*Recommended name for this file:*

*[feature name | project name] Software [Master | Unit | Integration | Feature] Test Plan - V<x.y>.docx*

[feature | project ] Software [Master | Unit | Integration | Feature] Test Plan

Version: Document version.

Status: Draft | Released

Date: Date (duh)

Document Author: Author name

Contributors: Name of people who contributed significantly to this document

Document List of Approvers:

Role: Name

Role: Name

Issuing Organization: The name of the organization originating the document

Applicable Standards: NA, ISO29119, ASPICE, ISO 26262 and/or IEC 61508…

Template Version: SW Test Plan template.v1.0.docx

**Reminder:** Projects with safety-relevant requirements has to follow the generic FuSa Lifecycle definition as defined at the project startup.

If the project decides to tailor any SW phase and/or activity, it is up to the project to provide the evidence the project still fulfills the customer requirements and the applicable standard (e.g. ISO26262).

LEGAL DISCLAIMERS

*Put here whatever your legal folks require. May not be applicable to your organization, in which case just remove this page.*

Table of Contents

[Table of Contents 3](#_Toc85799572)

[Revision History 7](#_Toc85799573)

[Opens 8](#_Toc85799574)

[1.0 Introduction 9](#_Toc85799575)

[1.1 Overview 9](#_Toc85799576)

[1.2 Purpose 9](#_Toc85799577)

[1.3 Audience 9](#_Toc85799578)

[1.4 Acronyms and Terminology 9](#_Toc85799579)

[1.5 Reference Documents 10](#_Toc85799580)

[2.0 Functional Safety Standards Scope 11](#_Toc85799581)

[2.1 Prerequisite Documents 11](#_Toc85799582)

[2.2 In Scope 11](#_Toc85799583)

[2.3 Out of Scope 12](#_Toc85799584)

[3.0 Unit Test Plan 13](#_Toc85799585)

[3.1 Test Scope 13](#_Toc85799586)

[3.1.1 In Scope 13](#_Toc85799587)

[3.1.2 Out of Scope 14](#_Toc85799588)

[3.2 Assumptions, Dependencies, and Constraints 14](#_Toc85799589)

[3.2.1 Assumptions 14](#_Toc85799590)

[3.2.2 Dependencies 15](#_Toc85799591)

[3.2.3 Constraints 15](#_Toc85799592)

[3.3 Unit Test Approach 15](#_Toc85799593)

[3.3.1 Unit Test Strategy 15](#_Toc85799594)

[3.3.2 Safety requirements test strategy 15](#_Toc85799595)

[3.3.3 Test Completion Criteria 15](#_Toc85799596)

[3.3.4 System configurations coverage strategy 16](#_Toc85799597)

[3.3.5 Test Tools & Automation Strategy 16](#_Toc85799598)

[3.3.6 Test Design specification 16](#_Toc85799599)

[3.3.7 Test Cases 16](#_Toc85799600)

[3.4 Test Environment 16](#_Toc85799601)

[3.4.1 Test Setups 16](#_Toc85799602)

[3.4.2 Hardware and Lab 17](#_Toc85799603)

[3.4.3 Software Environment 17](#_Toc85799604)

[3.4.4 Security & Privacy 18](#_Toc85799605)

[3.4.5 Test data requirements 18](#_Toc85799606)

[3.5 Test Execution 18](#_Toc85799607)

[3.5.1 Continuous Integration Test Strategy 18](#_Toc85799608)

[3.5.2 Metrics to be collected 18](#_Toc85799609)

[3.5.3 Test Monitoring and Control 18](#_Toc85799610)

[3.5.4 Bug Management 18](#_Toc85799611)

[3.5.5 Test reporting 18](#_Toc85799612)

[4.0 Integration Test Plan 19](#_Toc85799613)

[4.1 Test Scope 19](#_Toc85799614)

[4.1.1 In Scope 19](#_Toc85799615)

[4.1.2 Out of Scope 20](#_Toc85799616)

[4.2 Assumptions, Dependencies, and Constraints 21](#_Toc85799617)

[4.2.1 Assumptions 21](#_Toc85799618)

[4.2.2 Dependencies 21](#_Toc85799619)

[4.2.3 Constraints 21](#_Toc85799620)

[4.3 Integration Test Approach 21](#_Toc85799621)

[4.3.1 Integration test strategy 21](#_Toc85799622)

[4.3.2 Safety requirements test strategy 21](#_Toc85799623)

[4.3.3 Test Completion Criteria 22](#_Toc85799624)

[4.3.4 Suspension Criteria and Resumption Requirements 22](#_Toc85799625)

[4.3.5 Deviations from the Organizational Test Strategy 22](#_Toc85799626)

[4.3.6 Configurations coverage strategy 22](#_Toc85799627)

[4.3.7 Test Tools & Automation Strategy 22](#_Toc85799628)

[4.3.8 Test Design specification 22](#_Toc85799629)

[4.3.9 Testability Hooks 23](#_Toc85799630)

[4.4 Test Environment 24](#_Toc85799631)

[4.4.1 Test Setups 24](#_Toc85799632)

