# Factory Acceptance Testing
## *Guideline*

**Comments on this report are gratefully received by**
**Johan Hedberg**
**at SP Swedish National Testing and Research Institute**
**mailto:johan.hedberg@sp.se**

## Summary

According to the standard IEC 61551 the factory acceptance test (FAT) is not a requirement but is necessary to carry out if the application software of the logic solver is complex or if the architecture is using redundant arrangements. The general questions in the planning phase of the FAT concern the tests to be performed and how to deal with the tests. The FAT is a practical way to test and verify the correct operation of the safety instrumented system.

Table of contents

1. Introduction ..... 4
1.1. Purpose ..... 4
1.2. References ..... 4
1.3. Scope ..... 4
2. Definitions and abbreviations ..... 4
3. Factory acceptance test (FAT) ..... 6
3.1. Planning ..... 6
3.2. Test activities ..... 7
3.3. Test result ..... 8
3.4. Checklist ..... 9
FAT specification form ..... 11

# 1. Introduction

## 1.1. Purpose

The aim of this document is to try to describe the requirements concerning factory acceptance testing, FAT, according to the standard IEC 61511. The FAT is a customized testing procedure for different types of systems and the tests are executed before the final installation at the plant. The FAT is not a requirement but recommended to be carried out, according to the standard IEC 61511, if the application software of the logic solver is fairly complex or if the architecture of the safety instrumented system is using redundant arrangements. In many cases it is difficult to predict the correct operation of the safety instrumented system or consequences due to failures in some parts of the safety instrumented system. For that reason the FAT is a valuable check of the safety issues. The test cases are selected during the planning phase in order to test the safety measures as far as possible.

## 1.2. References

[1] IEC 61511-1 Functional safety- Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements

[2] IEC 61511-2 Functional safety- Safety instrumented systems for the process industry sector- Part 2: Guidelines for the application of IEC 61511-1

[3] IEC 61511-3 Functional safety- Safety instrumented systems for the process industry sector- Part 3: Guidance for the determination of the required safety integrity level

## 1.3. Scope

This document covers the parts in IEC 61511 concerning the FAT. The FAT can be used as an integration test or during validation of the safety instrumented system.

# 2. Definitions and abbreviations

**basic process control system (BPCS)**
system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1 (3.2.3 in IEC 61511-1)

**fault**
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (3.2.21 in IEC 61511-1)

**failure**
termination of the ability of a functional unit to perform a required function (3.2.20 in IEC 61511-1)

**error**
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition (3.2.18 in IEC 61511-1)

**hazard**

potential source of harm (3.2.31 in IEC 61511-1)

**hazardous situation**
circumstance in which a person is exposed to hazard(s) (3.1.3 in IEC 61508-4)

**hazardous event**
hazardous situation which results in harm (3.1.4 in IEC 61508-4)

**harm**
physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment (3.2.30 in IEC 61511-1)

**instrument**
apparatus used in performing an action (typically found in instrumented systems) (3.2.38 in IEC 61511-1)
NOTE Instrumented systems in the process sector are typically composed of sensors (for example, pressure, flow, temperature transmitters), logic solvers or control systems (for example, programmable controllers, distributed control systems), and final elements (for example, control valves). In special cases, instrumented systems can be safety instrumented systems (see 3.2.72 in IEC 61511-1).

**process risk**
risk arising from the process conditions caused by abnormal events (including BPCS malfunction)
NOTE 1 The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety). (3.2.54 in IEC 61511-1)

**safety instrumented function (SIF)**
safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function (3.2.71 in IEC 61511-1)

# 3. Factory acceptance test (FAT)

The main objective of the FAT is to test the safety instrumented system (logic solver and associated software together). The tests are normally executed during the final part of the design and engineering phase before the final installation at the plant. The FAT is a customized procedure of checking the safety instrumented system and the safety instrumented functions according to the safety requirements specification, see figure 1.

