



# Plan for Software 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
<b>1.0 INTRODUCTION</b> .....	<b>9</b>
1.1 Purpose.....	9
1.2 Scope .....	9
1.3 Part Number and Nomenclature .....	9
1.4 Team Members .....	10
1.4.1 <i>Independent Reporting Structure</i> .....	10
1.5 Acronyms and Abbreviations .....	11
1.6 Applicable Documents .....	12
1.6.1 <i>External Documents</i> .....	12
1.6.2 <i>Internal Documents</i> .....	13
<b>2.0 SYSTEM OVERVIEW</b> .....	<b>14</b>
2.1 System Description .....	14
2.1.1 <i>Top Level Block Diagram</i> .....	14
2.2 System Failure Conditions.....	14
2.2.1 <i>High-Level Software Functions and Contribution to Potential Failures</i> .....	14
2.3 System Architecture.....	15
2.3.1 <i>Architectural Method &lt; Example Text &gt;</i> .....	15
2.4 Processors <Example Text> .....	15
2.5 Hardware / Software Interfaces <Example Text> .....	15
2.6 Safety Features <Example Text> .....	15
<b>3.0 SOFTWARE OVERVIEW</b> .....	<b>16</b>
3.1 Software Description .....	16
3.2 Safety and Partitioning .....	16
3.3 Use of Object Oriented Technology .....	16
3.4 Deactivated Code Partitioning.....	16
3.4.1 <i>USB Interface Code</i> .....	16
3.4.2 <i>RS-232 Interface Code</i> .....	16
3.4.3 <i>Ethernet Interface Code</i> .....	16
3.4.4 <i>Boot Load Code Partitioning</i> .....	16
3.5 Resource Sharing <Example Text> .....	17
3.6 Redundancy .....	17
3.7 Fault Tolerance <Example Text> .....	17
3.8 Timing and Task Scheduling .....	17
3.8.1 <i>Timing &lt;Example Text&gt;</i> .....	17
3.8.2 <i>Task Scheduling &lt;Example Text&gt;</i> .....	17
<b>4.0 CERTIFICATION CONSIDERATIONS</b> .....	<b>18</b>
4.1 Certification Basis and Means of Compliance .....	18
4.1.1 <i>Reference to TC, STC, TSO, FAA Papers, Advisory Circulars, Etc.</i> .....	18
4.2 Software Level Determination.....	18
4.2.1 <i>System Safety Assessment Results</i> .....	19
4.3 Compliance Matrix .....	20
4.3.1 <i>Software Conformity Objectives</i> .....	41

<b>5.0 SOFTWARE LIFECYCLE .....</b>	<b>52</b>
5.1 Team Member Responsibilities .....	53
5.2 Relationship Between Processes and Activities .....	56
5.3 Interaction Among Processes.....	57
5.4 Means of Providing Feedback.....	57
5.5 Software Planning Process .....	58
5.5.1 Software Planning Process Objectives .....	58
5.5.2 Software Planning Process Inputs.....	58
5.5.3 Software Planning Process Outputs.....	59
5.5.4 Software Planning Process Activities .....	59
5.5.4.1 Technical Interfaces .....	59
5.5.4.2 Software Planning Process Tool Usage .....	60
5.5.4.3 Software Planning Process Transition Criteria.....	60
5.5.4.3.1 Transition Criteria for Entry into Planning Process.....	60
5.5.4.3.2 Transition Criteria for Exit from Planning Process.....	61
5.5.4.4 Integral Processes .....	62
5.5.4.4.1 Software Verification Process Objectives and Activities .....	62
5.5.4.4.1.1 Software Verification Plan Preparation.....	62
5.5.4.4.1.2 Software Reviews and Analysis .....	62
5.5.4.4.2 Software Configuration Management Objectives and Activities.....	64
5.5.4.4.2.1 Configuration Management Plan Preparation .....	64
5.5.4.4.2.2 Configuration Identification, Baselines and Traceability.....	64
5.5.4.4.2.3 Configuration Status Accounting.....	64
5.5.4.4.2.4 Problem Reporting, Tracking and Corrective Action .....	65
5.5.4.4.2.5 Change Control and Change Review.....	65
5.5.4.4.3 Software Quality Assurance Objectives and Activities .....	66
5.5.4.4.3.1 Software Quality Assurance Plan Preparation .....	66
5.5.4.4.3.2 SQA Independence during the Planning Process .....	66
5.5.4.4.3.3 SQA Audits .....	66
5.5.4.4.3.4 SQA Conformity Review Planning .....	66
5.5.4.4.3.5 Software Transition Criteria Satisfaction Review .....	67
5.5.4.4.3.6 SQA Reporting and Corrective Action .....	67
5.5.4.4.4 Certification Liaison Objectives and Activities .....	68
5.5.4.4.4.1 Means of Compliance and Planning .....	68
5.5.4.4.4.2 Compliance Substantiation .....	68