[4.4.2 Hardware and Lab 25](#_Toc85799633)

[4.4.3 Software Environment 25](#_Toc85799634)

[4.4.4 Security & Privacy 25](#_Toc85799635)

[4.4.5 Test data requirements 25](#_Toc85799636)

[4.5 Test Execution 25](#_Toc85799637)

[4.5.1 Test Entry Criteria 25](#_Toc85799638)

[4.5.2 Regression strategy 25](#_Toc85799639)

[4.5.3 Metrics to be collected 26](#_Toc85799640)

[4.5.4 Test Monitoring and Control 26](#_Toc85799641)

[4.5.5 Bug Management 26](#_Toc85799642)

[4.5.6 Test reporting 26](#_Toc85799643)

[5.0 System Test Plan 27](#_Toc85799644)

[5.1 Test Scope 27](#_Toc85799645)

[5.1.1 In Scope 27](#_Toc85799646)

[5.1.2 Out of Scope 28](#_Toc85799647)

[5.2 Assumptions, Dependencies, and Constraints 29](#_Toc85799648)

[5.2.1 Assumptions 29](#_Toc85799649)

[5.2.2 Dependencies 29](#_Toc85799650)

[5.2.3 Constraints 29](#_Toc85799651)

[5.3 System Test Approach 29](#_Toc85799652)

[5.3.1 Master | Feature test strategy 29](#_Toc85799653)

[5.3.2 Safety requirements test strategy 29](#_Toc85799654)

[5.3.3 Test Completion Criteria 30](#_Toc85799655)

[5.3.4 Suspension Criteria and Resumption Requirements 30](#_Toc85799656)

[5.3.5 Deviations from the Organizational Test Strategy 30](#_Toc85799657)

[5.3.6 Configurations coverage strategy 30](#_Toc85799658)

[5.3.7 Test Tools & Automation Strategy 30](#_Toc85799659)

[5.3.8 Test Design specification 30](#_Toc85799660)

[5.3.9 Testability Hooks 32](#_Toc85799661)

[5.4 Test Environment 32](#_Toc85799662)

[5.4.1 Test Setups 32](#_Toc85799663)

[5.4.2 Hardware and Lab 33](#_Toc85799664)

[5.4.3 Environment Configuration 33](#_Toc85799665)

[5.4.4 Security & Privacy 33](#_Toc85799666)

[5.4.5 Test data requirements 33](#_Toc85799667)

[5.5 Test Execution 34](#_Toc85799668)

[5.5.1 Test Entry Criteria 34](#_Toc85799669)

[5.5.2 BAT Strategy 34](#_Toc85799670)

[5.5.3 Continuous Integration Test Strategy 34](#_Toc85799671)

[5.5.4 Regression Strategy 34](#_Toc85799672)

[5.5.5 Compliance and Certification 34](#_Toc85799673)

[5.5.6 Milestone Release Testing 34](#_Toc85799674)

[5.5.7 Metrics to be collected 34](#_Toc85799675)

[5.5.8 Test Monitoring and Control 34](#_Toc85799676)

[5.5.9 Bug Management 35](#_Toc85799677)

[5.5.10 Test reporting 35](#_Toc85799678)

[6.0 Risk analysis 36](#_Toc85799679)

[7.0 Schedule, Project management and Staffing 37](#_Toc85799680)

[7.1 Schedule 37](#_Toc85799681)

[7.2 Project management 37](#_Toc85799682)

[7.2.1 Project ownership 37](#_Toc85799683)

[7.2.2 Coordination between test teams 37](#_Toc85799684)

[7.2.3 Test Cycle creation and tracking 37](#_Toc85799685)

[7.2.4 Standard meetings 37](#_Toc85799686)

[7.3 Staffing 38](#_Toc85799687)

[7.3.1 Roles, activities, and responsibilities 38](#_Toc85799688)

[7.3.2 Hiring needs 38](#_Toc85799689)

[7.3.3 External Test Resources 38](#_Toc85799690)

[7.3.4 3rd party IP providers 38](#_Toc85799691)

[7.3.5 Training Needs 38](#_Toc85799692)

[8.0 What did this template miss???? 39](#_Toc85799693)

[9.0 Appendix A – Checklist 39](#_Toc85799694)

[10.0 Appendix B – Safety related standards 42](#_Toc85799695)

Figures

No table of figures entries found.

Tables

[Table 1. Acronyms and Terminology 9](#_Toc84323123)

[Table 2 Reference Documents 10](#_Toc84323124)

[Table 3. Open & Follow up Needs **Error! Bookmark not defined.**](#_Toc84323125)

[Table 4 Unit Test Items 13](#_Toc84323126)

[Table 5: Units not to be tested 14](#_Toc84323127)

[Table 6: Integration Test environment components 17](#_Toc84323128)

[Table 7: Integration Test Items 19](#_Toc84323129)

[Table 8: Integration items not to be tested 20](#_Toc84323130)

[Table 9: Integration Test environment components 24](#_Toc84323131)

[Table 10: System Test Items 27](#_Toc84323132)

[Table 11: Features to be Tested 27](#_Toc84323133)

