|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Verification Plan for Personnel Safety Systems 0 |
|  |
|  |

|  | Name | **Role/Title** |
| --- | --- | --- |
| **Owner** | Stuart Birch | Senior Engineer for Protection Systems Group, ICS |
| **Author** | Paulina Skog | Technical Document Specialist for Protection Systems Group, ICS |
| **Reviewer** | Denis Paulic Morteza MansouriThilo Friedrich | Deputy Group Leader for Protection Systems Group, ICS Lead Integrator Engineer for Safety Critical Systems, ICSSystems Engineering and Engineering Process Coordinator, ICS |
| **Approver** | Annika Nordt | Group Leader for Protection Systems Group, ICS |

|  |  |
| --- | --- |
| Table of content | Page |

1. Introduction 5

1.1. Verification and validation 5

1.2. Scope and purpose 5

1.3. Applicable standards 5

1.4. PSS0 overview 5

Roles and Responsibilities 6

1.5. Responsible organization 6

1.5.1. ICS 6

1.5.2. The roles accountable 6

1.6. Documentation 6

1.6.1. Verification document requirements 7

1.6.2. Verification documents 7

1.6.2.1. Test specifications 7

1.6.2.2. Test reports 7

1.7. Traceability 7

1.8. The change control board 8

2. Verification 9

2.1. Verification strategy 9

2.2. Verification activities after handover 9

2.3. Verification methods 9

2.4. Verification activities 10

2.4.1. PSS0 verification activities 10

2.4.2. Parent system reviews 11

2.5. Verification tests 14

2.5.1. Hardware FAT 14

2.5.1.1. Entry criteria 14

2.5.1.2. Methods 14

2.5.1.3. Tools 14

2.5.1.4. Acceptance criteria 14

2.5.1.5. Roles 15

2.5.2. Hardware SAT 15

2.5.2.1. Entry criteria 15

2.5.2.2. Methods 15

2.5.2.3. Tools 15

2.5.2.4. Acceptance criteria 15

2.5.2.5. Roles 16

2.5.3. Software pre-FAT 16

2.5.3.1. Entry criteria 16

2.5.3.2. Methods 16

2.5.3.3. Tools 16

2.5.3.4. Acceptance criteria 16

2.5.3.5. Roles 17

2.5.4. SIT 17

2.5.4.1. Entry criteria 17

2.5.4.2. Methods 17

2.5.4.3. Tools 17

2.5.4.4. Acceptance criteria 17

2.5.4.5. Roles 18

2.5.5. FIT 18

2.5.5.1. Entry criteria 18

2.5.5.2. Methods 18

2.5.5.3. Tools 18

2.5.5.4. Acceptance criteria 18

2.5.5.5. Roles 19

3. System Validation 20

3.1. System demonstration and handover 20

3.2. Validation after changes 20

4. ABBREVIATIONS 21

5. References 22

Document Revision history 24

6. Appendix 25

list of tables

Table 1: Responsible for Hardware FAT. 15

Table 2: Responsible for Hardware SAT. 16

Table 3: Responsible for pre-FAT 17

Table 4: Responsible for SIT. 18

Table 5: Responsible for FIT. 19

Table 6: Responsible for system demonstration. 20

list of Figures

Figure 1: Independence of different roles. 6

Figure 2: Verification and validation activities. 13

Figure 3: Verification and validation activities in high resolution. 25

# Introduction

This document addresses the verification and validation planning for the Personnel Safety Systems 0 (PSS0). For the validation of the implemented safety performance, specific activities shall be identified and supported by assessment methods and documentation in this plan.

## Verification and validation

Verification and validation are the following in the context of PSS:

**Verification**: confirmation by examination and provision of objective evidence that the requirements have been fulfilled [1].

**Validation**: confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled [1].

## Scope and purpose

This verification and validation plan covers only PSS0 and addresses the verification and validation activity planning for hardware and software of the PSS. The purpose of this document is to provide a high-level plan for these activities.

Note that since this plan is a high level plan, it will not describe the test activity in detail, giving all complete approved test specifications and test reports, but should work as an input when designing the test specifications and test reports. The plan provides an overview of required tests and reviews that shall be performed.

