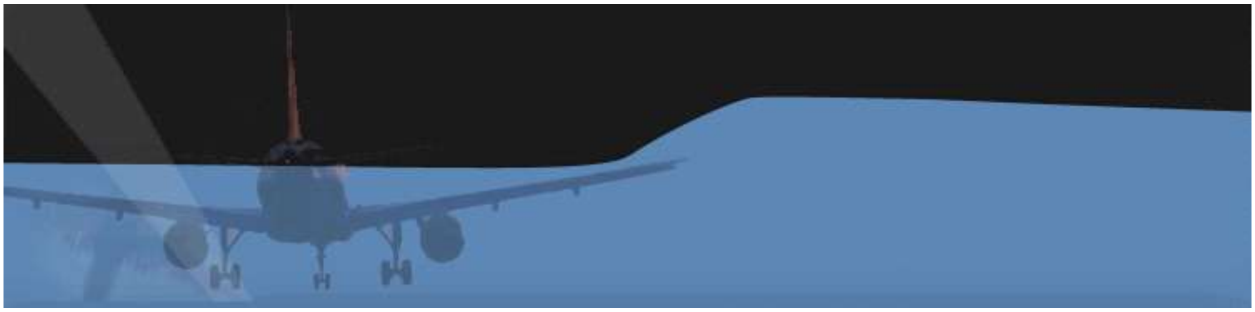


Plan for Hardware Aspects of Certification

for the

<Program Name>

Document No: <Doc Number>
Revision: -

<Name>, Program Manager	Date
<Name>, Technical Project Lead	Date
<Name>, Engineer	Date
<Name>, Quality Engineer	Date

Notice

This document and the information contained herein are the property of <company name>. Any reproduction, disclosure or use thereof is prohibited except as authorized in writing by <company name>. Recipient accepts the responsibility for maintaining the confidentiality of the contents of this document.

<table>
<tr><th colspan="4">REVISIONS</th></tr>
<tr><th>Rev.</th><th>Reason/Description</th><th>Requested/
Changed By</th><th>Date</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Table of Contents

Section **Page**

1.0 INTRODUCTION 11

1.1 Purpose 11
1.2 Scope 11
1.3 Part Number and Nomenclature 11
1.4 Team Members and Signature Authority 12
1.4.1 Independent Reporting Structure 13
1.5 Acronyms and Abbreviations 14
1.6 Applicable Documents 15
1.6.1 External Documents 15
1.6.2 Internal Documents 15

2.0 SYSTEM OVERVIEW 16

2.1 System Top Level Block Diagram 16
2.1.1 List of Major Functions Allocated To System-Level Hardware 17
2.1.1.1 List of Major Functions Allocated To Complex Hardware 17
2.1.1.1.1 FPGA #1 17
2.1.1.1.2 FPGA #2 17
2.1.1.2 List of Major Functions Allocated To Software 17
2.1.1.2.1 DSP #1 17
2.1.1.2.2 Microcontroller #1 17
2.2 System Functional Description 18
2.2.1 System Failure Conditions 19
2.2.2 High-Level Hardware Functions and Contribution to Potential Failures 19

3.0 HARDWARE OVERVIEW 20

3.1 Hardware Functions 20
3.1.1 Computation 21
3.1.2 Entry/Exit sensor 22
3.1.3 Keypad Entry Panel 22
3.1.4 Display Panel 22
3.1.5 PIC Controller Interface & Fault Monitoring 23
3.1.5.1 PIC Controller & ARINC 429 FPGA Interface 24
3.2 Hardware Safety and Partitioning 25
3.3 Hardware Device Characteristics 26
3.3.1 FPGA Device #1 26
3.3.1.1 Device Identification 26
3.3.1.2 SEU Susceptibility 26
3.3.1.2.1 Scrubbing and Readback with Compare 26
3.3.1.2.2 Triple Modular Redundancy 27
3.3.1.3 Errata Sheet Analysis 27
3.3.1.4 Operation Under Environmental Conditions 27
3.3.1.5 Hardware Functionality Allocated To Device 27
3.3.2 FPGA Device #2 27
3.3.2.1 Device Identification 27
3.3.2.2 SEU Susceptibility 28

3.3.2.2.1 Scrubbing and Readback with Compare 28
3.3.2.2.2 Triple Modular Redundancy 28
3.3.2.3 Errata Sheet Analysis 29
3.3.2.4 Operation Under Environmental Conditions 29
3.3.2.5 Hardware Functionality Allocated To Device 29
3.4 COTS Hardware Identification 29
3.4.1 Intellectual Property (IP) Core(s) 29
3.4.2 COTS Components 29
3.5 Safety and Partitioning 29

4.0 CERTIFICATION CONSIDERATIONS 30

4.1 Certification Basis and Means of Compliance 30
4.2 Issue Papers and Certification Review Items (CRI) 30
4.3 Hardware Level Determination 30
4.4 Compliance Matrix 32
4.5 Certification Authority Level of Involvement 48
4.5.1 Certification Authority Criteria for Level of Involvement 49
4.5.2 Proposed Level of Involvement 49

5.0 HARDWARE DESIGN LIFECYCLE 50

5.1 Team Member Responsibilities 51
5.2 Relationship Between Processes and Activities 55
5.3 Interaction Among Processes 56
5.3.1 Means of Providing Feedback 57
5.4 Planning Process 58
5.4.1 Planning Process Objectives 58
5.4.2 Planning Process Inputs 58
5.4.3 Planning Process Outputs 59
5.4.4 Planning Process Activities 59
5.4.5 Technical Interfaces 59
5.4.6 Planning Process Tool Usage 60
5.4.7 Planning Process Transition Criteria 60
5.4.7.1 Transition Criteria for Entry into Planning Process 60
5.4.7.2 Transition Criteria for Exit from Planning Process 61
5.4.8 Integral Processes 62
5.4.8.1 Validation & Verification Process Objectives and Activities 62
5.4.8.1.1 Hardware Validation & Verification Plan Preparation 62
5.4.8.1.2 Reviews and Analysis 62
5.4.8.1.2.1 Hardware Planning Review 63
5.4.8.2 Configuration Management Objectives and Activities 64
5.4.8.2.1 Configuration Management Plan Preparation 64
5.4.8.2.2 Configuration Identification, Baselines and Traceability 64
5.4.8.2.3 Configuration Status Accounting 64
5.4.8.2.4 Problem Reporting, Tracking and Corrective Action 65
5.4.8.2.5 Change Control and Change Review 65
5.4.8.3 Process Assurance Objectives and Activities 66
5.4.8.3.1 Process Assurance Plan Preparation 66
5.4.8.3.2 PA Independence during the Planning Process 66
5.4.8.3.3 PA Audits 66
5.4.8.3.4 PA Conformity Review Planning 66
5.4.8.3.5 Hardware Transition Criteria Satisfaction Review 67

