



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 of Contents

Section	Page
1.0 INTRODUCTION	13
1.1 Purpose	13
1.2 Scope	13
1.3 Definitions	13
1.4 Part Number and Nomenclature	15
1.5 Team Members and Signature Authority	16
1.5.1 Independent Reporting Structure	17
1.6 Acronyms and Abbreviations	18
1.7 Applicable Documents	19
1.7.1 External Documents	19
1.7.2 Internal Documents	19
2.0 SYSTEM OVERVIEW	20
2.1 Mechanical Systems Top level Diagram	20
2.1.1 System Functions Allocated to Mechanical Hardware	20
2.2 Electrical Systems Top Level Block Diagram	21
2.2.1 System Functions Allocated to Electrical Hardware and Software	22
2.2.1.1 Data Acquisition Printed Circuit Board #1	22
2.2.1.2 Input / Output Printed Circuit Board #2	22
2.2.1.3 Monitor Printed Circuit Board #3	22
2.3 System Functional Description	23
2.3.1 System Failure Conditions	24
2.3.2 High-Level Hardware Functions and Contribution to Potential Failures	24
2.3.3 Safety and Partitioning	24
3.0 HARDWARE OVERVIEW	25
3.1 Hardware Functions	25
3.1.1 Computation	26
3.1.2 Entry/Exit sensor	27
3.1.3 Keypad Entry Panel	27
3.1.4 Display Panel	27
3.1.5 PIC Controller Interface & Fault Monitoring	28
3.1.5.1 PIC Controller & ARINC 429 FPGA Interface	29
3.2 Hardware Safety and Partitioning	31
3.3 Single Event Upset Planning	31
3.3.1 Scrubbing and Readback with Compare	31
3.3.2 Triple Modular Redundancy	32

3.4	Hardware Components.....	33
3.4.1	Data Acquisition Printed Circuit Board #1	33
3.4.1.1	Major Function #1	33
3.4.1.2	Major Function #2.....	33
3.4.1.3	Major Function #3.....	33
3.4.1.4	Operation Under Environmental Conditions	33
3.4.1.5	FPGA #1	34
3.4.1.5.1	Intellectual Property Cores.....	34
3.4.1.5.2	Hardware Functions Allocated To Device	34
3.4.1.5.3	IP Core Compliance	34
3.4.1.5.4	SEU Susceptibility	34
3.4.1.5.5	Errata Sheet Analysis.....	34
3.4.1.5.6	Operation Under Environmental Conditions	34
3.4.1.6	COTS #1	35
3.4.1.6.1	Hardware Functions Allocated To Device	35
3.4.1.6.2	COTS Device Classification.....	35
3.4.1.6.3	COTS Lifecycle Data.....	36
3.4.1.6.4	Analysis of the component manufacturer Errata sheets	37
3.4.1.6.5	HW/HW and HW/SW integration	38
3.4.1.6.6	SEU Susceptibility	39
3.4.1.6.7	Errata Sheet Analysis.....	39
3.4.1.6.8	Operation Under Environmental Conditions	39
4.0	CERTIFICATION CONSIDERATIONS	40
4.1	Certification Basis and Means of Compliance	40
4.2	Issue Papers and Certification Review Items (CRI)	40
4.3	Hardware Level Determination	40
4.4	Compliance Matrix.....	42
4.5	Certification Authority Level of Involvement.....	58
4.5.1	Certification Authority Criteria for Level of Involvement.....	59
4.5.2	Proposed Level of Involvement.....	59

