DO Qualification Kit

Plan for Software Aspects of Certification (PSAC)

R2016b

How to Contact MathWorks

Latest news: [www.mathworks.com](http://www.mathworks.com/)

Sales and services: [www.mathworks.com/sales\_and\_services](http://www.mathworks.com/sales_and_services)

User community: [www.mathworks.com/matlabcentral](http://www.mathworks.com/matlabcentral/)

Technical support: [www.mathworks.com/support/contact\_us](http://www.mathworks.com/support/contact_us/)

Phone: 508-647-7000

The MathWorks, Inc.   
3 Apple Hill Drive  
Natick, MA 01760-2098

DO Qualification Kit: Plan for Software Aspects of Certification (PSAC)

© COPYRIGHT 2014 – 2015 by The MathWorks, Inc.

The software described in this document is furnished under a license agreement. The software may be used or copied only under the terms of the license agreement. No part of this manual may be photocopied or reproduced in any form without prior written consent from The MathWorks, Inc.

FEDERAL ACQUISITION: This provision applies to all acquisitions of the Program and Documentation by, for, or through the federal government of the United States. By accepting delivery of the Program or Documentation, the government hereby agrees that this software or documentation qualifies as commercial computer software or commercial computer software documentation as such terms are used or defined in FAR 12.212, DFARS Part 227.72, and DFARS 252.227-7014. Accordingly, the terms and conditions of this Agreement and only those rights specified in this Agreement, shall pertain to and govern the use, modification, reproduction, release, performance, display, and disclosure of the Program and Documentation by the federal government (or other entity acquiring for or through the federal government)and shall supersede any conflicting contractual terms or conditions. If this License fails to meet the government’s needs or is inconsistent in any respect with federal procurement law, the government agrees to return the Program and Documentation, unused, to The MathWorks, Inc.

Trademarks

MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See [www.mathworks.com/trademarks](http://www.mathworks.com/trademarks) for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.

Patents

MathWorks products are protected by one or more U.S. patents. Please see [www.mathworks.com/patents](http://www.mathworks.com/patents) for more information.

Revision History

March 2014 New for Version 2.3 (Applies to Release 2014a)

October 2014 Revised for Version 2.4 (Applies to Release 2014b)

March 2015 Revised for Version 2.5 (Applies to Release 2015a)

September 2015 Revised for DO Qualification Kit Version 3.0 (Applies to Release 2015b)

Document Title: **Plan for Software Aspects of Certification for <*Project*>.**

**Document Number: *<DocNo>***

Revision: ***<Revision>***

Project: **<*Project*>**

|  |  |  |
| --- | --- | --- |
| Approvals: |  |  |
| *<Name1>*, Author |  | Date |
|  |  |  |
| *<Name 2>*, Project Management |  | Date |
|  |  |  |
| *<Name 3>*, Engineering |  | Date |
|  |  |  |
| *<Name 4>*, Quality Engineering |  | Date |

| Change History | | | | |
| --- | --- | --- | --- | --- |
| Rev. | Modification / Description | Date | Author | Checked |
| 1.0 | *First release of Plan for Software Aspects of Certification (PSAC)* |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Contents

[1 Introduction 1-1](#_Toc472066821)

[1.1 Purpose and Scope 1-2](#_Toc472066822)

[1.2 Applicable Documents 1-3](#_Toc472066823)

[Table 1 – Regulations and Standards 1-3](#_Toc472066824)

[Table 2 – Company and Project Plans, Standards, and Documents 1-3](#_Toc472066825)

[1.3 Referenced Documents 1-5](#_Toc472066826)

[2 System Overview 2-1](#_Toc472066827)

[2.1 System Description 2-2](#_Toc472066828)

[2.2 System Architecture 2-3](#_Toc472066829)

[2.3 System Functions 2-4](#_Toc472066830)

[2.3.1 Function Allocation to Hardware 2-5](#_Toc472066831)

[2.3.2 Function Allocation to Software 2-5](#_Toc472066832)

[2.4 Processor Used 2-6](#_Toc472066833)

[2.5 Hardware and Software Interfaces 2-7](#_Toc472066834)

[2.6 Safety Features 2-8](#_Toc472066835)

[3 Software Overview 3-1](#_Toc472066836)

[3.1 Software Description 3-2](#_Toc472066837)

[3.2 Safety and Partitioning 3-3](#_Toc472066838)

[3.3 Timing and Scheduling Strategies 3-4](#_Toc472066839)

[4 Certification Considerations 4-1](#_Toc472066840)

[4.1 Certification Basis and Means of Compliance 4-2](#_Toc472066841)

[4.2 Software Level 4-3](#_Toc472066842)

[5 Software Life Cycle 5-1](#_Toc472066843)

[5.1 Software Life Cycle Description 5-2](#_Toc472066844)

[5.2 Software Planning Process 5-3](#_Toc472066845)

[5.2.1 Software Planning Process Objectives 5-3](#_Toc472066846)

[5.2.2 Software Planning Process Input 5-3](#_Toc472066847)

[5.2.3 Software Planning Process Output 5-4](#_Toc472066848)

[5.2.4 Software Planning Process Activities 5-5](#_Toc472066849)

[5.2.5 Software Planning Process Transition Criteria 5-5](#_Toc472066850)

[5.2.5.1 Software Planning Process Entry Criteria 5-5](#_Toc472066851)

[5.2.5.2 Software Planning Process Exit Criteria 5-5](#_Toc472066852)

[5.2.6 Integral Processes 5-5](#_Toc472066853)

[5.2.6.1 Software Configuration Management Activities 5-5](#_Toc472066854)

