**SIS life-cycle: Overview of typical activities and documents**

This document provides an overview of typical Functional Safety activities and documents based on IEC 61511:2017. The overview can be used to manage Functional Safety projects.

|  |  |  |
| --- | --- | --- |
| 1. **Set up functional safety management plan** | | *status* |
| *Responsible* | Project/plant manager | 🗸 |
| *Objective* | To manage the development, realisation and maintenance of a SIS | 🗸 |
| *Basis* | Project definition, basis for design, Process Flow Schemes, P&IDs | 🗴 |
| *Activities:*  *Personnel* | Determine which departments / personnel need to be involved during the relevant SIS lifecycle phases |  |
| Determine competence requirements for the key personnel |  |
| Check competence of key personnel |  |
| *Planning* | Determine the applicable SIS life-cycle phases and the relevant activities and documents (*this overview may help*) |  |
| Make a realistic planning when activities should be performed |  |
| *Development process* | A verification system should be set up in order to guarantee the quality of activities and documents  All documents shall be checked and approved |  |
| *Deliverables* | Functional safety management plan |  |
| Life-cycle planning |  |
| *Reference: IEC 61511 clauses 5, 6 and 7* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Hazard and risk assessment** | | *status* |
| *Responsible* | Process safety engineer / Process engineer |  |
| *Objective* | To identify all process hazards and to determine associated risks |  |
| *Basis* | P&IDs and other relevant conceptual documents |  |
| *Activities* | Determine scope of work |  |
| Organise HAZOP and risk assessment brainstorm sessions |  |
| Determine team composition for the brainstorm sessions |  |
| Check if the proposed HAZOP chairman is well-experienced |  |
| Ensure that appropriate HAZOP and risk assessment methodologies will be used |  |
| *Deliverable* | HAZOP and Risk Assessment report |  |
| *Reference: IEC 61511 clause 8* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Allocation of safety functions to protection layers** | | *status* |
| *Responsible* | Process engineer / Process safety engineer |  |
| *Objective* | To select appropriate risk reducing measures |  |
| *Basis* | HAZOP and Risk Assessment report and P&IDs |  |
| *Activities* | Inherently safe design is preferred  Mechanical safeguards may be selected as well as instrumental safeguards or other means of risk reduction  Determine the instrumental safeguards (SIFs) and associated SIL |  |
| *Deliverable* | Allocation report (might be an addendum of the HAZOP+RA report) |  |
| *Reference: IEC 61511 clause 9* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Safety Requirements Specifications (SRS)** | | *status* |
| *Responsible* | Process safety engineer |  |
| *Objective* | To specify the SIFs to be able to design these SIFs. |  |
| *Basis* | Allocation report, HAZOP and risk assessment report, P&IDs |  |
| *Activities* | Define all SIFs; sensors, logic solver function, final elements, overrides (if any), reset functions, Process Safety Times, if valves should be tight shut-off, required risk reduction factor (or PFD) |  |
| A SRS is a multidisciplinary document. It must be approved by the involved disciplines |  |
| Make Cause & Effect diagrams to be used by the FLD designers, during verification / validation and Operations |  |
| *Deliverables* | Detailed SRSs |  |
| Cause & Effects diagram(s) |  |
| *Reference: IEC 61511 clause 10* | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Functional Safety Assessment stage 1 (FSA 1)** | | *status* | |
| *Responsible* | Independent competent engineer | |  |
| *Objective* | To ensure that the SIS life-cycle activities up to and including the SRS have been performed correctly  Note: The SRS is a critical document, it will be used for the design of the SIFs and it will be used as basis for the verification / validation | |  |
| *Basis* | SRSs, P&IDs, HAZOP and risk assessment report, allocation report | |  |
| *Activities* | Verification if involved personnel are competent | |  |
| Verification if the SRSs are correct and complete | |  |
| Verification if the Cause & Effects diagrams are correct | |  |
| *Deliverable* | FSA 1 report | |  |
| *Reference: IEC 61511 clause 5.2.6.1* | | | |

