|  |
| --- |
|  |
|  |
|  |
| Chess Controlled Core Word |
|  |

|  | Name | Role/Title |
| --- | --- | --- |
| Owner | Stuart Birch | Senior Engineer for Protection Systems Group, ICS |
| Author | Meike Rönn | Technical Documentation Specialist for Protection Systems Group, ICS |
| Reviewer | Denis Paulic | Deputy Group Leader for Protection and Safety Systems Group, ICS |
| Morteza Mansouri | Lead Integrator Engineer for Safety Critical Systems, ICS |
| Fan Ye | PSS Safety Engineer, Isograph Expert, Engineering Safety Consultants Limited, UK |
| Approver | Annika Nordt | Group Leader for Protection Systems Group, ICS |

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

1. Introduction 5

1.1. Purpose 5

1.2. Scope 5

2. PSS Safety Life-cycle 6

2.1. Life-cycle phases 7

2.1.1. Phase 1: Hazard and Risk Analysis 7

2.1.1.1. Objective 7

2.1.1.2. Inputs 7

2.1.1.3. Outputs 7

2.1.1.4. Tools and methods 7

2.1.1.5. Resources 7

2.1.2. Phase 2: Allocation of overall safety requirements to protection layers 8

2.1.2.1. Objective 8

2.1.2.2. Inputs 8

2.1.2.3. Outputs 8

2.1.2.4. Tools and methods 8

2.1.2.5. Resources 8

2.1.3. Phase 3: Safety requirements specifications for the safety instrumented systems 8

2.1.3.1. Objective 8

2.1.3.2. Inputs 8

2.1.3.3. Outputs 8

2.1.3.4. Tools and methods 9

2.1.3.5. Resources 9

2.1.4. Phase 4: Design and engineering of safety instrumented functions 9

2.1.4.1. Objectives 9

2.1.4.2. Inputs 9

2.1.4.3. Outputs 9

2.1.4.4. Tools and methods 9

2.1.4.5. Resources 10

2.1.5. Phase 5: Installation, commissioning and validation 10

2.1.5.1. Objectives 10

2.1.5.2. Inputs 10

2.1.5.3. Outputs 10

2.1.5.4. Tools and methods 10

2.1.5.5. Resources 10

2.1.6. Phase 6: Operation and maintenance 11

2.1.6.1. Objectives 11

2.1.6.2. Inputs 11

2.1.6.3. Outputs 11

2.1.6.4. Tools and methods 11

2.1.6.5. Resources 11

2.1.7. Phase 7: Modification 11

2.1.7.1. Objectives 11

2.1.7.2. Inputs 11

2.1.7.3. Outputs 11

2.1.7.4. Tools and methods 11

2.1.7.5. Resources 12

2.1.8. Phase 8: Decommissioning 12

2.1.8.1. Objectives 12

2.1.8.2. Inputs 12

2.1.8.3. Outputs 12

2.1.8.4. Tools and methods 12

2.1.8.5. Resources 12

2.1.9. Verification and Validation 12

2.1.9.1. Objectives 12

2.1.9.2. Inputs 12

2.1.9.3. Outputs 12

2.1.9.4. Tools and methods 12

2.1.9.5. Resources 13

2.1.10. Functional Safety Assessment (FSA) 13

2.1.10.1. Objectives 13

2.1.10.2. Inputs 13

2.1.10.3. Outputs 13

2.1.10.4. Tools and methods 13

2.1.10.5. Resources 13

3. Safety management 13

3.1. Documentation 13

3.2. Procedures 19

3.3. Roles and responsibilities 20

3.4. Functional safety assessment 20

4. Glossary 22

5. References 23

6. Appendix A: Hazard Register 24

7. Appendix B: SIL determination and verification 27

7.1. General Concepts 27

7.1.1. Risk reduction 27

7.1.2. Safety integrity level 27

7.1.3. Risk Targets 29

7.2. LOPA 29

7.2.1. LOPA for low demand SIFs 29