[5.2.6.2 Software Quality Assurance Activities 5-5](#_Toc472066855)

[5.3 Software Requirements Process 5-6](#_Toc472066856)

[5.3.1 Software Requirements Process Objectives 5-6](#_Toc472066857)

[5.3.2 Software Requirements Process Input 5-6](#_Toc472066858)

[5.3.3 Software Requirements Process Output 5-6](#_Toc472066859)

[5.3.4 Software Requirements Process Activities 5-6](#_Toc472066860)

[5.3.5 Software Requirements Process Transition Criteria 5-7](#_Toc472066861)

[5.3.5.1 Software Requirements Process Entry Criteria 5-7](#_Toc472066862)

[5.3.5.2 Software Requirements Process Exit Criteria 5-7](#_Toc472066863)

[5.3.6 Integral Processes 5-7](#_Toc472066864)

[5.3.6.1 Software Configuration Management Activities 5-7](#_Toc472066865)

[5.3.6.2 Software Quality Assurance Activities 5-7](#_Toc472066866)

[5.4 Software Design Process 5-8](#_Toc472066867)

[5.4.1 Software Design Process Objectives 5-8](#_Toc472066868)

[5.4.2 Software Design Process Input 5-8](#_Toc472066869)

[5.4.3 Software Design Process Output 5-8](#_Toc472066870)

[5.4.4 Software Design Process Activities 5-8](#_Toc472066871)

[5.4.5 Software Design Process Transition Criteria 5-9](#_Toc472066872)

[5.4.5.1 Software Requirements Process Entry Criteria 5-9](#_Toc472066873)

[5.4.5.2 Software Requirements Process Exit Criteria 5-9](#_Toc472066874)

[5.4.6 Integral Processes 5-9](#_Toc472066875)

[5.4.6.1 Software Configuration Management Activities 5-9](#_Toc472066876)

[5.4.6.2 Software Quality Assurance Activities 5-9](#_Toc472066877)

[5.5 Software Coding Process 5-10](#_Toc472066878)

[5.5.1 Software Coding Process Objectives 5-10](#_Toc472066879)

[5.5.2 Software Coding Process Input 5-10](#_Toc472066880)

[5.5.3 Software Coding Process Output 5-10](#_Toc472066881)

[5.5.4 Software Coding Process Activities 5-10](#_Toc472066882)

[5.5.5 Software Coding Process Transition Criteria 5-11](#_Toc472066883)

[5.5.5.1 Software Requirements Process Entry Criteria 5-11](#_Toc472066884)

[5.5.5.2 Software Requirements Process Exit Criteria 5-11](#_Toc472066885)

[5.5.6 Integral Processes 5-11](#_Toc472066886)

[5.5.6.1 Software Configuration Management Activities 5-11](#_Toc472066887)

[5.5.6.2 Software Quality Assurance Activities 5-11](#_Toc472066888)

[5.6 Integration Process 5-12](#_Toc472066889)

[5.6.1 Integration Process Objectives 5-12](#_Toc472066890)

[5.6.2 Integration Process Input 5-12](#_Toc472066891)

[5.6.3 Integration Process Output 5-12](#_Toc472066892)

[5.6.4 Integration Process Activities 5-12](#_Toc472066893)

[5.6.5 Integration Process Transition Criteria 5-13](#_Toc472066894)

[5.6.5.1 Software Requirements Process Entry Criteria 5-13](#_Toc472066895)

[5.6.5.2 Software Requirements Process Exit Criteria 5-13](#_Toc472066896)

[5.6.6 Integral Processes 5-13](#_Toc472066897)

[5.6.6.1 Software Configuration Management Activities 5-13](#_Toc472066898)

[5.6.6.2 Software Quality Assurance Activities 5-13](#_Toc472066899)

[5.7 Software Verification Process 5-14](#_Toc472066900)

[5.7.1 Software Verification Process Overview 5-14](#_Toc472066901)

[5.7.2 Reviews and Analyses 5-14](#_Toc472066902)

[5.7.2.1 Review and Analysis of Software Planning Process 5-14](#_Toc472066903)

[5.7.2.2 Review and Analysis of Software High-Level Requirements 5-14](#_Toc472066904)

[5.7.2.3 Review and Analysis of Specification Model 5-14](#_Toc472066905)

[5.7.2.4 Review and Analysis of Software Design Description 5-15](#_Toc472066906)

[5.7.2.5 Review and Analysis of Design Model 5-15](#_Toc472066907)

[5.7.2.6 Review and Analysis of Source Code 5-15](#_Toc472066908)

[5.7.2.7 Test Coverage Analysis 5-15](#_Toc472066909)

[5.7.3 Model Simulation 5-16](#_Toc472066910)

[5.7.4 Testing 5-16](#_Toc472066911)

[5.7.5 Additional Verification Requirements 5-17](#_Toc472066912)

[5.7.5.1 Traceability 5-17](#_Toc472066913)

[5.7.6 Derived Requirements 5-17](#_Toc472066914)

[5.7.7 Independence of Verification 5-17](#_Toc472066915)

[5.7.8 Integral Processes 5-18](#_Toc472066916)

[5.7.8.1 Software Configuration Management Activities 5-18](#_Toc472066917)

[5.7.8.2 Software Quality Assurance Activities 5-18](#_Toc472066918)

[6 Additional Considerations 6-1](#_Toc472066919)

[6.1 Tool Use and Qualification 6-1](#_Toc472066920)

[6.1.1 General 6-1](#_Toc472066921)

[6.1.2 Tools Used in Software Planning Process 6-1](#_Toc472066922)