|  |  |  |
| --- | --- | --- |
| 1. **Design of the SIS** | | *status* |
| *Responsible* | Instrumentation engineer |  |
| *Objective* | To develop the detailed design of the SIS |  |
| *Basis* | SRS and P&IDs |  |
| Narratives, company / project terms of reference, FSA-1 report |  |
| *Activities* | Specify all instruments, systems and auxiliaries to be purchased |  |
| Design the wiring / cabling, power supply, instr. air provisions, etc. |  |
| Design the human-machine interfaces |  |
| Develop the Application Program |  |
| Perform a SIS security risk assessment |  |
| Perform audits |  |
| Verify if the SIF design comply with IEC 61511 / 61508 |  |
| *Typical design deliverables* | Specification / requisition of the SIS logic solver |  |
| SIS Instruments data sheets |  |
| Specification / requisition of the SIS instruments |  |
| SIS auxiliary cabinets configuration |  |
| Specification / requisition of the SIS auxiliary cabinets |  |
| Specification / requisitions of SIS valves / actuators / solenoid valves |  |
| SIS Functional Logic Diagrams |  |
| SIS Application Program |  |
| SIS Application Program verification report |  |
| Human-machine interfaces for Operations and Maintenance |  |
| Wiring diagrams |  |
| Lay out drawings |  |
| SIS Loop diagrams |  |
| Supporting provisions, tracing and insulation |  |
| *Typical other deliverables* | SIS security risk assessment report |  |
| SIL design verification report |  |
| Vendors audit reports. Reviews to be performed to ensure that the vendors functional safety management systems are in place |  |
| SIFs test procedures |  |
| Loop test procedures |  |
| FAT procedures |  |
| SIS maintenance management database |  |
| SIS installation plan |  |
| SIS validation procedures |  |
| Evaluation forms of suppliers quotations / documents / safety manuals |  |
| Spare parts list |  |
| *Reference: IEC 61511 clauses 11 and 12* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Factory Acceptance Tests (FATs)** | | *status* |
| *Responsible* | Instrumentation engineer |  |
| *Objective* | To verify if systems / cabinets are realised correctly |  |
| *Basis* | SRS and P&IDs, FAT procedures, Design documents, relevant specification / requisition, vendor documents (e.g. safety manuals), vendor audit report |  |
| *Activities* | Organise FATs, determine participants, vendor to make test provisions |  |
| Perform FATs |  |
| Verify the Application Program in the safety PLC |  |
| *Deliverables* | FAT reports |  |
| *Reference: IEC 61511 clause 13* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Functional Safety Assessment stage 2 (FSA 2)** | | *status* |
| *Responsible* | Competent independent engineer |  |
| *Objective* | To ensure that the activities of the SIS life-cycle phases ‘Design of the SIS’ and ‘FATs’ have been performed correctly |  |
| *Basis* | SRS and P&IDs, Design documents, FAT reports, specifications / requisitions and vendor documents |  |
| *Activities* | Verification if involved personnel are competent |  |
| Verification if the recommendations of FSA-1 are implemented |  |
| Verification of design documents |  |
| Verification of the Application Program documents |  |
| Verification if the FAT recommendations are implemented |  |
| *Deliverable* | FSA 2 report |  |
| *Reference: IEC 61511 clause 5.2.6.1* | | |

|  |  |  |
| --- | --- | --- |
| 1. **SIS installation and commissioning** | | *status* |
| *Responsible* | Instrumentation engineer |  |
| *Objectives* | To realise and pre-test the SIS |  |
| *Basis* | Installation plan, design documents, vendor documents, FAT reports, FSA 2 report, Loop test procedures |  |
| *Activities* | Installation of the SIS |  |
| Commissioning of the SIS so that it is ready for final system validation. |  |
| *Deliverables* | As built marked-up design documents |  |
| Records of the commissioning of the SIS |  |
| *Reference: IEC 61511 clause 14* | | |

|  |  |  |
| --- | --- | --- |
| 1. **SIS safety validation** | | *status* |
| *Responsible* | Instrumentation engineer |  |
| *Objective* | To validate that the installed and commissioned SIS and its associated SIFs achieve the requirements as stated in the SRS |  |
| *Basis* | SRS’s, proof test procedures, validation procedures, design documents, vendor documents, FAT reports |  |
| *Activities* | Perform inspections and tests |  |
| *Deliverables* | Validation report |  |
| Update of the SIS maintenance management database with the test results |  |
| *Reference: IEC 61511 clause 15* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Functional Safety Assessment 3 (FSA 3) – SIL Field validation** | | *status* |
| *Responsible* | Competent independent engineer |  |
| *Objective* | To ensure that the activities of the SIS life-cycle phases ‘SIS installation and Commissioning’ and ‘SIS safety validation’ have been performed correctly |  |
| *Basis* | P&ID’s, SRS, design documents, vendor documents, validation procedures & validation results, proof test procedures and proof test results |  |
| *Activities* | Verification if involved personnel are competent |  |
| Verification if the proof tests / validations procedures are adequate |  |
| Verification if all tests / validations are performed, evaluation of the test results |  |
| Visual inspection of SIS instruments |  |
| *Deliverable* | FSA 3 report |  |
| *Reference: IEC 61511 clause 5.2.6.1* | | |

|  |  |  |
| --- | --- | --- |
| 1. **Operation and maintenance** | | *status* |
| *Responsible* | Project / Operations / Maintenance managers |  |
| *Objective* | To maintain the SIL of each SIF, to operate and maintain the SIS in a way that sustains the required safety functions |  |
| *Basis* | Validated SIS and Up-to-date SIS documents |  |
| *Activities* | Implement the recommendations of FSA 3 |  |
| Take care of awareness and competence of personnel |  |
| Organise operators training |  |
| Organise maintenance training |  |
| Perform periodical proof tests and visual inspections |  |
| Keep the maintenance management database up-to-date |  |
| Use approved procedures for bypassing elements of the SIF when needed |  |
| Perform preventive and breakdown maintenance of the SIS, e.g. periodical overhaul of valves by valve vendor and calibration of sensors |  |
| Take care of adequate spare parts and service contracts |  |
| *Reference: IEC 61511 clause 16* | | |

|  |  |
| --- | --- |
| **Abbreviations** | |
| *FAT* | Factory Acceptance Test |
| *FLD* | Functional Logic Diagrams |
| *FSA* | Functional Safety Assessment |
| *HAZOP* | HAZARD & Operability |
| *PFD* | Average Probability of Failure on Demand |
| *PLC* | Programmable Logic Controller |
| *P&ID* | Piping & Instrumentation Diagram |
| *RA* | Risk Assessment |
| *SIF* | Safety Instrumented Function |
| *SIL* | Safety Integrity Level |
| *SIS* | Safety Instrumented System |
| *SRS* | Safety Requirements Specification |
| *Reference: IEC 61511 clause 3* | |