



Product Safety Manual

RadICS

(Radiy FSC — FPGA-based Safety Controller)

Document D11.1

Version V1, Revision R2

September 2014

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	7
1.5	Specific Definitions and Acronyms.....	8
1.6	Other Definitions and Acronyms	9
2	Certification	11
3	Management of Functional Safety with the FSC	12
4	Failure Rate Data for Application Selection and SIL Verification.....	14
4.1	Defined Safe State	14
4.2	Failure Rate Data	14
4.3	Time Domain Data.....	16
4.4	Using the Failure Rate Data for a Specific SIF.....	17
4.5	Low Demand Mode of Operation	18
4.5.1	Criteria for Low Demand Mode	18
4.5.2	General Requirements for Low Demand Mode	19
4.5.3	Proof Test Coverage (PTC) Considerations	19
4.5.4	Recommended Proof Test Procedures	21
4.6	High Demand Mode of Operation	22
4.7	Common Cause Failure Considerations	23
4.8	Operating Limits	23
4.8.1	Product Life.....	23
4.8.2	Environmental Conditions	24
4.8.3	EMI and Surge Withstand Ratings	24
4.8.4	Voltage & Current Limits	24
5	Operation	26
5.1	Theory of Operation.....	26
5.1.1	General.....	26
5.1.2	FSC Modes of Operation	27
5.2	Local Indications of FSC Modes and Status	30
5.3	Safety OverRide (SOR)	31
5.4	Response to Detected Failures.....	32
5.4.1	Concept	32
5.4.2	Automatic Response of the FSC	32
5.4.3	User Application Logic (UAL) Decisions.....	33
6	Wiring of Inputs and Outputs.....	40
6.1	FSC Physical Chassis: Use of Modules and Chassis Slots.....	40
6.2	Module I/O Capacities	40
6.3	Redundancy Options	41
6.4	EMI/Surge Protection Filters for I/O	41
6.5	Chassis Connectors	41

6.6	Power Supply Wiring	42
6.7	I/O Wiring	43
6.7.1	Wiring of SOR Inputs	43
6.7.2	Wiring of Logic Module Discrete I/O	45
6.7.3	Wiring of AIM Analog Inputs.....	46
6.7.4	Wiring of DIM Discrete Inputs.....	48
6.7.5	Wiring of DOM Discrete Outputs	50
6.7.6	Wiring of chassis fans control and diagnostic.....	51
6.8	Wiring to Accommodate Periodic Proof Tests	51
6.9	Wiring for the Safety OverRide (SOR)	52
6.10	Detection of Field Faults in Input Circuits.....	53
6.10.1	Failed Analog Transmitters or Wiring	53
6.10.2	Detecting Shorted Field Wiring.....	55
7	Installation.....	57
7.1	Installation of the FSC chassis.....	57
7.2	Installation of FSC Modules	58
7.3	Installation of EMI/Surge Protection Modules	60
7.4	Connections to the FSC.....	62
7.5	Authentication of the FSC Version.....	64
8	Maintenance, Calibration, Periodic Testing.....	65
8.1	FSC Module HMI	65
8.2	LED Indications on FSC Modules	66
8.3	4-Character Matrix Display on FSC Modules	66
8.3.1	Display Tiers	66
8.3.2	Temporary Display Values During Startup	67
8.3.3	Identifying Specific Failure Details Using the Display	68
8.3.4	Determining the Specific Fault with a Blank Display	68
8.4	Routine Maintenance Activities.....	69
8.4.1	Periodic Inspection.....	69
8.4.2	Proof Tests	70
8.4.3	Routine Maintenance	70
8.5	Maintenance in Response to Detected Failures.....	70
8.5.1	Overview Procedure.....	70
8.5.2	Detailed Diagnostic Procedure.....	71
8.6	Calibration	74
8.6.1	AIM Calibration	75
8.7	Personnel Safety	75
8.8	Inspection and Test Records	76
8.9	General Maintenance Issues	76
8.10	DownLoad Station (DLS)	76
9	Tuning of Application Parameters	77
10	Design and Installation of Application Logic.....	78
10.1	Application Logic Required for Compliance to IEC 61508.....	78

