix 7.1 C, Section 6.8 further states that where it is necessary to provide multiple setpoints as discussed in clause 6.8.2 of IEEE Standard 603-1991, the NRC staff interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required, and that SRP BTP 7-3 (Reference 55) provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

[

]a,c,e

12.1.25 IEEE 603-1991 Clause 7.1 – Automatic Control

Clause 7.1 of IEEE 603-1991 requires that the safety system have the capability incorporated into the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4.4 of the design basis. SRP Chapter 7, Appendix 7.1 C, Section 7.1, "Automatic Control," provides the same acceptance criteria for IEEE 603-1991 Clause 7.1 as was provided for IEEE 603-1991 Clause 6.1.

[

]a,c,e

12.1.26 IEEE 603-1991 Clause 7.2 – Manual Control

Clause 7.2 of IEEE 603-1991 states that if manual control of any actuated component in the execute features is provided, the additional features in the execute features necessary to accomplish such manual control shall not defeat the requirements of Clauses 5.1 and 6.2, and that capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis. SRP Chapter 7, Appendix 7.1 C, Section 7.2, "Manual Control," provides the same acceptance criteria for IEEE 603-1991 Clause 7.2 as was provided for IEEE 603-1991 Clause 6.2.

[

]a,c,e

12.1.27 IEEE 603-1991 Clause 7.3 – Completion of Protective Action

Clause 7.3 of IEEE 603-1991 states that the design of the execute features be such that once initiated, the protective actions of the execute features shall go to completion; however, this requirement shall not preclude the use of equipment protective devices identified in Clause 4.11 of the design basis or the provision for deliberate operator interventions. Clause 7.3 further states that when the sense and command features reset, the execute features shall not automatically return to normal, but shall require separate, deliberate operator action to be returned to normal. Finally, Clause 7.3 states that after the initial protection has gone to completion, the execute features may require manual control or automatic control of specific equipment to maintain completion of the safety function. SRP Chapter 7, Appendix 7.1 C, Section 7.3, "Completion of Protective Action," provides acceptance criteria for IEEE 603-1991 Clause 7.3. This acceptance criterion states the review should include review of functional and logic diagrams, and that the seal in feature may incorporate a time delay as appropriate for the safety function.

[

]^{a,c,e}

12.1.28 IEEE 603-1991 Clause 7.4 – Operating Bypasses

Clause 7.4 of IEEE 603-1991 has the same requirements as IEEE 603-1991 Clause 6.6. SRP Chapter 7, Appendix 7.1 C, Section 7.4, "Operating Bypass," provides the same acceptance criteria for IEEE 603-1991 Clause 7.4 as was provided for IEEE 603-1991 Clause 6.6.

[

]^{a,c,e}

12.1.29 IEEE 603-1991 Clause 7.5 – Maintenance Bypass

Clause 7.5 of IEEE 603-1991 states that the capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Clause 7.5 further states that portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability. SRP Chapter 7, Appendix 7.1 C, Section 7.5, "Maintenance Bypass," provides the same acceptance criteria for IEEE 603-1991 Clause 7.5 as was provided for IEEE 603-1991 Clause 6.7.

[

]^{a,c,e}

12.1.30 IEEE 603-1991 Clause 8 – Power Source Requirements

Clause 8 of IEEE 603-1991 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Clause 8 further states that specific criteria unique to the Class 1E power systems are given in IEEE Standard 308-1980 (Reference 45). Finally, Clause 8 states that the capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass and that portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability. SRP Chapter 7, Appendix 7.1 C, Section 8 does not provide acceptance criteria for IEEE 603-1991 Clause 8.

[

]^{a,c,e}

12.2 IEEE-7-4.3.2 Compliance

Regulatory Guide 1.152 “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants” (Reference 0), endorses IEEE Standard 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations” (Reference 4), as an acceptable method for satisfying NRC regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.

IEEE 7-4.3.2-2003 specifies computer specific requirements (incorporating hardware, software, firmware, and interfaces) to supplement the criteria and requirements of IEEE Standard 603-1991 (Reference 7). This standard is used in conjunction with IEEE 603-1991 to assure the completeness of the safety system design when a computer is to be used as a component of a safety system. For purposes of this report, the following discussion is limited to the ALS platform and its compliance with the requirements of the standard. Other components which may be a part of a complete ALS based safety system are discussed only to the extent necessary to ensure the acceptability of the ALS platform. The topics discussed in the following sections are presented in the same order as they appear in IEEE 7-4.3.2 2003.