7.2.2. LOPA for high demand or continuous SIFs 30

7.2.3. Independent protection layers 31

7.3. Hardware reliability assessment 32

7.3.1. Probability of Failure on Demand 32

7.3.2. Failure rate, λ 33

7.3.2.1. Failure Modes 33

7.3.2.2. Diagnostic Testing 33

7.3.3. PFD and Mean Down Time 34

7.3.3.1. PFD for Detected Failures 34

7.3.3.2. PFD for Undetected Failures 35

7.3.3.3. PFD for Subsystem 35

7.3.3.4. PFH for Subsystem 35

7.3.4. Voting configuration 35

7.3.5. Common cause failure (CCF) 35

7.4. Architectural assessment methodology 36

7.4.1. Hardware fault tolerance (HFT) 36

7.4.2. Safe failure fraction (SFF) 36

7.4.3. IEC 61508 architectural constraint (Route 1H) 37

8. Appendix C: Applicable safety regulations 38

9. Document Revision history 39

list of tables

Table 1: Tools used in design and engineering of safety instrumented functions 9

Table 2: Documentation required during PSS0 development 14

Table 3: Documentation covering procedures 19

Table 4: Roles of the PSS team 20

Table 5. SIL Specified PFD 26

Table 6. HFT for Type A and Type B Components 35

Table 7: Swedish authority voltage hazard categories. 36

list of Figures

Figure 1: safety life-cycle phases for PSS development [1] 6

Figure 2: The Concept of Risk Reduction 25

# Introduction

## Purpose

This safety plan defines the life-cycle activities for Personnel Safety Systems 0 (PSS0), establishes how the steps in the life-cycle are accomplished and ensures that the required activities during each life-cycle phase are adequately planned. These activities include ensuring that safety requirements are achieved, ensuring proper installation and commissioning, ensuring safety integrity of the PSS0 after installation, and maintaining this integrity during operation. It also defines the roles and responsibilities related to the life-cycle activities.

It shall be updated as necessary throughout the entire life-cycle of the PSS0.

## Scope

This safety plan applies to the PSS0 developed by Personnel Safety Systems (PSS) within the ESS facility.

# PSS Safety Life-cycle

PSS0 development follows IEC 61511 [1], which is an international standard for functional safety. It concerns safety instrumented systems, primarily implemented using electrical/ electronic/ programmable electronic technologies. The standard is focused on systems implemented with commercially available components certified to functional safety standards, and addresses the application of safety instrumented systems.

The IEC 61511 [1] safety life-cycle followed for PSS0 development is given in Figure 1. The yellow boxes depict life-cycle phases, where the corresponding activities are performed and documented by the PSS team (see section 3.3). The green and blue boxes depict the life-cycle phases to be performed and documented by other parties and stakeholders in collaboration with the PSS team. This life-cycle is followed by ESS for the development of Personnel Safety Systems.

