FSC Product Safety Manual

RadICS

(Radiy FSC — FPGA-based Safety Controller)

Document D11.1

Version V3, Revision R4

January 2018

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.

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 10
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 15
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 21
4.5.3 Proof Test Coverage (PTC) Considerations 22
4.5.4 Recommended Proof Test Procedures 23
4.6 High Demand Mode of Operation 27
4.7 Common Cause Failure Considerations 28
4.8 Operating Limits 28
4.8.1 Product Life 28
4.8.2 Environmental Conditions 29
4.8.3 EMI and Surge Withstand Ratings 29
4.8.4 Signal Ranges and Voltage & Current Limits 31
5 Operation 34
5.1 Theory of Operation 34
5.1.1 General 34
5.1.2 FSC Modes of Operation 37
5.2 Local Indications of FSC Modes and Status 40
5.3 Safety OverRide (SOR) 41
5.4 Response to Detected Failures 42
5.4.1 Concept 42
5.4.2 Automatic Response of the FSC 43
5.4.3 User Application Logic (UAL) Decisions 44
6 Wiring of Inputs and Outputs 44
6.1 FSC Physical Chassis: Use of Modules and Chassis Slots 44
6.2 Module I/O Capacities 45
6.3 Redundancy Options 47
6.4 EMI/Surge Protection Filters for I/O 48
6.5 Chassis Connectors 48
6.6 Power Supply Wiring 49
6.7 I/O Wiring 50
6.7.1 Wiring of SOR Inputs 51
6.7.2 Wiring of Logic Module 52
6.7.3 Wiring of AIM Analog Inputs 54
6.7.4 Wiring of DIM Discrete Inputs 56
6.7.5 Wiring of DOM Discrete Outputs 57
6.7.6 Wiring of AOM Analog Outputs 58

6.7.7 Wiring of AIFM Analog Inputs 60
6.7.8 Wiring of OCM Fiber Opto transceivers and RS-232/485 Outputs* ... 61
6.7.9 Wiring of chassis fans control and diagnostic 61
6.8 Wiring to Accommodate Periodic Proof Tests and Logic Changes 61
6.9 Wiring for the Safety OverRide (SOR) 63
6.10 Detection of Field Faults in Input Circuits 64
6.10.1 AIM Failed Analog Transmitters or Wiring 64
6.10.2 Detecting Shorted Field Wiring 66
6.10.3 AIFM Failed Analog Transmitters or Wiring 67
6.11 Wiring for the 'Armed' Contact for Tuning and Testing 68
7 Installation 68
7.1 Installation of the FSC chassis 68
7.2 Installation of FSC Modules 69
7.3 Installation of EMI/Surge Protection Modules 72
7.4 Installation of LM Unique Address connector 74
7.5 Connections to the FSC 76
7.6 Authentication of the FSC Version 78
8 Maintenance, Calibration, Periodic Testing 78
8.1 FSC Module HMI 79
8.2 LED Indications on FSC Modules 79
8.3 4-Character Matrix Display on FSC Modules 79
8.3.1 Display Tiers 79
8.3.2 Temporary Display Values During Startup 81
8.3.3 Identifying Specific Failure Details Using the Display 83
8.3.4 Determining the Specific Fault with a Blank Display 83
8.4 Routine Maintenance Activities 83
8.4.1 Periodic Inspection 84
8.4.2 Proof Tests 85
8.4.3 Routine Maintenance 85
8.5 Maintenance in Response to Detected Failures 85
8.5.1 Overview Procedure 85
8.5.2 Detailed Diagnostic Procedure 86
8.6 Calibration 91
8.6.1 AIM Calibration 92
8.6.2 AOM Calibration 92
8.6.3 AIFM Calibration 93
8.7 Personnel Safety 93
8.8 Inspection and Test Records 94
8.9 General Maintenance Issues 94
8.10 UpLoad Station (ULS) 94
9 Tuning of Application Parameters 95
10 Design and Installation of Application Logic 95
10.1 User Application Logic Required for Compliance to IEC 61508 95
10.1.1 Verification of Chassis Configuration 96
10.1.2 Verification of I/O Channel Status 96
10.1.3 Mitigation of Failures of Safety-Critical I/O Channels 97
10.1.4 Allowances for Analog Signal Tolerance 98
10.1.5 Setting the SOR to Reach a Safe State 100
10.1.6 Latching Trip Decisions 101
10.1.7 Monitoring Module Temperature 101
10.1.8 User Logic Tests Required for the AIFM 101

