
Personnel Safety System Configuration Management Plan

	Name	Role/Title
Owner	Yong Kian Sin	Electrical Controls Engineer, ICS Division, PS Group
Reviewer	Mattias Skarfar Stuart Birch	Head of Quality Division Senior Engineer Personnel Safety Systems, ICS Division, PS Group
Approver	Annika Nordt	Group Leader for Protection Systems Group, ICS Division

TABLE OF CONTENT		PAGE
1.	EXECUTIVE SUMMARY.....	4
2.	ABBREVIATIONS	4
3.	INTRODUCTION	4
4.	DOCUMENTS MANAGEMENT	5
4.1.	Revision and Submission History	5
4.2.	Convention for file names for software project files.....	6
5.	CONFIGURATION MANAGEMENT	7
5.1.	Description	7
5.2.	Hardware Configuration	7
5.3.	Software Configuration	7
5.3.1.	Password Protection of Safety Related Software.....	9
5.3.2.	Release of Safety Related Software	9
5.4.	Change Management	10
5.4.1.	No modification tracking	10
5.4.2.	Request for Modification.....	10
5.4.3.	Impact Analysis.....	11
5.4.4.	Classification of the modifications.....	11
5.4.5.	Verification of changed software modules	14
5.4.6.	Approval	15
5.4.7.	Modification Status	16
5.4.8.	Verify changed software/hardware module/s	16
5.4.9.	Regression Test Concept	16
5.4.10.	Regression Test Review	16
5.4.11.	Regression Testing.....	17
5.4.12.	Overview Change Management and failure documentation	17
6.	FAILURE TRACKING.....	19
7.	REFERENCES	20
8.	ATTACHMENT (TEMPLATES).....	21
8.1.	Configuration Correlation.....	21

Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

8.2. Software Release 23
8.3. Changes Tracking List 26
8.4. Design Change Request 27
8.5. Failure Description 30
DOCUMENT REVISION HISTORY 32

Review

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

1. EXECUTIVE SUMMARY

This document describes the generic Hardware and Software configuration management process during the development of European Spallation Source (ESS) Personnel Safety Systems (PSS). It follows Functional Safety of IEC 61508

2. ABBREVIATIONS

E/E/PE	Electrical/Electronic/Programmable Electronic safety related systems
ESS	European Spallation Source
CCB	Change Control Board
CCR	Configuration Correlation Record
CPU	Central Processing Unit
CTRL	Change Tracking List
DCR	Design Change Request
FAT	Factory Acceptance Test
HCCR	Hardware Configuration Correlation Record
HMI	Human Machine Interface
ID	Identity
I/O	Input / Output
PLC	Programmable Logic Controller
PSS	Personnel Safety System
SAT	Site Acceptance Test
SRS	Safety requirement specification
SIL	Safety Integrity Level

3. INTRODUCTION

3.1 Scope

The scope of this document is limited to the PSS for the ESS.

The PSS Configuration Management Plan gives requirements to the following:

- Planning of the process, including defining activities, responsibilities and the tools to be procured;
- Identify, name and version each configuration item with the unique reference and determine whether they are to be brought under configuration control (configuration identification);
- Identify the version of each software item, which together constitute a specific version of a software baseline, including re-used software, libraries, and purchased commercial off the shelf software;

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

- Identify the versions of relevant hardware modules including the hardware release and firmware version;
- Identify the versions of relevant hardware equipment;
- Identify, track and report the status of items, including all actions and changes resulting from a change request or problem, from initiation through to release (configuration status accounting);
- Provide release management for hardware and software before SAT.

3.2 Objectives

Configuration management will ensure that procedures to be used for uniquely identifying all constituent parts of an item (hardware and software) are followed. It also specifies procedures for preventing unauthorized items from entering service.

4. DOCUMENTS MANAGEMENT

4.1. Revision and Submission History

Well-defined document management ensures that in PSS Development all elements are clearly identifiable. This shall be referenced at the beginning of each document and software module (hereinafter referred to as 'documents').

The submission history is created at the beginning of the development and updated when a document is officially submitted to CHES. Document revision history (end of CHES document) shall be updated every time the document is changed.

The revision overview also points out, which modification was applied to the document in the different steps:

- New Feature → Something new was added to the system
- Maintenance → Modifications which change the information of chapters or sentences
- Correction → Modifications which rectify the information of chapters or sentences