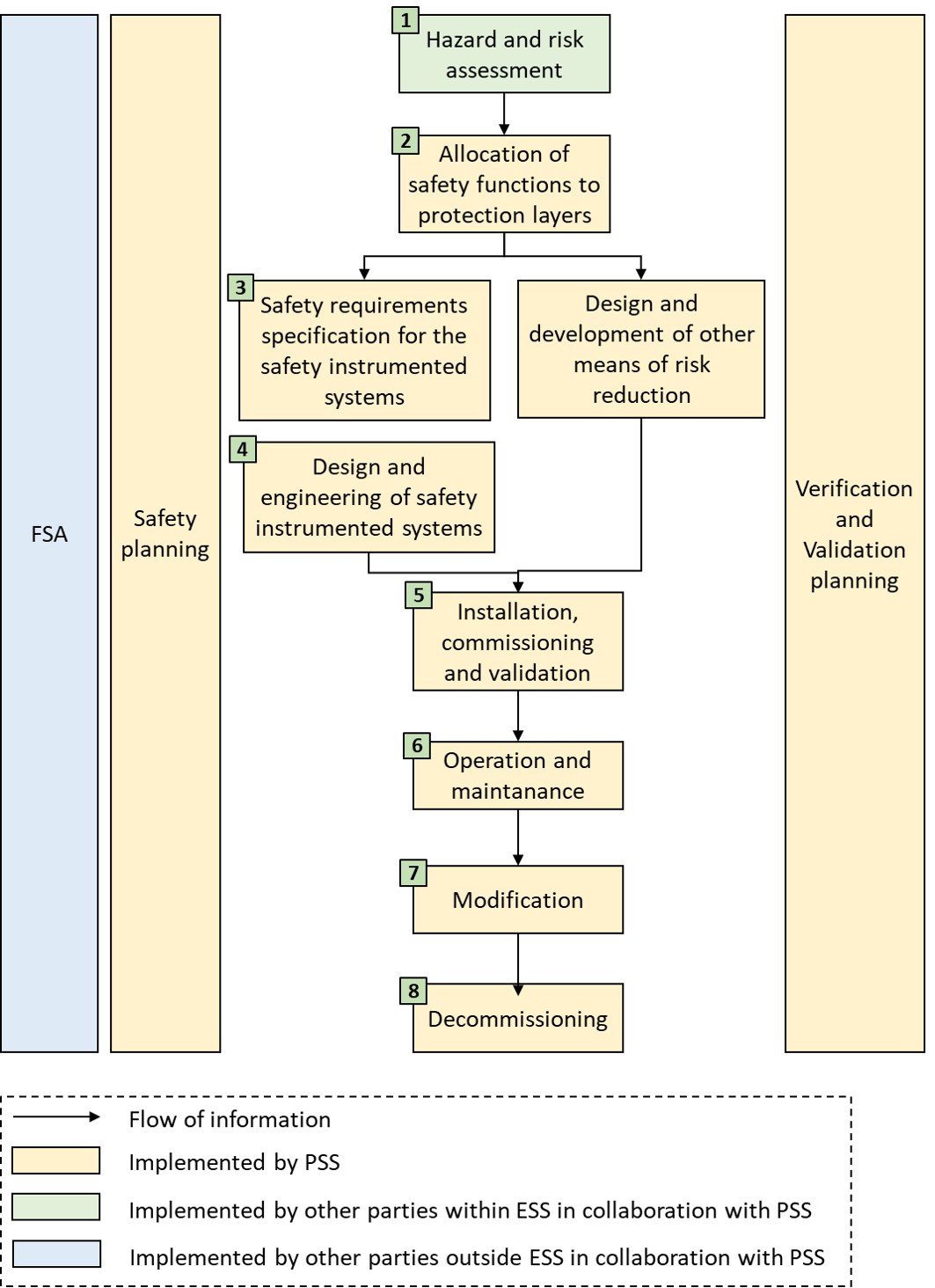


Figure 1: safety life-cycle phases for PSS development [1]

## Life-cycle phases

This section describes the IEC 61511 [1] safety life-cycle shown in Figure 1, and gives the objective, inputs and outputs of each lifecycle phase. Furthermore, the activities and tools required for each of the safety life-cycle phases are described, and the resources necessary for these activities. Documentation required for each life-cycle phase is covered in section 3.1.

The safety planning and verification and validation planning activities are carried out over the whole life-cycle of the safety instrumented systems. The verification and validation plan for PSS0 is defined in [2].

### Phase 1: Hazard and Risk Analysis

#### Objective

The hazards and risks of the Equipment Under Control (EUC)[[1]](#footnote-1), as well as hazardous events, are determined by a Hazard and Risk Analysis. This phase analyses the hazards and hazardous events of the EUC, identifies initiating events and event sequences, determines the risks associated with the hazardous events, requirements for risk reduction, and identifies overall safety requirements to mitigate the hazards and hazardous events.