5.0	HARDWARE DESIGN LIFECYCLE	60
5.1	Team Member Responsibilities	61
5.2	Relationship Between Processes and Activities.....	66
5.3	Interaction Among Processes	67
5.3.1	System Lifecycle Flow Diagram.....	67
5.3.2	Hardware and Software Lifecycle Flow Diagram.....	68
5.4	Means of Providing Feedback	69
5.5	Planning Process	70
5.5.1	Planning Process Objectives	70
5.5.2	Planning Process Inputs.....	70
5.5.3	Planning Process Outputs.....	71
5.5.4	Planning Process Activities	71
5.5.5	Technical Interfaces.....	71
5.5.6	Planning Process Tool Usage	72
5.5.7	Planning Process Transition Criteria	72
5.5.7.1	Transition Criteria for Entry into Planning Process	72
5.5.8	Integral Processes	74
5.5.8.1	Validation & Verification Process Objectives and Activities	74
5.5.8.1.1	Hardware Validation & Verification Plan Preparation.....	74
5.5.8.1.2	Reviews and Analysis.....	74
5.5.8.1.2.1	Hardware Planning Review	75
5.5.8.2	Configuration Management Objectives and Activities	76
5.5.8.2.1	Configuration Management Plan Preparation.....	76
5.5.8.2.2	Configuration Identification, Baselines and Traceability	76
5.5.8.2.3	Configuration Status Accounting.....	76
5.5.8.2.4	Problem Reporting, Tracking and Corrective Action.....	77
5.5.8.2.5	Change Control and Change Review	77
5.5.8.3	Process Assurance Objectives and Activities	78
5.5.8.3.1	Process Assurance Plan Preparation	78
5.5.8.3.2	PA Independence during the Planning Process	78
5.5.8.3.3	PA Audits	78
5.5.8.3.4	PA Conformity Review Planning	78
5.5.8.3.5	Hardware Transition Criteria Satisfaction Review.....	79
5.5.8.3.6	PA Reporting and Corrective Action	79
5.5.8.4	Certification Liaison Objectives and Activities	80
5.5.8.4.1	Means of Compliance and Planning	80
5.5.8.4.2	Compliance Substantiation.....	80
5.6	Development Flow Diagrams	81
5.6.1	Analog Hardware Development Flow.....	81
5.6.2	Complex Hardware Development Flow	82

- 5.7 Requirements Capture Process 85
 - 5.7.1 Requirements Capture Process Objectives 85
 - 5.7.2 Requirements Capture Process Inputs..... 85
 - 5.7.3 Requirements Capture Process Outputs 85
 - 5.7.4 Requirements Capture Process Activities 86
 - 5.7.5 Technical Interfaces 88
 - 5.7.6 Requirements Capture Process Tool Usage 88
 - 5.7.7 Requirements Capture Process Transition Criteria..... 88
 - 5.7.7.1 Transition Criteria for Entry into Requirements Process 88
 - 5.7.7.2 Transition Criteria for Exit from Requirements Process 89
 - 5.7.8 Integral Processes 90
 - 5.7.8.1 Validation & Verification Process Objectives and Activities 90
 - 5.7.8.1.1 Reviews and Analysis 90
 - 5.7.8.1.1.1 Hardware Requirements Peer Reviews 90
 - 5.7.8.1.1.2 Hardware Requirements Transition Review 91
 - 5.7.8.2 Configuration Management Objectives and Activities 92
 - 5.7.8.2.1 Configuration Identification, Baselines and Traceability 92
 - 5.7.8.2.2 Configuration Status Accounting 92
 - 5.7.8.2.3 Problem Reporting, Tracking and Corrective Action..... 93
 - 5.7.8.2.4 Change Control and Change Review 93
 - 5.7.8.3 Process Assurance Objectives and Activities 94
 - 5.7.8.3.1 PA Audits 94
 - 5.7.8.3.2 Hardware Transition Criteria Satisfaction Review..... 94
 - 5.7.8.3.3 PA Reporting and Corrective Action 94
 - 5.7.8.4 Certification Liaison Objectives and Activities 95
 - 5.7.8.4.1 Means of Compliance and Requirements 95
 - 5.7.8.4.2 Compliance Substantiation..... 95
 - 5.8 Conceptual Design Process 96
 - 5.8.1 Conceptual Design Process Objectives 96
 - 5.8.2 Conceptual Design Process Inputs..... 96
 - 5.8.3 Conceptual Design Process Outputs..... 96
 - 5.8.4 Conceptual Design Process Activities 97
 - 5.8.5 Technical Interfaces 97
 - 5.8.6 Conceptual Design Process Tool Usage..... 98
 - 5.8.7 Conceptual Design Process Transition Criteria 99
 - 5.8.7.1 Transition Criteria for Entry into Conceptual Design Process 99
 - 5.8.7.2 Transition Criteria for Exit from Conceptual Design Process 100

