



Product Safety Manual

RadICS

(Radiy FSC — FPGA-based Safety Controller)

Document D11.1

Version V2, Revision R3

February 2016

Table of Contents

1	Introduction	6
1.1	Scope and Purpose of this Document	6
1.2	Applicability and Version Information	6
1.3	Reference Standards	7
1.4	Other Documents Referenced by this Product Safety Manual	8
1.5	Specific Definitions and Acronyms	8
1.6	Other Definitions and Acronyms	9
2	Certification	10
3	Management of Functional Safety with the FSC	12
4	Failure Rate Data for Application Selection and SIL Verification	15
4.1	Defined Safe State	15
4.2	Failure Rate Data	16
4.3	Time Domain Data	19
4.4	Using the Failure Rate Data for a Specific SIF	19
4.5	Low Demand Mode of Operation.....	21
4.5.1	Criteria for Low Demand Mode	21
4.5.2	General Requirements for Low Demand Mode	22
4.5.3	Proof Test Coverage (PTC) Considerations.....	22
4.5.4	Recommended Proof Test Procedures	24
4.6	High Demand Mode of Operation.....	27
4.7	Common Cause Failure Considerations.....	27
4.8	Operating Limits	28
4.8.1	Product Life.....	28
4.8.2	Environmental Conditions	28
4.8.3	EMI and Surge Withstand Ratings	29
4.8.4	Signal Ranges and Voltage & Current Limits	31
5	Operation	33
5.1	Theory of Operation	33
5.1.1	General	33
5.1.2	FSC Modes of Operation	36
5.2	Local Indications of FSC Modes and Status.....	39
5.3	Safety OverRide (SOR).....	39
5.4	Response to Detected Failures	41
5.4.1	Concept.....	41
5.4.2	Automatic Response of the FSC.....	42
5.4.3	User Application Logic (UAL) Decisions.....	43
6	Wiring of Inputs and Outputs	50
6.1	FSC Physical Chassis: Use of Modules and Chassis Slots.....	50
6.2	Module I/O Capacities	51
6.3	Redundancy Options.....	53
6.4	EMI/Surge Protection Filters for I/O.....	53
6.5	Chassis Connectors	54
6.6	Power Supply Wiring.....	55
6.7	I/O Wiring	55
6.7.1	Wiring of SOR Inputs	57
6.7.2	Wiring of Logic Module Discrete I/O.....	58
6.7.3	Wiring of AIM Analog Inputs.....	59
6.7.4	Wiring of DIM Discrete Inputs	61
6.7.5	Wiring of DOM Discrete Outputs.....	63
6.7.6	Wiring of AOM Analog Outputs	64

6.7.7	Wiring of AIFM Analog Inputs	66
	Note: it is strongly recommended to follow polarity requirements as described in Table 6-7	66
6.7.8	Wiring of OCM Fiber Opto transceivers and RS-232/485 Outputs* ...	66
6.7.9	Wiring of chassis fans control and diagnostic	67
6.8	Wiring to Accommodate Periodic Proof Tests	67
6.9	Wiring for the Safety OverRide (SOR).....	68
6.10	Detection of Field Faults in Input Circuits	70
6.10.1	AIM Failed Analog Transmitters or Wiring.....	70
6.10.2	Detecting Shorted Field Wiring	71
6.10.3	AIFM Failed Analog Transmitters or Wiring	73
6.11	Wiring for the 'Armed' Contact for Tuning and Testing	73
7	Installation.....	73
7.1	Installation of the FSC chassis	73
7.2	Installation of FSC Modules.....	75
7.3	Installation of EMI/Surge Protection Modules.....	78
7.4	Connections to the FSC	80
7.5	Authentication of the FSC Version	81
8	Maintenance, Calibration, Periodic Testing	81
8.1	FSC Module HMI.....	82
8.2	LED Indications on FSC Modules.....	82
8.3	4-Character Matrix Display on FSC Modules	83
8.3.1	Display Tiers	83
8.3.2	Temporary Display Values During Startup.....	84
8.3.3	Identifying Specific Failure Details Using the Display	85
8.3.4	Determining the Specific Fault with a Blank Display	86
8.4	Routine Maintenance Activities	86
8.4.1	Periodic Inspection.....	86
8.4.2	Proof Tests.....	87
8.4.3	Routine Maintenance	87
8.5	Maintenance in Response to Detected Failures	88
8.5.1	Overview Procedure.....	88
8.5.2	Detailed Diagnostic Procedure.....	89
8.6	Calibration	93
8.6.1	AIM Calibration	95
8.6.2	AOM Calibration.....	95
8.6.3	AIFM Calibration	96
8.7	Personnel Safety	96
8.8	Inspection and Test Records.....	96
8.9	General Maintenance Issues.....	97
8.10	DownLoad Station (DLS).....	97
9	Tuning of Application Parameters	98
10	Design and Installation of Application Logic	98
10.1	User Application Logic Required for Compliance to IEC 61508	98
10.1.1	Verification of Chassis Configuration	98
10.1.2	Verification of I/O Module Status.....	99
10.1.3	Mitigation of Failures of Safety-Critical I/O Channels.....	100
10.1.4	Allowances for Analog Signal Tolerance.....	102
10.1.5	Setting the SOR or Tripping to Reach a Safe State	102
10.1.6	Latching Trip Decisions.....	103
10.1.7	Monitoring Module Temperature	103