#### Inputs

The inputs to this phase are EUC design, layout, manning arrangements and safety targets, as well as the concept of operations for the EUC.

#### Outputs

The output of this phase are descriptions of the hazards and hazardous events, of the initiating events, of the overall safety requirements and of the associated risk reduction requirements.

#### Tools and methods

The hazards are identified using the HAZID identification method or similar. At first, a risk assessment is done to identify hazards of the EUC, where for a subset of these hazards the development of a PSS is assigned to the PSS team. The overall safety requirements then give general requirements on the PSS to be developed. For the hazards to be mitigated by the PSS to be developed, initiating events are identified. From this an initial design concept for the PSS is developed. The information gathered during this phase and more details on the relevant hazards, initiating events and possible safety functions are summarized in a hazard register. For details on the hazard register, see Appendix A (Section 6)

Electrical hazards are identified in accordance with standard Swedish authority’s voltage hazard categories (see Appendix C, section 8). Table 7 in section 8 lists the three main voltage categories described in the Swedish standards and regulations.

#### Resources

The initial risk assessment of the EUC shall be carried out by the owner of the EUC and ES&H, in collaboration with the PSS team. The overall safety requirements are derived from this by the PSS team. The initiating events identification, the initial design concept and the hazard register are also delivered by the PSS team

### Phase 2: Allocation of overall safety requirements to protection layers

#### Objective

The Safety Instrumented Functions (SIFs) required to achieve necessary risk reduction are determined. Furthermore, the required Safety Integrity Levels (SIL) for each SIF are derived. This phase determines and verifies the SILs for each SIF to be implemented by the PSS0 system.

#### Inputs

The inputs to this phase are the results of the H&RA from phase 1, including risk reduction requirements, and the overall safety requirements.

#### Outputs

The outputs of this phase are a list of protection layers, SIFs and the SIL for each of the SIFs. These outcomes shall be documented.

#### Tools and methods

To determine the SILs for each SIF, the Layer of Protection Analysis (LOPA) shall be used, and all related calculations and results shall be documented. The SIL levels are then verified using the FTA/ETA analysis. Details about the methods used for SIL determination and verification, and assumptions made for this, are given in in Appendix B (Section 7).

#### Resources

The SIL determination and verification is carried out by the PSS team (see section 3.3).

### Phase 3: Safety requirements specifications for the safety instrumented systems

#### Objective

The objective of this phase is to specify the requirements for each SIF of the safety instrumented system. The requirements shall be stated in terms of the required SIF, and the safety integrity level needed to reach the required functional safety for each of the SIF.

#### Inputs

The inputs to this phase are a description of the SIFs and protection layers, and the SIL for each SIF determined in the previous phase.

#### Outputs

The outputs of this phase are safety requirement specifications and application program safety requirement specifications.

#### Tools and methods

The safety requirements specification (SRS) defines requirements on the safety instrumented system to be developed, and the software SRS defines requirements on the application program of the safety instrumented systems based on the SRS. These include general requirements as well as specific requirements for each SIF.

The SRS serves as a reference for design and engineering of the safety instrumented systems, as well as for the validation and verification activities.

#### Resources

The safety requirements for the safety instrumented systems and each SIF (including application program SRS) are specified by the PSS team (see section 3.3).

### Phase 4: Design and engineering of safety instrumented functions

#### Objectives

The objective of this phase is to design the safety instrumented systems (including hardware and application program) to implement the SIFs and fulfil the safety requirements for the SIF and the associated safety integrity in terms of required SIL.

#### Inputs

The inputs to this phase are the safety requirement specifications and application program safety requirement specifications.

#### Outputs

The outputs of this phase are the design of the hardware and application program of the safety instrumented systems in conformance with the SRS and application program SRS, and a plan for integration testing.

#### Tools and methods

During design, the tools listed in Table 1 are used. All documentation and related information shall be uploaded to CHESS.