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

4.2. Convention for file names for software project files

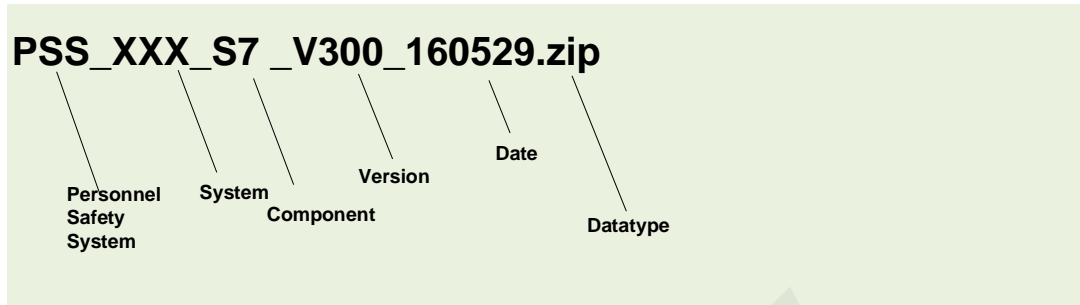


Figure 1: Convention for File Names in PSS for projecting files

- **PSS**
 - This is a Personnel Safety System related file.
- **System**
 - PSS subsystems.
- **Component**
 - S7 → S7 – Project
 - HMI → WinCC Project
 - EPL → ePLAN drawings
 - MDS → Message Display System
 - ACS → Access Control System
 - PA → Public Address System
- **Version according to baselines of PSS.**
 - Version 0.x.y → Realization phase
 - Version 1.x.y → After FAT (Phase 1)
 - Version 2.x.y → After Final Integration Test (Phase 1)
 - Version 3.x.y → After Requirement Validation (Phase 1)
 - Version 4.x.y → After FAT (Phase 2)
 - Version 5.x.y → After Final Integration Test (Phase 2)
 - Version 6.x.y → After Requirement Validation (Phase 2)
 - Version 7.x.y → After FAT (Phase 3)
 - Version 8.x.y → After Final Integration Test (Phase 3)
 - Version 9.x.y → After Requirement Validation (Phase 3)

“x” describes a major change, “y” describes a minor change.

- **Date**
 - Format: YYMMDD
- **Datatype**
 - Depending on the tool used for creating the file

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

5. CONFIGURATION MANAGEMENT

5.1. Description

Configuration management should apply administrative and technical controls throughout the lifecycle, in order to manage changes and thus ensure that the specified requirements for safety continue to be satisfied. Furthermore, it shall guarantee that all necessary operations have been carried out to demonstrate that the required safety integrity has been achieved.

CHESS shall be used as the default Configuration Management Tool. This tool guarantees that defined management procedure is maintained and traceability throughout the process, taking into account the roles described in the PSS Development and Quality Assurance Plan [1]

5.2. Hardware Configuration

During PSS development, all corresponding configurations shall be summarized in a record, called Hardware Configuration Correlation Record (HCCR).

The PSS Manager [1] shall be responsible for the maintenance of the HCCR (attachment 8.1).

The aim of the HCCR is to guarantee that appropriate configuration is used in the further development. A change to a specific configuration shall enforce a modification on the related configurations (refer to the Figure 4, Change management flow chart).

5.3. Software Configuration

Safety program can be created using program editor. Safety checks are automatically performed and additional fail-safe blocks for error detection and fault reaction are inserted when safety program is compiled. This ensures that failures and errors are detected and appropriate reactions are triggered to maintain the F-system in the safe-state or bring it to safe-state.

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

In addition to the safety program, a standard user program can be run on the F-CPU. A standard program can coexist with a safety program in an F-CPU because the safety related data of the safety program are protected from being affected unintentionally by data of the standard user program. Data can be exchanged between safety program and the standard user program in the F-CPU by means of bit memory or data of a standard DB or by accessing the process image input and output.

Safety Administrator Editor shall use to determine the correct safety program was downloaded to the F-CPU by compare the collective F-signature of the safety program.

If the collective F-signature is different for the safety program online and offline, this means:

- The offline safety program was modified after the last downloading, or
- An incorrect F-CPU was addressed. Check the latter based on the collective F-signature.

The screenshot shows the 'General' tab of the Safety Administrator Editor. It is divided into three main sections:

- Safety mode status:** Includes a 'Disable safety mode' button and a text field showing 'Current mode: Safety mode is activated.'
- Safety program status:** Includes two text fields: 'Offline program: The offline safety program is consistent.' and 'Online program: The online safety program is consistent.'
- Program signature:** A table with the following data:

Description	Status	Offline signature	Online signature	Version comparison
Collective F-signature	●	0F544E9A	0F544E9A	●

The collective F-signature must be documented in the Software Release template (refer to attachment 8.2), including the date and time of compilation, provided by Step 7 TIA Portal.

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

5.3.1. Password Protection of Safety Related Software

With the Siemens SIMATIC safety F-System, it is essential to provide access control to the SIMATIC Safety F-system by two password prompts; one for the safety program and another for F-CPU. (Refer to SIMATIC Safety – Configuring and Programming, Programming and Operating Manual, 03/2017, A5E02714440-AF)

The password for safety program is available in two forms:

- The offline password is part of the safety program in the offline project on the programming device or PC.
- The online password is part of the safety program in the F-CPU.

Safety-related engineering tool “F System”, safety- related code is protected by a password from unauthorized changes. The software password must be entered before any modification can be applied to the software, the system password must be entered before the download of software or hardware configuration to the PLC.