- 5.8.8 Integral Processes 101
 - 5.8.8.1 Validation & Verification Process Objectives and Activities 101
 - 5.8.8.1.1 Reviews and Analysis 101
 - 5.8.8.1.1.1 Hardware Conceptual Design Peer Reviews 101
 - 5.8.8.1.1.2 Hardware Preliminary Design Transition Review 102
 - 5.8.8.2 Configuration Management Objectives and Activities 103
 - 5.8.8.2.1 Configuration Identification, Baselines and Traceability 103
 - 5.8.8.2.2 Configuration Status Accounting 103
 - 5.8.8.2.3 Problem Reporting, Tracking and Corrective Action 104
 - 5.8.8.2.4 Change Control and Change Review 104
 - 5.8.8.3 Process Assurance Objectives and Activities 105
 - 5.8.8.3.1 PA Audits 105
 - 5.8.8.3.2 Hardware Transition Criteria Satisfaction Review 105
 - 5.8.8.3.3 PA Reporting and Corrective Action 105
 - 5.8.8.4 Certification Liaison Objectives and Activities 106
 - 5.8.8.4.1 Means of Compliance and Requirements 106
 - 5.8.8.4.2 Compliance Substantiation 106
- 5.9 Detail Design Process 107
 - 5.9.1 Detail Design Process Inputs 107
 - 5.9.2 Detail Design Process Outputs 107
 - 5.9.3 Detail Design Process Activities 108
 - 5.9.4 Technical Interfaces 109
 - 5.9.5 Detail Design Process Tool Usage 110
 - 5.9.6 Detail Design Process Transition Criteria 110
 - 5.9.6.1 Transition Criteria for Entry into Detailed Design Process 110
 - 5.9.6.2 Transition Criteria for Exit from Detailed Design Process 111
 - 5.9.7 Integral Processes 112
 - 5.9.7.1 Validation & Verification Process Objectives and Activities 112
 - 5.9.7.1.1 Reviews and Analysis 112
 - 5.9.7.1.1.1 Hardware Detailed Design Peer Reviews 112
 - 5.9.7.1.1.2 Hardware Critical Design Transition Review 113
 - 5.9.7.2 Configuration Management Objectives and Activities 114
 - 5.9.7.2.1 Configuration Identification, Baselines and Traceability 114
 - 5.9.7.2.2 Configuration Status Accounting 114
 - 5.9.7.2.3 Problem Reporting, Tracking and Corrective Action 115
 - 5.9.7.2.4 Change Control and Change Review 115
 - 5.9.7.3 Process Assurance Objectives and Activities 116
 - 5.9.7.3.1 PA Audits 116
 - 5.9.7.3.2 Hardware Transition Criteria Satisfaction Review 116
 - 5.9.7.3.3 PA Reporting and Corrective Action 116
 - 5.9.7.4 Certification Liaison Objectives and Activities 117
 - 5.9.7.4.1 Means of Compliance and Requirements 117
 - 5.9.7.4.2 Compliance Substantiation 117