Table 1: Tools used in design and engineering of safety instrumented functions

|  |  |
| --- | --- |
| Tool | Use |
| ePLAN | Design tool, used for preparation of circuit diagrams and drawings for electrical systems, subsystems and components. |
| CATIA | Design tool, used for 3D mechanical design of components, pipe routing and cable raceways space allocation |
| AVEVA E3D | Cable management system detailed design |
| Siemens TIA portal | An integrated programming and commissioning environment for Siemens Automation equipment. |

#### Resources

The design and engineering are carried out by the PSS team (see section 3.3).

### Phase 5: Installation, commissioning and validation

#### Objectives

The objective of this phase is to install and integrate the software and hardware and to test the safety instrumented systems. Furthermore, the objective is to validate that the safety instrumented system meets the safety requirements in terms of the required SIF and their SIL in every respect.

#### Inputs

The inputs to this phase are the design of the safety instrumented systems, the verification test plans for installation, integration and commissioning tests, the safety requirement specifications, and the verification and validation plan.

#### Outputs

The outputs of this phase are a fully functional safety instrumented system conforming with the safety requirements, and approved reports of verification activities for installation, integration and commissioning tests.

#### Tools and methods

The installation is done according to the design drawings and specifications. All measuring tools and meters shall be calibrated before use.

Upon successful verification of hardware installation, the application program is downloaded to the PSS0 PLC. This is followed by integration tests for PSS0.

After commissioning, the safety instrumented system is ready for final validation. Validation ensures that the requirements defined in phase 3 (see section 2.1.3) are met, and that the installed and commissioned safety instrumented systems and the corresponding SIFs achieve these requirements.

After commissioning and validation, the PSS0 system is signed by stakeholders and ES&H and handed over to stakeholders for operation.

#### Resources

The design and engineering are carried out by the PSS team (see section 3.3).

### Phase 6: Operation and maintenance

#### Objectives

The objective of this phase is to ensure that the functional safety of the SIS is maintained during operation and maintenance.

#### Inputs

The inputs to this phase are the safety requirements specifications, the design for the safety instrumented systems and the plan for operation and maintenance.

#### Outputs

The outputs of this phase are the results of the operation and maintenance activities-

#### Tools and methods

At pre-determined intervals, the PSS team carries out planned maintenance. If during operation planned or unplanned maintenance is required, the PSS0 system shall be handed back to the PSS team, which carries out the maintenance.

All measuring tools and meters shall be calibrated before use. All the maintenance activities shall be documented.

#### Resources

Operation of the PSS0 is carried out by the operations team. However, planned and unplanned maintenance is done by the PSS team (see section 3.3).

### Phase 7: Modification

#### Objectives

The objective of this phase is to make corrections, enhancements or adaptations to the safety instrumented system, and to ensure that the required SIL is achieved and maintained for each of the SIFs. Controlling changes and modifications to the systems ensures the required safety integrity despite of any changes made.

#### Inputs

The inputs to this phase are the revised safety requirements specifications.

#### Outputs

The outputs for this phase are the results of the modification.

#### Tools and methods

In case modifications are required during operation of the safety instrumented system, change management process and impact assessment of the changes shall be performed using configuration management as detailed in [4] to ensure continued safety integrity.

#### Resources

Modifications are carried out by the PSS team (see section 3.3). If modifications are necessary during operation, the safety instrumented system requiring modification shall be handed back to the PSS team.

### Phase 8: Decommissioning

#### Objectives

The objective of this phase is to ensure a proper review, proper sector organisation, and to ensure that the SIF remain appropriate. The required SIFs shall remain operational, in order to ensure safety integrity even during the last phase of the safety life-cycle.

#### Inputs

The inputs to this phase are the as built safety requirements and process information.

#### Outputs

The outputs from this phase are the SIF placed out of service

#### Tools and methods

Details for decommissioning plans shall be developed and updated in this document.

#### Resources

The decommissioning shall be done by the PSS team (see section 3.3). Details concerning decommissioning shall be developed during the operational lifetime of the facility.