## Applicable standards

* IEC 61511 [1]
* SS-EN 62381 [2]

## PSS0 overview

The primary role of the PSS0 is to protect workers from the hazards specified in the Hazard and risk analysis document for PSS0 [3], which analyses the hazards connected to the Ion Source (ISrc) and Low Energy Beam Transport (LEBT) test stand. Note that the ISrc and LEBT test stand is sometime referred to as the parent system in this plan.

The ISrc and LEBT test stand will be installed in the ESS accelerator tunnel. The ISrc HV platform will be enclosed by a safety fence, which functions as a barrier against direct contact to the ISrc HV platform when it is energised. Technical details of ISrc and LEBT can be found in [4]. PSS0 scope, hardware and software design are detailed in [5], [6] and [7] respectively. Specification of the relevant modes of the EUC operation with their relationship to the E/E/PE safety-related system are explained in [8].

# Roles and Responsibilities

## Responsible organization

### ICS

The Protection Systems Group (PSG) in ICS is responsible to develop, install, commission, validate and maintain PSS0 and for providing and maintaining this document.

### The roles accountable

Requirement specification Validator (VAL)

Verification and testing Verifier (VER)

Software/Hardware development and integration Designer (DES)

Validation Validator (VAL)



Figure 1: Independence of different roles.

Any resulting changes in requirements, corrective actions, reverification and revalidation must be documented and approved according to configuration management [9].

## Documentation

Test specifications and test reports with attached checklists shall be approved in CHESS. The test reports shall be signed by the involved personnel and relevant stakeholders. The signed copies shall be scanned and uploaded to CHESS.

### Verification document requirements

The following information shall be available in the test documents:

* The Facility Breakdown Structure (FBS) for the equipment/system being tested
* CHESS id
* Date information
* Signing section for approval signing
* List of test equipment
* Test list with test description or reference to a test description
* Checklists and punch list available designed in a structured way, making it easy to see what is approved and not, and why.
* Roles of the ones performing the test
* In the SIT and FIT specification and report it shall be clear that all safety functions are tested. All safety functions shall be tested and approved before validation.

### Verification documents

The following verification documents shall be produced, approved and uploaded to CHESS before validation. For more information about entry criteria, methods, tools, acceptance criteria’s and roles for the specific tests, see section 2.5.

#### Test specifications

* Hardware Factory Acceptance Test (FAT) specification
* Hardware Loop check specification
* Hardware Site Acceptance Test (SAT) specification
* Pre Factory Acceptance Test (pre-FAT) specification
* Site Integration Test (SIT) specification
* Final Integration Test (FIT) specification

#### Test reports

* Hardware FAT report
* Hardware Loop check report
* Hardware SAT report
* Pre-FAT report
* SIT report
* FIT report

## Traceability

The Safety Requirement Specification (SRS) defines the safety requirements for each (SIF). It includes specifications of both the functional and safety integrity requirements for the system.

Traceability is established from the requirements that are stated in the Safety Requirements Specification Document for PSS0 [10] and the Software Safety Requirements Specifications for Personnel Safety System 0 [11] and trough verification and validation activity documents.

These requirements shall be tested and verified using checklists, the checklists should be attached to the activity reports, which shall be uploaded to CHESS. The requirements shall be verified again during the SIT, when the software and hardware are integrated. This shall also be documented via a checklist and validated during the last independent validation demonstration.

For deviation traceability please see [9] for more information.

## The change control board

The change control board is responsible for approval or refusal of change requests. This is described in the configuration management document [12].

# Verification

A verification strategy is an outline that describes the verification approach that maximizes the operational coverage for a system while it minimizes risks of design mistakes and system failure. It is created to inform managers, testers, and developers about some key issues of the verification activities and to demonstrate that systems performs as expected. This includes the verification objective, methods of testing new functions, resources required for the project and the testing environment [13].

Prior to any operation or energisation of the systems interlocked by PSS0, the PSS0 shall be verified and validated. This means all safety instrumented functions (SIF) described in the Safety requirements specification document for PSS shall be fully verified and validated.