5.4.8.3.6 PA Reporting and Corrective Action 67
5.4.8.4 Certification Liaison Objectives and Activities 68
5.4.8.4.1 Means of Compliance and Planning 68
5.4.8.4.2 Compliance Substantiation 68
5.5 Requirements Capture Process 72
5.5.1 Requirements Capture Process Objectives 72
5.5.2 Requirements Capture Process Inputs 72
5.5.3 Requirements Capture Process Outputs 72
5.5.4 Requirements Capture Process Activities 73
5.5.5 Technical Interfaces 75
5.5.6 Requirements Capture Process Tool Usage 75
5.5.7 Requirements Capture Process Transition Criteria 75
5.5.7.1 Transition Criteria for Entry into Requirements Process 75
5.5.7.2 Transition Criteria for Exit from Requirements Process 76
5.5.8 Integral Processes 77
5.5.8.1 Validation & Verification Process Objectives and Activities 77
5.5.8.1.1 Reviews and Analysis 77
5.5.8.1.1.1 Hardware Requirements Review 78
5.5.8.2 Configuration Management Objectives and Activities 79
5.5.8.2.1 Configuration Identification, Baselines and Traceability 79
5.5.8.2.2 Configuration Status Accounting 79
5.5.8.2.3 Problem Reporting, Tracking and Corrective Action 80
5.5.8.2.4 Change Control and Change Review 80
5.5.8.3 Process Assurance Objectives and Activities 81
5.5.8.3.1 PA Audits 81
5.5.8.3.2 Hardware Transition Criteria Satisfaction Review 81
5.5.8.3.3 PA Reporting and Corrective Action 81
5.5.8.4 Certification Liaison Objectives and Activities 82
5.5.8.4.1 Means of Compliance and Requirements 82
5.5.8.4.2 Compliance Substantiation 82
5.6 Conceptual Design Process 83
5.6.1 Conceptual Design Process Objectives 83
5.6.2 Conceptual Design Process Inputs 83
5.6.3 Conceptual Design Process Outputs 83
5.6.4 Conceptual Design Process Activities 84
5.6.5 Technical Interfaces 85
5.6.6 Conceptual Design Process Tool Usage 85
5.6.7 Conceptual Design Process Transition Criteria 86
5.6.7.1 Transition Criteria for Entry into Conceptual Design Process 86
5.6.7.2 Transition Criteria for Exit from Conceptual Design Process 87
5.6.8 Integral Processes 88
5.6.8.1 Validation & Verification Process Objectives and Activities 88
5.6.8.1.1 Reviews and Analysis 88
5.6.8.1.1.1 Hardware Preliminary Design Review 89
5.6.8.2 Configuration Management Objectives and Activities 90
5.6.8.2.1 Configuration Identification, Baselines and Traceability 90
5.6.8.2.2 Configuration Status Accounting 90
5.6.8.2.3 Problem Reporting, Tracking and Corrective Action 91
5.6.8.2.4 Change Control and Change Review 91
5.6.8.3 Process Assurance Objectives and Activities 92
5.6.8.3.1 PA Audits 92
5.6.8.3.2 Hardware Transition Criteria Satisfaction Review 92

5.6.8.3.3 PA Reporting and Corrective Action 92
5.6.8.4 Certification Liaison Objectives and Activities 93
5.6.8.4.1 Means of Compliance and Requirements 93
5.6.8.4.2 Compliance Substantiation 93
5.7 Detail Design Process 94
5.7.1 Detail Design Process Inputs 94
5.7.2 Detail Design Process Outputs 94
5.7.3 Detail Design Process Activities 95
5.7.4 Technical Interfaces 96
5.7.5 Detail Design Process Tool Usage 97
5.7.6 Detail Design Process Transition Criteria 97
5.7.6.1 Transition Criteria for Entry into Detailed Design Process 97
5.7.6.2 Transition Criteria for Exit from Detailed Design Process 98
5.7.7 Integral Processes 99
5.7.7.1 Validation & Verification Process Objectives and Activities 99
5.7.7.1.1 Reviews and Analysis 99
5.7.7.1.1.1 Hardware Critical Design Review 100
5.7.7.2 Configuration Management Objectives and Activities 100
5.7.7.2.1 Configuration Identification, Baselines and Traceability 100
5.7.7.2.2 Configuration Status Accounting 101
5.7.7.2.3 Problem Reporting, Tracking and Corrective Action 102
5.7.7.2.4 Change Control and Change Review 102
5.7.7.3 Process Assurance Objectives and Activities 103
5.7.7.3.1 PA Audits 103
5.7.7.3.2 Hardware Transition Criteria Satisfaction Review 103
5.7.7.3.3 PA Reporting and Corrective Action 103
5.7.7.4 Certification Liaison Objectives and Activities 104
5.7.7.4.1 Means of Compliance and Requirements 104
5.7.7.4.2 Compliance Substantiation 104
5.8 Implementation Process 105
5.8.1 Implementation Process Objectives 105
5.8.2 Implementation Process Inputs 105
5.8.3 Implementation Process Outputs 105
5.8.4 Implementation Process Activities 105
5.8.5 Technical Interfaces 106
5.8.6 Implementation Process Tool Usage 106
5.8.7 Implementation Process Transition Criteria 107
5.8.7.1 Transition Criteria for Entry into Implementation Process 107
5.8.7.2 Transition Criteria for Exit from Implementation Process 108
5.8.8 Integral Processes 109
5.8.8.1 Validation & Verification Process Objectives and Activities 109
5.8.8.1.1 Reviews and Analysis 109
5.8.8.1.1.1 Hardware Implementation Review 109
5.8.8.2 Configuration Management Objectives and Activities 110
5.8.8.2.1 Configuration Identification, Baselines and Traceability 110
5.8.8.2.2 Configuration Status Accounting 110
5.8.8.2.3 Problem Reporting, Tracking and Corrective Action 111
5.8.8.2.4 Change Control and Change Review 111
5.8.8.3 Process Assurance Objectives and Activities 112
5.8.8.3.1 PA Audits 112
5.8.8.3.2 Hardware Transition Criteria Satisfaction Review 112
5.8.8.3.3 PA Reporting and Corrective Action 112

5.8.8.4 Certification Liaison Objectives and Activities 113
5.8.8.4.1 Means of Compliance and Requirements 113
5.8.8.4.2 Compliance Substantiation 113
5.9 Testing Process 114
5.9.1 Testing Process Objectives 114
5.9.2 Testing Process Inputs 114
5.9.3 Testing Process Outputs 115
5.9.4 Testing Process Activities 115
5.9.4.1 Test Case and Test Procedure Development 115
5.9.5 Technical Interfaces 116
5.9.6 Testing Process Tool Usage 116
5.9.6.1 Simulation and On-Target Testing 117
5.9.6.2 Test Execution and Test Results Compilation 117
5.9.6.3 Elemental Analysis Resolution 117
5.9.7 Testing Process Transition Criteria 118
5.9.7.1 Transition Criteria for Entry into Testing Process 118
5.9.7.2 Transition Criteria for Exit from Testing Process 118
5.9.8 Integral Processes 119
5.9.8.1 Validation & Verification Process Objectives and Activities 119
5.9.8.1.1 Reviews and Analysis 119
5.9.8.1.1.1 Test Case and Test Procedure Reviews and Analysis 119
5.9.8.1.1.2 Requirements-Based Test Coverage Analysis 119
5.9.8.1.1.3 Elemental Analysis 119
5.9.8.2 Configuration Management Objectives and Activities 120
5.9.8.2.1 Configuration Identification, Baselines and Traceability 120
5.9.8.2.2 Configuration Status Accounting 120
5.9.8.2.3 Problem Reporting, Tracking and Corrective Action 121
5.9.8.2.4 Change Control and Change Review 121
5.9.8.3 Process Assurance Objectives and Activities 122
5.9.8.3.1 PA Audits 122
5.9.8.3.2 Hardware Transition Criteria Satisfaction Review 122
5.9.8.3.3 PA Reporting and Corrective Action 122
5.9.8.4 Certification Liaison Objectives and Activities 123
5.9.8.4.1 Means of Compliance and Requirements 123
5.9.8.4.2 Compliance Substantiation 123
5.10 Production Transition Process 124
5.10.1 Production Transition Process Objectives 124
5.10.2 Production Transition Process Inputs 124
5.10.3 Production Transition Process Outputs 124
5.10.4 Production Transition Process Activities 125
5.10.5 Technical Interfaces 125
5.10.6 Hardware Production Transition Process Tool Usage 125
5.10.7 Production Transition Process Transition Criteria 126
5.10.7.1 Transition Criteria for Entry into Production Transition Process 126
5.10.7.2 Transition Criteria for Exit from Production Transition Process 127
5.10.8 Integral Processes 127
5.10.8.1 Validation & Verification Process Objectives and Activities 127
5.10.8.1.1 Reviews and Analysis 127
5.10.8.1.1.1 Production Transition Review 128
5.10.8.1.1.2 Hardware Conformity Review 128
5.10.8.2 Configuration Management Objectives and Activities 129
5.10.8.2.1 Configuration Identification, Baselines and Traceability 129