[6.1.3 Tools Used in Software Development Process 6-1](#_Toc472066923)

[6.1.4 Tools Used in Software Verification Process 6-2](#_Toc472066924)

[6.1.5 Development Environment and Documentation Tools 6-3](#_Toc472066925)

[6.2 Use of Floating Point Numbers 6-4](#_Toc472066926)

[6.3 Use of Software Libraries 6-4](#_Toc472066927)

[6.4 Compiler Considerations 6-4](#_Toc472066928)

[6.5 Programming Languages 6-4](#_Toc472066929)

[7 Software Configuration Management Process 7-1](#_Toc472066930)

[8 Software Quality Assurance Process 8-1](#_Toc472066931)

[9 Certification Liaison Process 9-1](#_Toc472066932)

[10 Software Life Cycle Data 10-1](#_Toc472066933)

[11 Organization and Responsibilities 11-1](#_Toc472066934)

[12 Milestones and Schedule 12-1](#_Toc472066935)

# Introduction

## Purpose and Scope

The purpose of this document is to provide the Plan for Software Aspects of Certification (PSAC) for the project <*Project*>. This document provides the planning data defined in DO-178C, Section 11.1. The certification authority uses the PSAC for a project as the primary means to determine whether an applicant is proposing a software life cycle that is commensurate with the rigor required for the level of software being developed.

Therefore, this document contains an overview of the project *<Project>*, including:

* Overview of system and its software.
* Statement of certification considerations.
* Discussion of the software development plan, including the software life cycle processes and corresponding data.
* Project milestones and schedule.

The purpose of the PSAC is to describe the software life cycle for the project <*Project*>, its development process, and all integral processes.

This document provides the planning data defined in [DO-178C] Section 11.1 and [DO-331] Section MB.11.1, respectively. It summarizes or references the software development, verification, configuration management, and quality assurance activities for the project <*Project*>.

You can use this PSAC template as a resource when creating a PSAC. If you are updating an existing PSAC to support Model-Based Design (MBD), you can use this template as a reference document. Although representative of PSACs used in the industry, this PSAC template has not been reviewed, approved, or accepted by any certification authority. It is the user’s responsibility to gain approval and acceptance of their PSAC by the appropriate certification authority.

**Note** This document does not include the systems or hardware aspects of certification for the project <*Project*>.

## Applicable Documents

Table 1 – Regulations and Standards

| ID | Document Title |
| --- | --- |
| DO-178C | *Software Considerations in Airborne Systems and Equipment Certification*.  RTCA, Inc., 2011 |
| DO-330 | *Software Tool Qualification Considerations*.  RTCA, Inc., 2011 |
| DO-331 | *Model-Based Development and Verification Supplement to DO-178C and DO-278A*.  RTCA, Inc., 2011 |
|  | *<List additional documents here, e.g. Advisory Circulars, EASA Certification Memos, etc.>* |

Table 2 – Company and Project Plans, Standards, and Documents

| Document | Document Title |
| --- | --- |
| PSAC | ***Plan for Software Aspects of Certification for*** <*Project*> This document. |
| SDP | ***Software Development Plan for*** <*Project*> |
| SVP | ***Software Verification Plan for*** <*Project*> |
| SCMP | ***Software Configuration Management Plan for*** <*Project*> |
| SQAP | ***Software Quality Assurance Plan for*** <*Project*> |
| SRS | ***Software Requirements Standards for*** <*Project*> |
| SDS | ***Software Design Standards for*** <*Project*> |
| SCS | ***Software Code Standards for*** <*Project*> |
| SMS | ***Software Model Standards for*** <*Project*> |
| SCI | ***Software Configuration Index for*** <*Project*> \* |
| SECI | ***Software Life Cycle Environment Configuration Index for*** <*Project*> \*\* |
| SAS | *Software Accomplishment Summary* ***for*** <*Project*> |
|  | *<List additional documents>* |

\* The information that defines the software configuration for the project <*Project*> is recorded in the *Software Configuration Index* (SCI).

\*\* The tool environment used for the project <*Project*> is defined in the *Software Life Cycle Environment Configuration Index* (SECI).

This initial release will identify the versions of completed documents, versions of the tools used, and the initial software configuration.

At the completion of the project, the SCIs and SECI will be updated with the final configuration information and final document version information.

If any of the plans are revised during the project, the reasons for the changes are captured and documented in the *Software Accomplishment Summary* (SAS).

## Referenced Documents

| ID | Document Title |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  | *<List additional documents here.>* |

# System Overview

## System Description

* <Insert your system description here.>

## System Architecture

* <Insert your system architecture here, including any block diagrams.>

## System Functions

* <Insert a list of your system functions here.>

### Function Allocation to Hardware

* <List the functions here from Section 2.3 that are allocated to hardware.>

### Function Allocation to Software

* <List the functions here from Section 2.3 that are allocated to software.>

## Processor Used

The microprocessor used in <*Project*> is <CPU Type>, version <CPUVer>.

## Hardware and Software Interfaces

* <Describe your hardware/software interfaces here.>

## Safety Features

* <Describe your system safety features here.>

# Software Overview

## Software Description

* <Insert your software description here. Consider top-level software architecture, external interfaces, and interfaces between software modules. Define which modules will be developed using Model-Based Design. >

## Safety and Partitioning

* <Describe your safety and partitioning strategy here, including resource sharing, redundancy, multiple-version dissimilar software, and fault tolerances aspects.>

## Timing and Scheduling Strategies

* <Describe your software timing and scheduling strategies and techniques here. Consider using Model-Based Design for the implementation of the scheduling algorithms (e.g. using Stateflow).>

# Certification Considerations

## Certification Basis and Means of Compliance

* <Describe the means of compliance to be used for this project. Normally this section will reference DO-178C and supplements. This section must also include references to TC, STC, TSO, Advisory Circulars, Special Conditions, Certification Memoranda, etc.>

Means of compliance are based on the stringent application of [DO-178C] and [DO-331]. The development assurance strategy shall be based on a structured software development approach, as described in Chapter 5, “Software Life Cycle”.

