Guideline
Installation and commissioning
Validation
Operation and maintenance
Modification
Decommissioning

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

Summary

Installation and commissioning of a safety instrumented system needs to be tested, verified and validated before the hazards are present. In order to be sure that the safety integrity is according to the requirements, relevant activities and producers shall be followed.

During the operation and maintenance of the plant the safety integrity shall be maintained by regular inspections and proof tests. The operators or other involved personnel need training and procedures to follow.

The modification of a safety relevant part of a system shall be performed in a proper manner (procedures and necessary activities) in order to ensure that the functional safety for any safety instrumented function is appropriate both during and after the modification and retrofit phase.

The decommissioning activity ensures that the functional safety of the safety instrumented system is appropriate in the circumstances during and after the activities of decommissioning.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

TABLE OF CONTENTS

1 Introduction

After the installation and commissioning of the safety instrumented system the validation shall be performed in order to be sure that everything works according to the requirements given by the safety requirements specification.

The operation and maintenance activities shall follow procedures in order to eliminate the possible risks with the actual process. The safety instrumented system shall regularly be inspected and proof tested according to the integrity requirements.

The modification activities shall follow procedures and relevant activities shall be performed in order to maintain the safety integrity during modification and retrofit phase.

Decommissioning shall be authorized and the work shall follow procedures relevant activities in order to maintain the safety integrity during decommissioning.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

1.1 Purpose

The purpose with the safety lifecycle deified by IEC 61511 is that the functional safety is maintained during every phase. Since the hazards and hazardous events are different depending on the actual plant the relevant requirement has to be decided during the planning. In order to fulfil the requirements the relevant procedures shall be followed for each phase and the required activities during each phase are decided during the planning.

The aim with this document is to try to describe the requirements concerning installation and commissioning, validation, operation and maintenance, modification and decommissioning phases.

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

The scope is the different actives and procedures necessary for the installation and commissioning, validation, operation and maintenance, modification and decommissioning phases of a 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, IEC 61511-1)

final element
part of a safety instrumented system which implements the physical action necessary to achieve a safe state (3.2.24 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, IEC 61511-1)

safety instrumented system (SIS)
instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) (3.2.72 IEC 61511-1)

sensor
device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches) (3.2.80, IEC 61511-1)

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 (3.2.91, IEC 61511-1)

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 (3.2.92 IEC 61511-1)

3 Installation and commissioning

The objectives for the SIS installation and commissioning are to install the safety instrumented system according to the specifications and drawings. Furthermore the safety instrumented system shall be ready for the final system validation.

The scope for the installation phase covers all field instruments, power supplies, valves, cabling and hardware used in control room or equipment room. The installation activities coves the safety instrumented system and the basic process control system. There are no specific requirements for site installation beyond the need to ensure that the safety instrumented system is not impaired by other non safety related systems. In order to prevent influence on the SIS from other non safety relevant systems ensure e.g. the following:

- Segregation of SIS and BPCS equipment
- Segregation between signal and control loops
- Separate cabling systems
- Identification of safety critical items e.g. specific colour for junction boxes and cables
- Provision of on- line proof testing
- Correct sensors are installed and calibrated

The main purpose of segregation is to minimize the risk of common cause failures.

The planning involves all activities for installation and commissioning and when these activities shall take place. The responsible persons, departments and organisations shall be identified. The procedures for installation and commissioning shall be identified e.g. measures and techniques.

3.1 Planning

The objective is to develop an overall installation plan and the overall commissioning plan so that the safety- related systems and external risk reduction facilities are installed and commissioned in a controlled manner to ensure that the required functional safety is achieved.

3.2 Activities

The installation phase needs to be verified by using physical inspection and functional inspection. The main purpose with the physical inspection is to ensure that the installation is according to the drawings and specifications for each field device.

The functional inspection aims to verify that included sensors and final elements behave according to the safety requirements specification.

When the physical inspection and functional inspection are executed successfully the installed system is ready for pre- start-up acceptance tests. These tests provide a full functional test before introduction of hazardous materials.

3.3 Results

Appropriate records of the physical inspection need to be produced in order to verify that the installation is correct performed.