5.10.8.2.2 Configuration Status Accounting 129
5.10.8.2.3 Problem Reporting, Tracking and Corrective Action 129
5.10.8.2.4 Change Control and Change Review 130
5.10.8.3 Process Assurance Objectives and Activities 130
5.10.8.3.1 PA Audits 130
5.10.8.3.2 Hardware Transition Criteria Satisfaction Review 130
5.10.8.3.3 PA Reporting and Corrective Action 130
5.10.8.4 Certification Liaison Objectives and Activities 131
5.10.8.4.1 Means of Compliance and Requirements 131
5.10.8.4.2 Compliance Substantiation 131

6.0 HARDWARE DESIGN LIFECYCLE DATA 132

6.1 Overview 132
6.2 Trace Data 132
6.2.1 Trace Data Objective Evidence of Compliance 133
6.3 Hardware Lifecycle Data To Be Produced and Controlled 134
6.4 Hardware Lifecycle Data to Be Submitted To Certification Authority 139
6.5 Hardware Control Categories 140
6.6 Hardware Lifecycle Data DER Delegation Plan 141

7.0 ADDITIONAL CONSIDERATIONS 142

7.1 Use of Previously Developed Hardware 142
7.1.1 ARINC 429 I/O FPGA 142
7.1.1.1 Product Service Experience Data Acceptability Criteria 142
7.1.1.1.1 Similarity – Application, Function, Operating Environment, and DAL .. 142
7.1.1.1.1 Product Service Experience Calculation 143
7.1.2 ARINC 429 I/O FPGA Re-verification 144
7.2 Use of Commercial-Off-The-Shelf (COTS) Components 144
7.3 SH-1 Issue paper compliance 144
7.3.1 Modifiable Devices 144
7.3.2 Certification Plan 144
7.3.3 Validation Processes 144
7.3.4 Verification Processes 144
7.3.5 Traceability 144
7.3.6 Configuration Management 144
7.3.7 Simple Electronic Hardware (SEH) 145
7.3.8 Legacy Airborne Systems & Equipment Electronic Hardware 145
7.3.9 Commercial Off-The-Shelf (COTS) Microprocessors 145
7.3.10 Random Access Memory (RAM) based FPGAs 145
7.4 Safety Considerations 145
7.5 Tool Assessment and Qualification 146
7.5.1 Development Tools 147
7.5.1.1 Qualification of Development Tools 147
7.5.2 Verification Tools 148
7.5.2.1 Qualification of Verification Tools 148
7.6 Design Assurance Considerations 149
7.7 Use of Suppliers, Sub-Tier Suppliers and Off-Shore Facilities 149
7.7.1 Supplier Identification and Roles 150
7.7.1.1 Acme Consultants, Inc. 150
7.8 Deviations and Modifications to Plans 152

8.0 ALTERNATIVE METHODS 153

9.0 CERTIFICATION SCHEDULE 154

9.1 Master Project Schedule 154
9.1.1 Stages of Involvement Audit Schedule 155
9.2 Certification Authority Web Interface 156
9.2.1 Project-Level Integrated Compliance Management System 157
9.2.1.1 SecureWeb Security Management System 158
9.2.1.2 Problem Reporting Management System 159
9.2.1.3 Change Impact Analysis Management System 160
9.2.1.4 Document Review Management System 161
9.2.1.5 Reviews and Analysis Management System 162
9.2.1.6 Requirements Traceability Management System 163

List of Figures

Figure 1-1 Independent Reporting Structure 13
Figure 2-1 System Level Block Diagram 16
Figure 2-2 System Functional Diagram 18
Figure 5-1 Relationship Between Processes and Activities 55
Figure 5-2 Consolidated Lifecycle Flow Diagram 56
Figure 5-3 Lifecycle Process Feedback Flow Diagram 57
Figure 5-4 Hardware Development Process 71
Figure 5-5 Detail Design Process Outputs 94
Figure 9-1 Certification Master Schedule 154
Figure 9-2 Certification Authority Web Interface 156
Figure 9-3 Integrated Compliance Management System 157
Figure 9-4 SecureWeb Login Screen 158
Figure 9-5 Problem Reporting System 159
Figure 9-6 Change Impact Analysis Management System 160
Figure 9-7 Document Review Management System 161
Figure 9-8 Reviews and Analysis Management System 162
Figure 9-9 Requirements Traceability Management System 163

List of Tables

Table 1-1 Part Number and Nomenclature 11
Table 1-2 Team Members and Signature Authority 12
Table 2-1 System Failure Conditions 19
Table 4-1 List of Compliance Documents 30
Table 4-2 List of Issue Papers and CRI's 30
Table 4-3 Design Assurance Levels 31
Table 4-4 Compliance Matrix – Planning Process 33
Table 4-5 Compliance Matrix – Requirements Capture Process 34
Table 4-6 Compliance Matrix – Conceptual Design Process 35
Table 4-7 Compliance Matrix – Detailed Design Process 36
Table 4-8 Compliance Matrix – Implementation Process 38
Table 4-9 Compliance Matrix – Production Transition Process 40
Table 4-10 Compliance Matrix – Validation and Verification Process 43
Table 4-11 Compliance Matrix – Configuration Management Process 44
Table 4-12 Compliance Matrix – Process Assurance Process 45
Table 4-13 Compliance Matrix – Certification Liaison Process 46
Table 4-14 Compliance Matrix – Appendix B Design Assurance Considerations 47
Table 4-15 Certification Authority Involvement Based on DAL 48
Table 4-16 Hardware Certification Experience 48
Table 4-17 Hardware Development Capability 48
Table 4-18 Hardware Service History 48
Table 4-19 System and Hardware Application Complexity 49
Table 4-20 FAA DER Capabilities – Todd R. White 49
Table 4-21 Level of Involvement Criteria Scoring 49
Table 5-1 Team Member Responsibilities 54
Table 5-2 Planning Process Objectives 58
Table 5-3 Planning Process Tools 60
Table 5-4 Requirements Capture Process Objectives 72
Table 5-5 Requirements Capture Process Tools 75
Table 5-6 Conceptual Design Process Objectives 83
Table 5-7 Conceptual Design Process Tools 85
Table 5-8 Detail Design Process Objectives 94
Table 5-9 Detail Design Process Tools 97
Table 5-10 Implementation Process Objectives 105
Table 5-11 Implementation Process Tools 106
Table 5-12 Testing Process Objectives 114
Table 5-13 Testing Process Tools 116
Table 5-14 Production Transition Process Objectives 124
Table 5-15 Production Transition Process Tools 125
Table 6-1 Lifecycle Data To Be Produced 138
Table 6-2 Lifecycle Data To Certification Authority 139
Table 6-3 Hardware Control Categories 140
Table 6-4 Hardware DER Delegation Plan 141
Table 7-1 Hardware Development Tools 147
Table 7-2 Hardware Verification Tools 148

1.0 INTRODUCTION

1.1 Purpose

This Plan for Hardware Aspects of Certification (PHAC) defines the processes, procedures, methods and standards to be used and the lifecycle data to be produced in order to satisfy the objectives of DO-254 and any additional objectives required to satisfy the certification basis of the aircraft. Once approved, this PSAC represents an agreement between the applicant and the customer and/or certification authority.