For software development use the following development assurance methods:

* Traceability evidence: Traceability evidence will be generated during development to provide traceability between the applicable documents, the derived development artifacts (e.g. models, source code), through to the verification items.
* Reviews and analysis: Reviews and static analysis activities shall provide the evidence of the accuracy, completeness, and verifiability of the requirements, architecture, design, and implementation.
* Software testing: Dynamic testing will consist of systematic testing of all software functions of the project.
* Model simulation: Model simulation will be used to support model coverage analysis and to support the development of requirements-based functional test cases. It will not replace software integration testing, hardware software integration testing, or testing of the executable object code based on its requirements.

## Software Level

The preliminary safety assessment process for the system resulted in the determination of the software level *<SoftwareLevel>* for the project *<Project>*.

* <Insert a justification of the software level here, based on the preliminary system safety assessment.>

# Software Life Cycle

## Software Life Cycle Description

* <Provide a description of the intended software life cycle here. Consider defining a unified life cycle for conventional and model-based developed components. Provide details for each workflow in the Software Development Plan and Software Verification Plan as described in DO-331 MB4.0. You can use MathWorks "Model-Based Design Workflow for DO-178C" document for support. See also DO-331 Section MB.11.1.d.>

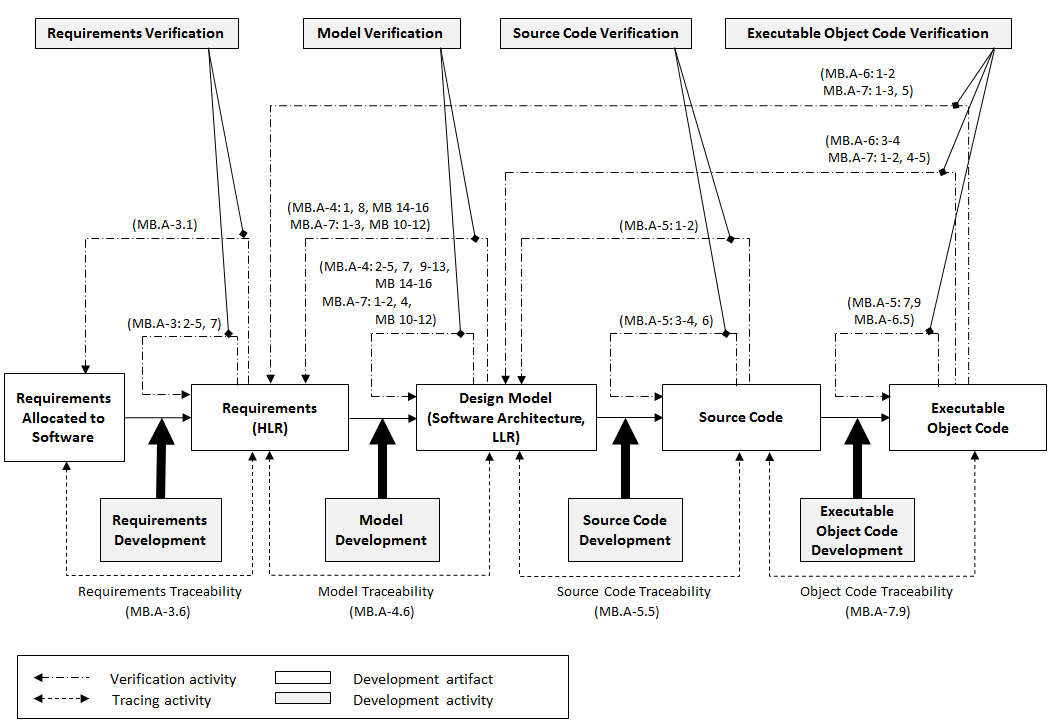


Figure 5‑1 Verification and Traceability Activities and Objectives (Model-Based Design Workflow for DO-178C)

## Software Planning Process

### Software Planning Process Objectives

* <The objectives of the software planning process are defined in DO-178C Section 4.1 and DO-331 Section MB.4.1.>

### Software Planning Process Input

The input to the software planning process is:

* DO-178C, DO-330, DO-331 and DO-333.
* The System Requirements for <*Project*>.
* The preliminary System Safety Assessment for <*Project*>.
* <Add any other document references here (e.g. CRIs, Cert Memos, CAST papers, and others). These document references can also include company standards and process documents.>

### Software Planning Process Output

The output of the software planning process:

* Plan for Software Aspects of Certification for <*Project*> (this document)
* Software Development Plan for <*Project*>
* Software Verification Plan for <*Project*>
* Software Configuration Management Plan for <*Project*>
* Software Quality Assurance Plan for <*Project*>
* Software Requirements Standards for <*Project*>
* Software Design Standards for <*Project*>
* Software Code Standards for <*Project*>
* Software Model Standards for <*Project*>
* Simulink Report Generator Tool Qualification Plan for <*Project*>
* Simulink Verification and Validation Tool Qualification Plan for <*Project*>
* Simulink Code Inspector Tool Qualification Plan for <*Project*>
* Polyspace Code Prover Tool Qualification Plan for <*Project*>
* Polyspace Bug Finder Tool Qualification Plan for <*Project*>
* Simulink Test Tool Qualification Plan for <*Project*>