### Verification and Validation

#### Objectives

The objective is to test and evaluate the outputs of a given phase, in order to ensure correctness and consistency with respect to the input to that phase.

#### Inputs

The input is a plan for verification for each life-cycle phase. This is provided by the Verification and Validation plan [2].

#### Outputs

The outputs are the results of the verification activities for each phase of the safety life-cycle.

#### Tools and methods

The verification and validation activities are described in a plan. This plan describes methods used for validation and verification to minimise risks and to ensure safety and operational requirements are met. Details about these methods can be found in the Verification and Validation plan [2].

The results of the different verification and validation activities are recorded in verification and validation reports for each activity planned in [2].

All related documentation shall be uploaded to CHESS.

#### Resources

The verification and validation activities are developed by the PSS team (see section 3.3).

### Functional Safety Assessment (FSA)

#### Objectives

The objective is to investigate and arrive at a judgement on the functional safety achieved by the safety instrumented systems.

#### Inputs

The inputs to the FSA are analysis, design and development documentation, as well as test descriptions and reports needed to perform the assessment.

#### Outputs

The outputs are the results of the FSA.

#### Tools and methods

For details on the FSA see section 3.4.

#### Resources

The FSA is carried out by an external evaluator.

# Safety management

## Documentation

As part of the overall safety life-cycle, a full set of approved documents shall be authored, where each phase of the life-cycle shall be documented. This section gives an overview over the documentation that shall be provided by the PSS team for the PSS0 system.

As an input for the overall safety requirements and SIL assessment activities and the corresponding documentation, the PSS team takes the Hazards and Risk Analysis document of the EUC created by the owner of the EUC and the ES&H division.

The required documents to be delivered by the PSS team and their inputs and outputs are shown in Table 2. Note that this table does not include the concept of the EUC, the scope and the hazard and risk assessment of the EUC, since these documents are not prepared by the PSS team. The actual delivered documentation is given in the document of documents [5], which also references the H&RA, the scope and the concept of the EUC.