- 5.10 Implementation Process 118
 - 5.10.1 Implementation Process Objectives 118
 - 5.10.2 Implementation Process Inputs..... 118
 - 5.10.3 Implementation Process Outputs..... 118
 - 5.10.4 Implementation Process Activities 118
 - 5.10.5 Technical Interfaces 119
 - 5.10.6 Implementation Process Tool Usage 119
 - 5.10.7 Implementation Process Transition Criteria 120
 - 5.10.7.1 Transition Criteria for Entry into Implementation Process 120
 - 5.10.7.2 Transition Criteria for Exit from Implementation Process 121
 - 5.10.8 Integral Processes 122
 - 5.10.8.1 Validation & Verification Process Objectives and Activities 122
 - 5.10.8.1.1 Reviews and Analysis 122
 - 5.10.8.1.1.1 Hardware Implementation Peer Reviews 122
 - 5.10.8.1.1.2 Hardware Implementation Transition Review..... 122
 - 5.10.8.2 Configuration Management Objectives and Activities 123
 - 5.10.8.2.1 Configuration Identification, Baselines and Traceability 123
 - 5.10.8.2.2 Configuration Status Accounting 123
 - 5.10.8.2.3 Problem Reporting, Tracking and Corrective Action 124
 - 5.10.8.2.4 Change Control and Change Review 124
 - 5.10.8.3 Process Assurance Objectives and Activities..... 125
 - 5.10.8.3.1 PA Audits 125
 - 5.10.8.3.2 Hardware Transition Criteria Satisfaction Review 125
 - 5.10.8.3.3 PA Reporting and Corrective Action 125
 - 5.10.8.4 Certification Liaison Objectives and Activities 126
 - 5.10.8.4.1 Means of Compliance and Requirements 126
 - 5.10.8.4.2 Compliance Substantiation 126
 - 5.11 Testing Process..... 127
 - 5.11.1 Testing Process Objectives 127
 - 5.11.2 Testing Process Inputs..... 127
 - 5.11.3 Testing Process Outputs..... 128
 - 5.11.4 Testing Process Activities 128
 - 5.11.4.1 Test Case and Test Procedure Development 128
 - 5.11.5 Technical Interfaces 129
 - 5.11.6 Testing Process Tool Usage 129
 - 5.11.6.1 Simulation and On-Target Testing 130
 - 5.11.6.2 Test Execution and Test Results Compilation 130
 - 5.11.6.3 Elemental Analysis Resolution 130
 - 5.11.7 Testing Process Transition Criteria..... 131
 - 5.11.7.1 Transition Criteria for Entry into Testing Process 131
 - 5.11.7.2 Transition Criteria for Exit from Testing Process..... 131

- 5.11.8 Integral Processes 132
 - 5.11.8.1 Validation & Verification Process Objectives and Activities 132
 - 5.11.8.1.1 Reviews and Analysis 132
 - 5.11.8.1.1.1 Hardware Verification Peer Reviews 132
 - 5.11.8.1.1.2 Requirements-Based Test Coverage Analysis..... 132
 - 5.11.8.1.1.3 Elemental Analysis 132
 - 5.11.8.1.1.4 Hardware Verification Transition Review 133
 - 5.11.8.2 Configuration Management Objectives and Activities 133
 - 5.11.8.2.1 Configuration Identification, Baselines and Traceability 133
 - 5.11.8.2.2 Configuration Status Accounting 134
 - 5.11.8.2.3 Problem Reporting, Tracking and Corrective Action 134
 - 5.11.8.2.4 Change Control and Change Review 135
 - 5.11.8.3 Process Assurance Objectives and Activities 136
 - 5.11.8.3.1 PA Audits 136
 - 5.11.8.3.2 Hardware Transition Criteria Satisfaction Review 136
 - 5.11.8.3.3 PA Reporting and Corrective Action 136
 - 5.11.8.4 Certification Liaison Objectives and Activities 137
 - 5.11.8.4.1 Means of Compliance and Requirements 137
 - 5.11.8.4.2 Compliance Substantiation 137
 - 5.12 Production Transition Process..... 138
 - 5.12.1 Production Transition Process Objectives 138
 - 5.12.2 Production Transition Process Inputs 138
 - 5.12.3 Production Transition Process Outputs 138
 - 5.12.4 Production Transition Process Activities 139
 - 5.12.5 Technical Interfaces 139
 - 5.12.6 Hardware Production Transition Process Tool Usage 139
 - 5.12.7 Production Transition Process Transition Criteria..... 140
 - 5.12.7.1 Transition Criteria for Entry into Production Transition Process..... 140
 - 5.12.7.2 Transition Criteria for Exit from Production Transition Process..... 141
 - 5.12.8 Integral Processes 141
 - 5.12.8.1 Validation & Verification Process Objectives and Activities 141
 - 5.12.8.1.1 Reviews and Analysis 141
 - 5.12.8.1.1.1 Production Transition Review 142
 - 5.12.8.1.1.2 Hardware Conformity Review 142
 - 5.12.8.2 Configuration Management Objectives and Activities 143
 - 5.12.8.2.1 Configuration Identification, Baselines and Traceability 143
 - 5.12.8.2.2 Configuration Status Accounting 143
 - 5.12.8.2.3 Problem Reporting, Tracking and Corrective Action 143
 - 5.12.8.2.4 Change Control and Change Review 144
 - 5.12.8.3 Process Assurance Objectives and Activities 144
 - 5.12.8.3.1 PA Audits 144
 - 5.12.8.3.2 Hardware Transition Criteria Satisfaction Review 144
 - 5.12.8.3.3 PA Reporting and Corrective Action 144
 - 5.12.8.4 Certification Liaison Objectives and Activities 145
 - 5.12.8.4.1 Means of Compliance and Requirements 145
 - 5.12.8.4.2 Compliance Substantiation 145