## Verification strategy

* Hardware and software component tests and system integration tests, the tests planning, and documentation shall be carried out according to SS-EN 62381:2012 [2] and IEC 61511 [1].
* The software shall have documented code reviews, described later in the review section.
* All documents shall be reviewed and approved by appropriate reviewers, this will be further detailed later in this document.

## Verification activities after handover

A change management process shall be available after the handover of the system. Depending on the level of a change and how it effects the whole system, the system shall be tested accordingly. The change shall be reviewed and approved by the change control board. The changes shall follow the change management flow described in the configuration management plan [9].

## Verification methods

The following standard methods are used [14]:

* **Analysis:** Critical and careful evaluation of a situation or problem that shows the theoretical compliance, e.g. by use of simulation or analytical data.
* **Test:** Program or procedure that is designed to verify that a system conforms to its requirements.
* **Inspection:** Visual examination of a system and associated descriptive documentation.
* **Demonstration**: Verification by witnessing an actual operation in the expected or simulated environment, without need for measurement data, additional test equipment or post demonstration analysis.
* **Review:** A formal assessment or evaluation of documentation, procedures, decisions or design, with the intention of ensuring that specific requirements are fulfilled. The different reviews are specified further in the next section.

## Verification activities

### PSS0 verification activities

The following verification activities shall be performed for PSS0.

* **Preliminary Design Review (PDR)**: verifies that the conceptual design and the planned technical approach will meet the requirements [13].
* **Critical Design Review (CDR):** verifies that the specified requirements are met by the detailed, or critical, design [13]. A CDR demonstrates that the maturity of the design is appropriate to proceed into system development, demonstration and testing.
* **Factory Acceptance Test for PSS0 hardware (Hardware FAT):** verifies that the as-built hardware system meets the specified design. The FAT includes component test, integration test and system test. The FAT shall be performed by the vendor [13], but it should be designed and accepted by ESS. The scope of hardware FAT for PSS is described in 2.5.1.

***Note:***

* This Hardware FAT is not the same as the FAT defined in IEC61511 standard. The FAT from IEC 61511 standard is part of the SIT described below.
* The Hardware FAT follows the ESS guideline for FAT [15].
* In case of PSS0, FAT activities are different for hardware and software. The software FAT follows the recommendations from IEC 61511 standard and has two stages:
	+ Software pre-FAT - preparation for software FAT, where the software developer tests the code in test environment, mainly through simulation.
	+ Software FAT (included in PSS0 SIT and FIT, see below) – hardware and software integration testing.
* **Site Acceptance Test (Hardware SAT):** verifies that the hardware system is installed as specified in its operational environment. SAT include the same tests as the FAT, once the hardware is delivered to ESS. The SAT shall be performed by ESS on the site. The scope of hardware SAT for PSS is described in 2.5.2.

***Note:*** This hardware SAT does not follow the IEC61511 standard definition of SAT. The SAT according to the standard is included in the validation presented below.

* **Preparation for software FAT (Software pre-FAT):** verifies the software functionality through simulations in test environment. It includes the software code review to reveal potential software design defects and avoid systematic failures. An independent software developer (not involved in developing the ODHDS software) shall review the code. The test shall be documented in a software simulation test document, which shall include a confirmation from independent software code review that software is ready for SIT.
* **Site Integration Test (SIT):** verifies that installed hardware and software work together properly, ensuring that their combination is serving the purpose of PSS safety functions and procedures. The scope of SIT for PSS0 is described in 2.5.4.

***Note:*** To reduce the risk of damaging the Equipment Under Control (EUC) due to repeated tests, the EUC shall be disconnected from PSS during PSS SIT.

* **Final Integration Test (FIT):** FIT is a repetition of SIT whilst EUC is operational and connected to PSS.
* **Functional Safety assessment (FSA)**: All of the documents produced for PSS0 until that point in time are reviewed internally at ESS and externally by an independent team from Zurich University of Applied Sciences (ZHAW). The purpose of the analysis documents, the test specifications, the test reports with checklists and punch lists is to systematically produce the material necessary to give a judgement on each safety aspect and to evaluate the safety of the overall system. The shortcomings of the items under validation shall be specified and recommendations on modifications shall be proposed.