Table 2: Documentation required during PSS0 development

|  |  |  |  |
| --- | --- | --- | --- |
| Safety life-cycle phase | Document | Objective | Inputs / Outputs |
| Phase 1: Hazard and Risk Analysis | Overall safety requirements and initiating events | To specify general requirements for the SIS; to identify initiating events. | **Inputs**: Description of a general assessment of EUC hazards, and a specification which are to be mitigated by a system to be developed by the PSS team  **Outputs**:  Description of high-level safety requirements; Description of identified initiating events |
| Concept of Operations (ConOps) | To provide a description of the concept of the PSS0 systems and their expected operations, and to identify stakeholder needs and interfaces to existing and future systems. | **Inputs:** Description of a general assessment of EUC hazards, and a specification which are to be mitigated by a system to be developed by the PSS team; Description of identified initiating events; Overall safety requirements  **Outputs:** A high-level description of PSS0 systems, expected operations |
| Hazard register | To provide a detailed summary of the hazards to be mitigated by a system developed by the PSS team, including initiating events and related likeliness, and possible safety functions | **Inputs:** Description of a general assessment of EUC hazards, and a specification which are to be mitigated by a system to be developed by the PSS team; Description of high-level safety requirements; Description of initiating events and associated likeliness  **Outputs:** Summary of hazards, initiating events, event frequencies, safety functions |
| Phase 2: Allocation of safety functions to protection layers | SIL Assessment Report | To allocate safety functions to protection layers, determine the required SIFs, and determine for each SIF the associated SIL. | **Inputs**:  A description of the hazards and hazardous events (including associated risks), and of necessary safety functions for the required risk reduction; Description of high-level safety requirements  **Outputs**:  Description of allocation of safety requirements; Description of required SIL for each SIF. |
| Phase 3: Safety requirements specification for the safety instrumented systems | Safety requirements specification (SRS) | Specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety | **Inputs**:  Allocation of safety requirements description and SIL description for each SIF  **Outputs**: SIS safety requirements; |
| Software Safety requirements specification (SW SRS) | Specify the requirements for the application program, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety | **Inputs**:  Allocation of safety requirements description and SIL description for each SIF; SIS safety requirements;  **Outputs**: application program safety requirements |
| Phase 4: Design and engineering of safety instrumented systems | Software planning | To plan the design of the software of the SIS, in order to meet the requirements for SIF and their associated safety integrity. | **Inputs**: Information and results of the overall safety requirements; SIL Assessment Report;  **Outputs**: Plan for the SIS application program in conformance with the SIS safety requirements; planning for the SIS integration test |
| Installation and commissioning plan | To develop a plan for the installation of the safety instrumented systems in a controlled manner, to ensure that the required functional safety is achieved; To develop a plan for the commissioning of the safety instrumented systems in a controlled manner, to ensure that the required functional safety is achieved. | **Inputs**:  Information and results of the overall safety requirements allocation and the SRS.  **Outputs**: A plan for the installation of the safety instrumented systems; A plan for the commissioning of the safety instrumented systems. |
| Software design | To design the software of the SIS to meet the requirements for SIF and their associated safety integrity. | **Inputs**: Application program safety requirements  **Outputs**: Design of the SIS application program in conformance with the SIS safety requirements |
| Hardware design | To design the hardware of the SIS to meet the requirements for SIF and their associated safety integrity. | **Inputs**: SIS safety requirements  **Outputs**: Design of the SIS hardware in conformance with the SIS safety requirements; planning for the SIS integration test |
| Mechanical drawings |
| Electrical drawings |
| Interface control documents |
| Phase 5: installation, commissioning and validation | SAT specification | To specify the verification tests ensuring the requirements of the corresponding phase are fulfilled. For more information see [2]. | **Inputs**:  Verification planning; safety requirements specification; SIS design  **Outputs**:  planning of the verification activity |
| SIT specification |
| FAT specification |
| FIT specification |
| SAT report | To verify that the system meets the requirements of the corresponding design phase. For more information see [2]. | **Inputs**:  Verification planning; test specifications; safety requirements specification; SIS design  **Outputs**:  results of the verification activity |
| SIT report |
| FAT report |
| FIT report |
|  | Validation report | To validate that the SIS meets the safety requirements in terms of SIF and their associated safety integrity | **Inputs**:  SIS design; SIS safety requirements specification; Plan for the safety validation of the SIS  **Outputs**: Results of the validation test |
| Phase 6: Operation and maintenance | Maintenance manual | To describe how the maintenance shall be performed for PSS0 systems | **Inputs**: safety requirements specification; SIS design  **Outputs**: A description of maintenance to be performed |
|  | Operations manual | To describe procedures necessary for a successful operation of the PSS0, and the handling of failures and errors. | **Inputs**: Design documentation;  **Outputs**: A description of the operating procedure of the PSS0 system |
| Phase 7: Modification | Configuration management | Currently under development;  To plan the management of changes and modifications in order to establish and maintain safety integrity of the SIS | **Inputs**:  Safety requirements specification; SIS design  **Outputs**:  Plan and procedures for handling modifications and changes |
| Phase 8: Decommissioning | Shall be developed during the operational life-time of the facility. | | |
| Verification and Validation | Verification and Validation plan | To define the verification and validation activities required during the design of the PSS0 system, ensuring that design, installation and commissioning achieve the requirements specified in the SRS | **Inputs**:  Safety planning; Information and results of the overall safety requirements allocation.  **Outputs**:  Plan for the required validation and verification activities |
| Functional safety assessment | FSA report | To evaluate the functional safety achieved by the safety instrumented systems. | **Inputs**: All relevant documentation for the assessment.  **Outputs**: The results of an evaluation of functional safety, including any recommendations. |

## Procedures

Procedures for PSS0 supporting functional safety activities are covered in the following documentation, as listed in Table 3.