6.0	HARDWARE DESIGN LIFECYCLE DATA.....	146
6.1	Overview	146
6.2	Trace Data	146
6.2.1	Trace Data Objective Evidence of Compliance	147
6.3	Hardware Lifecycle Data To Be Produced and Controlled	148
6.4	Hardware Lifecycle Data to Be Submitted To Certification Authority	153
6.5	Hardware Control Categories	154
6.6	Hardware Lifecycle Data DER Delegation Plan.....	155
7.0	ADDITIONAL CONSIDERATIONS	156
7.1	Use of Previously Developed Hardware.....	156
7.1.1	ARINC 429 I/O FPGA.....	156
7.1.1.1	Product Service Experience Data Acceptability Criteria.....	156
7.1.1.1.1	Similarity – Application, Function, Operating Environment, and DAL ..	156
7.1.1.1.1	Product Service Experience Calculation.....	157
7.1.2	ARINC 429 I/O FPGA Re-verification.....	158
7.2	Use of Commercial-Off-The-Shelf (COTS) Components	158
7.3	SH-1 Issue paper compliance.....	158
7.3.1	Modifiable Devices	158
7.3.2	Certification Plan	158
7.3.3	Validation Processes	158
7.3.4	Verification Processes.....	158
7.3.5	Traceability.....	158
7.3.6	Configuration Management	158
7.3.7	Simple Electronic Hardware (SEH).....	159
7.3.8	Legacy Airborne Systems & Equipment Electronic Hardware.....	159
7.3.9	Commercial Off-The-Shelf (COTS) Microprocessors.....	159
7.3.10	Random Access Memory (RAM) based FPGAs	159
7.4	Safety Considerations.....	159
7.5	Tool Assessment and Qualification	160
7.5.1	Development Tools	161
7.5.1.1	Qualification of Development Tools	161
7.5.2	Verification Tools.....	162
7.5.2.1	Qualification of Verification Tools.....	162
7.6	Design Assurance Considerations	163
7.7	Use of Suppliers, Sub-Tier Suppliers and Off-Shore Facilities	163
7.7.1	Supplier Identification and Roles.....	164
7.7.1.1	Acme Consultants, Inc.	164
7.7.1.2	Supplier Competence Questionnaire Example	166
7.7.1.3	Supplier Management Plan	168
7.8	Deviations and Modifications to Plans.....	169