Password is defined by the Designer [1]. Approval needed from Manager [1] for password handover to other party, and the handover shall be recorded

5.3.2. Release of Safety Related Software

Software is officially released for the first time, after FAT and Safety Assessment is finished. Programming errors, other failures or change requests are then tracked via the “Changes Tracking List” (CTRL) (attachment 8.3).

In this list all relevant information to a specific modification is tracked. For an official release of changed software, the corresponding descriptions to the modifications in the CTRL are deployed with the released software.

All important software information is documented using the Software Release template (refer to attachment 8.2) . This template includes the name of the released software and modifications in the CTL. For each controller all collective F-signatures are included in the Software Release template.

Software Release template and the HCCR will form the PSS Configuration Correlation Record [refer to attachment 8.1] for the complete system.

5.4. Change Management

5.4.1. No modification tracking

The first change management stage is “no modification tracking”.

This stage is applied as long as:

- A document or software is in work and has not been sent for approval (all documents need to be approved before verification)
- Changes to the document are reduced to correction of spelling mistakes

5.4.2. Request for Modification

Any request for modification makes it necessary to use the process. The complexity of the modification is not relevant for using this process, so every modification has to be handled in the same way.

All people, involved in the system can place a Modification Request (refer to template...), but only in written form using the CTRL and the Design Change Request (DCR) template (refer to attachment 8.4). Modification Requests that are ready to be processed shall be recorded in the CTRL

Whenever a modification is requested, it is set to status “OPEN” in the CTRL:

OPEN	Request for modification has been placed, but was not processed until now. This status is set by the initiator of the Modification Request
------	--

Modifications can be used to guide corrections, enhancements or adaptations to the validated software, ensuring that the required software systematic capability is sustained.

The modifications shall consider:

- Completeness and correctness with respect to requirements;
- Introduction of intrinsic design faults;
- Avoidance of unwanted behaviour;

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

- Verifiable and testable design;
- Regression testing and verification coverage.

5.4.3. Impact Analysis

The responsible person (chosen by Manager [1]) shall carry out an impact analysis for the Modification Request.

If at any phase of the software safety lifecycle, a modification is required pertaining to an earlier lifecycle phase, then an impact analysis shall determine:

- Which software modules are impacted?
- Which earlier safety lifecycle activities shall be repeated?
- Which hazard/s is/are affected?

During the integration testing of the safety related programmable electronics (hardware and software), any change to the integrated system shall be subject to an impact analysis. The impact analysis shall determine all software modules impacted, and the necessary re-verification activities.

The impact shall be classified as Light or Heavy depends on the effect of the modification.

The classification shall be recorded in the CTRL.

5.4.4. Classification of the modifications

In the classification, the Designer defines whether the modification is “Major”, “Medium” or “Minor”(Figure 2). Manager shall approve the modification.

The classification depends on the parameters, classified during Risk Assessment and Impact Analysis. As the classification of the different parameters is done by the Designer and proven by the Verifier, it is subject to their individual understanding.