<Add additional documents here.>

### Software Planning Process Activities

* <The activities of the software planning process are defined in DO-178C Section 4.2 and DO-331 Section MB.4.2.>

### Software Planning Process Transition Criteria

#### Software Planning Process Entry Criteria

* <Add the entry criteria for the planning process here. Normally, this criteria includes a reference to the complete planning process input.>

#### Software Planning Process Exit Criteria

* <Add the exit criteria for the planning process here. Normally, this criteria includes a reference to the complete planning process outputs, the configured outputs, and the plans agreed to by the certification authority.>

### Integral Processes

#### Software Configuration Management Activities

* <Add a description here of how compliance to the software configuration management process described in Chapter 7 "Software Configuration Management Process" of this document will be achieved for the software planning process (as far as applicable).>

Details are provided in the applicable Software Configuration Management Plan (SCMP).

#### Software Quality Assurance Activities

* <Add a description here of how compliance to the software quality assurance process described in Chapter 8 "Software Quality Assurance Process" of this document will be achieved for the software planning process.>

Details are provided in the applicable Software Quality Assurance Plan (SQAP).

## Software Requirements Process

### Software Requirements Process Objectives

* <The objectives of the software requirements process are defined in DO-178C Section 5.1.1 and DO-331 Section MB.5.1.1.>

### Software Requirements Process Input

The input to the software requirements process is:

* The System Requirements for <*Project*>.
* The Software Requirements Standards for <*Project*>.
* The Software Development Plan / or Plan of Software Aspects of Certification for <*Project*>.
* <Add any other document references here, e.g., the Software Model Standards, if Specification Models are used. These references can include company standards and process documents.>

### Software Requirements Process Output

The output of the software requirements process is:

* The Software Requirements Document

<Add any other document references here, e.g. Specification Models (if used).>

### Software Requirements Process Activities

* <The activities of the software requirements process are defined in DO-178C Section 5.1.2 and DO-331 Section MB.5.1.2.>

### Software Requirements Process Transition Criteria

#### Software Requirements Process Entry Criteria

* <Add the entry criteria for the requirements process here.>

#### Software Requirements Process Exit Criteria

* <Add the exit criteria for the requirements process here.>

### Integral Processes

#### Software Configuration Management Activities

* <Add a description here of how compliance to the software configuration management process described in Chapter 7 "Software Configuration Management Process" of this document will be achieved for the software requirements process.>

Details are provided in the applicable Software Configuration Management Plan (SCMP).

#### Software Quality Assurance Activities

* <Add a description here of how compliance to the software quality assurance process described in Chapter 8 "Software Quality Assurance Process" of this document will be achieved for the software requirements process.>

Details are provided in the applicable Software Quality Assurance Plan (SQAP).

## Software Design Process

### Software Design Process Objectives

* <The objectives of the software design process are defined in DO-178C Section 5.2.1 and DO-331 Section MB.5.2.1.>

### Software Design Process Input

The input to the software design process is:

* The Software Requirements Document
* The Software Specification Model <*if used*>
* The Software Design Standards
* The Software Model Standards
* The Software Development Plan or Plan of Software Aspects of Certification for <*Project*>
* <Add any other document references here. These references can include company standards and process documents.>

### Software Design Process Output

The output of the software design process is:

* The Software Design Description
* The Software Design Model
* <Add any other document references here.>

### Software Design Process Activities

* <The activities of the software design process are defined in DO-178C Section 5.2.2 and DO-331 Section MB.5.2.2.>

### Software Design Process Transition Criteria

#### Software Requirements Process Entry Criteria

* <Add the entry criteria for the requirements process here.>

#### Software Requirements Process Exit Criteria

* <Add the exit criteria for the requirements process here.>

### Integral Processes

#### Software Configuration Management Activities

* <Add a description here of how compliance to the software configuration management process described in Chapter 7 "Software Configuration Management Process" of this document will be achieved for the software design process.>

Details are provided in the applicable Software Configuration Management Plan (SCMP).

#### Software Quality Assurance Activities

* <Add a description here of how compliance to the software quality assurance process described in Chapter 8 "Software Quality Assurance Process" of this document will be achieved for the software design process.>

Details are provided in the applicable Software Quality Assurance Plan (SQAP).

## Software Coding Process

### Software Coding Process Objectives

* <The objectives of the software coding process are defined in DO-178C Section 5.3.1 and DO-331 Section MB.5.3.1.>

### Software Coding Process Input

The input to the software coding process is:

* Software Design Description
* Software Design Model
* Software Code Standards
* Software Development Plan or Plan of Software Aspects of Certification for <*Project*>
* <Add any other document references here. This might include company standards and process documents.>

### Software Coding Process Output

The output to the software coding process is:

* Source Code
* <Add any other document references here.>

### Software Coding Process Activities

<The activities of the software coding process are defined in DO-178C Section 5.3.2.>

### Software Coding Process Transition Criteria

#### Software Requirements Process Entry Criteria

* <Add the entry criteria for the requirements process here.>

#### Software Requirements Process Exit Criteria

* <Add the exit criteria for the requirements process here.>

### Integral Processes

#### Software Configuration Management Activities

* <Add a description here of how compliance to the software configuration management process described in Chapter 7 "Software Configuration Management Process" of this document will be achieved for the software coding process.>

Details are provided in the applicable Software Configuration Management Plan (SCMP).

#### Software Quality Assurance Activities

* <Add a description here of how compliance to the software quality assurance process described in Chapter 8 "Software Quality Assurance Process" of this document will be achieved for the software coding process.>

Details are provided in the applicable Software Quality Assurance Plan (SQAP).