[Table 12: Features not to be Tested 28](#_Toc84323134)

[Table 13: System Test environment components 32](#_Toc84323135)

[Table 14: Project and Product Risk and Mitigation 36](#_Toc84323136)

[Table 15: Milestones schedule 37](#_Toc84323137)

[Table 16: Roles and Responsibilities 38](#_Toc84323138)

Revision History

*[Follow your org standard version taxonomy. Recommned: Sort this table so the last update is at the top.]*

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Revision | Author | Description |
|  |  |  |  |

**Color codes inside this document**

* *Black italics*: Suggested text to put in this section.
* *Purple italics*: Explanations. Remove once you understand what to do.
* *Green italics*: Explanations relevant only to FUSA (Functional Safety, and compliance to ISO 26262). Remove once you understand what to do. Ignore if your product has nothing to do with FUSA.

Opens

*[Collect here items that still need to be resolved / updated inside the document.]*

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description | Owner | Status |
|  |  |  |  |
|  |  |  |  |

# Introduction

## Overview

*[Give the reader context to understand the rest of the document by identifying the product and providing a concise overview of the items that are covered in this plan.]*

[For FuSa – make sure to mention the ASIL level covered by this Test plan.]

## Purpose

*[Briefly describe the purpose of this document.]*

*This Software Test Plan is used as a tool to create a coherent and well-coordinated <System | Integration | Unit | Component| … > test strategy of the <component> feature-set by <team name>.*

*When done reading this document, you will have a fairly good idea how <team> plans to conduct <test level> testing of the <component> of <this product>, on <OS, platforms>.*

## Audience

*The audience for this document are architects, developers, testers and project managers.*

## Acronyms and Terminology

A summary of terminology used in this document is outlined in the table below.

Table 1. Acronyms and Terminology

|  |  |
| --- | --- |
| Term | Description |
|  |  |
|  |  |

## Reference Documents

*[Items that are needed for FuSa are in green.]*

Table 2 Reference Documents

| **Mnemonic** | **Document Name** | **Version** | **Location** |
| --- | --- | --- | --- |
| *[SAS]* | *Software Architecture Specification* | *The latest version is always in the Location URL.* | *URL* |
| *[PRD]* | *Product Requirements Document* | *The latest version is always in the Location URL.* | *URL* |
| *[REQ]* | *Requirements document (or URL to database)* |  |  |
| *[OTS]* | *Organization Test Strategy* |  |  |
| *[MTP]* | *Master Test Plan* |  |  |
| *[ChMgt]* | *Change management process / strategy document* |  |  |
| *[STP-HB]* | *Guide for SW Test Plan writing* |  | *URL* |

# Functional Safety Standards Scope

[Provides information about the sections of relevant Functional Safety standards that are addressed by this template. This section of the Test Plan is relevant only for Safety-related requirements. For features or products that do not have any such requirements, delete all sub-sections below and write “NA”].

## Prerequisite Documents

This template has no prerequisite documents.

## In Scope

*This document is intended to address the following functional safety requirements.*

* *IEC 61508-2:2010 (systems/hardware development)*
  + *7.3.2*
  + *7.5.2.2*
  + *7.5.2.4*
  + *7.5.2.6*
  + *7.9.2.1*
  + *7.9.2.2*
  + *7.9.2.3*
  + *7.9.2.4*
  + *7.9.2.9*
  + *7.9.2.10*
* *IEC 61508-3:2010 (software development)*
  + *7.9.2.1*
  + *7.9.2.2*
  + *7.9.2.3*
* *ISO 26262-6:2011 (verification supporting process)*
  + *9.4.3*
  + *9.4.4*
  + *9.4.5*
  + *10.4.3*
  + *10.4.4*
  + *10.4.6*
  + *10.4.8*
  + *11.4.2*
* *ISO 26262-8:2011 (verification supporting process)*
  + *9.4.1.1*
  + *9.4.1.2*

## Out of Scope

*This document addresses the verification plan requirements and does not address the verification specification or report requirements.*

*This document does not address Static Analysis or Reviews*

* *ISO 26262-6:2011 (verification supporting process)*
  + *8.4.4*
  + *8.4.5*

# Unit Test Plan

## Test Scope

[Provides information about what is covered – and what is not – by this test plan.]

### In Scope

#### Test Items

[Enumerate the code units that are in scope of this test plan.]

Table 3 Unit Test Items

|  |  |  |
| --- | --- | --- |
| **ID** | **Unit** | **Path** |
| Item.1 | FWUpdate tool | //… |
| Item.2 | FWUpdate library | //… |
|  |  |  |

#### Safety requirements

*[“NA” if there are no safety requirements in the code under test.]*

#### Configurations to be tested

##### Platforms, OS and Platform-OS configurations list

[Target platforms, OS and the Platform-OS combinations used.]

**Platforms**

**OS**

**Platform-OS configurations**

##### Software Configurations

*[ISO-26262:6-2011 Annex C Configuration data and Calibration data; worth a thought also for non-FuSa features]*

### Out of Scope

#### Units not to be tested

Identify any code that is in the “test items” folders but will not be unit-tested. Give an explanation why this is OK.