10.1.1 Verification of Chassis Configuration.....	78
10.1.2 Verification of I/O Module Status.....	79
10.1.3 Detection of Safety-Critical I/O Failures	79
10.1.4 Analog Input Signal Tolerance	79
10.1.5 Setting the SOR or Tripping to Reach a Safe State.....	80
10.1.6 Latching Trip Decisions.....	80
10.1.7 Monitoring Module Temperature	81
10.2 Use of Quartus to Program (Design) Application Logic.....	81
10.3 Installing a Logic Configuration in an FSC Logic Module	81
11 Security	83
11.1 Physical Security	83
11.2 Application Logic Configuration	83
11.3 Cyber Security.....	83
12 Product Forum	84

Figures

Figure 1-1 Radiy FSC Chassis Partly Filled with I/O Modules.....	7
Figure 4-1 Illustration of the Impact of PTC < 100%	20
Figure 5-1 Theory of Operation of the FSC.....	26
Figure 5-2 Timeline of FSC Operating Modes.....	28
Figure 5-3 Example of End-User Failsafe Logic for Failures	38
Figure 6-1 FSC Chassis Slots	40
Figure 6-2 FSC Chassis Showing Location of Optional EMI Filters.....	41
Figure 6-3 Rear of FSC Chassis Showing Connectors	42
Figure 6-4 FSC Chassis Power Supply Connections	42
Figure 6-5 FSC I/O Slot Connector Pinout Designations	43
Figure 6-6 Interpretation of FSC Discrete I/O Pinout Polarities	45
Figure 6-7 Interpretation of FSC Analog I/O Pinout Polarities for Current	47
Figure 6-8 Interpretation of FSC Analog I/O Pinout Polarities for Voltage	47
Figure 6-9 Wiring to Facilitate Proof-Testing.....	52
Figure 6-10 Example of Wiring of SOR for Selected DOMs	53
Figure 6-11 Use of 225 Ω Input Resistor with Analog Inputs.....	54
Figure 6-12 Extrapolation in ‘Shoulder’ Regions with 225 Ω Input Resistor	54
Figure 6-13 Diagnostic Field Resistor Used to Detect Shorted Field Circuit.....	55
Figure 7-1 Installation of the FSC Chassis.....	57
Figure 7-2 Locking Brackets for Chassis Installation.....	58
Figure 7-3 Installing/Removing an FSC Module.....	59
Figure 8-1 FSC Module Local HMI	65
Figure 10-1 STATEnn Block Use	78
Figure 10-2 Function Blocks to Reach a Safe State	80

Tables

Table 1-1 FSC Version Information	6
Table 4-1 FSC Failure Rates at MSL (Relative Flux = 1)	16
Table 4-2 FSC Failure Rates at Relative Flux = 10	16
Table 4-3 FSC Response Times.....	16
Table 4-4 Example: Calculating the PF of the FSC for a SIF – step 1.....	17
Table 4-5 Example: Calculating the PF of the FSC for a SIF – step 2.....	17
Table 4-6 FSC and Cabinet Environmental Limits	24
Table 4-7 EMI and Surge Withstand Ratings.....	24
Table 5-1 Function Blocks that Report FSC Module Status	34
Table 5-2 Function Blocks that Report I/O Channel Status	34
Table 5-3 State of Field Signals – How Failures are Detected	35
Table 5-4 Response to I/O Input Failures	35
Table 5-5 Response to I/O Output Failures	36
Table 5-6 Controlling the FSC State After Failures Have Been Detected.....	37
Table 5-7 Effects of FSC Module Failures	38
Table 6-1 SOR Pinouts.....	43
Table 6-2 Logic Module I/O Pinouts.....	46
Table 6-3 Analog Input Module I/O Pinouts	47
Table 6-4 Discrete Input Module I/O Pinouts	49
Table 6-5 Discrete Output Module I/O Pinouts.....	50
Table 6-6 Fan Control Board I/O Pinouts.....	51
Table 8-1 Temporary Error Codes Optionally Displayed During Startup on I/O Modules	67
Table 8-2 Temporary Error Codes Optionally Displayed During Startup on the LM	68