1.2 Scope

As the severity of complex electronic hardware failures may impact the capability of the system to perform its intended function safely, their design life cycle processes will follow the guidance provided in DO-254. All the other hardware items will be developed following internal design life cycle processes. The complex electronic hardware items are those for which a comprehensive combination of deterministic tests, ensuring correct functional performance under all foreseeable operating conditions, is difficult to be achieved. These electronic hardware items are the Programmable Hardware Devices (hardware) that include Field Programmable Gate Arrays (FPGA) and Complex Programmable Logic Devices (CPLDs).

This Plan for Hardware Aspects of Certification complies with the documentation requirements of RTCA/DO-254, Section 10.1.1.

1.3 Part Number and Nomenclature

Part Number	Nomenclature

Table 1-1 Part Number and Nomenclature

1.4 Team Members and Signature Authority

Name	Title
Signature Authority:	
John Smith	Project Manager
John Smith	Lead Hardware Engineer
John Smith	Independent Verification Engineer
John Smith	Process Assurance Engineer
Team Members:	
John Smith	Systems Engineer
John Smith	Reliability & Safety Engineer
John Smith	Hardware Design Engineer
John Smith	Configuration Management Engineer
John Smith	FAA Software Designated Engineering Representative

Table 1-2 Team Members and Signature Authority

1.4.1 Independent Reporting Structure

The following chart shows that the Quality Assurance Organization is independent from Engineering. It also demonstrates that the verification and test activities are performed independently by someone other than the development engineer.

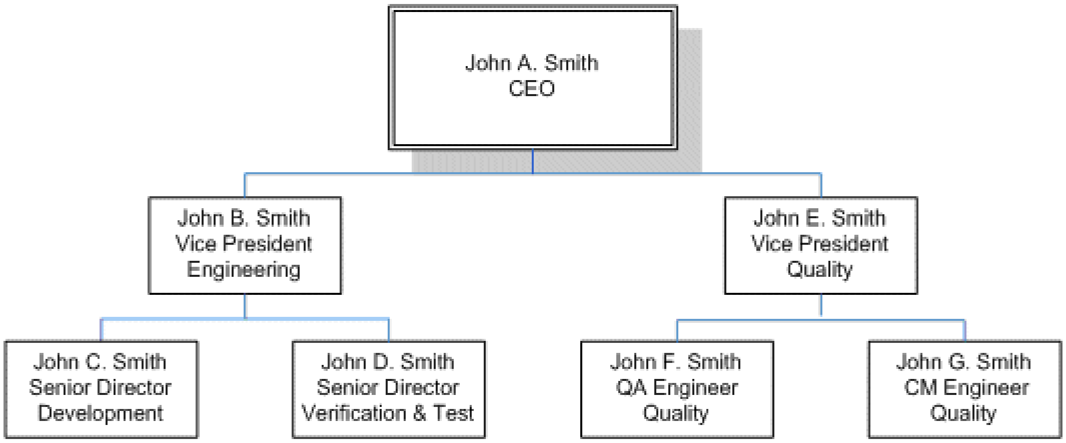


Figure 1-1 Independent Reporting Structure

1.5 Acronyms and Abbreviations

AIMS	Reviews and Analysis Management System
ALU	Arithmetic Logic Unit
ARP	Aerospace Recommended Practice
ASIC	Application Specific Integrated Circuit
DRMS	Document Review Management System
HAS	Hardware Accomplishment Summary
HC1	Hardware Control Category 1
HC2	Hardware Control Category 2
COTS	Commercial-Off-The-Shelf
EUROCAE	European Organization for Civil Aviation Equipment
FAR	Federal Aviation Regulations
FFP	Functional Failure Path
FFPA	Functional Failure Path Analysis
FHA	Functional Hazard Assessment
F-FMEA	Functional Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HDL	Hardware Description Language
JAR	Joint Aviation Requirements
LRU	Line Replaceable Unit
PHAC	Plan for Hardware Aspects of Certification
PLD	Programmable Logic Device
PSSA	Preliminary System Safety Assessment
RTMS	Requirements Traceability Management System
SAE	Society of Automotive Engineers
SC	Special Committee
SSA	System Safety Assessment
WG	Working Group

1.6 Applicable Documents

The following documents are listed for reference only. Each document is applicable to this plan only to the extent specified herein.

1.6.1 External Documents

RTCA/DO-254	Design Assurance for Airborne Electronic Hardware
FAA Order 8110.4C	Type Certification
FAA Order 8110.105	FAA, Simple and Complex Electronic Hardware Approval Guidance
AC 20-152	Advisory Circular, RTCA Inc., Document DO-254, Design Assurance for Airborne Electronic Hardware

1.6.2 Internal Documents

<Ref Doc>	Plan for Hardware Aspects of Certification (Ref. DO-254, 10.1.1)
<Ref Doc>	Hardware Design Plan (Ref. DO-254, 10.1.2)
<Ref Doc>	Hardware Validation & Verification Plan (Ref. DO-254, 10.1.3/10.1.4)
<Ref Doc>	Configuration Management Plan (Ref. DO-254, 10.1.5)
<Ref Doc>	Process Assurance Plan (Ref. DO-254, 10.1.6)
<Ref Doc>	Hardware Requirements Standards (Ref. DO-254, 10.2.1)
<Ref Doc>	Hardware Design Standards (Ref. DO-254, 10.2.2)
<Ref Doc>	Validation and Verification Standards (Ref. DO-254, 10.2.3)
<Ref Doc>	Hardware Archive Standards (Ref. DO-254, 10.2.4)
<Ref Doc>	Hardware Requirements Document (Ref. DO-254, 10.3.1)
<Ref Doc>	Hardware Design Data (Ref. DO-254, 10.3.2)
<Ref Doc>	Hardware Test Procedures (Ref. DO-254, 10.4.4)
<Ref Doc>	Hardware Lifecycle Environment Configuration Index (Ref. CAST 27)
<Ref Doc>	Hardware Configuration Index (Ref. CAST 27)
<Ref Doc>	Hardware Accomplishment Summary (Ref. DO-254, 10.9)

2.0 SYSTEM OVERVIEW

This section provides an overview of the system, including a description of its functions and their allocation to hardware and software, the architecture, processor(s) used, hardware / software interfaces and safety features.

<Example Text>
The Avionics Passenger Counter is a module that will keep track of how many passengers are currently in the aircraft/cabin. The current number of passengers in the cabin will be displayed on a display panel in real-time. The system will have a keypad entry so that the flight attendant can enter a passenger headcount correction/adjustment. The passenger headcount and any fault status information collected will be transmitted via ARINC 429 via the PIC processor and ARINC 429 I/O FPGA.