12.2.1 IEEE 7-4.3.2 Clause 4 – Safety System Design Basis

Clause 4 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603-1991.

[

]^{a,c,e}

12.2.2 IEEE 7-4.3.2 Clause 5.1 – Single-Failure Criterion

Clause 5.1 of IEEE 7-4.3.2-2003 states that there are no requirements beyond those contained in IEEE 603-1991.

[

]^{a,c,e}

12.2.3 IEEE 7-4.3.2 Clause 5.2 – Completion of Protective Action

Clause 5.2 of IEEE 7-4.3.2-2003 states that there are no requirements beyond those contained in IEEE 603-1991.

[

]^{a,c,e}

12.2.4 IEEE 7-4.3.2 Clause 5.3 – Quality

Clause 5.3 of IEEE 7-4.3.2-2003 states that hardware quality is addressed in IEEE 603-1991, and that software quality is addressed in IEEE/EIA Standard 12207.0-1996 (Reference 56) and supporting standards.

[

]^{a,c,e}

12.2.5 IEEE 7-4.3.2 Clause 5.3.1 – Software Development

Clause 5.3.1 of IEEE 7-4.3.2-2003 requires an approved QA plan consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at run time.

[

]^{a,c,e}

12.2.6 IEEE 7-4.3.2 Clause 5.3.1.1 – Software Quality Metrics

Clause 5.3.1.1 of IEEE 7 4.3.2 2003 states that the use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met.

[

]a,c,e

12.2.7 IEEE 7-4.3.2 Clause 5.3.2 – Software Tools

Clause 5.3.2 of IEEE 7 4.3.2 2003 states that software tools used to support software development processes and V&V processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety related software, or that they shall be used in a manner such that defects not detected by the tools are detected by V&V activities.

[

]a,c,e

12.2.8 IEEE 7-4.3.2 Clause 5.3.3 – V&V

Clause 5.3.3 of IEEE 7 4.3.2-2003 requires that a V&V program exists throughout the system life cycle, and that the software V&V effort be performed in accordance with IEEE Standard 1012 1998 (Reference 58).

[

]a,c,e

12.2.9 IEEE 7-4.3.2 Clause 5.3.4 – Independent V&V Requirements

Clause 5.3.4 of IEEE 7 4.3.2 2003 defines the levels of independence required for the V&V effort in terms of technical independence, managerial independence, and financial independence.

[

]a,c,e

12.2.10 IEEE 7-4.3.2 Clause 5.3.5 – Software Configuration Management

Clause 5.3.5 of IEEE 7 4.3.2-2003 states that software configuration management shall be performed in accordance with IEEE Standard 1042 1987 (Reference 61), and that IEEE Standard 828 1990 (Reference 62) provides guidance for the development of software configuration management plans. IEEE Standard 828 1990 and IEEE Standard 1042 1987 are endorsed by Regulatory Guide 1.169 (Reference 63).

[

]a,c,e

12.2.11 IEEE 7-4.3.2 Clause 5.3.6 – Software Project Risk Management

Clause 5.3.6 of IEEE 7 4.3.2 2003 defines the risk management requirements for a software project. SRP Chapter 7, Appendix 7.1 D, Section 5.3.6, "Software Project Risk Management" provides acceptance criteria for software project risk management. This section states that software project risk management is a tool for problem prevention, and shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that software project risks may include technical, schedule, or resource related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Additional guidance on the topic of risk management is provided in IEEE/EIA 12207.0 1996 and IEEE Standard 1540 2001, "IEEE Standard for Life Cycle Processes & Risk Management" (Reference 64).

[

]^{a,c,e}

12.2.12 IEEE 7-4.3.2 Clause 5.4 – Equipment Qualification

Clause 5.4 of IEEE 7 4.3.2 2003 defines the Equipment Qualification requirements for a software project. SRP Chapter 7, Appendix 7.1 D, Section 5.4, "Equipment Qualification," provides acceptance criteria for equipment qualification. This section of Appendix 7.1 D states that in addition to the equipment qualification criteria provided by IEEE 603 1991 and Section 5.4 of SRP Chapter 7, Appendix 7.1 C, additional criteria, as defined in Sections 5.4.1 and 5.4.2, are necessary to qualify digital computers for use in safety systems. [

]^{a,c,e}

12.2.12.1 IEEE 7-4.3.2 Clause 5.4.1 – Computer System Testing

Clause 5.4.1 of IEEE 7 4.3.2 2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1 D, Section 5.4.1, "Computer System Testing," provides acceptance criteria for equipment qualification. This section states that computer system equipment qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation.