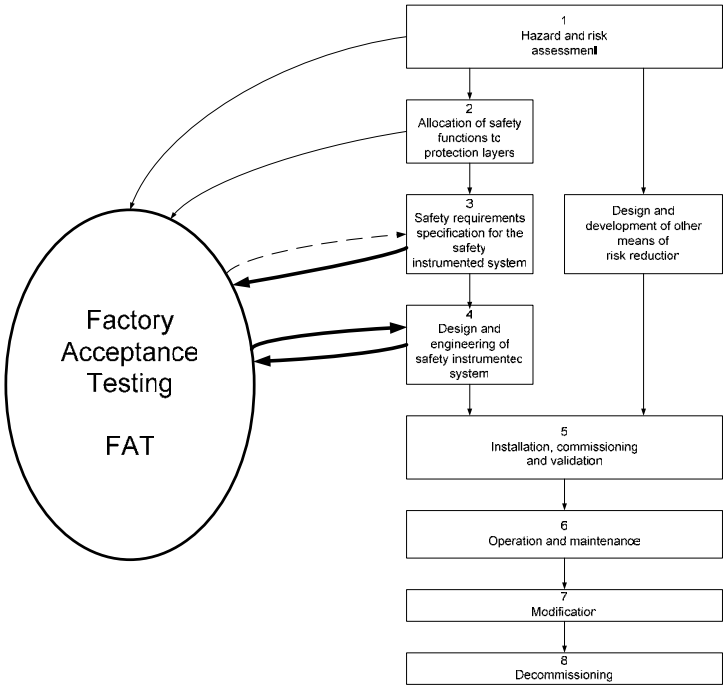


Figure 1. Factory acceptance testing

The FAT includes appropriate general testing procedures for verification of the correct operation of the safety instrumented system. Since the testing activities are general methods the FAT is applicable to programmable or non programmable safety instrumented systems. The most important part of the FAT addresses specification of the test cases i.e. clear description of the test cases, well structured test procedures and relevant test cases.

## 3.1. Planning

The planning presents a set op of the appropriate tests to be carried out and who is responsible for developing the test cases. Appropriate levels of competence and independence of assessors are required. The realization of tests shall be described as well as the personnel responsible to carry out the test. The test protocol is developed during the planning and furthermore who is responsible to attest the test protocol.

The procedures to carry out the FAT shall be well defined and documented in a proper way. Each test procedure shall be described in a logical sequence i.e. how to test the application software and hardware. The needed competence for involved test personnel is described during the planning. It is recommended that personnel with experience suitable for the intended process application and safety instrumented system deals with the FAT planning. Experience form different areas such as process

design, hardware design, and software design will contribute the FAT planning with relevant test cases. The content of the FAT tests shall be appropriate for the intended safety instrumented system.

The planning includes procedures for corrective action in case of discovered failure during execution of the tests. The test planning shall also include the test criteria on which the completion of the tests shall be judged. The safety instrumented systems physical location and the function dependency of other systems or interfaces are issues that are specified during the planning phase.

The configuration of the logic solver is needed during the planning in order to prepare the tests.

In order to develop integration tests it may be required to contact the supplier of the logic solver or other relevant suppliers for the included units in the safety instrumented system.

## 3.2. Test activities

The FAT is normally performed at the manufacturers work shop. The manufacturer checks that the safety instrumented system works as intended and according to the requirements stated in the safety requirements specification, SRS. During the FAT the manufacturer checks as far as possible that:

- the used equipment are according to the specification e.g. compatible HW and SW versions
- the used equipment are installed according to manufacturer's specification
- the inputs and the outputs are connected according to the drawings
- the calibration of the equipment are correct
- the trip points operate according to the requirements in the SRS
- the logic solver and associated software operate according to the requirements in the SRS
- the outputs and their actions behave according to the SRS
- the reset functions operate according to the SRS
- the alarms operate according to the SRS
- the operator functions operate according to the SRS
- the bypass functions operate according to the SRS
- the manual shutdown functions operate according to the SRS
- the diagnostic alarm functions operate according to the SRS

The outputs from the safety instrumented function are examined during different test cases e.g. simulation of inputs in order to verify that the safety instrumented functions meet the requirements in the safety requirements specification.

If the FAT reveals weaknesses in the design and engineering phase or in the safety requirements specification phase these phases have to be modified according to the result of the FAT. In order to check the modifications the safety instrumented system has to be re- tested.

The FAT should take place on a defined version of the logic solver and the configuration of the logic solver has to be specified in order to establish relevant test cases.

In order to perform the tests the need of tools is described and also a description of the test environment.

Any modifications or change should be subject to a safety analysis in order to determine the extent of the impact on each safety instrumented function and the extent of re-test should be defined and implemented.