## Integration Process

### Integration Process Objectives

* <The objectives of the software integration process are defined in DO-178C Section 5.4.1 and DO-331 Section MB.5.4.1.>

### Integration Process Input

The input to the software integration process is:

* Software Architecture
* Source Code
* Software Development Plan / or Plan of Software Aspects of Certification for <*Project*>
* <Add any other document references here (e.g. compiler libraries or precompiled COTS software components). This might include company standards and process documents.>

### Integration Process Output

The output of the software integration process is:

* Object Code
* Executable Object Code
* Parameter Data Item Files
* Compiling, Linking and Loading Data
* <Add any other document references here.>

### Integration Process Activities

<The activities of the software coding process are defined in DO-178C Section 5.4.2.>

### Integration Process Transition Criteria

#### Software Requirements Process Entry Criteria

* <Add the entry criteria for the requirements process here.>

#### Software Requirements Process Exit Criteria

* <Add the exit criteria for the requirements process here.>

### Integral Processes

#### Software Configuration Management Activities

* <Add a description here of how compliance to the software configuration management process described in Chapter 7 "Software Configuration Management Process" of this document will be achieved for the software integration process.>

Details are provided in the applicable Software Configuration Management Plan (SCMP).

#### Software Quality Assurance Activities

* <Add a description here of how compliance to the software quality assurance process described in Chapter 8 "Software Quality Assurance Process" of this document will be achieved for the software integration process.>

Details are provided in the applicable Software Quality Assurance Plan (SQAP).

## Software Verification Process

### Software Verification Process Overview

* <The software verification process is an integral process (DO-178C Section 3.1 and DO-331 Section MB.3.1) that runs in parallel with the development processes. The purpose and activities of the software verification process are defined in DO-178C Section 6.1 - 6.2 and DO-331 Section MB.6.1 – MB.6.2. Add a general description of your software verification process here.>

### Reviews and Analyses

#### Review and Analysis of Software Planning Process

* <The objective of this review and analysis is to demonstrate that the software plans and software development standards comply with the applicable regulations and purchaser specifications. The verification objectives of the software planning process are defined in DO-178C Section 4.1 (f and g) and DO-331 Section 4.1 (f and g). The reviews and assurances of the software planning process are defined in DO-178C Section 4.6 and DO-331 Section MB.4.6. Add a description here explaining how the objectives, reviews, and assurances will be achieved>

#### Review and Analysis of Software High-Level Requirements

* <The objectives of the reviews and analysis of high-level requirements are defined in DO-178C Section 6.3.1 and DO-331 Section MB.6.3.1. For details, see DO-178C Table A-3 and DO-331 Table MB.A-3.
* Add a description here explaining how the objectives, reviews, and assurances will be achieved.>

#### Review and Analysis of Specification Model

* <If you use specification models, the objectives of the review and analysis of high-level requirements expressed by a specification model are defined in DO-331 Sections MB.6.3.1 and MB.6.8. For details, see also DO-331 Table MB.A-3.
* Add a description here explaining how the objectives, reviews, and assurances will be achieved.>

#### Review and Analysis of Software Design Description

* <The objectives of the review and analysis of the software design are defined in DO-178C Section 6.3.2 and 6.3.3. For details, see DO-178C Table A-4 and DO-331 Table MB.A-4.
* Add a description here explaining how the objectives, reviews, and assurances will be achieved>

#### Review and Analysis of Design Model

* <The objectives of the review and analysis of the design model are defined in DO-331 Section MB.6.3.2 and MB.6.3.3. According to Table MB.A-4 objective 1, a model coverage analysis must be performed to demonstrate the compliance of the design model with its high-level requirements. Therefore, DO-331 Section MB.6.7 and MB.6.8 also apply. The Simulink Model Advisor and Simulink Report Generator can support the review of the design model. For details, see DO-331 Table MB.A-4.
* Add a description here explaining how the objectives, reviews, and assurances will be achieved.>

#### Review and Analysis of Source Code

* <The objectives of the review and analysis of the source code are defined in DO-178C Section 6.3.4 and DO-331 Section MB.6.3.4. Polyspace Bug Finder can support the code review activities. Simulink Code Inspector can support the review of the auto-generated source code. For details, see DO-178C Table A-5.
* Add a description here explaining how the objectives, reviews, and assurances will be achieved.>

#### Test Coverage Analysis

* <Add a description here explaining how the objectives of test coverage of high-level requirements, of low-level requirements, and of software structure according to DO-178C Section 6.4.4 and DO-331 Section MB.6.4.4 will be achieved. For details, see DO-178C Table A-7 and DO-331 Table MB.A-7.
* Also, consider performing the analysis of data and control coupling (DO-178c Section 6.4.4.d and DO-331 Section MB.6.4.4.d) in parallel with the structural coverage analysis. The use of Polyspace Code Prover and Simulink Code Inspector can assist this analysis.>

### Model Simulation

< As defined in DO-331 Section MB.6.8, model simulation is different from testing. Typical benefits of model simulation are:

* Earlier and easier verification of the algorithm than during testing of the executable object code.
* Development of test cases for the testing the executable object code and to support model coverage analysis.

Add a description here explaining how model simulation will be used to support the objectives listed in DO-331 Table MB.A-3, MB.A-4, MB.A-6 and MB.A-7.>

### Testing

< Testing the executable object code is typically performed on the target computer hardware or in an equivalent environment. It consists of software integration testing where the integration of handwritten parts and auto-generated parts of the software is verified and hardware software integration testing where the correctness of the executable object code and the CPU is verified.>

Processor-in-the-loop testing is a state-of-the-art method to demonstrate the correctness of the modeled functionality in its target environment using requirements based test cases. Consider reusing the test cases from model simulation.