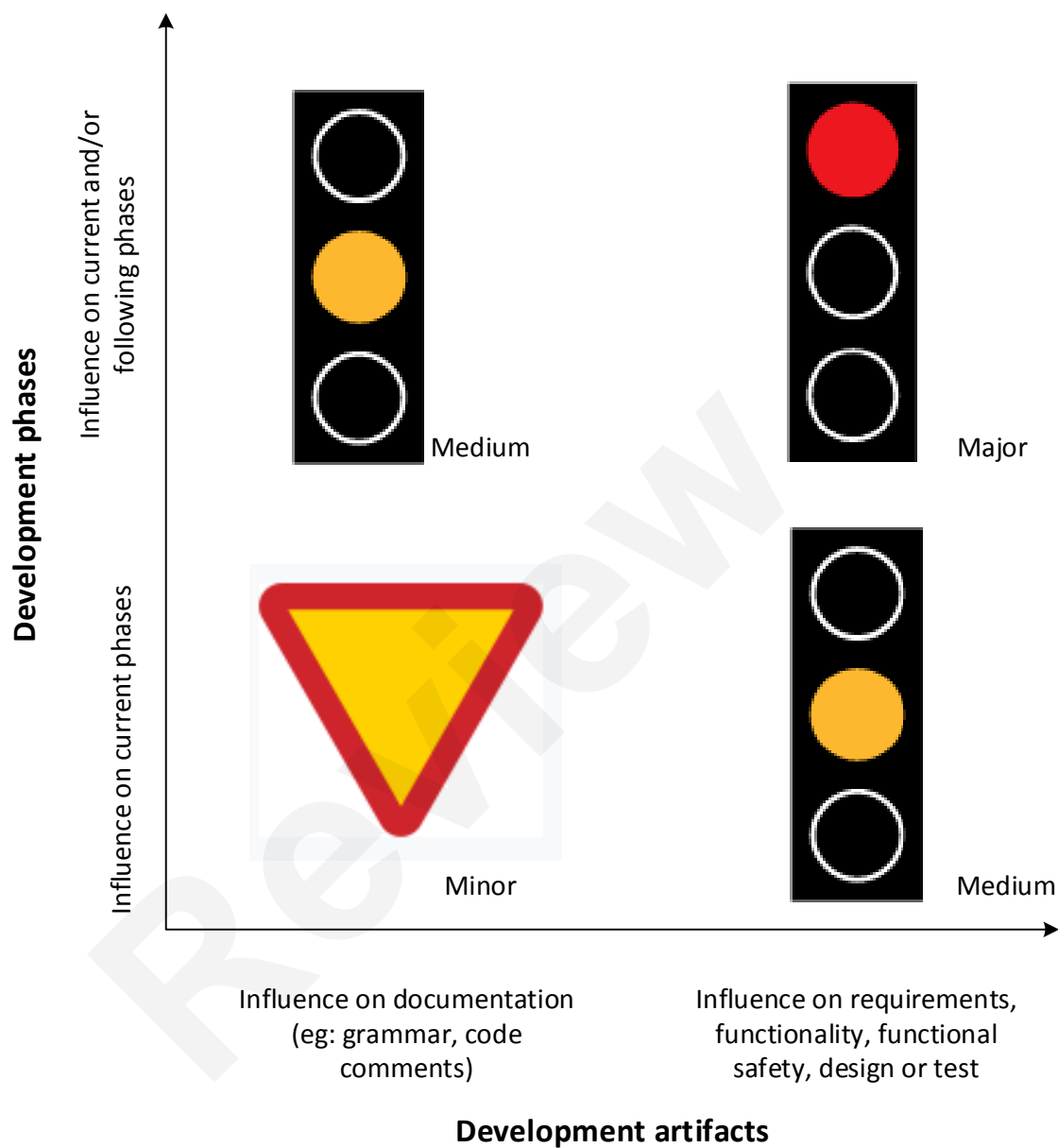





Figure 2 Classification of modifications

	<p>Problem severity: minor</p> <ul style="list-style-type: none"> - Continuing of current phase activities possible - Transition to following phase is possible - Adjustment of relevant development artefacts falls to judgement by the PSS CCB
	<p>Problem severity: medium</p> <ul style="list-style-type: none"> - Continuing of current phase activities possible - Transition to following phase is not possible before clarification of failures / problem - Exact investigation of the influence - Adjustment of relevant development artefacts
	<p>Problem severity: major</p> <ul style="list-style-type: none"> - Stopping of current phase activities - Exact investigation of the influence - Adjustment of relevant development artefacts. A step back to a preceding phase maybe necessary

If the Modification Request has been classified, its status is set to “ANALYSED”:

ANALYSED	The request for modification is analysed. The Designer gives a recommendation for implementation of the modification request (YES or NO with explanation)
----------	---

The classification is dependent on the kind of modification and thus has to be done individually. Nevertheless, some examples are given below.

To ensure an effective modification processing it is necessary to have qualified personnel doing this classification for each request separately. Classifiers shall also take into account requirement specification (SRS) issues. The raise of cost or extension of time shall be evaluated and documented.

Example	Modification Impact	Risk	Classification
Firmware update	Bad firmware → Heavy	Firmware update is implemented, the system supports such actions → High	Major
Safety related programming update	Collective signature will be updated → Heavy	Test need to be performed to prove same or improved safety function → High	Major
Replacement of standard IO modules	Modules are checked for correct functionality by the supplier before release → Light	module replacement may cause system shutdown → High	Medium
Replacement of safety modules	Modules are certified and checked for correct functionality by the supplier before release → Light	Safety Modules replacement will cause system shutdown → High	Major
Change of communication from Industrial Ethernet to PROFINET	Changes in code, full test of communication necessary → Heavy	Low	Major
EPLAN Drawing update due to typo in one page of the DI module	Changes only applied in the EPLAN drawing → Light	Low	Minor

Table 1: Examples for the Classification of a Modification

Note: Safety related modification is always categorized as a major modification.

5.4.5. Verification of changed software modules

The system stakeholder shall test and evaluate the output of a given software safety lifecycle phase to ensure correctness and consistency with respect to the input to that phase.

After each verification or re-verification:

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

- Identification of items shall be verified;
- Identification of the information against which the verification has been completed;
- Non-conformance to relevant specification documents

In this step, the Designer has to identify whether the modification is affecting any system-part with safety-relevant functionality. E.g. if the code which is only relevant for diagnosis in the failsafe system is affected, it is not needed to classify the modification as safety-relevant.

This step is mainly necessary for modification of software.

