TSS Verification and Validation plan

	Name	Role/Title
Owner	Atefeh Sadeghzadeh	Control engineer, Target controls and Safety
Reviewer	Mikael Olsson	Control engineer, Target controls and Safety
Reviewer	Anders Malm	Electrical designer, Target controls and Safety
Reviewer	Ola Ingemansson	Instrument engineer, Target controls and Safety
Approver	Linda Coney	Group leader, Target controls and Safety

TABLE OF CONTENT **PAGE**

1. SCOPE

The goal for TSS is to protect the public from exposure to unsafe levels of radiation, and preventing the release of radioactive material beyond permissible limits and to bring the target station into a safe state in case of an abnormal event from nuclear radiation safety point of view. To get more general overview and overall understanding of TSS, see [1].

The scope of this document is overall planning of verification and validation of the TSS.

This document relates to chapter 12.7 (part of lifecycle phase 9), chapter 13 and chapter 14-15 (lifecycle phase 5) of [2], see Figure 1.

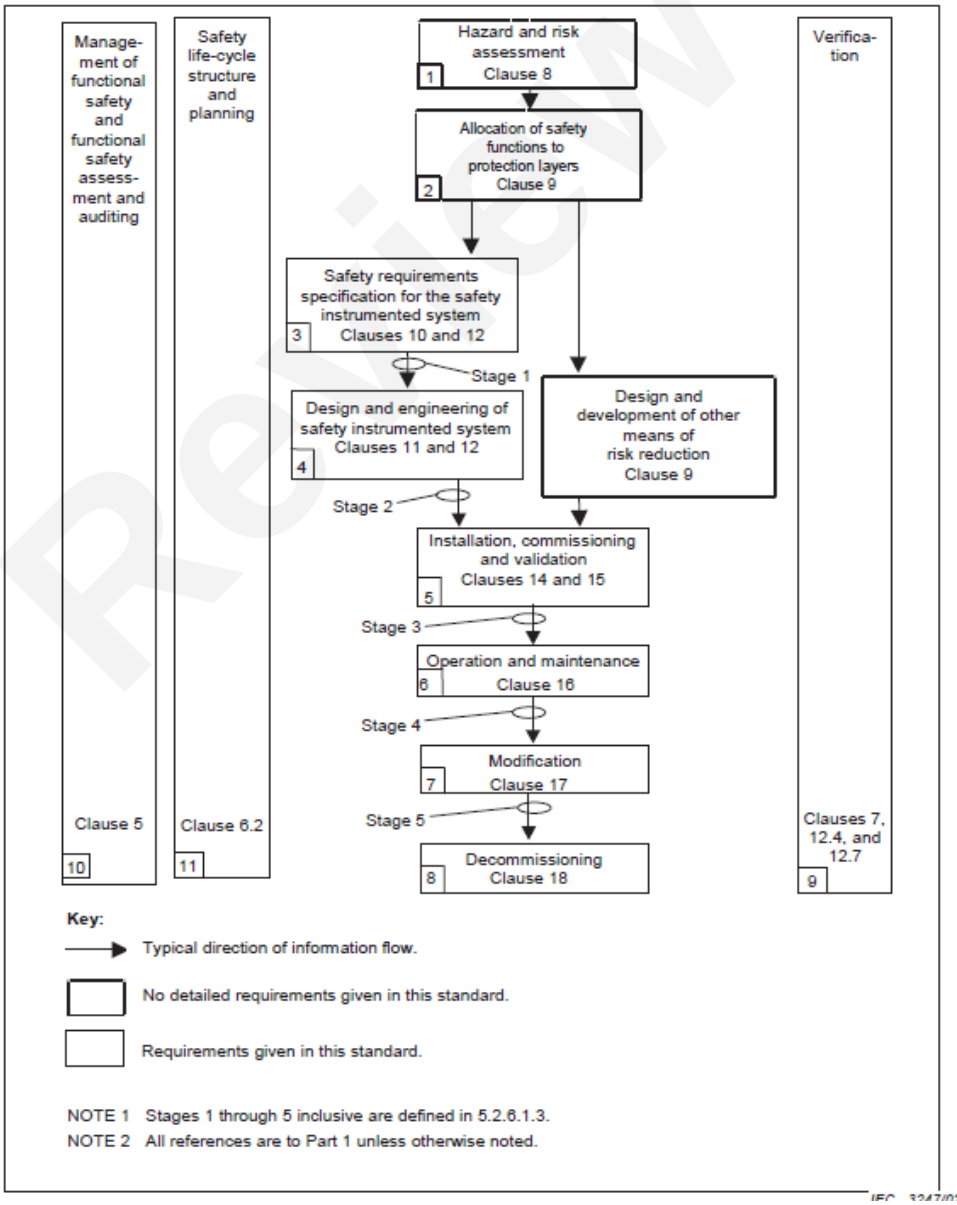

Figure 1 IEC 61511 system safety life-cycle (Figure 8)

1.1. Objective

The objective of this document is to plan verification and validation activities for hardware and software of the TSS [4]. The details of these activities will be covered in separate documents.