Appropriate records of the functional inspection of the safety instrumented system shall be recorded. For each sensor witness and sign off the test result for:

- Process simulation
- Calibrated range
- Trip set point
- Alarm set point
- Warning indicators
- Overrides
- Bypass functions affecting security functions

For each final element witness and sign off the test result for:

- Trip actions
- Response time
- Feedback functions e.g. position
- Trip functions
- Interlock functions
- Loss of power or air
- Latch functions
- Reset functions
- Output forcing

The pre- start-up acceptance test is a compete test of the SIS system and includes

- Trip set points
- Shut down sequence
- SIS components are according to requirements given by SRS
- SIS communication to external equipment
- Accuracy of computations
- Accuracy of calibration equipment are according to required accuracy and resolution
- Alarm functions
- Reset functions
- Bypass functions
- Display information are according to SRS
- SIS documentation is consistent with install and operator procedures
- Proof test intervals are according to

The pre- start-up acceptance test shall be recorded properly.

4 Validation

The objective of the SIS safety validation is to validate that the installed and commissioned safety instrumented system and its associated safety instrumented functions achieve the requirements as stated in the safety requirements specification.

The procedures and techniques used for validation shall be defied e.g simulation activities, calibration procedures, hardware tests, software tests and when these activities shall take place.

The responsible persons, departments and organizations shall be defined and the level of independence.

Any references used for the validation activities shall be defined e.g cause and effect chart.

4.1 Planning

The objective is to develop the overall safety validation plan to enable the validation of the total combination of safety- related systems and external risk reduction facilities to take place. The planning shall define all activities required for validation (hardware and software) and when these activities shall take place.

The validation planning for the safety application software deals with identification of the safety related software, information on the technical strategy to be used, conforming activities for the safety related software used in each safety instrumented function, the required environment and test equipment, the pass/ fall criteria and the policies and procedures for evaluation the results of the validation.

4.2 Activities

All necessary activities shall be included in the validation and the different modes of operation for the safety instrumented shall be tested (normal and abnormal conditions): The validation activities concern the different modes of operation for the process e.g. preparation for use, start-up, re-setting, shutdown, maintenance and reasonable foreseen abnormal conditions. Attention for the special features for the safety instrumented system shall be performed for e.g.:

- Start- up overrides
- Bypass functions
- Manual shutdown
- Diagnostic alarm functions

Abnormal conditions for the process instrumentation e.g. degraded mode of operation, loss off power, (electrical power, hydraulics, air) shall be conformed so that the safety instrumented system performs as required. When the power is restored the safety instrumented system shall return to desired state.

The software validation shall confirm that the software is correctly implemented and that the software is not affected by fault conditions and degraded mode of operation.

Confirmation shall state that:

- The EMC requirements are fulfilled for the installed system.
- The basic process control system or any other system does not affect the proper operation of the safety instrumented system.
- The sensors, logic solver, and final elements perform in accordance with the safety requirements specification.
- The documentation for the safety instrumented system is consistent with the installed system.
- The operator interface (display, annunciation) are proper and according to requirements
- Computations performed by the safety instrumented system are correct
- Invalid process parameters do not affect the safety instrumented system.
- The different types of operating modes are tested
- The proof test intervals are according to the required SIL levels and documented in the maintenance procedures

After a successfully validation activity and before the hazards are being present, the SIS and BPCS system shall be ready for start up. The following activities have to be carried out:

- All bypass functions (forces, disabled alarms etc) shall be removed.
- All process devices (valves etc) shall be according to start up requirements
- All manual forces shall be removed
- All test materials shall

4.3 Results

The final outcome shall give appropriate information of the results of the validation. The outcome provides:

- Applied requirements
- The version of the validation plan.
- The tested safety instrumented functions
- Results of each test
- The version of the test plan
- The version of SIS hardware
- The version of SIS software
- The analyses made
- The final result
- Discrepancy between expected and actual results

If discrepancies were found the decision taken to continue the validation or a necessary modification request shall be provided in the outcome of the validation. If modifications are required the modification issues returns to an earlier design part of the safety life cycle for the safety instrumented system.

5 Operation and maintenance

When the safety instrumented system is put in to service it is necessary to ensure that the required SIL level of each safety instrumented function (SIF) is maintained during operation and maintenance. It is also important to operate and maintain the safety instrumented system (SIS) in order to ensure that the functional safety is maintained.

5.1 Planning

The objective is to develop an overall operation and maintenance plan to ensure that the functional safety of safety- related systems and external risk reduction facilities are maintained during operation and maintenance.

5.2 Activities

The operation and maintenance procedures shall be developed and described in order to maintain the functional safety for the SIS. The procedures to be written explain safe and correct methods and the limits of safe operation (trip points) and consequences. The procedures explain the safety instrumented system (how it works) and the correct operator response. The operating procedures include:

- The actions and constraint that are necessary to prevent an unsafe state or reduce the consequences
- Correct use of bypasses, resets, permissive etc.