EXAMINED	The classification of the Designer is examined, the Modification must be approved
OPEN	Request for Modification has been examined but not verified, changes in classification are necessary

5.4.6. Approval

The safety relevant Modification Request shall be approved before the implementation. Approval shall be given by the PSS Change Control Board, which consists of:

- Work Package Manager
- Designer
- Verifier
- Functional Safety Manager (optional)

The decision shall be documented; comments by each member of the board can be added.

If the modification is approved, its status is set to "APPROVED", otherwise in case of refusal the request is set to "REJECTED"

APPROVED	The modification is approved and can be implemented
REJECTED	The modification is not approved, no change is done

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

5.4.7. Modification Status

The Designer implements the changes and modifies the documentation. If the Modification has been carried out, the status is set to “MODIFIED” (refer to the template).

MODIFIED	Changes are implemented but not yet tested.
----------	---

During Change Management, finished status (refer to the template) is directly set after the implementation of the modification has been carried out, as the verification is performed independently with the relevant test concepts.

FINISHED	The modification has been implemented successfully, and the test has been carried out and is finished.
----------	--

5.4.8. Verify changed software/hardware module/s

The result of each verification activity shall be documented, stating either that the safety relevant modules have passed the verification, or the reason of errors/failures.

5.4.9. Regression Test Concept

In parallel to the modification process, the Verifier develops the Regression Test concept. The mechanisms for the Regression Tests are dependent on the influence on the system, identified during impact analysis (refer to the section 5.4.3)

5.4.10. Regression Test Review

Before Regression Testing, the Designer shall check the Regression Test scenario for covering all critical items from the Impact Analysis. In addition, the Designer shall decide whether the modifications are testable with the Regression Test Concept:

REVIEWED	The Regression Test concept has been reviewed and no changes are necessary
REJECTED	The Regression Test has been reviewed and changes are necessary. The Designer shall provide a detailed failure description in order to enable the Verifier to correct the failure.

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

5.4.11. Regression Testing

After the modification has been implemented, the Verifier shall check the correctness of the modification according to the test mechanisms developed in parallel to the modification phase. After the regression testing has been carried out successfully, finished status is set. The regression test shall be classified as shown in the table below:

FAILURE	The modification has not been implemented correctly, changes are necessary. The Verifier shall provide a detailed failure description in order to enable the Designer to correct the failure. After the failure/error has been corrected, modified status is set. (refer to section 5.4.8)
REJECTED	If the test case is not usable, the Regression Test Concept must be adapted. The status is set to reject and the Verifier shall change the Regression Test Case. Before the test is carried out with the corrected Regression Test Concept, the Designer shall review the test case
FINISHED	The modification has been implemented successfully, and the test has been carried out and is finished. (refer to section 5.4.8)

5.4.12. Overview Change Management and failure documentation

The following figure gives an overview about the interactions between change management and documenting errors/failures during test.

For error/failure documentation, the relevant checklist and Failure Description template is used. (Refer to attachment 8.5)

The Designer classifies the error/failure as “safety relevant” or “not safety relevant”. In case it is not safety-relevant, the error/failure is only documented using the failure description template (refer to attachment 8.5).

The document number of this failure description is the line number of the test list with always five digits ID. For example: 1XXXX is related to hardware, 2XXXX is related to software, 3XXXX is related to electrical. Or to make use the remaining 4 digits to separate the issue within a system, for example: 21XXX is related to PLC CPU, 22XXX is related to digital I/O cards.

Document Type Specification
 Document Number ESS-0058389
 Date Feb 6, 2018
 Revision 1 (5)
 State Review
 Confidentiality Level Internal

If the error/failure is classified as safety- relevant, a modification request is generated using the Design Change Request template (refer to attachment 8.4).

In this Design Change Request template, the IDs of the failure descriptions are documented. The Design Change Requests are tracked via the CTRL. After the Modification has been implemented, the test in the relevant check list shall be carried out again to verify the modification for being implemented correctly.