Examples for “reason” (these are not always correct! It depends on the project/feature at hand! They are just to give an example for possible reasons).

* Not to be included in this release
* Third party code software that will not be tested by our team
* Tested by other team in your company
* Etc.

Examples:

Table 4: Units not to be tested

| **Code that will not be unit-tested** | **Reason** |
| --- | --- |
| *Common .h files used by the FW Update tool* | *Covered by the OS test team* |
| *Service routines called by the FW Update code* | *Stubbed out by the unit test tool* |
|  |  |

## Assumptions, Dependencies, and Constraints

### Assumptions

*[Things beyond your control upon which this test plan depends.]*

### Dependencies

[Dependencies on other groups; prerequisites.]

### Constraints

[Stuff that bound the scope of validation and narrows the choices you have]

## Unit Test Approach

### Unit Test Strategy

*[General strategy for unit-testing your code.]*

*[See [STP-HB] for specific items to cover here for FuSa compliance]*

### Safety requirements test strategy

*[“NA” if there are no safety requirements in the code under test.]*

#### Methods for Software Unit Testing

*[ISO 26262-6:2011; 9.4.3, Table 10 – including explanations as needed]*

#### Methods for deriving test cases for Software Unit Testing

*[ISO 26262-6:2011; 9.4.4, Table 11 – including explanations as needed]*

#### Structural coverage metrics at the software unit level

*[ISO 26262-6:2011; 9.4.5, Table 12 – including explanations as needed]*

### Test Completion Criteria

*[Also known as “Exit criteria”.]*

### System configurations coverage strategy

[If you plan to do unit test in isolation, this section is not relevant. ]

### Test Tools & Automation Strategy

*[Overarching automation strategy used for Unit Test?]*

*[What tools will be used for verification (if applicable)? ISO 26262-8:2011; 9.4.1.1e]*

### Test Design specification

*[High level description of the tests. Not a test list.]*

*[See [STP-HB] for specific items to cover here for FuSa compliance]*

### Test Cases

*[A pointer where the test cases are.]*

## Test Environment

*[Test bench setup and general lab environment needs.]*

*[Describe the verification environment. ISO 26262-8:2011; 9.4.1.1d]*

### Test Setups

[Test environments or configurations.]

#### Setup 1 [Setup ID]

**Environment Diagram**

[Add a diagram here.]

**Environments Components**

Table 5: Integration Test environment components

|  |  |
| --- | --- |
| **HW Components** | |
| **Equipment Name** | **Details** |
| *Platform X* | *OS, memory config if relevant, IMU, platform camera, etc.* |
|  |  |

|  |  |  |
| --- | --- | --- |
| **SW Components** | | |
| **Type** | **Name** | **Version** |
| *Unit Test exe file* | *FwUpdate\_UT.exe* | *The version of the test code* |
| *abc.dll* | *Code coverage post-processor* | *The version of the dll* |

**Setup assembly instructions**

*[Instructions for assembling the test setup.]*

#### Setup 2 [Setup ID]

*…*

*[Add more setups as needed.]*

### Hardware and Lab

*[Items needed to execute the test plan. Usually NA for unit testing.]*

### Software Environment

*[Special OS or tools needed. Usually NA.]*

### Security & Privacy

*[Controls for unique, proprietary hardware; for data. Usually NA for Unit testing.]*

### Test data requirements

*[What test data, if any, is needed?]*

## Test Execution

### Continuous Integration Test Strategy

*[Is unit testing going to be part of the CI tests?]*

### Metrics to be collected

*[Coverage metrics types.]*

### Test Monitoring and Control

*[Execution verification and results tracking.]*

### Bug Management

*[Bug management process. Usually a pointer to where the process is defined.]*

*[What actions will be taken if anomalies are detected? ISO 26262-8:2011; 9.4.1.1f]*

#### Bug Fix Verification (“re-test”)

*[Anything special? Usually:]*

*All unit tests are expected to pass prior to checking in the code. Therefore, re-test is being done on the fly as part of the development process.*

### Test reporting

*[How are unit test results and test evidence collected and reported?]*

# Integration Test Plan

## Test Scope

*[What Integration Test means in your organization? What is covered?]*

### In Scope

*[What are the work products and/or safety integrity requirements to be verified? ISO 26262-8:2011; 9.4.1.1a]*

#### Test Items

[Items whose integration is the target of this integration test plan.]

Table 6: Integration Test Items

| **Test Item** | **Interfaces** |
| --- | --- |
|  |  |
| *Services.dll* | *dll - OS APIs* |
|  | *dll - application level APIs* |
|  | *dll – remote authentication server REST Messages* |
|  |  |
| *mouhid.sys* | *SW – HW (via shared memory registers)* |
|  | *OS – driver (using ioctls)* |
|  |  |

*If you are testing more than just the interfaces, you can modify the above table to convey this:*

| **Test Item** | **Test targets** |
| --- | --- |
|  |  |
| *Services.dll* | *Interfaces with the OS, application and remote server* |
|  | *Basic functionality* |
|  | *Specific performance aspects* |
|  |  |

#### Configurations to be tested

##### Platforms, OS and Platform-OS configurations list

[Target platforms, OS and the Platform-OS combinations used.]