10.1.8 User Logic Tests Required for the AIFM	104
10.1.9 Redundancy in User Wiring of I/O	104
10.1.10 UAL Requirements to Mitigate Output Module Failures	105
10.2 Use of Quartus to Program (Design) Application Logic	106
10.3 Installing a Logic Configuration in an FSC Logic Module	106
11 Security	107
11.1 Physical Security	107
11.2 Application Logic Configuration	107
11.3 Cyber Security	108
12 Product Forum	108
Annex A List of FSC modules fault codes	109

Figures

Figure 1-1 Radly FSC Chassis Partially Filled with I/O Modules	7
Figure 4-1 Illustration of the Impact of PTC < 100%	24
Figure 4-2 Illustration of the AIFM data processing path	26
Figure 5-1 Theory of Operation of the FSC	33
Figure 5-2 Timeline of FSC Operating Modes	36
Figure 5-3 Example of End-User Failsafe Logic for Failures	49
Figure 6-1 FSC Chassis Slots	51
Figure 6-2 Time delays affecting inter-chassis SIFs in multi-chassis configurations	52
Figure 6-3 FSC Chassis Showing Location of Optional EMI Filters	54
Figure 6-4 Rear of FSC Chassis Showing Connectors	55
Figure 6-5 FSC Chassis Power Supply Connections	55
Figure 6-6 FSC I/O Slot Connector Pinout Designations	56
Figure 6-7 AIFM Slot Connector Pinout Designations	56
Figure 6-8 OCM Slot RS-232 Connector Pinout Designations	56
Figure 6-9 OCM Slot RS-485 Connector Pinout Designations	56
Figure 6-10 FSC Discrete I/O Pinout Polarities	59
Figure 6-11 FSC Analog I/O Pinout Polarities for Current	60
Figure 6-12 FSC Analog I/O Pinout Polarities for Voltage	60
Figure 6-13 Single DI pinout with “diagnostic” resistor	62
Figure 6-14 FSC Analog Output Pinout Polarities for Current	64
Figure 6-15 FSC Analog Output Pinout Polarities for Voltage	65
Figure 6-16 FSC Analog Input Pinout Polarities for Neutron detector connection.	66
Figure 6-17 Wiring to Facilitate Proof-Testing	68
Figure 6-18 Example of Wiring of SOR for Selected DOMs	69
Figure 6-19 Use of 225 Ω Input Resistor with Analog Inputs	70
Figure 6-20 Extrapolation in ‘Shoulder’ Regions with 225 Ω Input Resistor	71
Figure 6-21 Diagnostic Field Resistor Used to Detect Shorted Field Circuit	72
Figure 7-1 Installation of the FSC Chassis	74
Figure 7-2 Locking Brackets for Chassis Installation	74
Figure 7-3 Installing/Removing an FSC Module	76
Figure 7-4 The pegs in the bottom rail	77
Figure 7-5 The pegs for plug-in modules	77
Figure 7-6 The pegs in the bottom and top horizontal rail	77
Figure 7-7 Slots and rails for EMI/Surge Protection module	78
Figure 7-8 Installation EMI/Surge Protection module into the rails and slots	79
Figure 7-9 Installed EMI/Surge Protection module	79

Figure 7-10 Power Cable Connections.....	80
Figure 7-11 Connector XG2 with dust cap	80
Figure 8-1 FSC Module Local HMI.....	82
Figure 10-1 STATEnn Block Use.....	99
Figure 10-2 Function Blocks to Reach a Safe State.....	103

Tables

Table 1-1 FSC Version Information.....	6
Table 1-2 Reference standards	7
Table 1-3 Reference documents	8
Table 1-4 Time Domain Parameters	8
Table 1-5 Failure Modes	8
Table 1-6 Failure Rates	9
Table 1-7 Parameters Related to Proof Testing.....	9
Table 4-1 FSC Failure Rates at MSL (Relative Flux = 1).....	17
Table 4-2 FSC Failure Rates at Relative Flux = 10	18
Table 4-3 FSC Response Times	19
Table 4-4 Example: Calculating the PF of the FSC for a SIF – step 1	20
Table 4-5 Example: Calculating the PF of the FSC for a SIF – step 2	20
Table 4-6 FSC and Cabinet Environmental Limits	28
Table 4-7 EMI and Surge Withstand Ratings	29
Table 5-1 Function Blocks that Report FSC Module Status	43
Table 5-2 Function Blocks that Report I/O Channel and Field Signal Status.....	44
Table 5-3 State of Field Signals – How Failures are Detected	44
Table 5-4 Response to I/O Input Failures	45
Table 5-5 Response to I/O Output Failures.....	46
Table 5-6 Controlling the FSC State After Failures Have Been Detected.....	47
Table 5-7 Effects of FSC Module Failures	49
Table 6-1 SOR Pinouts.....	57
Table 6-2 Logic Module I/O Pinouts	59
Table 6-3 Analog Input Module I/O Pinouts.....	61
Table 6-4 Discrete Input Module I/O Pinouts	62
Table 6-5 Discrete Output Module I/O Pinouts	63
Table 6-6 Analog Output Module I/O Pinouts	65
Table 6-7 Analog Input Pinouts for AIFM.....	66
Table 6-8 Pinouts for OCM RS-232/485 Outputs.....	66
Table 6-9 Fan Control Board I/O Pinouts	67
Table 8-1 Temporary Error Codes Optionally Displayed During Startup on I/O Modules.....	85
Table 8-2 Temporary Error Codes Optionally Displayed During Startup on the LM	85
Table 8-3 AOM Calibration Signal Levels	96