5.6	Software Requirements Process .....	69
5.6.1	Software Requirements Process Objectives .....	69
5.6.2	Software Requirements Process Inputs .....	69
5.6.3	Software Requirements Process Outputs .....	69
5.6.4	Software Requirements Process Activities .....	70
5.6.5	Technical Interfaces .....	71
5.6.6	Software Requirements Process Tool Usage .....	71
5.6.7	Software Requirements Process Transition Criteria .....	72
5.6.7.1	Transition Criteria for Entry into Requirements Process .....	72
5.6.7.2	Transition Criteria for Exit from Requirements Process .....	73
5.6.8	Integral Processes .....	73
5.6.8.1	Software Verification Process Objectives and Activities .....	73
5.6.8.1.1	Software Reviews and Analysis .....	74
5.6.8.2	Software Configuration Management Objectives and Activities .....	76
5.6.8.2.1	Configuration Identification, Baselines and Traceability .....	76
5.6.8.2.2	Configuration Status Accounting .....	76
5.6.8.2.3	Problem Reporting, Tracking and Corrective Action .....	77
5.6.8.2.4	Change Control and Change Review .....	77
5.6.8.3	Software Quality Assurance Objectives and Activities .....	78
5.6.8.3.1	SQA Audits .....	78
5.6.8.3.2	Software Transition Criteria Satisfaction Review .....	78
5.6.8.3.3	SQA Reporting and Corrective Action .....	78
5.6.8.4	Certification Liaison Objectives and Activities .....	79
5.6.8.4.1	Means of Compliance and Requirements .....	79
5.6.8.4.2	Compliance Substantiation .....	79
5.7	Software Design Process .....	80
5.7.1	Software Design Process Objectives .....	80
5.7.2	Software Design Process Inputs .....	80
5.7.3	Software Design Process Outputs .....	80
5.7.4	Software Design Process Activities .....	80
5.7.5	Technical Interfaces .....	81
5.7.6	Software Design Process Tool Usage .....	81
5.7.7	Software Design Process Transition Criteria .....	82
5.7.7.1	Transition Criteria for Entry into Design Process .....	82
5.7.7.2	Transition Criteria for Exit from Design Process .....	83
5.7.8	Integral Processes .....	84
5.7.8.1	Software Verification Process Objectives and Activities .....	84
5.7.8.1.1	Software Reviews and Analysis .....	84
5.7.8.2	Software Configuration Management Objectives and Activities .....	87
5.7.8.2.1	Configuration Identification, Baselines and Traceability .....	87
5.7.8.2.2	Configuration Status Accounting .....	87
5.7.8.2.3	Problem Reporting, Tracking and Corrective Action .....	88
5.7.8.2.4	Change Control and Change Review .....	88
5.7.8.3	Software Quality Assurance Objectives and Activities .....	89
5.7.8.3.1	SQA Audits .....	89
5.7.8.3.2	Software Transition Criteria Satisfaction Review .....	89
5.7.8.3.3	SQA Reporting and Corrective Action .....	89
5.7.8.4	Certification Liaison Objectives and Activities .....	90
5.7.8.4.1	Means of Compliance and Requirements .....	90
5.7.8.4.2	Compliance Substantiation .....	90

5.8	Software Coding Process.....	91
5.8.1	Software Coding Process Objectives .....	91
5.8.2	Software Coding Process Inputs.....	91
5.8.3	Software Coding Process Outputs.....	91
5.8.4	Software Coding Process Activities .....	92
5.8.5	Technical Interfaces .....	92
5.8.6	Software Coding Process Tool Usage.....	92
5.8.7	Software Coding Process Transition Criteria .....	92
5.8.7.1	Transition Criteria for Entry into Code Process.....	92
5.8.7.2	Transition Criteria for Exit from Code Process.....	93
5.8.8	Integral Processes .....	94
5.8.8.1	Software Verification Process Objectives and Activities .....	94
5.8.8.1.1	Software Reviews and Analysis .....	94
5.8.8.2	Software Configuration Management Objectives and Activities.....	95
5.8.8.2.1	Configuration Identification, Baselines and Traceability.....	95
5.8.8.2.2	Configuration Status Accounting.....	95
5.8.8.2.3	Problem Reporting, Tracking and Corrective Action .....	96
5.8.8.2.4	Change Control and Change Review.....	96
5.8.8.3	Software Quality Assurance Objectives and Activities .....	97
5.8.8.3.1	SQA Audits .....	97
5.8.8.3.2	Software Transition Criteria Satisfaction Review .....	97
5.8.8.3.3	SQA Reporting and Corrective Action .....	97
5.8.8.4	Certification Liaison Objectives and Activities .....	98
5.8.8.4.1	Means of Compliance and Requirements.....	98
5.8.8.4.2	Compliance Substantiation .....	98
5.9	Integration Process.....	99
5.9.1	Integration Process Objectives.....	99
5.9.2	Integration Process Inputs .....	99
5.9.3	Integration Process Outputs .....	99
5.9.4	Integration Process Activities.....	99
5.9.5	Technical Interfaces .....	99
5.9.6	Software Integration Process Tool Usage.....	100
5.9.7	Integration Process Transition Criteria .....	100
5.9.7.1	Transition Criteria for Entry into Integration Process .....	100
5.9.7.2	Transition Criteria for Exit from Integration Process .....	101
5.9.8	Integral Processes .....	102
5.9.8.1	Software Verification Process Objectives and Activities .....	102
5.9.8.1.1	Software Reviews and Analysis .....	102
5.9.8.2	Software Configuration Management Objectives and Activities.....	103
5.9.8.2.1	Configuration Identification, Baselines and Traceability.....	103
5.9.8.2.2	Configuration Status Accounting.....	103
5.9.8.2.3	Problem Reporting, Tracking and Corrective Action .....	104
5.9.8.2.4	Change Control and Change Review.....	104
5.9.8.3	Software Quality Assurance Objectives and Activities .....	105
5.9.8.3.1	SQA Audits .....	105
5.9.8.3.2	Software Transition Criteria Satisfaction Review .....	105
5.9.8.3.3	SQA Reporting and Corrective Action .....	105
5.9.8.4	Certification Liaison Objectives and Activities .....	106
5.9.8.4.1	Means of Compliance and Requirements.....	106
5.9.8.4.2	Compliance Substantiation .....	106