2.1 System Top Level Block Diagram

<This is a diagram of equipment showing a high-level interconnect of black boxes with emphasis on identifying the printed circuit boards relative to the processors and complex hardware (ASIC's, FPGA's, PLD's & Processors).>

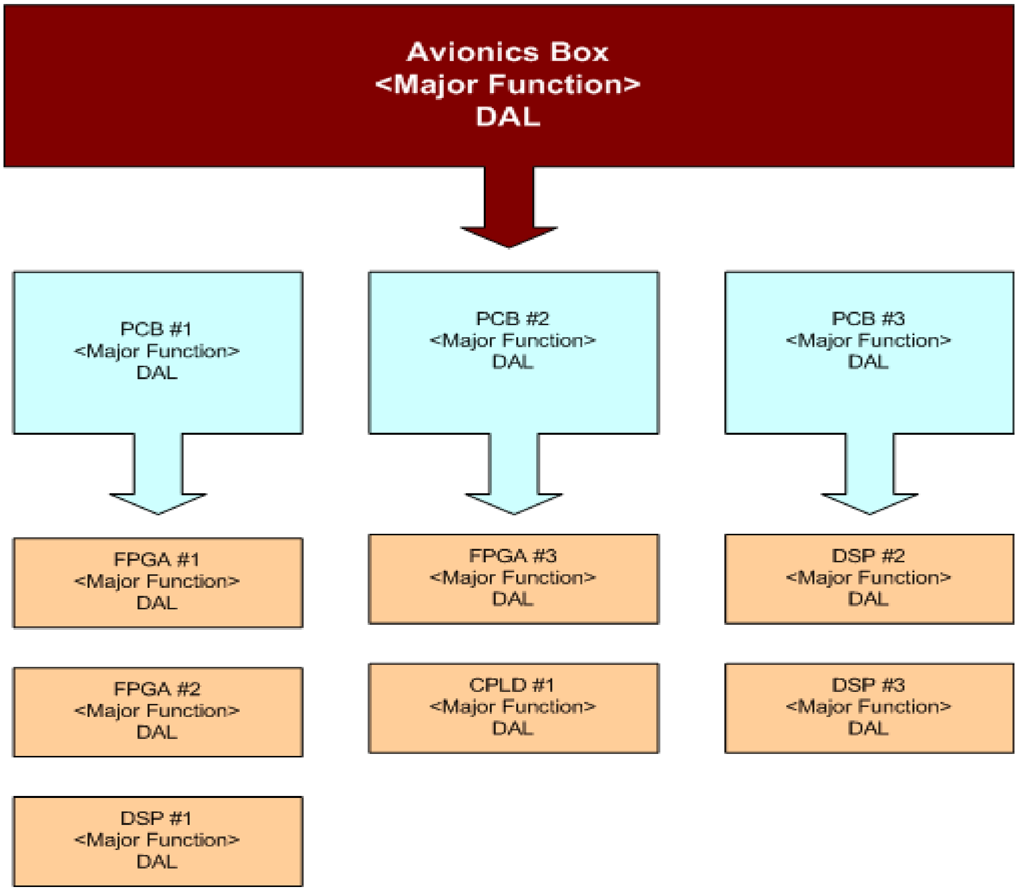


Figure 2-1 System Level Block Diagram

2.1.1 List of Major Functions Allocated To System-Level Hardware

- System-Level Hardware Function #1
- System-Level Hardware Function #2

2.1.1.1 List of Major Functions Allocated To Complex Hardware

2.1.1.1.1 FPGA #1

- Complex Hardware Function #1
- Complex Hardware Function #2

2.1.1.1.2 FPGA #2

- Complex Hardware Function #1
- Complex Hardware Function #2

2.1.1.2 List of Major Functions Allocated To Software

2.1.1.2.1 DSP #1

- Software Function #1
- Software Function #2

2.1.1.2.2 Microcontroller #1

- Software Function #1
- Software Function #2

2.2 System Functional Description

<Example Text>
The passenger headcount function is performed by counting the number of entries and exits. The module uses an Entry/Exit-Sensor to detect passengers' movements in and out of the cabin. The number of passengers in the cabin is tracked by an up/down counter in an FPGA. The passenger load is displayed in real-time on the display panel. The keypad entry can asynchronously load the counter thereby adjusting/correcting the passenger load on the display/system.

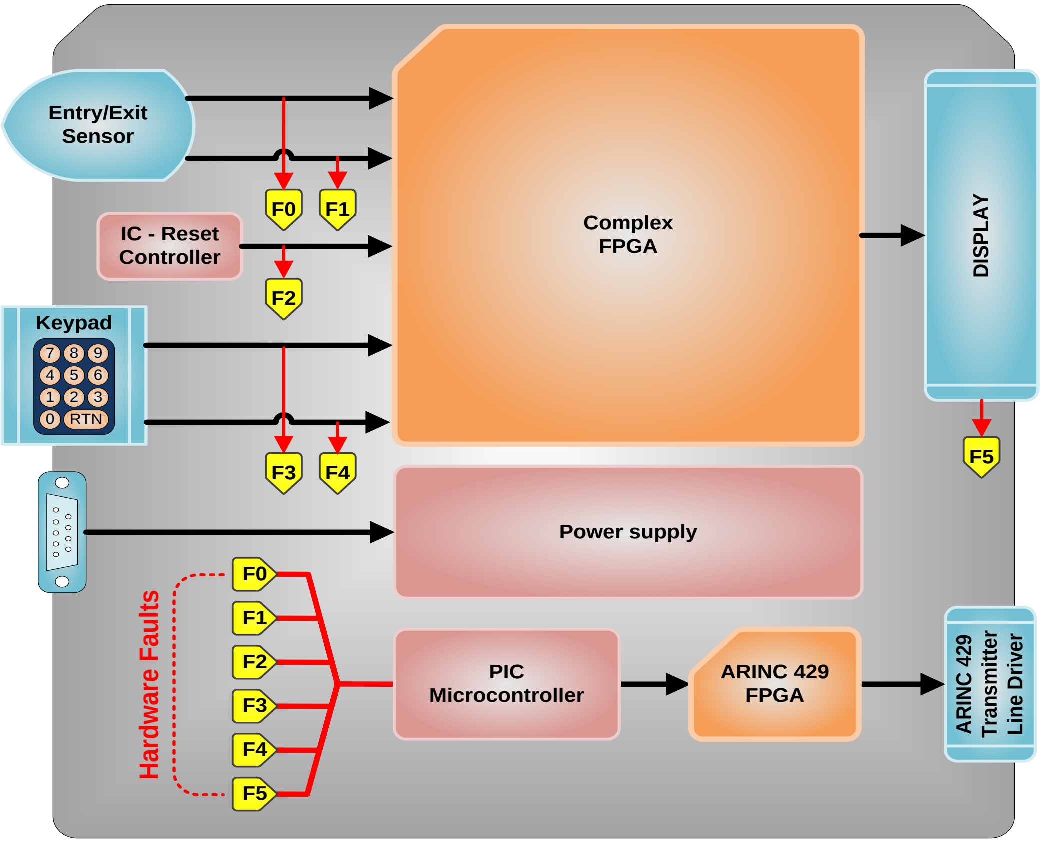


Figure 2-2 System Functional Diagram

2.2.1 System Failure Conditions

2.2.2 High-Level Hardware Functions and Contribution to Potential Failures

No	AEH/CEH Function	Example of Potential Failure	DAL
01	Provision of secure and timely data flow to and from applications and Input / output devices, e.g. sensors and actuators	Transmission of deploy command to landing gear in flight	A
02	Controlled access to processing facilities	Omission in schedule of fuel system pumping control partition	B
03	Provision of secure data storage and memory management	Corruption of fuel system execution code by lower integrity partition	B
04	Provision of consistent execution state	Incorrect or inconsistent flight data is loaded into system	B
05	Provision of health monitoring and failure management	Fuel system partition shut down when no error has occurred	A
06	General provision of computing capability	Total loss of IMA platform	A