### Parent system reviews

The reviews listed below are generally conducted for the parent system by the stakeholders of all systems and sub-systems to confirm readiness. PSS may be required to participate in these reviews:

* **Installation readiness review (IRR):** verifies the final technical design, emphasising on interfaces between components, subsystems, controls integration, plans, staff, and tooling required for the installation work itself. The final technical review of the system prior to the start of installation [16].
* **Test readiness review (TRR):** verifies that the product, its test equipment, support personnel, and test procedures are ready for the PSS SIT and FIT and validation. The test templates for the SIT, should be delivered and verified at this point.
* **Safety readiness review (SRR):** An independent review capturing both conventional and radiation safety aspects. The purpose of the SRR is to review the readiness to safely commission any system [16].

Figure 2 shows a plan of the different verification and validation activities. See Figure 3, for a larger representation of Figure 2. There are two types of verification activities in PSS0: tests and reviews. Figure 2 presents a preliminary order of events, with arrows, when there is an important order or relationship. Note that it is not possible to make out the specific time or date, by compering distances in the figure.

The blue boxes in the figure represent reviews conducted by the PSS team specifically for the PSS0. Note that the white box with the small yellow box on top presents an integration test, since the software FAT is performed during the SIT. The orange shapes represent the parent system reviews, for example the parent system needs to conduct an SRR, for which the readiness of PSS0 is an input. PSG shall provide the documentation presented in Figure 2.



Figure 2: Verification and validation activities.

## Verification tests

### Hardware FAT

#### Entry criteria

* The vendor and ESS shall agree on a full hardware FAT test acceptance specification. The test acceptance specification and test templates shall be available for review before the FAT tests commence [15].
* Manufacturer in-house tests completed [2].
* PSS0 racks and field devices (if applicable) are populated with hardware components according to PSS hardware design document for that system [15]. ESS shall witness the FAT.

#### Methods

* Inspection
* Test
	+ Test which check insultation resistance, disruptive discharge, residual voltage etc are covered in the Factory Acceptance Test Template for PSS [17].

#### Tools

* Windows laptop with PLC programming tool to force and/or simulate signals to PLC modules.
* Multimeter for continuity tests.
* Insulation tester for PSS racks insulation tests.
* Loop calibrator to simulate analogue signals to test PLC analogue modules.

#### Acceptance criteria

* The PSS0 hardware FAT shall be carried out successfully.
* Non-conformities shall be documented, and mitigating measures shall be completed by the contractor.
* The result is accepted by ESS.
* The result from performed hardware FAT shall be documented in a test report in CHESS, all failures shall be documented.

#### Roles

Table 1: Responsible for Hardware FAT.

|  | Role |
| --- | --- |
| Manager | Manager [12] |
| Designer | Hardware designer [12] |
| Verifier | Hardware verifier [12] |

### Hardware SAT

#### Entry criteria

* Hardware FAT completed and approved.
* Test specifications templates shall be available for review before the SAT tests commence.
* The Loop check specification and report template shall be available for review before the SAT.
* PSS hardware are shipped to site.
* PSS racks and field devices properly installed and connected at site according to hardware design documents.
* PSS racks energized.

#### Methods

* Inspection
* Test
	+ Test which check insultation resistance, disruptive discharge, residual voltage etc are covered in the Site Acceptance Test Template for PSS [18].

#### Tools

* Windows laptop with PLC programming tool to force/simulate signals to PLC modules.
* Multimeter for continuity tests.

#### Acceptance criteria

* The PSS0 hardware SAT shall be carried out successfully according to the approved test procedures.
* Non-conformities shall be documented, and mitigating measures shall be completed, or the conformities shall be accepted by ESS.
* The result from performed hardware SAT and Loop check test shall be documented in a test report in CHESS, all failures shall be documented.

#### Roles

Table 2: Responsible for Hardware SAT.

|  | Role |
| --- | --- |
| Manager | Manager [12] |
| Designer | Installation coordinator [12] |
| Verifier | Hardware verifier [12] |

### Software pre-FAT

The Software development planning document [7] defines all inputs, outputs and development activities for PSS0 software development.