**Platforms**

**OS**

**Platform-OS configurations**

##### Software Configurations

*[ISO-26262:6-2011 Annex C Configuration data and Calibration data; worth a thought also for non-FuSa features]*

### Out of Scope

#### Integration items not to be tested

[Interfaces / areas / items / modules that won’t be tested.]

Table 7: Integration items not to be tested

| **Test item / Interface not to be tested** | **Reason** |
| --- | --- |
| *mouhid.sys driver-HW* | *Already tested thoroughly on previous release; no code change done on this driver for the current project and no change to the HW device.* |
|  |  |
|  |  |

## Assumptions, Dependencies, and Constraints

### Assumptions

*[Things beyond your control upon which this test plan depends.]*

### Dependencies

[Dependencies on other groups; prerequisites.]

### Constraints

[Stuff that bound the scope of validation and narrows the choices you have]

## Integration Test Approach

### Integration test strategy

*[General strategy for integration testing.]*

### Safety requirements test strategy

*[“NA” if there are no safety requirements in the code under test.]*

#### Methods for Software Integration Testing

*[ISO 26262-6:2011; 10.4.3, Table 13 – including explanations as needed]*

#### Methods for deriving test cases for Software Integration Testing

*[ISO 26262-6:2011; 10.4.4, Table 14 – including explanations as needed]*

#### Structural coverage metrics at the software architectural level

*[ISO 26262-6:2011; 10.4.6, Table 15 – including explanations as needed]*

### Test Completion Criteria

*[Also known as “Exit criteria”.]*

### Suspension Criteria and Resumption Requirements

*[In case you have such criteria. Usually:]*

*We do not have preset criteria. This is a case-by-case decision, made by Validation managers in consultation with the validation feature owners and the program manager.*

### Deviations from the Organizational Test Strategy

*[Any deviations from the Organizational Test Strategy?]*

### Configurations coverage strategy

[Coverage plan for HW-OS-SKU combinations and for ISO 26262 Configuration and Calibration]

**Platform and OS coverage strategy**

**Software configuration and calibration coverage strategy**

### Test Tools & Automation Strategy

*[Existing or to-be-developed tools and automation systems.]*

*[What tools will be used for verification (if applicable)? ISO 26262-8:2011; 9.4.1.1e]*

### Test Design specification

*[See [STP-HB] for specific items to cover here for FuSa compliance]*

#### <Test Module #1>

*[Convey the aspect of integration testing covered by the module.]*

**Description**

*[2-3 sentences are enough.]*

**Test Strategy & Validation Method**

[The method used to validate the aspects covered by this test module.]

*[If not using the target environment, explain why. ISO 26262-6:2011, section 10.4.8]*

**Test Steps**

*[Generic steps.]*

**Test Tools**

*[Just the tool names.]*

**Restrictions, Limitation and Exclusions**

*[“NA” if there are none.]*

#### < Test Module #2>

#### < Test Module #3>

*[Add modules as needed]*

### Testability Hooks

*[Existing or committed test hooks; not wishes.]*

## Test Environment

*[Test bench setup and general lab environment needs.]*

*[Describe the verification environment. ISO 26262-8:2011; 9.4.1.1d]*

### Test Setups

[Test environments or configurations.]

#### Setup 1 [Setup ID]

**Environment Diagram**

[Add a diagram here.]

**Environments Components**

Table 8: Integration Test environment components

|  |  |
| --- | --- |
| **HW Components** | |
| **Equipment Name** | **Details** |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **SW Components** | | |
| **Type** | **Name** | **Version** |
|  |  |  |

**Setup assembly instructions**

*[Instructions for assembling the test setup.]*

#### Setup 2 [Setup ID]

…

*[Add more setups as needed.]*

### Hardware and Lab

*[Items needed to execute the test plan.]*

### Software Environment

*[Special OS or tools needed.]*

### Security & Privacy

*[Controls for unique, proprietary hardware; for data.]*

### Test data requirements

*[What test data, if any, is needed?]*

## Test Execution

### Test Entry Criteria

*[What’s the minimum functionality needed before starting?]*

### Regression strategy

*[What is the regression strategy for re-execution of verification after a change to the work products under verification? ISO 26262-8:2011; 9.4.1.1g]*

### Metrics to be collected

*[What metrics will be collected and tracked?]*

### Test Monitoring and Control

*[Execution verification and results tracking.]*

### Bug Management

*[Bug management process. Usually a pointer to where the process is defined.]*

*[What actions will be taken if anomalies are detected? ISO 26262-8:2011; 9.4.1.1f]*

#### Bug Fix Verification (“re-test”)

*[Anything special?]*

### Test reporting

*[How are integration test results and test evidence collected and reported?]*

# System Test Plan

## Test Scope

### In Scope

*[What are the work products and/or safety integrity requirements to be verified? ISO 26262-8:2011; 9.4.1.1a]*

#### Test Items

[Items (binaries) that are the target of this system test plan.]