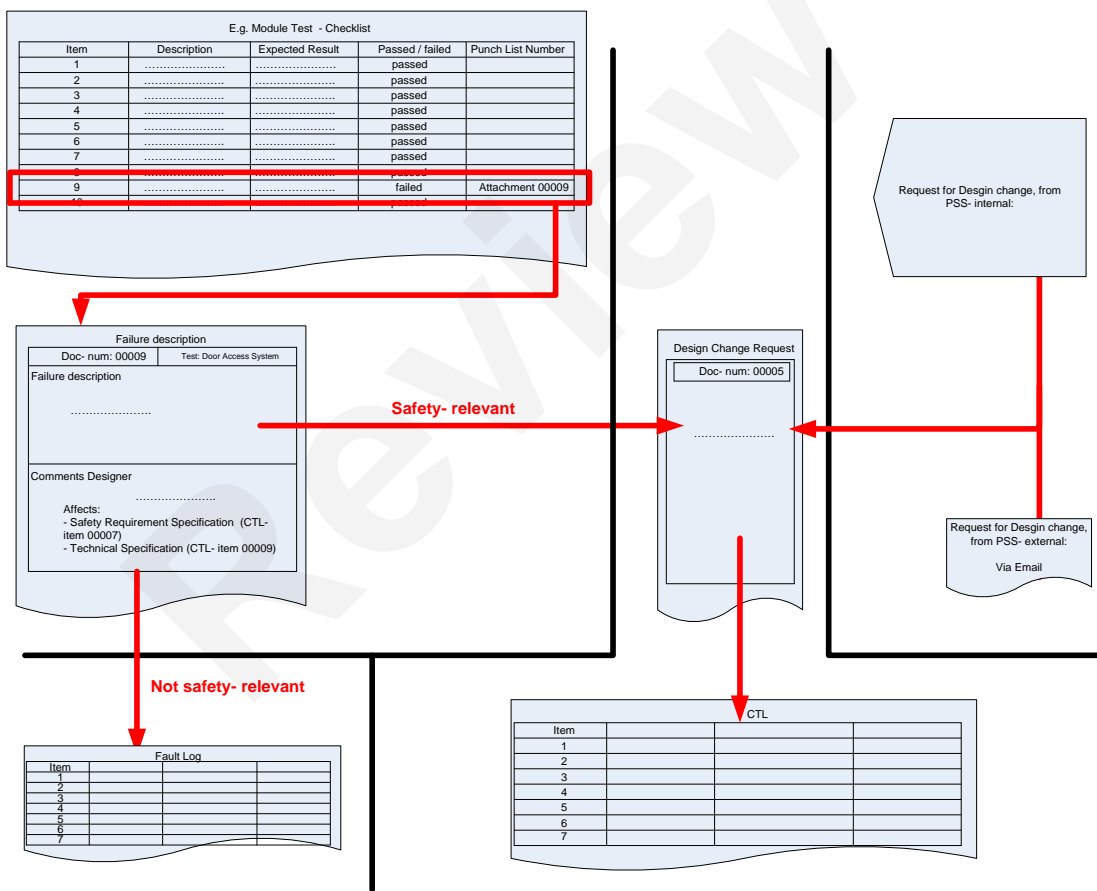


Figure 3: Document interactions during the change management process

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

6. FAILURE TRACKING

Failures found at any time during the development of PSS shall be documented in the CTL if they are safety relevant. The tracking of non-safety relevant failures is carried out, via a Fault Description (refer to attachment 8.5). The process for correcting failures is then carried out, according to Modification Management described in chapter 5.

Manager is responsible for the Modification Management to be implemented. During Validation, the CTRL and the Fault Description are checked for being fully processed.

Review

Document Type	Specification
Document Number	ESS-0058389
Date	Feb 6, 2018
Revision	1 (5)
State	Review
Confidentiality Level	Internal

7. REFERENCES

- [1] ESS-0061709, PSS Development and Quality Assurance Plan

- [2] SIMATIC Safety – Configuring and programming, programming and operating manual, 03/2017, A5E02714440-AF

- [3] IEC61508: 2010 Functional Safety of electrical/electronic/programmable electronic safety-related systems

- [4] ESS-0018781, ESS Process for Configuration Management

- [5] ESS-0068713, ESS definition of facility documentation

Document Type Specification
 Document Number ESS-0058389
 Date Feb 6, 2018
 Revision 1 (5)
 State Review
 Confidentiality Level Internal

8. ATTACHMENT (TEMPLATES)

8.1. Configuration Correlation



PSS Hardware Configuration Correlation Record

PSS Hardware Configuration Correlation Record		Project	
		Division :	ICS PSS
		Responsible	
		Version	
Approved	Department	Place, Date	Sign
Reviewed	Department	Place, Date	Sign
Prepared	Department	Place, Date	Sign
Yong Kian Sin	PSS	Lund	

Note:
 This document is seen as lifecycle document and thus subject to a continuous change.

Legend			
Color	Unit	PLC-Rack	IO_Rack
	Accelerator		
	ODH		
	Neutron Instrument		
	Engineering Station		

Editors			
Family Name	First Name	E-Mail	Telephone
Sin	Yong Kian	yongkian.sin@esss.se	

Internal Revision Log

Internal Revisions					
Rev.	Issue	Responsible	Type	Reason for Change	Changed Sections
1	2017-06-15	Yong Kian Sin	new feature	first issue	all

Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

Rack	Slot	Order No.	Designation	Hardware	Version	Setpoint
A	-	2866763	Quint PS, DIN rail power supply unit 110V DC -24V DC/5 A	Rev. 05	1109	--
	1	6ES7407-0KA02-0AA0	Power supply PS407 10A: AC 120/230V -> DC 5V/24V		--	2 batt Indic.
	3	6ES7 417-4HT14-0AB0	S7-CPU 1518; 2x1: 1 MPI/DP, 1 DP	1	V4.5.5	--
	-	6ES7960-1AA04-0XA0	Sync. Module for Patch Cable up to 10 m	5	--	--
	-	6ES7960-1AA04-0XA0	Sync. Module for Patch Cable up to 10 m	5	--	--
	-	6ES7952-1AP00-0AA0	RAM MEMORY CARD, 8 MBYTE	7	--	--
	5	6GK7443-1EX20-0XE0	CP 443-1, Industrial Ethernet, S7-400	5	V2.1	--
	-	6GK5204-2BC10-2AA3	SCALANCE X204-2LD, MANAGED IE SWITCH, 4 X 10/100MBIT/S RJ45 PORTS	6	V4.2	--