#### Entry criteria

* Software planning document, Software safety requirements specification and Software design document shall be available.
* Software programming tool (including the simulation add-on) shall be installed.
* Test environment hardware shall be configured.
* Software code shall be developed, reviewed by a competent person not involved in original software development and prepared for simulation.
* The test specification with test description, activity steps and acceptance criteria shall be available.
* The checklist for Software pre-FAT test report shall be available.

#### Methods

* CDR with design walkthrough.
* Code, configurable hardware and firmware visual inspections to ensure compliance with software design document and software SRS.
* Code simulation in test environment.
* Visual inspection of pre-FAT results (checklists), which includes structural tests (verifying data structures and its control and procedural logic) carried at the unit level.

#### Tools

* Windows laptop with Siemens TIA portal installed (v 14 SP1 or higher), including the safety advanced optional package, WinCC Comfort and PLC Sim.
* Test environment PLCs and HMIs (can be PSS0 PLCs).

#### Acceptance criteria

* Non-conformities have been documented and mitigating measures have been taken care of by the software developer.
* The results from performed pre-FAT shall be documented in CHESS.
* The PSS0 software shall be downloaded successfully to PSS0 PLCs and versioned as described in software SRS.

#### Roles

Table 3: Responsible for pre-FAT

|  | Role |
| --- | --- |
| Manager | Manager [12] |
| Designer | Software developer [12] |
| Verifier | Software verifier [12] |

### SIT

#### Entry criteria

* Hardware SAT complete.
* Software pre-FAT complete.
* Test specifications and test report templates shall be available for review before the SIT tests commence.
* Software uploaded to PSS0 PLCs.
* PSS0 network communication equipment configured.

#### Methods

* Test
	+ For software (A.12.5.3 in IEC 61511-2 [1]):
		- Performance tests
		- Integration-level structural tests
		- System-level integration tests
* Demonstration

#### Tools

* Windows laptop with PLC programming tool
* Multimeter for continuity tests
* PSS0 PLCs
* PSS0 HMI-s

#### Acceptance criteria

* Integration test for the PSS0 hardware and software shall be carried out successfully according to the approved test procedures in a test report template.
* Non-conformities with respect to the current requirements meant for SIT shall be documented in a punch list. The test leader shall perform a judgment for every non-conformity and come to a decision if the test must be aborted or continue.
* The result from performed SIT shall be documented and stored in CHESS.

#### Roles

Table 4: Responsible for SIT.

|  | Role |
| --- | --- |
| Manager | Manager [12] |
| Designer | Software developer [12] |
| Verifier | Software verifier [12] |

### FIT

#### Entry criteria

* SIT complete.
* Test specifications and test report templates shall be available for review before the FIT tests commence.
* EUC properly connected to PSS0.
* EUC energized and ready to test.
* ES&H permit issued to energize the EUC for test purposes.

#### Methods

* Test
* Demonstration

#### Tools

* Windows laptop with PLC programming tool
* Multimeter for continuity tests
* PSS0 PLCs
* PSS0 HMI-s

#### Acceptance criteria

* Integration test for the PSS0 hardware, software and EUC shall be carried out successfully according to the approved test procedures.
* Non-conformities with respect to the current requirements meant for FIT shall be documented in a punch list. The test leader shall perform a judgment for every non-conformity and come to a decision if the test must be aborted or continue.
* The result from performed FIT shall be documented.

#### Roles

Table 5: Responsible for FIT.

|  | Role |
| --- | --- |
| Manager | Manager [12] |
| Designer | Software developer [12] |
| Verifier | Software verifier [12] |

# **System Validation**

## System demonstration and handover

To present that PSS0 meets the safety and operational requirements, a demonstration of operational and emergency procedures shall be presented to all identified stakeholders (AD and ES&H). The stakeholders shall have the access to all PSS0 documentation, test specifications and test reports. The demonstration shall be carried out on the real system at the ESS site and cover the positive tests from the FIT.

The demonstration shall be documented. The document shall be signed, uploaded to CHESS and approved by the attendees.