Table 2-1 System Failure Conditions

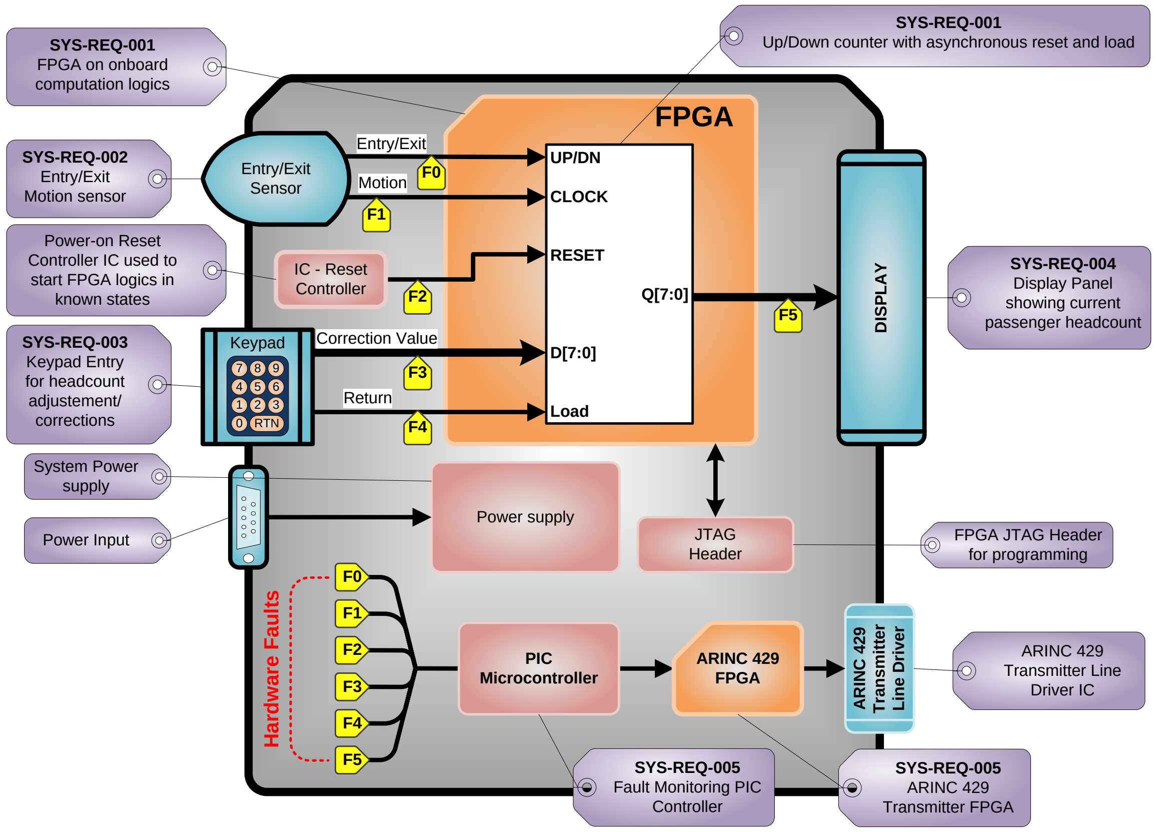
3.0 HARDWARE OVERVIEW

<Example Text>
This section describes the hardware functions, hardware items, architecture, new technologies to be used, and any fail-safe, fault tolerant redundancy and partitioning techniques to be used.

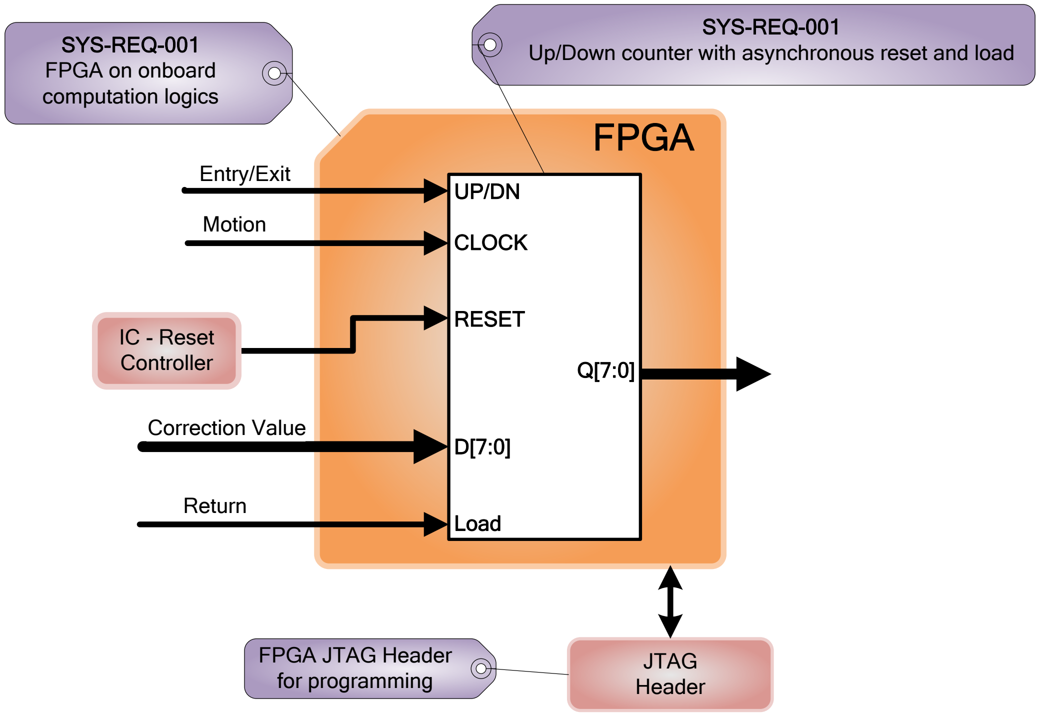
3.1 Hardware Functions

There are five main hardware functions:

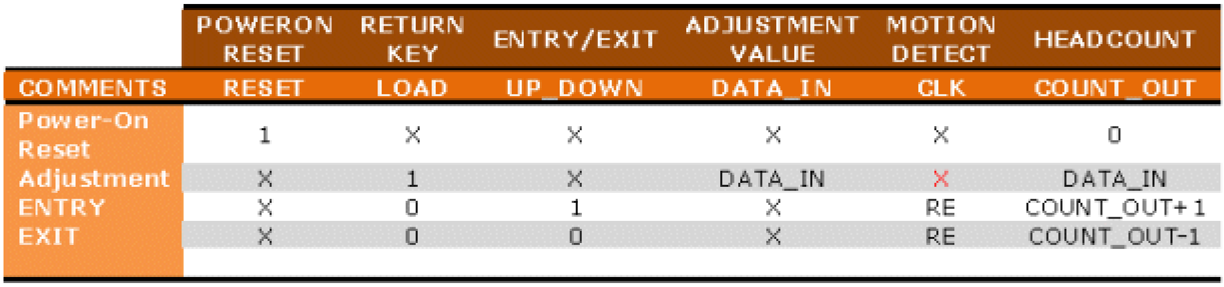
1. Computation (Derived)
2. Entry/Exit Detection
3. Keypad entry
4. Display
5. Fault monitoring and ARINC 429 data transmit