10.1.9 Redundancy in User Wiring of I/O 102
10.1.10 UAL Requirements to Mitigate Output Module Failures 102
10.1.11 Behaviour of OCLs in RUN(SAFE) and FAULTED Modes 104
10.2 Use of RPCT to Design Application Logic 104
10.3 Installing a Logic Configuration in an FSC Logic Module 105
11 Security 107
11.1 Physical Security 107
11.2 Application Logic Configuration 107
11.3 Cyber Security 107
12 Product Forum 108
Annex A List of FSC modules fault codes 109
Annex B RadICS Platform Components List 110

Figures

Figure 1-1 Radiy FSC Chassis Partially Filled with I/O Modules 7
Figure 4-1 Illustration of the Impact of PTC < 100% 23
Figure 4-2 Illustration of the AIFM data processing path 26
Figure 5-1 Theory of Operation of the FSC 34
Figure 5-2 Timeline of FSC Operating Modes 37
Figure 6-1 FSC Chassis Slots 45
Figure 6-2 Time delays affecting inter-chassis SIFs in multi-chassis configurations 47
Figure 6-3 FSC Chassis Showing Location of Optional EMI Filters 48
Figure 6-4 Rear of FSC Chassis Showing Connectors 49
Figure 6-5 FSC Chassis Power Supply Connections 50
Figure 6-6 FSC I/O Slot Connector Pinout Designations 50
Figure 6-7 AIFM Slot Connector Pinout Designations 50
Figure 6-8 OCM Slot RS-232/485 Connector Pinout Designations 51
Figure 6-9 FSC Discrete I/O Pinout Polarities 53
Figure 6-10 FSC Analog I/O Pinout Polarities for Current 54
Figure 6-11 FSC Analog I/O Pinout Polarities for Voltage 55
Figure 6-12 Single DI pinout with “diagnostic” resistor 56
Figure 6-13 FSC Analog Output Pinout Polarities for Current 59
Figure 6-14 FSC Analog Output Pinout Polarities for Voltage 59
Figure 6-15 FSC Analog Input Pinout Polarities for Neutron detector connection. 60
Figure 6-16 Wiring to Facilitate Proof-Testing and Tuning 62
Figure 6-17 Example of Wiring of SOR for Selected DOMs 64
Figure 6-18 Use of 225 Ω Input Resistor with Analog Inputs 65
Figure 6-19 Extrapolation in ‘Shoulder’ Regions with 225 Ω Input Resistor 66
Figure 6-20 Diagnostic Field Resistor Used to Detect Shorted Field Circuit 66
Figure 7-1 Installation of the FSC Chassis 68
Figure 7-2 Locking Brackets for Chassis Installation 69
Figure 7-3 Installing/Removing an FSC Module 70
Figure 7-4 The pegs in the bottom rail 71
Figure 7-5 The pegs for plug-in modules 71
Figure 7-6 The pegs in the bottom and top horizontal rail 72
Figure 7-7 Slots and rails for EMI/Surge Protection module 73
Figure 7-8 Installation EMI/Surge Protection module into the rails and slots 73
Figure 7-9 Installed EMI/Surge Protection module 74
Figure 7-10 Installed Connector with Pre-Installed Jumpers 75

Figure 7-11 Empty slot for Address Connector 76
Figure 7-12 Power Cable Connections 77
Figure 7-13 Connector XG2 with dust cap 77
Figure 8-1 FSC Module Local HMI 79
Figure 10-1 Monitorable Signals of FSC Modules 96
Figure 10-2 LM Input Ports to Set the SOR 100

Tables

Table 1-1 Reference standards 7
Table 1-2 Reference documents 7
Table 1-3 Time Domain Parameters 8
Table 1-4 Failure Modes 8
Table 1-5 Failure Rates 8
Table 1-6 Parameters Related to Proof Testing 8
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 19
Table 4-5 Example: Calculating the PF of the FSC for a SIF – step 2 20
Table 4-6 FSC and Cabinet Environmental Limits 29
Table 4-7 EMI and Surge Withstand Ratings 29
Table 6-1 SOR Pinouts 51
Table 6-2 Logic Module I/O Pinouts 53
Table 6-3 Analog Input Module I/O Pinouts 55
Table 6-4 Discrete Input Module I/O Pinouts 56
Table 6-5 Discrete Output Module I/O Pinouts 57
Table 6-6 Analog Output Module I/O Pinouts 59
Table 6-7 Analog Input Pinouts for AIFM 60
Table 6-8 Pinouts for OCM RS-232/485 Outputs 61
Table 6-9 Fan Control Board I/O Pinouts 61
Table 8-1 Temporary Error Codes Optionally Displayed During Startup on I/O Modules 82
Table 8-2 Temporary Error Codes Optionally Displayed During Startup on the LM 82
Table 8-3 AOM Calibration Signal Levels 93