Table 6: Responsible for system demonstration.

|  | Role/Title |
| --- | --- |
| Manager | Manager [12] |
| Designer | Integration coordinator [12] |
| Validator | Senior Electrical Safety Engineer, ES&H DivisionIon source and LEBT system leader, AD |

## Validation after changes

The changes shall follow the change management flow described in the configuration management plan [9]. For more information see the configuration management plan.

# ABBREVIATIONS

CDR Critical Design Review

ConOps Concept of Operations

AD Accelerator Division

CHESS Collaboration Home ESS

DES Designer

E/E/PE Electrical/Electronic/Programmable Electronic safety related systems

EIS Engineering and Integration Support

ES&H Environment Safety and Health

ESS European Spallation Source

EUC Equipment Under Control

FAT Factory Acceptance Test

FIT Final Integration Test

FSA Functional Safety Assessment

HMI Human Machine Interface

HV High Voltage

ICS Integrated Control System

IRR Installation Readiness Review

ISrc Ion Source

LEBT Low Energy Beam Transport

ORR Operational Readiness Review

PDR Preliminary Design Review

PSG Protection Systems Group

PSS Personnel Safety Systems

PSS0 Accelerator Personnel Safety System 0

SAT Site Acceptance Test

SAR System Acceptance Review

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIT Site Integration Test

SRR Safety Readiness Review

SRS Safety Requirement Specification

TRR Test Readiness Review

VAL Validator

VER Verifier

ZHAW Zurich University of Applied Sciences

# References

|  |  |
| --- | --- |
| [1]  | Functional safety – Safety instrumented systems for the process industry sector (IEC 61511), 2016.  |
| [2]  | Automation systems in the process industry – Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT) (SS-EN 62381), 2012.  |
| [3]  | Hazard and Risk Analysis Document for PSS0 (ESS-0229506), 2018.  |
| [4]  | Technical description of the ESS Normal Conducting Front End (ESS-0159957), 2018.  |
| [5]  | Scope Document for Accelerator personnel Safety System 0 (ESS-0237881), 2018.  |
| [6]  | PSS0 Hardware Design Requirements Specifications (ESS-0237967), 2018.  |
| [7]  | PSS0 Software Planning Document (ESS-0237557), 2018.  |
| [8]  | Accelerator Personnel Safety System 0 and Ion Source Interface Control Document (ESS-0237562).  |
| [9]  | Configuration management plan for Personnel Safety Systems (ESS-0058389), 2018.  |
| [10]  | Safety Requirements Specification Document for PSS0 (ESS-0238059), 2018.  |
| [11]  | Software Safety Requirements Specifications for Personnel Safety System 0 (ESS-0407101), 2018.  |
| [12]  | Systems Engineering Management Plan for Personnel Safety Systems (ESS-0454273)\*, 2018.  |
| [13]  | ESS Handbook for System Verification (ESS-0117128) \*\*, 2018.  |
| [14]  | System engineering handbook- a guide for system lifecycle processes and activities (INCOSE), 2006.  |
| [15]  | ESS Guideline for Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) (ESS-0094204), 2018.  |
| [16]  | ESS Handbook for Engineering Management (ESS-0092276), 2018.  |
| [17]  | Factory Acceptance Test Template for PSS (ESS-0286218), 2018.  |
| [18]  | Site Acceptance Test Template for PSS (ESS-0328961).  |
| [19]  | Machine Protection Configuration Management Plan (ESS-0436437)\*\*, 2018.  |

\* The Systems Engineering Management Plan for Personnel Safety Systems (ESS-0454273) is under development

\*\* The ESS Handbook for System Verification (ESS-0117128) is under development, however the parts reffered in this document is not expected to be changed.

Document Revision history

| Revision | Reason for and description of change | Author | Date |
| --- | --- | --- | --- |
| 1 | First issue | Yong Kian Sin | 2018-01-29 |
| 2 | Written to comply with IEC 61508  | Paulina Skog | 2018-05-29 |
| 3 | Written to comply with IEC 61511  | Paulina Skog | 2018-09-18 |
|  |  |  |  |

#  Appendix

Figure 3: Verification and validation activities in high resolution.