Table 9: System Test Items

|  |  |  |
| --- | --- | --- |
| **Test Item** | **Description & version** | **Main focus area** |
| *ABC DLL* | *Authentication and Access control engine* | *Authentication* |
| *XYZ Driver* | *Device driver (User mode)* | *Authentication support* |
|  |  |  |

#### Features to be tested

[A breakdown of the high level feature or component into Test Modules.]

Table 10: Features to be Tested

| **Feature / Capability** | **Additional breakdown** | **Owning team** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### Configurations to be tested

##### Platforms, OS and Platform-OS configurations list

[Target platforms, OS and the Platform-OS combinations used.]

**Platforms**

**OS**

**Platform-OS configurations**

*[Just the list. Why this list was selected is explained in the Test strategy section]*

##### Software Configurations

*[ISO-26262:6-2011 Annex C Configuration data and Calibration data; worth a thought also for non-FuSa features]*

#### Documentation to be tested

[Manuals, user guides etc.]

### Out of Scope

#### Features not to be tested

Table 11: Features not to be Tested

| **Feature / Capability that will not be tested** | **Reason** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

## Assumptions, Dependencies, and Constraints

### Assumptions

*[Things beyond your control upon which this test plan depends.]*

### Dependencies

[Dependencies on other groups; prerequisites.]

### Constraints

[Stuff that bound the scope of validation and narrows the choices you have]

## System Test Approach

### Master | Feature test strategy

*[General strategy for system testing.]*

### Safety requirements test strategy

*[“NA” if there are no safety requirements in the code under test.]*

#### Methods for Software Feature Testing

*[ISO 26262-6:2011; 10.4.3, Table 13 – including explanations as needed]*

#### Methods for deriving test cases for Software Feature Testing

*[ISO 26262-6:2011; 10.4.4, Table 14 – including explanations as needed]*

#### Structural coverage metrics at the software architectural level

*[ISO 26262-6:2011; 10.4.6, Table 15 – including explanations as needed]*

#### Test environments for conducting the software safety requirements verification

*[ISO 26262-6:2011; 11.4.2, Table 16 – including explanations as needed]*

### Test Completion Criteria

*[Also known as “Exit criteria”.]*

### Suspension Criteria and Resumption Requirements

*[In case you have such criteria. Usually:]*

*We do not have preset criteria. This is a case-by-case decision, made by Validation managers in consultation with the validation feature owners and the program manager.*

### Deviations from the Organizational Test Strategy

*[Any deviations from the Organizational Test Strategy?]*

### Configurations coverage strategy

[Coverage plan for HW-OS-SKU combinations and for ISO 26262 Configuration and Calibration]

**Platform and OS coverage strategy**

**Software configuration and calibration coverage strategy**

### Test Tools & Automation Strategy

*[Existing or to-be-developed tools and automation systems.]*

*[What tools will be used for verification (if applicable)? ISO 26262-8:2011; 9.4.1.1e]*

### Test Design specification

*[See [STP-HB] for specific items to cover here for FuSa compliance]*

#### <Test Module #1>

*[Convey the aspect of system testing covered by the module.]*

**Description**

*[2-3 sentences are enough.]*

**Test Strategy & Validation Method**

[The method used to validate the aspects covered by this test module.]

*[If not using the target environment, explain why. ISO 26262-6:2011, section 10.4.8]*

##### Sub-Test-Module A

*[Optional; for large test modules]*

**Sub-Test-Module Test Strategy**

*[If different than the one listed for the whole test module.]*

##### Sub-Test-Module B

##### Sub-Test-Module C

*[Add sub-test-modules as needed.].*

**Test Steps**

*[Generic steps.]*

**Test Tools**

*[Just the tools names.]*

**Restrictions, Limitation and Exclusions**

*[“NA” if there are none.]*

#### < Test Module #2>

#### < Test Module #3>

*[Add modules as needed]*

*… etc.*

### Testability Hooks

*[Existing or committed test hooks; not wishes.]*

## Test Environment

*[Test bench setup and general lab environment needs.]*

*[Describe the verification environment. ISO 26262-8:2011; 9.4.1.1d]*

### Test Setups

[Test environments or configurations.]

#### Setup 1 [Setup ID]

**Environment Diagram**

[Add a diagram here.]

**Environments Components**

Table 12: System Test environment components

|  |  |
| --- | --- |
| **HW Components** | |
| **Equipment Name** | **Details** |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **SW Components** | | |
| **Type** | **Name** | **Version** |
|  |  |  |

**Setup assembly instructions**

*[Instructions for assembling the test setup.]*

#### Setup 2 [Setup ID]

…

*[Add more setups as needed.]*

### Hardware and Lab

*[Items needed to execute the test plan.]*

### Environment Configuration

*[Special OS or tools needed.]*

### Security & Privacy

*[Controls for unique, proprietary hardware; for data.]*

### Test data requirements

*[What test data, if any, is needed?]*

## Test Execution

### Test Entry Criteria

*[What’s the minimum functionality needed before starting?]*

### BAT Strategy

*[Selection criteria for tests included in Build Acceptance Test (“Smoke Test”)]*