SYS-REQ-001
FPGA on onboard computation logics
SYS-REQ-001
Up/Down counter with asynchronous reset and load
FPGA
SYS-REQ-002
Entry/Exit Motion sensor
Entry/Exit Sensor
Entry/Exit
Motion
F0
F1
UP/DN
CLOCK
Power-on Reset Controller IC used to start FPGA logics in known states
IC - Reset Controller
F2
RESET
Q[7:0]
F5
DISPLAY
SYS-REQ-004
Display Panel showing current passenger headcount
SYS-REQ-003
Keypad Entry for headcount adjustement/ corrections
Keypad
7 8 9
4 5 6
1 2 3
0 RTN
Correction Value
F3
D[7:0]
Return
F4
Load
System Power supply
Power Input
Power supply
JTAG Header
FPGA JTAG Header for programming
Hardware Faults
F0
F1
F2
F3
F4
F5
PIC Microcontroller
ARINC 429 FPGA
ARINC 429 Transmitter Line Driver
ARINC 429 Transmitter Line Driver IC
SYS-REQ-005
Fault Monitoring PIC Controller
SYS-REQ-005
ARINC 429 Transmitter FPGA

3.1.1 Computation

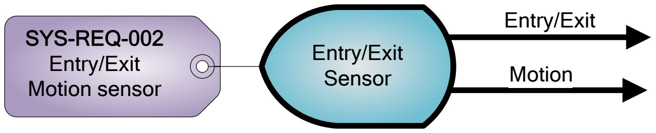


The headcount function is done by an up/down counter inside the FPGA. Every time the Entry/Exit motion sensor detects an entry or an exit, the counter increments or decrements accordingly. Ever time the user presses return, the current headcount output is loaded with previously typed value. The truth table is shown below.



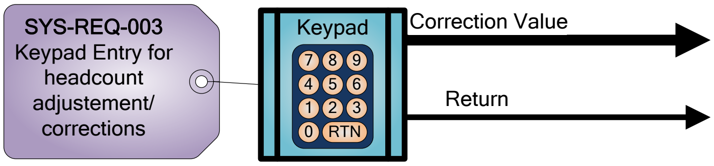
	POWERON RESET	RETURN KEY	ENTRY/EXIT	ADJUSTMENT VALUE	MOTION DETECT	HEADCOUNT
COMMENTS	RESET	LOAD	UP_DOWN	DATA_IN	CLK	COUNT_OUT
Power-On Reset	1	X	X	X	X	0
Adjustment	X	1	X	DATA_IN	X	DATA_IN
ENTRY	X	0	1	X	RE	COUNT_OUT+1
EXIT	X	0	0	X	RE	COUNT_OUT-1

3.1.2 Entry/Exit sensor



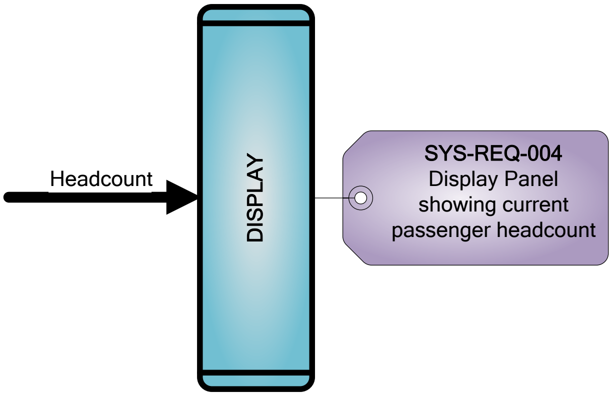
The Entry/Exit Detection function is performed by the Entry/Exit sensor. This sensor will detect human motion and decipher whether the motion is inward or outward. The information is then sent to the FPGA for headcount computation.

3.1.3 Keypad Entry Panel



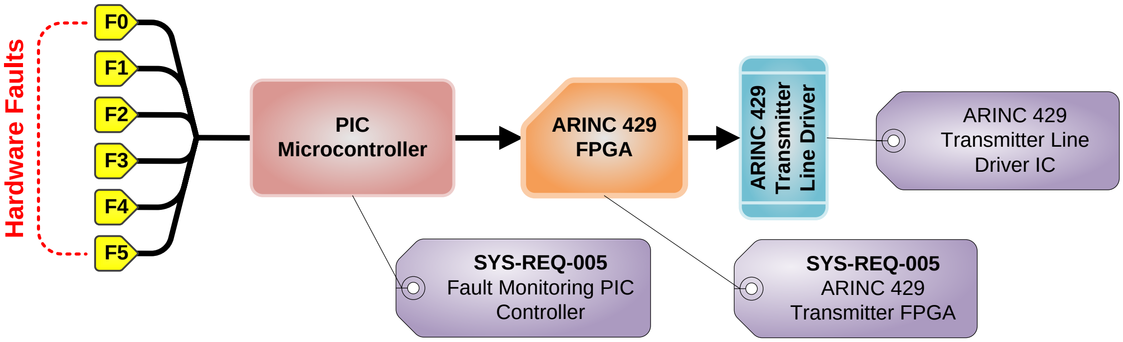
The headcount adjustment/correction data is generated by the keypad entry panel. This panel puts out a value typed by the user as well as a return key strobe signal. Both signals are sent to the FPGA for headcount adjustment/correction. The return key strobe signal is used to latch the value typed by the user into the FPGA logics.

3.1.4 Display Panel



The display panel simply displays the current headcount outputted by the FPGA.

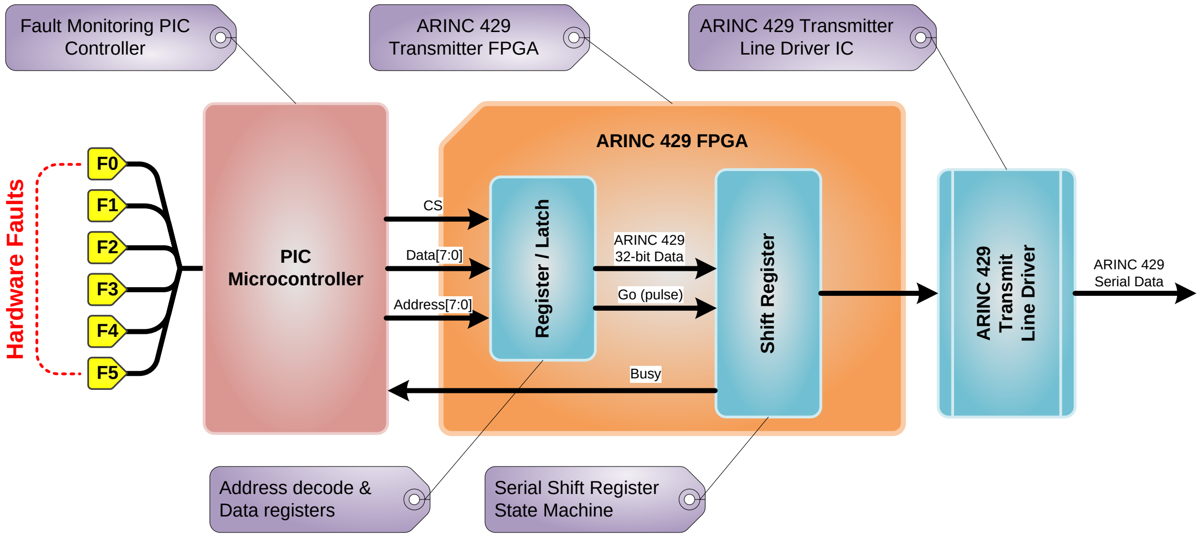
3.1.5 PIC Controller Interface & Fault Monitoring