[

]^{a,c,e}

12.2.12.2 IEEE 7-4.3.2 Clause 5.4.2 – Qualification of Existing Commercial Computers

Clause 5.4.2 of IEEE 7 4.3.2 2003 specifies the process for qualification of existing commercial computers for use in safety related applications in nuclear power plants. SRP Chapter 7, Appendix 7.1 D, Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for equipment qualifications. This section states that EPRI TR 106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (Reference 65), and EPRI TR 107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants" (Reference 66), provide specific guidance for the evaluation of commercial grade digital equipment and existing programmable logic controllers (PLC).

[

]^{a,c,e}

[

]^{a,c,e}

12.2.13 IEEE 7-4.3.2 Clause 5.5 – System Integrity

Clause 5.5 of IEEE 7 4.3.2-2003 states that in addition to the system integrity criteria provided by IEEE 603 1991, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self diagnostics activities. These attributes are further defined in IEEE 7 4.3.2, Clauses 5.5.1, "Design for computer integrity," Clause 5.5.2, "Design for test and calibration," and Clause 5.5.3, "Fault detection and self diagnostics." There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1 D, Section 5.5, "System Integrity." However, the three Clauses below discuss the necessary aspects of this Clause that achieve overall system integrity.

12.2.13.1 IEEE 7-4.3.2 Clause 5.5.1 – Design for Computer Integrity

Clause 5.5.1 of 7 4.3.2-2003 states that the computer be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function.

[

]^{a,c,e}

12.2.13.2 IEEE 7-4.3.2 Clause 5.5.2 – Design for Test and Calibration

Clause 5.5.2 of 7 4.3.2-2003 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further requires that V&V, configuration management, and QA be required for test and calibration functions on separate computers, such as test and calibration computers, that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

[

]^{a,c,e}

12.2.13.3 IEEE 7-4.3.2 Clause 5.5.3 – Fault Detection and Self-diagnostics

Clause 5.5.3 of 7 4.3.2-2003 discusses fault detection and self diagnostics, and states that if reliability requirements warrant self diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner, and that these self diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. This clause further requires that these self diagnostic functions be subject to the same V&V processes as the safety system functions.

[

]^{a,c,e}

12.2.14 IEEE 7-4.3.2 Clause 5.6 – Independence

Clause 5.6 of IEEE 7-4.3.2-2003 (Reference 4) states that, in addition to the requirements of IEEE 603 1991, data communication between safety channels or between safety and non safety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1 D, Section 5.6, "Independence" provides acceptance criteria for equipment qualifications. This section states 10 CFR 50, Appendix A, GDC 24, "Separation of protection and control systems," states that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

[

]a,c,e

12.2.15 IEEE 7-4.3.2 Clause 5.7 – Capability for Test and Calibration

Clause 5.7 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[

]a,c,e

12.2.16 IEEE 7-4.3.2 Clause 5.8 – Information Displays

Clause 5.8 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[ ]a,c,e

12.2.17 IEEE 7-4.3.2 Clause 5.9 – Control of Access

Clause 5.9 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[ ]a,c,e

12.2.18 IEEE 7-4.3.2 Clause 5.10 – Repair

Clause 5.10 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE Standard 603 1991.

[ ]a,c,e

12.2.19 IEEE 7-4.3.2 Clause 5.11 – Identification

Clause 5.11 of IEEE 7 4.3.2-2003 states that identification requirements specific to software (i.e., firmware and software) identification shall be used to assure the correct software is installed in the correct hardware component; means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools; and physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE 603 1991. SRP Chapter 7, Appendix 7.1 D, Section 5.11, "Identification" provides acceptance criteria and adds that the identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision for equipment qualifications.

[

]a,c,e

12.2.20 IEEE 7-4.3.2 Clause 5.12 – Auxiliary Features

Clause 5.12 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[ ]a,c,e

12.2.21 IEEE 7-4.3.2 Clause 5.13 – Multi-Unit Stations

Clause 5.13 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[

]a,c,e

12.2.22 IEEE 7-4.3.2 Clause 5.14 – Human Factors Considerations

Clause 5.14 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE Standard 603 1991.

[

]a,c,e

12.2.23 IEEE 7-4.3.2 Clause 5.15 – Reliability

Clause 5.15 of IEEE 7 4.3.2-2003 states that, in addition to the requirements of IEEE 603 1991, when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1 C, Section 5.15.