The procedures include the information needed to be maintained on system failure or demand rates on the safety instrumented system and the results of audits and tests. The safety instrumented system shall be periodically inspected in order to detect unauthorized changes or no observable deterioration.

The proof test activities shall be described for each safety instrumented function and tested according to the SIL requirement (the maximum interval between two proof tests). The proof test activities shall be described in a clear way (every step) in order to prevent accidents and to be sure that the safety instrumented function is tested according to the requirements. The entire safety instrumented function shall be tested in order to reveal undetected failures. Identified deficiencies during the proof test shall be repaired in a safe way. Any modification of the application logic require full proof testing exception is allowable if appropriate measures are carried out to ensure that the modifications are correctly implemented. The user shall maintain records showing that proof tests and inspections were competed as required including:

- Name of the persons performing the tests
- Dates of the tests
- Description of the tests
- Identification of the tested items
- The result of the tests, pass or fail
- Remaining issues to be solved

The maintenance procedure for the safety instrumented system includes:

- Fault diagnostic
- Repair
- Revalidation
- Maintenance reporting
- Tracking maintenance
- Reporting failures
- Analyses of systematic failures

The operators shall be trained for the actual SIS and they shall understand the following aspects:

- The hazards that are protected by the SIS
- The SIS functions
- The trip points and the action taken by the SIS
- The manual shut down systems
- The manual start up system
- When to use manual systems
- The operation of bypasses
- When it is allowed to use bypasses
- The alarms and corresponding action

Maintenance personnel shall be trained to sustain the full functional performance of the safety instrumented system to its target safety integrity level.

Discovered discrepancies between the excepted behaviour of the safety instrumented system and the actual behaviour shall be analysed and be modified in order to maintain the target safety integrity level. In order to detect discrepancies it is important to monitor failures, the cause of the demands, the cause false trips and the action taken following a demand.

In order to be sure that the operation and maintenance procedures are correct specified these procedures may require tests on the safety instrumented system and functional safety audits.

5.3 Results

The operation and maintenance actives concerns:

- Planning activities
- Operator training
- Operator activities
- Maintenance activities
- Regular proof tests according to SIL reqirements for each safety instrumented function
- Regular inspections
- Maintain records showing that proof test and regular inspections were competed according to requirements

For above mentioned activities relevant documentation, procedures and instructions shall be provided.

6 Modification

The objective for modification of safety instrumented system is to ensure that the functional safety for any safety instrumented function is appropriate both during and after the modification and retrofit phase. This requires properly planning, reviews and approval prior to make the change and to ensure that the safety integrity level is maintained. For functional safety systems the risk is that safety instrumented system can be affected due to changes, therefore it is important that stringent procedures are followed.

6.1 Planning

The planning deals with the relevant activities to be done in order to ensure that the modification is not affecting the safety integrity for the safety instrumented system.

6.2 Activities

The modification activity requires authorization. In order to carry out the modification of a safety instrumented system procedures shall be developed. These procedures concerns:

- The work to be done
- Authorization
- Risk analysis (hazards affected or new hazards)
- Analysis of the impact on safety due to the modification
- Control of the changes
- The necessary tests for modified part and non modified parts
- Information of the changes

The involved personnel needs to be properly qualified and trained to manage the modification.

6.3 Results

Information of the changes shall be maintained which includes the reason for the modification, a description of the modification and the affected hazards or new hazards. An analysis shall be made showing the impact on safety for the modification activity concerning the safety instrumented system. Further on the result includes information on:

- Required approvals for the modification activity
- The tests used to verify the modification and that the modified safety instrumented system behaves according to the requirements
- The tests used to verify impact on not modified parts of the safety instrumented system
- The involved personnel

7 Decommissioning

The objective is to ensure that the functional safety of the safety instrumented system is appropriate in the circumstances during and after the activities of decommissioning.

7.1 Planning

The planning of the decommissioning phase deals with the required procedures needed to be developed.

7.2 Activities

The decommissioning activities include procedures for authorization and controlling the changes. The activities concerns:

- The work to be done (defined in a clear and proper way)
- The identified hazards that may are affected
- An update of the risk analysis
- The need of re- take earlier phases of the safety- life cycle
- The functional safety aspects during the decommissioning

7.3 Results

The result of the activities is used for re- verification and re- validation of the safety instrumented system. The activities during the decommissioning shall be recorded.