Add a description here explaining how the objectives of DO-178C Section 6.4 and DO-331 Section MB.6.4 will be achieved. For details, see DO-178C Table A-6 and DO-331 Table MB.A-6.>

### Additional Verification Requirements

#### Traceability

The traceability between artifacts is a fundamental objective of DO-178C and the corresponding supplements. According to DO-178C Section 11.21 and DO-331 Section MB.11.21, traceability shall be ensured between:

* System requirements and high-level requirements (Section (MB.)6.3.1.f)
* High-level requirements and low-level requirements (Section (MB.)6.3.2.f)
* Source code and low-level requirements (Section (MB.)6.3.4.e)
* Software requirements and test cases (Section 6.5 a)
* Test cases and test procedures (Section 6.5 b)
* Test procedures and test results (Section 6.5 c)

< Add a description here explaining how the objectives above will be achieved. MathWorks Model Advisor and Code Inspector can support the traceability review.>

### Derived Requirements

<The software development processes might produce derived high-level or low-level requirements. In either case, these requirements shall be provided to the system safety process. Additional verification effort will be required to ensure the correctness of the resulting functionality (DO-331 Table MB.6-1).>

### Independence of Verification

<Depending on the software design assurance level, the independence between software development processes and the software verification process might be mandatory. Add a description here explaining how this independence will be achieved. Consider the use of verification tools like the Simulink Code Inspector to claim credit for satisfied independence.>

### Integral Processes

#### Software Configuration Management Activities

* <Add a description here of how compliance to the software configuration management process described in Chapter 7 "Software Configuration Management Process" of this document will be achieved for the software verification process.>

Details are provided in the applicable Software Configuration Management Plan (SCMP).

#### Software Quality Assurance Activities

* <Add a description here of how compliance to the software quality assurance process described in Chapter 8 "Software Quality Assurance Process" of this document will be achieved for the software verification process.>

Details are provided in the applicable Software Quality Assurance Plan (SQAP).

# Additional Considerations

## Tool Use and Qualification

### General

According to DO-178C Section 12.2, "Qualification of a tool is needed when processes of this document are eliminated, reduced, or automated by the use of a software tool without its output being verified as specified in Section 6. The purpose of the tool qualification process is to ensure that the tool provides confidence at least equivalent to that of the process(es) eliminated, reduced, or automated."

Therefore, DO-178C defines three categories of tools in table 12-1. The tool qualification process will be conducted in accordance with DO-330.

Sections 6.1.2 to 6.1.5 of this document discuss the use of tools, the determination of the tool qualification level (TQL), and qualification of tools throughout this project.

### Tools Used in Software Planning Process

| Software Tool | Version  (Release) | Tool Vendor | Tool Criteria | Usage Description and Tool Qualification |
| --- | --- | --- | --- | --- |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<…>* |

### Tools Used in Software Development Process

| Software Tool | Version  (Release) | Tool Vendor | Tool Criteria | Usage Description and Tool Qualification |
| --- | --- | --- | --- | --- |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Requirements Engineering and Management Tool>* |
| MATLAB | See SCI | MathWorks, Inc. | 1 | Modeling and simulation environment. The output of the tool will be verified as specified in Section 6 of DO-331. No credit is sought for the use of the tool. Therefore, no tool qualification is required. |
| Simulink | See SCI | MathWorks, Inc. | 1 | Modeling and simulation environment. The output of the tool will be verified as specified in Section 6 of DO-331. No credit is sought for the use of the tool. Therefore, no tool qualification is required. |
| Stateflow | See SCI | MathWorks, Inc. | 1 | Modeling and simulation environment. The output of the tool will be verified as specified in Section 6 of DO-331. No credit is sought for the use of the tool. Therefore, no tool qualification is required. |
| Embedded Coder | See SCI | MathWorks, Inc. | 1 | Embedded Coder is used to automatically generate C code from a Simulink model. The output of the tool will be verified as specified in Section 6 of DO-331. No credit is sought for the use of the tool. Therefore, no tool qualification is required. |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Software development environment (e.g. Eclipse IDE)>* |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | Compiler. According to DO-178C Section 4.4.2, for a compiler, no specific tool qualification is required. For more information on the compiler, see Section 6.4 "Compiler Considerations" of this document. |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Debugger>* |
| *<Insert additional tools>* | *<…>* | *<…>* | *<…>* | *<…>* |