8.0	ALTERNATIVE METHODS	170
9.0	CERTIFICATION SCHEDULE	171
9.1	Master Project Schedule.....	171
9.1.1	Stages of Involvement Audit Schedule.....	172
9.2	Certification Authority Web Interface	173
9.2.1	Project-Level Integrated Compliance Management System	174
9.2.1.1	SecureWeb Security Management System	175
9.2.1.2	Problem Reporting Management System.....	176
9.2.1.3	Change Impact Analysis Management System.....	177
9.2.1.4	Document Review Management System	178
9.2.1.5	Reviews and Analysis Management System.....	179
9.2.1.6	Requirements Traceability Management System	180

List of Figures

Figure 1-1	Independent Reporting Structure	17
Figure 2-1	System Level Block Diagram	21
Figure 2-2	System Functional Diagram.....	23
Figure 5-1	Relationship Between Processes and Activities	66
Figure 5-2	System Lifecycle Flow Diagram	67
Figure 5-3	Hardware and Software Lifecycle Diagram	68
Figure 5-4	Lifecycle Process Feedback Flow Diagram	69
Figure 5-5	Hardware Development Process	84
Figure 9-1	Certification Master Schedule.....	171
Figure 9-2	Certification Authority Web Interface	173
Figure 9-3	Integrated Compliance Management System	174
Figure 9-4	SecureWeb Login Screen	175
Figure 9-5	Problem Reporting System	176
Figure 9-6	Change Impact Analysis Management System.....	177
Figure 9-7	Document Review Management System	178
Figure 9-8	Reviews and Analysis Management System	179
Figure 9-9	Requirements Traceability Management System	180

List of Tables

Table 1-1 Definitions	14
Table 1-2 Part Number and Nomenclature	15
Table 1-3 Team Members and Signature Authority	16
Table 2-1 System Failure Conditions	24
Table 4-1 List of Compliance Documents	40
Table 4-2 List of Issue Papers and CRI's	40
Table 4-3 Design Assurance Levels	41
Table 4-4 Compliance Matrix – Planning Process	43
Table 4-5 Compliance Matrix – Requirements Capture Process	44
Table 4-6 Compliance Matrix – Conceptual Design Process	45
Table 4-7 Compliance Matrix – Detailed Design Process	46
Table 4-8 Compliance Matrix – Implementation Process	48
Table 4-9 Compliance Matrix – Production Transition Process	50
Table 4-10 Compliance Matrix – Validation and Verification Process	53
Table 4-11 Compliance Matrix – Configuration Management Process	54
Table 4-12 Compliance Matrix – Process Assurance Process	55
Table 4-13 Compliance Matrix – Certification Liaison Process	56
Table 4-14 Compliance Matrix – Appendix B Design Assurance Considerations	57
Table 4-15 Certification Authority Involvement Based on DAL	58
Table 4-16 Hardware Certification Experience	58
Table 4-17 Hardware Development Capability	58
Table 4-18 Hardware Service History	58
Table 4-19 System and Hardware Application Complexity	59
Table 4-20 FAA DER Capabilities – Todd R. White	59
Table 4-21 Level of Involvement Criteria Scoring	59
Table 5-1 Team Member Responsibilities	65
Table 5-2 Planning Process Objectives	70
Table 5-3 Planning Process Tools	72
Table 5-4 Requirements Capture Process Objectives	85
Table 5-5 Requirements Capture Process Tools	88
Table 5-6 Conceptual Design Process Objectives	96
Table 5-7 Conceptual Design Process Tools	98
Table 5-8 Detail Design Process Objectives	107
Table 5-9 Detail Design Process Tools	110
Table 5-10 Implementation Process Objectives	118
Table 5-11 Implementation Process Tools	119
Table 5-12 Testing Process Objectives	127
Table 5-13 Testing Process Tools	129
Table 5-14 Production Transition Process Objectives	138
Table 5-15 Production Transition Process Tools	139
Table 6-1 Lifecycle Data To Be Produced	152
Table 6-2 Lifecycle Data To Certification Authority	153
Table 6-3 Hardware Control Categories	154
Table 6-4 Hardware DER Delegation Plan	155
Table 7-1 Hardware Development Tools	161
Table 7-2 Hardware Verification Tools	162