Hardware Faults
F0
F1
F2
F3
F4
F5
PIC Microcontroller
ARINC 429 FPGA
ARINC 429 Transmitter Line Driver
ARINC 429 Transmitter Line Driver IC
SYS-REQ-005 Fault Monitoring PIC Controller
SYS-REQ-005 ARINC 429 Transmitter FPGA

The Fault monitoring circuit monitors the sequences, timings and states of the Entry / Exit Detection sensor, Reset controller, keypad entry and the display panel. All of this information is fed to and analyzed by the PIC microcontroller. The PIC microcontroller's software knows all the correct signal sequences, timing & states for all the interfaces. A fault is detected when a signal set is not within the predetermined constraints. The PIC controller then generates a fault message in the form able to fit into two 429 words which are sent to the FPGA. The FPGA then generates the appropriate serial ARINC 429 streams to the line driver which translates it out into the appropriate ARINC 429 signal level. The fault message is then sent to the maintenance computer via the ARINC 429 link. The cockpit multifunction display is used in maintenance aspects of the system. This is not a critical function and is used for maintenance and information only in the cockpit. The display reader provides the current passenger headcount to the flight attendant as the critical record for total headcount.

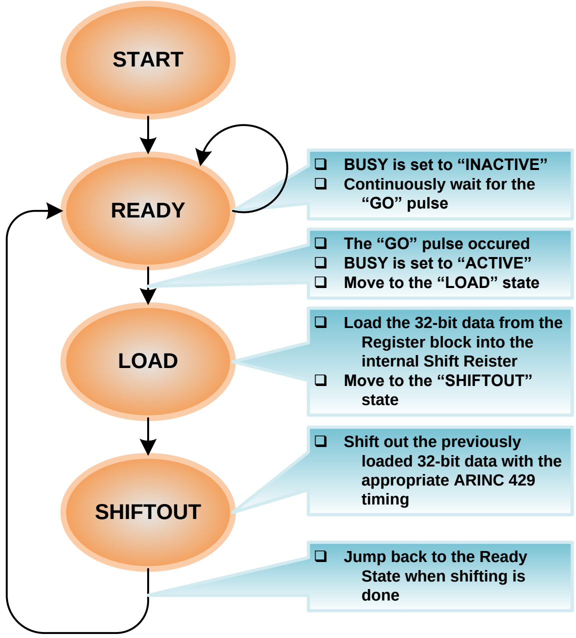
3.1.5.1 PIC Controller & ARINC 429 FPGA Interface

The ARINC 429 FPGA is connected to the PIC Microcontroller via a standard 8-bit bus interface. There are 8-bit data, 8-bit address and a chip-select (CE) line. There is also one GPIO that is used as an input to the PIC Microcontroller to indicate when the ARINC 429 FPGA is busy / sending data.


Fault Monitoring PIC Controller
ARINC 429 Transmitter FPGA
ARINC 429 Transmitter Line Driver IC
Hardware Faults
F0
F1
F2
F3
F4
F5
PIC Microcontroller
ARINC 429 FPGA
CS
Data[7:0]
Address[7:0]
Register / Latch
ARINC 429 32-bit Data
Go (pulse)
Shift Register
Busy
ARINC 429 Transmit Line Driver
ARINC 429 Serial Data
Address decode & Data registers
Serial Shift Register State Machine

The ARINC 429 FPGA has to internal blocks: the Latch and the Shift Register. The Latch contains four 8-bit register that the Microcontroller can write to: each representing ¼ of the full ARINC 429 packet. These four register are made available to the next block in the form of a complete 32-bit bus/register to be loaded to the shift register. The Latch also contains a dummy register which, when written to, will send short pulse to the Shift Register. This short pulse will trigger the next block, the Shift register to load the data and serially shift out the data in the appropriate ARINC 429 for format.

The final block in the ARINC 429 FPGA is the Shift Register. This block is really combination of a state machine and a shift register (shown in the figure below). The sole purpose of this block is to serially shift the 32-bit ARINC 429 data with the appropriate timings.


START
READY
LOAD
SHIFTOUT
❑ BUSY is set to "INACTIVE"
❑ Continuously wait for the "GO" pulse
❑ The "GO" pulse occured
❑ BUSY is set to "ACTIVE"
❑ Move to the "LOAD" state
❑ Load the 32-bit data from the Register block into the internal Shift Reister
❑ Move to the "SHIFTOUT" state
❑ Shift out the previously loaded 32-bit data with the appropriate ARINC 429 timing
❑ Jump back to the Ready State when shifting is done

When a fault is detected, the PIC controller determines that a message needs to be sent. It internally constructs the 32-bit ARINC 429 packet in four bytes and writes them out into the FPGA Registers. The Microcontroller then waits for the Busy signal (from the FPGA Shift Register block) to indicate a ready state (inactive). When the Busy signal indicates a "ready" state, the controller writes to a dummy register to initiate the serial transfer.

3.2 Hardware Safety and Partitioning

The system is composed of diagnostics and other fail-safe mechanisms used to ensure that failures of the system are detected and that the system goes to a safe state if it's unable to perform a safety function. The hardware will be designed so that it will continue to operate, possibly at a reduced level, rather than failing completely, when some part of the system fails. During this condition, a visible fault indication will be present.

3.3 Hardware Device Characteristics

3.3.1 FPGA Device #1

<Description of major functions here>

3.3.1.1 Device Identification

<Device ID, Manufacturer, etc.>

3.3.1.2 SEU Susceptibility

The FPGA has non-volatile logic that performs a continuous CRC (CRC-32) test against the volatile configuration data. If a mismatch is detected, it is assumed the system no longer has integrity and resets.

The FPGA has non-volatile logic that performs a continuous CRC (CRC-32) test against the volatile configuration data. If a mismatch is detected, it is assumed the system no longer has integrity and resets. The following techniques will be used to mitigate this effect.

3.3.1.2.1 Scrubbing and Readback with Compare

The periodic refresh of the FPGA configuration memory is called configuration scrubbing (or simply, scrubbing). Scrubbing will be performed periodically to ensure that a single upset is present no longer than the time it takes to refresh the entire FPGA configuration memory. Alternatively, the configuration bitstream may be read and compared to a golden copy and the configuration refresh only done when an error in the bitstream is detected. This is the preferred method as reading the configuration memory is faster than writing to it. This procedure is called readback with compare, and is also often referred to as scrubbing.

Although scrubbing ensures that the configuration bistream is free of errors, there is a period of time between the moment the upset occurs and the moment when it is repaired in which the FPGA configuration is incorrect. Thus the design may not function correctly during that time. To completely mitigate the errors caused by SEUs, scrubbing must be used in conjunction with another form of mitigation that masks the faults in the bitstream. The most popular of these techniques is triple modular redundancy (TMR). TMR is a well-known technique that masks any single-bit fault in the configuration bitstream. Combined with scrubbing, which is used to ensure that no more than one configuration bit is upset at any point in time, TMR can completely mask the effects of SEUs.