### Tools Used in Software Verification Process

| Software Tool | Version  (Release) | Tool Vendor | Tool Criteria | Usage Description and Tool Qualification |
| --- | --- | --- | --- | --- |
| Simulink® Verification and Validation™  Model Advisor | See SCI | MathWorks, Inc. | 3 | Simulink Verification and Validation Model Advisor is used for static analysis of the Specification Model. See Simulink Verification and Validation TQP for determination of TQL and for credits sought. |
| Simulink® Verification and Validation™  Model Coverage | See SCI | MathWorks, Inc. | 3 | Simulink Verification and Validation Model Coverage is used for model coverage analysis according to DO-331 MB.6.7. See Simulink Verification and Validation TQP for determination of TQL and for credits sought. |
| Simulink® Verification and Validation™  Requirements Management Interface | See SCI | MathWorks, Inc. | 3 | Simulink Verification and Validation comprises a Requirements Management Interface that is being used to link requirements to Simulink model elements. The output of the tool will be verified by review according to DO-331 MB.6.3.2. No credit is sought for the use of the tool. Therefore, no tool qualification is required. |
| Simulink Code Inspector | See SCI | MathWorks, Inc. | 2 | Simulink Code Inspector supports the verification of the source code according to DO-331 MB.6.3.4. See Simulink Code Inspector TQP for determination of TQL and for credits sought. |
| Simulink Report Generator | See SCI | MathWorks, Inc. | 3 | Simulink Report Generator comprises capabilities to generate System Design Description (SDD) and Model XML Comparison reports. See Simulink Report Generator TQP for detailed information. |
| Simulink® Test™ | See SCI | MathWorks, Inc. | 3 | Simulink Test supports the verification of the models according to DO-331 MB.6.8.3.2 and executable object code according to DO-331 MB.6.4.2, 6.4.3 and 6.4.4. See Simulink Test TQP for determination of TQL and for credits sought. |
| Polyspace® Bug Finder | See SCI | MathWorks, Inc. | 2 | Polyspace Bug Finder supports the verification of the source code according to DO-331 MB.6.3.4 and DO-333 FM.6.3.4. See Polyspace Bug Finder TQP for determination of TQL and for credits sought. |
| Polyspace® Code Prover | See SCI | MathWorks, Inc. | 2 | Polyspace Code Prover supports the verification of the source code and executable object code according to DO-331 MB6.3.4 and DO-333 FM.6.2.1, FM.6.3 and FM.6.7. See Polyspace Coder Prover TQP for determination of TQL and for credits sought. |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Structural coverage analysis tool>* |
| *<Insert additional tools>* | *<…>* | *<…>* | *<…>* | *<…>* |

### Development Environment and Documentation Tools

| Software Tool | Version  (Release) | Tool Vendor | Tool Criteria | Usage Description and Tool Qualification |
| --- | --- | --- | --- | --- |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Desktop Operating System (e.g. Windows)>* |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Documentation Tools (e.g. Microsoft Office)>* |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Configuration management tool>* |
| *<Insert tool>* | *<…>* | *<…>* | *<…>* | *<Problem reporting tool>* |
| *<Insert additional tools>* | *<…>* | *<…>* | *<…>* | *<…>* |

## Use of Floating Point Numbers

* <If floating-point arithmetic and number representation is used, reference the standard to be applied (e.g. IEEE 754), define the format to be used (e.g. simple accuracy or double accuracy), and provide the restrictions and constraints and guidelines in the Software Code Standards and Software Model Standards (e.g. comparison of floating-point numbers for in-/ equality).>

## Use of Software Libraries

* <Add a description here explaining how calls to software libraries will be handled. If your software development environment does not support calls to standard compiler libraries, configure your model to avoid calls to the standard libraries in the generated code. In your model, to avoid calls, consider using:
* Code Replacement Libraries (CRLs) to remap standard library calls.
* Blocks and model constructs that do not generate calls to standard compiler libraries.>

## Compiler Considerations

* <Provide a brief description of the cross-compiler to be used including information on "what compiler will be used", "product service history", and "compiler settings".>

## Programming Languages

The programming language to be used is ANSI C. To assure the proper use of the programming language by defining guidelines and restrictions, the Software Code Standards shall be applied.

The modeling languages to be used are MATLAB, Simulink, and Stateflow, as defined and restricted in the Software Model Standards.

Assembly language shall be used for time-critical and hardware-related functions only.

# Software Configuration Management Process

* <The objectives of the software configuration management process are defined in DO-178C Section 7.1 and DO-331 Section MB.7.1.
* Add a description here explaining how the software configuration management process will be established.>

# Software Quality Assurance Process

* <The objectives of the software quality assurance process are defined in DO-178C Section 8.1 and DO-331 Section MB.8.1.
* Add a description here explaining how the software quality assurance process will be established.>

# Certification Liaison Process

* <The objectives of the certification liaison process are defined in DO-178C Section 9 and DO-331 Section MB.9.
* Add a description here explaining how the certification liaison process will be established.>

# Software Life Cycle Data

The software life cycle data that will be produced in the project <*Project*> is:

| **Document Title** | **Notes** |
| --- | --- |
| **Software Plans** |  |
| Plan for Software Aspects of Certification | (this document) |
| Software Development Plan |  |
| Software Verification Plan |  |
| Software Configuration Management Plan |  |
| Software Quality Assurance Plan |  |
| Software Requirements Standards |  |
| Software Design Standards |  |
| Software Code Standards |  |
| Software Model Standards |  |
| Simulink Report Generator Tool Qualification Plan |  |
| Simulink Verification and Validation Tool Qualification Plan |  |
| Simulink Code Inspector Tool Qualification Plan |  |
| Polyspace Code Prover Tool Qualification Plan |  |
| Polyspace Bug Finder Tool Qualification Plan |  |
| Simulink Test Tool Qualification Plan |  |
|  |  |
| **Software Documents** |  |
| Software Requirements Document |  |
| Software Design Description |  |
|  |  |
| **Software Artifacts** |  |
| Specification Model |  |
| Design Model |  |
| Source Code |  |
| Executable Object Code |  |
|  |  |
| **Verification Documents** |  |
| Software Verification Test Cases and Procedures |  |
| Software Accomplishment Summary |  |
| Software Configuration Index |  |
| *<Insert additional artifacts here.>* |  |

# Organization and Responsibilities

< Add a description here explaining the management structure within the project. Clearly define the required roles and responsibilities to ease the demonstration of independence (if required).>

# Milestones and Schedule

*<* Add an overview about the project schedule and the defined milestones here to ease the communication and planning of audits with the authorities.*>*