[

]a,c,e

12.2.24 IEEE 7-4.3.2 Clause 6 – Sense and Command Features

Clause 6 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[

]a,c,e

12.2.25 IEEE 7-4.3.2 Clause 7 – Execute Features

Clause 7 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[ ]a,c,e

12.2.26 IEEE 7-4.3.2 Clause 8 – Power Source Requirements

Clause 8 of IEEE 7 4.3.2-2003 states that there are no requirements beyond those found in IEEE 603 1991.

[ ]a,c,e

12.3 DI&C ISG-04 Highly-Integrated Control Rooms- Communications Issues

The NRC Digital I&C Task Working Group #4, "Highly Integrated Control Rooms—Communications Issues," has provided interim NRC staff guidance on the review of communications issues.' DI&C ISG 04 contains three sections: 1) Interdivisional Communications, 2) Command Prioritization, and 3) Multidivisional Control and Display Stations.

Section 1 of DI&C ISG-04 (Reference 60) provides guidance on communications, including transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety related. The ALS platform communication architecture complies with the ISG-04 Section 1 guidance as it pertains to interdivisional and safety/non-safety communication.

The generic architecture design for the ALS platform does not include any equipment related to command prioritization so compliance with ISG-04 Section 2 is not necessary or meaningful for the generic ALS platform communication architecture. Adherence to NRC staff positions 1 through 10 of ISG-04 Section 2 would be demonstrated on an application-specific basis during the development of an ALS Safety System where command prioritization is used.

The ALS platform communication architecture supports multidivisional communication for control and display stations which is discussed in ISG-04 Section 3. The ALS platform multidivisional communication is for the final voting logic and divisional displays as discussed in Section 5 of this report. For ALS plant specific implementations that require multidivisional control and display stations, all applicable portions of this ISG-04 section will be addressed at that time.

Section 5 of this report provides a discussion on communications and includes matrices (i.e., Table 5-2 and Table 5-3) showing compliance with the applicable positions of DI&C ISG-04.

12.4 BTP 7-14, R5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

ALS platform compliance with the software life cycle follows the guidance specified in BTP 7-14 for the applicable life cycle activities. Section 6 provides a discussion regarding the five lifecycle activities for the ALS platform. The last activity includes both installation and operation.

12.5 BTP 7-19, Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems and ISG-02, Diversity and Defense-in-Depth Issues

Because of the uniqueness of the ALS digital platform design (FPGA based rather than processor based), CSI is able to provide a generic description of the Defense-in-Depth and Diversity (D3) design concept for the ALS platform design that can be used in plant specific applications eliminating the need for any diverse actuation system or best-estimate safety analysis . The ALS design utilizes three main design concepts for achieving an acceptable inherent diversity level. These three main design concepts are:

- Paired core diversity
- Embedded design diversity
- Board diversity

[

]^{a,c,e}

12.6 RG 1.152, Revision 3 (Draft), Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

RG 1.152 provides the NRC endorsement of IEEE Standard 7-4.3.2-2003 and, secondly, provides security guidance as it relates to life cycle process for safety related digital platforms. Details regarding ALS platform compliance with IEEE Standard 7-4.3.2 are provided in this Section of the TR.

[

]a,c,e

12.7 ISG-06, Digital I&C Licensing Process

ISG-06 is draft guidance for the submission of necessary documents to enable the NRC to initiate and complete its review of a digital platform such as the ALS platform. CSI has developed a matrix showing the documentation details for the first three phases of this project, Table 12-1 below provides the document name, related ISG-06 Section, topic under discussion, the platform review item and the License Amendment Request topic. Phase 1 documentation is to be submitted along with the Topical Report; Phase 2 and 3 documentation will follow thereafter.

Table 12-1: Document Map – ISG06, Revision 44

a,c,e

a,c,e

a,c,e

a, c, e

a, c, e

a, c, e

a, c, e

Appendix A Reactor Protection System (RPS)/Engineered Safety Features Actuation System (ESFAS) Application

a,c,e

a,c,e

Figure A-1: [**]**^{a,c,e}

a,c,e

a,c,e

A-2: [ ]a,c,e

a,c,e

a,c,e

a,c,e

Figure A-3: [ ]^{a,c,e}

a,c,e

a,c,e

Figure A-4: [ ]^{a,c,e}

a,c,e

a,c,e

Appendix B Train Diverse Application

a,c,e

a,c,e

Figure B-1: [ ]^{a,c,e}

a,c,e

Appendix C Dual Train Application

a,c,e

Table C-1: [ ]a,c,e

a,c,e

a,c,e

a,c,e

a,c,e

Figure C-1: [ ]^{a,c,e}

a,c,e