### Continuous Integration Test Strategy

*[Selection criteria for tests included in CI.]*

### Regression Strategy

*[Selection criteria for tests included in regression test cycles. Regression cycle strategy.]*

*[What is the regression strategy for re-execution of verification after a change to the work products under verification? ISO 26262-8:2011; 9.4.1.1g]*

### Compliance and Certification

*[Test activities due to certification / compliance requirements.]*

### Milestone Release Testing

*[Selection criteria for tests included in milestone test cycles.]*

### Metrics to be collected

*[What metrics will be collected and tracked.]*

### Test Monitoring and Control

*[Execution verification and results tracking.]*

### Bug Management

*[Bug management process.]*

*[What actions will be taken if anomalies are detected? ISO 26262-8:2011; 9.4.1.1f]*

#### Bug Fix Verification (“re-test”)

*[Anything special? Usually:].*

*Bug fix verification is the first task done on a new release, before the start of any test cycle.*

### Test reporting

*[How are integration test results and test evidence collected and reported?]*

# Risk analysis

[Project and Product major risks to the successful execution of this test plan.]

*[See [STP-HB] for specific items to cover here for FuSa compliance]*

Table 13: Project and Product Risk and Mitigation

| **Risk** | **Risk Type** | **Level** | **Owner** | **Contingency** | **Status** |
| --- | --- | --- | --- | --- | --- |
|  | *Project* | *Low* |  |  |  |
|  | *Product* | *Medium* |  |  |  |
|  |  | *High* |  |  |  |

# Schedule, Project management and Staffing

*[Usually: reference the system used in your org for project management and NA this section]*

## Schedule

*[High level project schedule.]*

Table 14: Milestones schedule

|  |  |
| --- | --- |
| **Milestone** | **Date** |
|  |  |
|  |  |
|  |  |

## Project management

### Project ownership

*[Who is running the project?]*

### Coordination between test teams

*[List teams and coordination methods.]*

### Test Cycle creation and tracking

*[Test cycle creation, frequency, tracking.]*

### Standard meetings

*[Any standard meetings?]*

## Staffing

### Roles, activities, and responsibilities

*[Who does what.]*

Table 15: Roles and Responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| **Team** | **Manager/ Owner/Lead** | **Geo Location** | **Primary responsibility** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Hiring needs

### External Test Resources

*[Test houses, offshore]*

### 3rd party IP providers

*[3rd party components list and how/how tests them.]*

### Training Needs

*Training needed to execute this test plan.]*

# What did this template miss????

*[Think!...].*

# Appendix A – Checklist

The following checklist aims to help the document writer ensure nothing is missing in the test plan. Note that that this is a tracking system – it does not have to be 100% when you start.

The checklist currently includes the requirements from 26262:8 section 9 / 26262:6 sections 9, 10, 11.

**Generic Verification Plan**

| **Checklist Item** | **Unit** | **Integration** | **Master | Feature** | **Standard reference** |
| --- | --- | --- | --- | --- |
| What are the work products and/or safety integrity requirements to be verified? | 3.1.1.2 | 4.1.1.2 | 5.1.1.3 | [ISO 26262-8:2011; 9.4.1.1a] [IEC 61508-3:2010; 7.9.2.2a] |
| What techniques/methods will be used for verification? | 3.3.6 | 4.3.7 | 5.3.7 | [ISO 26262-8:2011; 9.4.1.1b] [IEC 61508-2:2010; 7.9.2.2] [IEC 61508-3:2010; 7.9.2.2b] |
| What are the pass and fail criteria and process for evaluation of verification results? | 3.3.7 | 4.3.8 | 3.3.8 | [ISO 26262-8:2011; 9.4.1.1c] [IEC 61508-2:2010; 7.9.2.2] [IEC 61508-3:2010; 7.9.2.2d] |
| Describe the verification environment. | 3.4 | 4.4 | 5.4 | [ISO 26262-8:2011; 9.4.1.1d] |
| What tools will be used for verification (if applicable)? | 3.3.5 | 4.3.6 | 5.3.6 | [ISO 26262-8:2011; 9.4.1.1e] [IEC 61508-2:2010; 7.9.2.2] [IEC 61508-3:2010; 7.9.2.2c] |
| What actions will be taken if anomalies are detected? | 3.5.4 | 4.5.4 | 5.5.9 | [ISO 26262-8:2011; 9.4.1.1f] [IEC 61508-3:2010; 7.9.2.2e] |
| What is the regression strategy for re-execution of verification after a change to the work products under verification? | NA | 4.5.1 | 5.5.4 | [ISO 26262-8:2011; 9.4.1.1g] |
| Why are the verification methods planned adequate for the verification activity? | 3.3.6 | 4.3.7 | 5.3.7 | [ISO 26262-8:2011; 9.4.1.2a] |
| How is the size of project comprehended? | NA | NA | NA | [IEC 61508-3:2010; 7.9.2.3 NOTE] |
| How is the complexity of the work product to be verified comprehended? | 6.0 | 6.0 | 6.0 | [ISO 26262-8:2011; 9.4.1.2b] [IEC 61508-3:2010; 7.9.2.3 NOTE] |
| How are prior experiences related to the verification of the subject material (novelty of design) comprehended? | 6.0 | 6.0 | 6.0 | [ISO 26262-8:2011; 9.4.1.2c] [IEC 61508-3:2010; 7.9.2.3 NOTE] |
| How is the degree of maturity of the technologies (novelty of technology) used or the risks associated with the use of these technologies comprehended? | 6.0 | 6.0 | 6.0 | [ISO 26262-8:2011; 9.4.1.2d] [IEC 61508-3:2010; 7.9.2.3 NOTE] |
| Provide evidence that the verification plan is developed concurrently with the lifecycle phase in which the work product under verification is created. | NA | NA | NA | [IEC 61508-2:2010; 7.9.2.1] [IEC 61508-3:2010; 7.9.2.1] |