Hardware

Device	CHES No. :	Setpoint

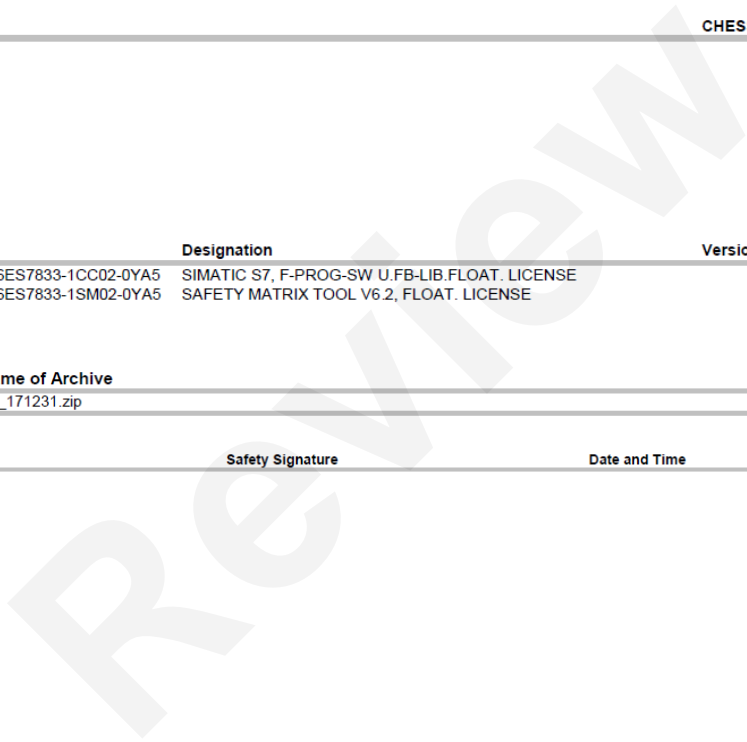
Software

Device	Designation	Version	Setpoint
6ES7833-1CC02-0YA5	SIMATIC S7, F-PROG-SW U.FB-LIB.FLOAT. LICENSE		
6ES7833-1SM02-0YA5	SAFETY MATRIX TOOL V6.2, FLOAT. LICENSE		

Actual Filename of Archive

PSS_S7_V300_171231.zip

Project	Safety Signature	Date and Time
...		



Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

8.2. Software Release



Personnel Safety Systems

PSS Software Release Version -

Prepared by : _____
Reviewed by : _____
Released by : _____

Name	Department	Date	Signature
------	------------	------	-----------



NOTE

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a model or design, are reserved.

Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

Table of Contents

1 Submittal of Software3
1.1 Version of Software3
1.2 Modified Part of Software3
2 Submittal of HMI.....4
2.1 Version of HMI4
2.2 Modified HMI System4
3 Corresponding Documentation5
3.1 Version Technical Specification5
4 Attachments6
 A) Current CTL (only modifications in submitted software shown)6
 B) Current CCR6

1 Submittal of Software

1.1 Version of Software

Submitted Software	Covered Objects in CTL (No.)	Current Version of CCR

1.2 Modified Part of Software

Modified Project	Relevant Safety Program	Safety Signature	Overall Signature	Timestamp Compile

Document Type Specification
 Document Number ESS-0058389
 Date Feb 6, 2018
 Revision 1 (5)
 State Review
 Confidentiality Level Internal

2 Submittal of HMI

2.1 Version of HMI

Submitted Software	Covered Objects in CTL (No.)	Current Version of CCR

2.2 Modified HMI System

Modified HMI System	Timestamp Compile

3 Corresponding Documentation

3.1 Version Technical Specification

Submitted Software	Covered Objects in CTL (No.)	Current Version

4 Attachments

A) Current CTL (only modifications in submitted software shown)	page/s
B) Current CCR	page/s

Document Type Specification
 Document Number ESS-0058389
 Date Feb 6, 2018
 Revision 1 (5)
 State Review
 Confidentiality Level Internal

8.3. Changes Tracking List



PSS Changes Tracking List

No.	Object of Change	Subject	Classification	Status	Responsible	Date Raised	Date Approved
20001	Software	Modification of safety programming for door access	Major	Finished	Yong Kian Sin	2017-06-01	2017-06-15
10001	Hardware	Replace fault DO module	Medium	Approved	Morteza Mansouri	2017-06-07	