5.10	Software Testing Process .....	107
5.10.1	<i>Software Testing Process Objectives</i> .....	107
5.10.2	<i>Software Testing Process Inputs</i> .....	107
5.10.3	<i>Software Testing Process Outputs</i> .....	107
5.10.4	<i>Software Testing Process Activities</i> .....	108
5.10.4.1	Test Case and Test Procedure Development .....	108
5.10.4.2	Test Execution and Test Results Compilation .....	108
5.10.4.3	Structural Coverage Analysis Resolution .....	108
5.10.5	<i>Technical Interfaces</i> .....	108
5.10.6	<i>Software Testing Process Tool Usage</i> .....	109
5.10.7	<i>Software Testing Process Transition Criteria</i> .....	109
5.10.7.1	Transition Criteria for Entry into Software Testing Process .....	109
5.10.7.2	Transition Criteria for Exit from Software Testing Process .....	110
5.10.8	<i>Integral Processes</i> .....	111
5.10.8.1	Software Verification Process Objectives and Activities .....	111
5.10.8.1.1	Software Reviews and Analysis .....	111
5.10.8.2	Software Configuration Management Objectives and Activities .....	113
5.10.8.2.1	Configuration Identification, Baselines and Traceability .....	113
5.10.8.2.2	Configuration Status Accounting .....	113
5.10.8.2.3	Problem Reporting, Tracking and Corrective Action .....	114
5.10.8.2.4	Change Control and Change Review .....	114
5.10.8.3	Software Quality Assurance Objectives and Activities .....	115
5.10.8.3.1	SQA Audits .....	115
5.10.8.3.2	Software Transition Criteria Satisfaction Review .....	115
5.10.8.3.3	SQA Reporting and Corrective Action .....	115
5.10.8.4	Certification Liaison Objectives and Activities .....	116
5.10.8.4.1	Means of Compliance and Requirements .....	116
5.10.8.4.2	Compliance Substantiation .....	116
<b>6.0</b>	<b>SOFTWARE LIFECYCLE DATA</b> .....	<b>117</b>
6.1	Software Lifecycle Data to Be Produced and Controlled .....	118
6.2	Relationship of Lifecycle Data to Other Data Defining the System .....	120
6.3	Software Lifecycle Data to be Submitted to Certification Authority .....	121
6.4	Software Lifecycle Data DER Delegation Plan .....	122

<b>7.0 SCHEDULE.....</b>	<b>123</b>
7.1 Master Project Schedule .....	123
7.1.1 <i>Stages of Involvement Audit Schedule</i> .....	124
7.2 Certification Authority Web Interface .....	125
7.2.1 <i>Integrated Compliance Management System</i> .....	126
7.2.1.1 SecureWeb Security Management System .....	127
7.2.1.2 Problem Reporting Management System .....	128
7.2.1.3 Document Review Management System .....	129
7.2.1.4 Action Item Management System.....	130
7.2.1.5 Requirements Traceability Management System .....	131
7.2.1.6 Coverage Analysis Management System.....	132
<b>8.0 ADDITIONAL CONSIDERATIONS .....</b>	<b>133</b>
8.1 Use of Previously Developed Software .....	133
8.2 Tool Qualification.....	133
8.2.1 <i>Development Tools</i> .....	133
8.2.1.1 Qualification of Development Tools.....	133
8.2.2 <i>Verification Tools</i> .....	133
8.2.2.1 Qualification of Verification Tools.....	134
8.3 Alternative Methods .....	134
8.4 Field Loadable Software.....	134
8.5 Option Selectable Software .....	135
8.6 User Modifiable Software .....	135
8.7 Multiple-Version Dissimilar Software.....	135
8.8 COTS Software.....	135
8.9 Use of Contractors and Development at Off-Shore Facilities .....	135
8.10 Deviations and Modifications to Plans.....	135