**Generic Verification Specification**

| **Checklist Item** | **Unit** | **Integration** | **Master | Feature** | **Standard reference** |
| --- | --- | --- | --- | --- |
| What are the specific methods/strategies/activities that will be used for verification of the correctness and consistency of the work product with respect to its input? Why were they chosen? | 3.3.6 | 4.3.7 | 5.3.7 | [ISO 26262-8:2011; 9.4.2.1] [IEC 61508-2:2011; 7.9.2.3] [IEC 61508-2:2011; 7.9.2.4a, c] |
| Complete a), b), c) or a combination of a), b), and c). a) Provide review or analysis checklist to be used in verification and rationale for sufficiency b) Provide details of simulation scenarios which will be used in verification and rationale for sufficiency c) Provide details of the test cases, test data, and test objects to be used for verification and rationale for sufficiency | 3.3.7 + test cases in a Unit test framework | 4.3.8 + Test cases in a test management system | 5.3.8 + Test cases in a test management system | [ISO 26262-8:2011; 9.4.2.1] [ISO 26262-8:2011; 9.4.2.1a] [ISO 26262-8:2011; 9.4.2.1b] [ISO 26262-8:2011; 9.4.2.1c] |
| If testing is applied (Option c) above), provide the following details for each test case a)      Unique identification of test case b)     Version of work product to be verified c)      Preconditions and configurations for test d)     Environmental conditions needed for test e)      Input data required, including time sequence and values f)       Expected behavior of work product under test – including output data, acceptable ranges of output, time behavior, and tolerance behavior | Test cases in the unit test framework  Test results in <URL> | Test cases in the test case management system  <URL>  Test results in <URL> | Test cases in the test case management system  <URL>  Test results in <URL> | [ISO 26262-8:2011; 9.4.2.2] |
| If testing is applied (Option c) above), provide the following details for each test method applied (group of test cases) a)      Test environment to be applied per test method b)     Logical and temporal dependencies per test method c)      Resources required for each test method (tools, setup, etc) | 3.3.7 + test cases in a Unit test framework | 4.3.8 + Test cases in a test management system | 5.3.8 + Test cases in a test management system | [ISO 26262-8:2011; 9.4.2.3] |
| If testing is applied, document the test equipment to be used and provide the rationale for sufficiency. | NA | NA | NA | [IEC 61508-2:2010; 7.9.2.4b] |
| How are verification results to be evaluated? | NA | NA | NA | [IEC 61508-2:2010; 7.9.2.4d] |

**Software Verification Specification**

| **Checklist Item** | **Unit** | **Integration** | **Master | Feature** | **Standard reference** |
| --- | --- | --- | --- | --- |
| Methods of Software testing | 3.3.2.1 | 4.3.2.1 | 5.3.2.1 | [ISO 26262-6:2011; 9.4.3]  [ISO 26262-6:2011; 10.4.3] |
| Methods for deriving test cases for Software Testing | 3.3.2.2 | 4.3.2.2 | 5.3.2.2 | [ISO 26262-6:2011; 9.4.4]  [ISO 26262-6:2011; 10.4.4] |
| Structural coverage metrics | 3.3.2.3 | 4.3.2.3 | 5.3.2.3 | [ISO 26262-6:2011; 9.4.5]  [ISO 26262-6:2011; 10.4.6] |
| Test environments for conducting the software safety requirements verification | NA | NA | 5.3.2.4 | [ISO 26262-6:2011; 11.4.2] |

# Appendix B – Safety related standards

*For documents that must be compliant to a standard, add the “applicable standards” to the reference table in the Reference Documents section. For IEC 61508 and ISO 26262, you can use the entries in the table below:*

|  |  |
| --- | --- |
| Document | Document Number / Location |
| IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related-systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems | [www.iec.ch](http://www.iec.ch) |
| IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related-systems – Part 3: Software requirements | [www.iec.ch](http://www.iec.ch) |
| ISO 26262-4:2011, Road vehicles — Functional safety — Part 4: Product development at the system level | [www.iso.org](http://www.iso.org) |
| ISO 26262-6:2011, Road vehicles — Functional safety — Part 6: Product development at the software level | [www.iso.org](http://www.iso.org) |
| ISO 26262-8:2011, Road vehicles — Functional safety — Part 8: Supporting processes | [www.iso.org](http://www.iso.org) |