Review


Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

8.4. Design Change Request



Design Change Request

Doc Number *

Date * 
Month Day Year

Originator *

Title *

Fault concerns

- Software
- Hardware
- HMI
- Document
- Other

Additional Information

Reason for Design Change:

Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

Description for Design Change

Modification is safety-relevant? (DES) * Yes No

Impact Analysis (DES) * Heavy Light

Justification (DES) *

Classification (DES) Minor
 Medium
 Major

Signature and Date (DES) *

[Clear](#)

Examination (VER) * Accepted
 Not Accepted
 Not relevant

Document Type Specification
Document Number ESS-0058389
Date Feb 6, 2018
Revision 1 (5)
State Review
Confidentiality Level Internal

**Signature and Date
(VER) ***

Clear

Review

Document Type Specification
 Document Number ESS-0058389
 Date Feb 6, 2018
 Revision 1 (5)
 State Review
 Confidentiality Level Internal

8.5. Failure Description



Personnel Safety Systems

PSS Failure Description			
Doc No.:		Date: / /	Originator:
Title:			
Description of failure (responsible Verifier):			Fault concerns <input type="checkbox"/> Software <input type="checkbox"/> Hardware <input type="checkbox"/> HMI <input type="checkbox"/> Documents
Classification of failure (responsible Designer): <input type="checkbox"/> Major <input type="checkbox"/> Medium <input type="checkbox"/> Minor			
Date, Signature, Dept _____			
Comment (responsible Designer)			
<input type="checkbox"/> Affects safety- relevant part <input type="checkbox"/> No affect safety- relevant part			
Date, Signature, Place _____			
Accepted by Verifier			
Date, Signature, Place _____			

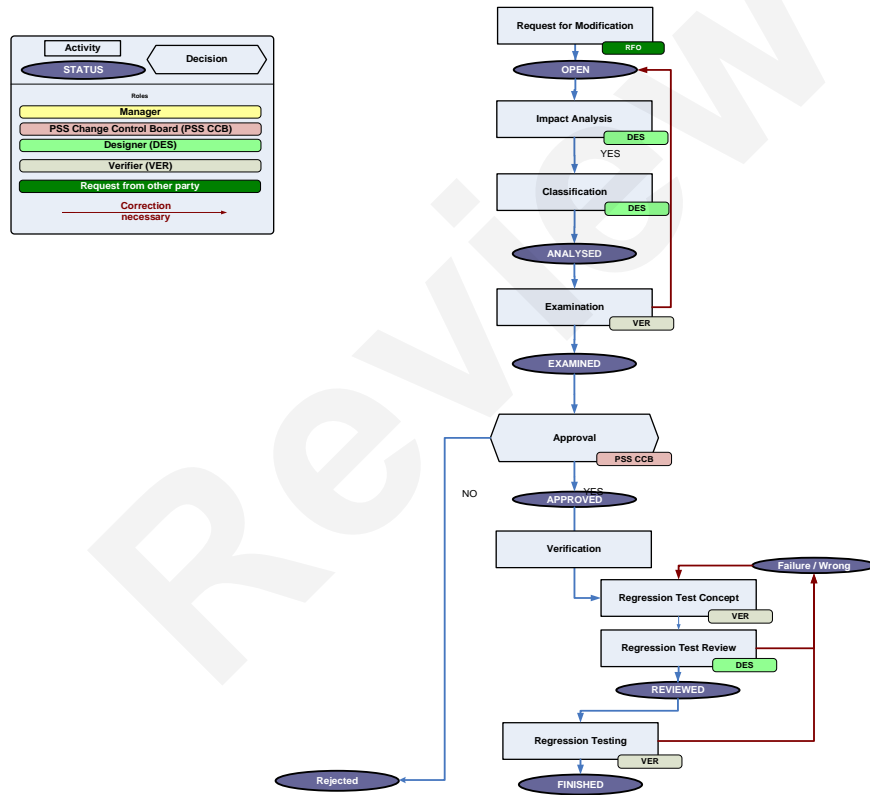


Figure 4: Change management flow chart

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	First issue	Yong Kian Sin	2016-05-09
2	<p>Second issue</p> <p>After document review by ZHAW, the following modifications were made to the document:</p> <p>Chapter 4.1: Correction explanation updated</p> <p>Chapter 4.2: Component updated</p> <p>Chapter 5.3: Software Configuration added more details according to IEC61508</p> <p>Chapter 5.4.3: Impact Analysis added more details according to IEC61508</p> <p>Chapter 5.4.4 Figure for Classification for modifications added,</p> <p>table Example of Classification of Modification updated</p> <p>Chapter 5.4.5: Verification of changed software modules added</p> <p>Chapter 5.4.6: Status of approval updated</p> <p>Chapter 8: Templates added</p>	Yong Kian Sin	2017-06-06
3	<p>Reviewer and Approver list updated</p> <p>References updated</p>	Yong Kian Sin	2017-10-19

The document has been reviewed by ZHAW, and fulfilled the requirements of IEC61508