## 3.3. Test result

All the test cases of the FAT shall be described in the documentation and furthermore if the objectives and criteria of the tests have been met or not. Discovered failures during the test are documented and the reasons for the failures are also documented supported by necessary actions to correct the failures.

If there are modifications of the safety instrumented system it is necessary to carry out a safety analysis in order to determine if the safety is affected and if re- testing is necessary.

## 3.4. Checklist

FAT checklist

| | Yes/No | Comments |
|---|---|---|
| Is the FAT necessary? | | |
| Is the FAT planning performed? | | |
| Are personal skills considered? | | |
| Are all test cases described? | | |
| Are corrective actions in case of failures considered? | | |
| Are the expected test results for each test case described? | | |
| Are the procedures to carry out the FAT well defined and documented in a proper way? | | |
| Are the CE requirements fulfilled? | | |
| Are all HW and SW parts delivered according to the specification? | | |
| Are all the safety instrumented functions identified? | | |
| Have skills and competence resources been considered of the involved personnel? | | |
| Are all modes of operation identified? | | |
| Are the safe states identified? | | |
| Are process inputs, trip points and normal operating range identified? | | |
| Are all equipment installed according to manufacturer's specification? | | |

| | | |
|---|---|---|
| Are process inputs identified and their trip points tested, according to the SRS? | | |
| Are process outputs identified and their actions tested according to the SRS? | | |
| Are relationships between inputs and outputs tested and behave according to the SRS? | | |
| Are computations by the SIS performed correct? | | |
| Is the response time tested and according to the SRS? | | |
| Are reset functions tested and behave according to the SRS? | | |
| Are operator functions tested and behave according to the SRS? | | |
| Are alarms tested and behave according to the SRS? | | |
| Is degraded mode of operation tested e.g. missing air supply, missing electrical supply? | | |
| Are bypass functions working properly and according to the SRS? | | |
| Is manual shutdown working properly and according to the SRS? | | |
| Are diagnostic alarm functions working properly and according to the SRS? | | |

| FAT ID: | | SIS name: | |
|---|---|---|---|

# FAT specification form

| A. Document issued for: |
|---|
| **Project:** |
| **Company:** |
| **Process:** |
| **Plant / Site:** |
| **SIS Safety Instrumented System:** |
| **SIF Safety Instrumented Function(s):** |

| FAT ID: | | **SIS name:** | |
|---|---|---|---|

B. Document sources:

| Safety Requirements Specification: | Organization: | Date/version: |
|---|---|---|
| | | |

| Risk assessment by: | Organization: | Date/version: |
|---|---|---|
| | | |

C. Related documents:

| **Type:** | Document ID: | Rev: | Comments: |
|---|---|---|---|
| | | | |

| FAT ID: | | SIS name: | |
|---|---|---|---|

**Test case no (SIF id and nr):**

| 1A General information for test cases | |
|---|---|
| **The test case concerns SIF (name):** | |
| **Name of the test case:** | |
| **The objectives and criteria of the test:** | |
| **The test case concerns SIF:** | **Physical location (process part)** |
| **Developer of the test case:**<br>**(Name and Company)** | |
| **Responsible to carry ot the test case:**<br>**(Name and Company)** | |
| **Responsible to attest the test protocol:**<br>**(Name and Company)** | |
| **Test environment (used test equipment):** | |
| **Description of configuration of the logic solver:**<br>Including components ( e.g. type, brand) | |
| **Software:** | **Version number** |
| **HW parts** | **Version number** |

| FAT ID: | | SIS name: | |
|---|---|---|---|

**Test case no (SIF id and nr):**

| 1B. Logical description |
|---|
| **Logical description of the test cases:** |

| FAT ID: | | SIS name: | |
|---|---|---|---|

**Test case no (SIF id and nr):**

| 1C. Expected result |
|---|
| **Description:** |

| 1D. Corrective action on failure of the test |
|---|
| **Description:** |

| FAT ID: | | SIS name: | |
|---|---|---|---|
| **Test case no (SIF id and nr):** | | | |

| 1E. FAT Result | |
|---|---|
| **The test criteria have been met or not (Yes/No):** | **Date and signature:** |
| **Description of the test result:** | **Date and signature** |
| **Remaining actions:** | **Date and signature** |

Date: .....

Name.....
(Responsible to attest the test protocol)

Company.....