1.2. Purpose

The purpose of this document is to provide high-level plan for verification and validation activities. It should be used as base for further detailed verification and validation activities.

This document is part of the integration activity planning.

1.3. Definitions

[2], section 3.2.92: **verification** - activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

Example of verification activities

- reviews on outputs (documents from all phases of the safety life cycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed products to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner

[2], section 3.2.91: **validation** - activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification

2. ISSUING ORGANISATION

This document is issued by Target Controls and Safety (WP7) within Target division.

3. SCHEDULE

Figure 2 shows the steps of TSS verification and validation activities:

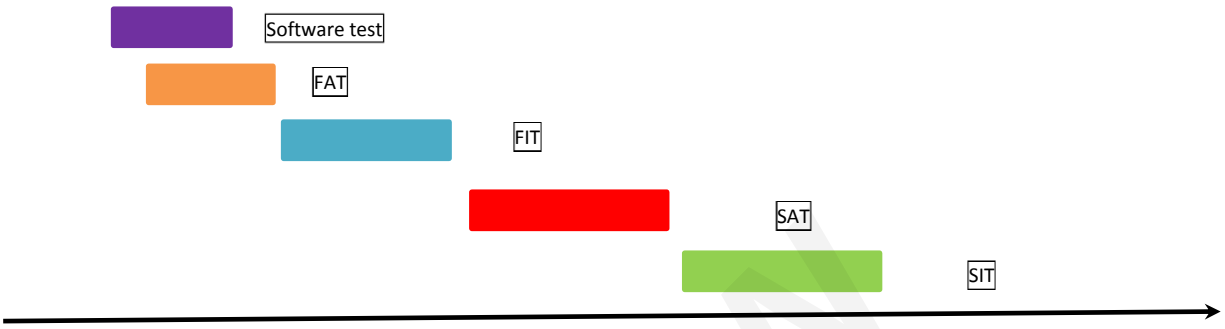

Figure 2 appearance of different tests vs. time

4. DOCUMENTATION

Documentation after each verification and validation activity shall:

- Show that the verification/validation has been carried out and the results were as expected
- Allow an assessment of the adequacy of the verification/validation
- Allow an independent person to repeat the verification/validation and review the coverage achieved
- Follow the TSS configuration management criteria
- Follow procedures for corrective actions if any failure was detected by the verification/validation

5. VERIFICATION

Verification activities include:

- **Software test**
- **Factory Acceptance Test (FAT)**
- **Factory Integration test (FIT)**

5.1. Software test

This chapter refers to section 12.7 in [2]. The objective of the verification is to test the logic parts and associated software to make sure the specific functional requirements are fulfilled. This software test is independent of the hardware verification tests and can be done in parallel with it. The test is recommended to be performed by a person who is a member of an independent department, and should for example:

- Address testability, readability, traceability
- Confirm that data used within the application software is correct and where appropriate unique (for example TAG names are uniquely assigned, that data is not misused by subsequent functions and that constants such as alarm set points are valid and correct).
- Include check of test operations performed by test tool

Two stages can be defined:

5.1.1. Software simulation

In this review the software shall be verified through analysis, simulation and testing techniques to confirm that the application program functions meet the requirements and that unintended functions are not executed.

5.1.2. Software integration

In this test, the software is downloaded on the CPU and it will be tested together with the TSS mock-up in the lab that includes the IO modules, switches, HMI and actuators.

5.2. FAT

This chapter refers to chapter 13 in [2]. The FAT verifies that the TSS manufactured equipment meets the specified electrical design. It should be carried out according to [9].

FAT will be done at the manufacturer. Some parts will be carried out by the manufacturer such as:

- isolation test
- voltage test

and the rest will be done by ESS such as:

- checking lay out labelling and electrical connection
- hardware and firmware tests by correct LED blinking and forced signals

All conditions, procedures, acceptance criteria and documentation shall be according to [6]. ESS Guideline for FAT and SAT shall be followed [9] and FAT document template [10] shall be used.

5.2.1. Planning

The FAT planning shall consist of

- Location, environment, tools and interfaces for testing
- Acceptance criteria for each test
- Procedures for corrective actions if failure on test

The FAT is completed when the result is documented based on [7] and accepted by the TSS.

5.3. FIT

The FIT verifies that the TSS equipment approved during FAT and the downloaded software are correctly integrated and can perform the specific functional requirements. It should be carried out according to [3].

The FIT is performed off the site in lab environment. The aim is to make sure that:

- the requirements in [4] are fulfilled on system level
- communication of the cabinets is well performed
- the system is ready for installation and commissioning

5.3.1. Planning

The FIT planning shall consist of

- Location, environment, tools and interfaces for testing
- Acceptance criteria for each test
- Procedures for corrective actions if failure on test

6. VALIDATION

Validation activities include:

- **Site Acceptance Test (SAT):**
- **Site Integration Test (SIT):**

6.1. SAT

This chapter refers to chapter 15 in [2]. The SAT validates that the TSS fulfills the functional and system requirements in its operational environment. It should be carried out according to [9].

This test shall be done at the ESS with the TSS cabinets installed in their operational environment. It is based on hardware and software that have passed previous tests, and it is performed before the integration of the TSS to the interfacing systems.

All conditions, procedures, acceptance criteria and documentation shall be according to [6]. ESS Guideline for FAT and SAT shall follow [9]. SAT document template [8] shall be used.

It may be unnecessary to repeat software testing in this validation phase. The decision shall be based on

- overall test planning
- maturity of verification during FAT
- if identical software version as FAT

6.1.1. Planning

The SAT planning shall consist of

- Location, environment, tools and interfaces for testing
- Acceptance criteria for each test
- Procedures for corrective actions if failure on test

The SAT is completed when the result is documented based on [7] and accepted by the TSS.

6.2. SIT

The SIT validates that the TSS equipment approved during SAT and the interfaced systems are correctly integrated and fulfill the functional and system requirements in their operational environment. It should be carried out according to [3].

The interfaced systems are listed below. Details of the interfaces can be found in the related ICD-Rs.

- Conventional facility: rooms and infrastructure
- Ion Source: interface to ion source auxiliary electrical supply, shut-down timing
- RFQ: interface to RFQ auxiliary electrical supply, shut-down timing
- Dipole magnet: interface to dipole magnet auxiliary electrical supply
- TSS Monitoring System (TSS MS): graphical display on operator work station, data archiving, communication from TSS Gateway PLC to EPICS
- Target He Cooling: sensors reading correct values of the process
- Monolith Vessel: sensors reading correct values of the process
- Target Wheel: sensors reading correct values of the process
- Machine Protection: communication
- Target Electrical: Auxiliary electrical supply
- Acc. Electrical: Auxiliary electrical supply
- MCR Electrical: Auxiliary electrical supply

The infrastructure and the environment shall be ready for this test. However, TSS has no impact on environment nor infrastructure.

Information regarding schedule and resources and their allocation is provided in the Primavera P6 Plan.

6.2.1. Planning

The SIT planning shall consist of

- Location, environment, tools and interfaces for testing
- Acceptance criteria for each test
- Procedures for corrective actions if failure on test

The SIT is completed when the result is documented based on [7] and accepted by the TSS.

7. ROLES AND RESPONSIBILITIES

The Target Controls and Safety group within the Target division is responsible to develop, install, commission and validate the TSS.

Before each verification/validation activity, relevant roles and responsibilities shall be pointed out, see below:

- Requirements Test Specification — Validator (VAL)
- Verification and Testing — Verifier (VER)
- Software/Hardware Integration — Designer (DES)
- Validation — Validator (VAL)

8. GLOSSARY

Term	Definition
FAT	Factory Acceptance Test
SAT	Site Acceptance Test
FIT	Factory integration test
SIT	Site integration test

9. REFERENCES

[1] ESS-0037596, Concept specification of Target Station Safety System
[2] IEC 61511-1:2016, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements
[3] SS-EN62381, Automation systems in the process industry-Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)
[4] ESS-0002776, TSS system requirements specification
[5] ESS-0117128, ESS handbook for system verification
[6] ESS-0015433, ESS Rules for electrical design
[7] ESS-0145268, Target Safety System Configuration Management plan
[8] ESS-0113711, Site Acceptance Test (SAT)
[9] ESS-0094204, ESS Guideline for FAT and SAT
[10] ESS-0113710, Factory Acceptance Test (FAT)

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	Approved as baseline before PDR	Mikael Olsson	2016-02-05
2	Approved for the TSS CDR2	Atefeh Sadeghzadeh	2019-04-02