Table 3: Documentation covering procedures

|  |  |
| --- | --- |
| Document | Objective |
| Concept of Operations (ConOps) | To provide a high-level description of the PSS0 systems and their expected operations, and to identify stakeholder needs and interfaces to existing and future systems. |
| Operations Manual | To describe procedures necessary for a successful operation of the PSS0, and the handling of failures and errors. |
| Maintenance manual | To describe how maintenance shall be carried out for PSS0. |
| Configuration management plan | To define how configuration management is organised for PSS0, and to describe the procedure used for the management of changes, including impact analysis of the change. |

## Roles and responsibilities

The roles within the PSS team with regards to PSS0 life-cycle activities are listed in Table 4. More information on the responsibilities for each role shall be detailed in the Systems engineering management plan [6].

Table 4: Roles of the PSS team

|  |  |  |
| --- | --- | --- |
| Role | Name | Title |
| Line Manager | Annika Nordt | Protection Systems Group Leader |
| Work Package Manager | Stuart Birch | Senior Engineer Personnel Safety Systems, ICS |
| Hardware designer/technician | Morteza Mansouri | Lead Integrator Engineer for Safety Critical Systems, ICS |
| Alberto Toral Diez | Technician Personnel Safety Systems, ICS |
| Mattias Eriksson | Technician Personnel Safety Systems, ICS |
| Software developer | Denis Paulic | Deputy Group Leader for Protection and Safety Systems Group, ICS |

## Functional safety assessment

A functional safety assessment shall be completed by an external, independent, assessor at regular intervals, in order to evaluate the functional safety and safety integrity achieved by every SIF the safety instrumented systems.

An FSA shall be performed to review the work carried out in the previous stage and the corresponding results at the following stages:

* After safety life-cycle phase 3: Safety requirements specification
* After safety life-cycle phase 4: Design and engineering
* After safety life-cycle phase 5: Installation, commissioning and validation
* In safety life-cycle phase 6: Operation and maintenance
* In safety life-cycle phase 7: Modifications, before implementation of a modification.

Bi-annual audits shall be held to investigate functional safety. During these audits, the SIT and FIT verification activities shall be repeated to ensure that the safety requirements specifications remain fulfilled as defined.

All FSA results shall be documented and made available together with any recommendations.

# Glossary

| **Term** | **Definition** |
| --- | --- |
| ConOps | Concept of Operations document |
| EUC | Equipment Under Control |
| FAT | Factory Acceptance Test |
| FIT | Factory Integration Test |
| FSA | Functional Safety Assessment |
| H&RA | Hazard and Risk Analysis |
| LOPA | Layers of Protection Analysis |
| PSS | Personnel Safety Systems |
| PSS0 | Personnel Safety System 0 |
| SAT | Site Acceptance Test |
| SIF | Safety Instrumented Functions |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| SIT | Site Integration Test |
| SRS | Safety Requirements Specification |

# References

|  |  |
| --- | --- |
| [1] | “IEC 61511:2016 Functional safety - Safety instrumented systems for the process industry sector,” 2016. |
| [2] | “Verification and validation for PSS0 (ESS-0233615)”. |
| [3] | 0379511Risk Matrix for Conventional Safety Risks (0379511). |
| [4] | “Personnel Safety Systems Configuration Management Plan (ESS-0058389)”. |
| [5] | PSS0 Document of Documents (ESS-0338636). |
| [6] | *Systems Engineering Management Plan for PSS (ESS-0061709).* |
| [7] | UK HSE, “Management of instrumented systems providing safety functions of low / undefined safety integrity,” [Online]. Available: http://www.hse.gov.uk/foi/internalops/hid\_circs/technical\_general/spc-tech-gen-51.htm#action. [Accessed 10 June 2014]. |
| [8] | HSE, *Reducing risks, protecting people (R2P2),* 2001. |
| [9] | T. A. I. o. C. E. (. C. f. C. P. S. (CCPS), Layer of Protection Analysis (LOPA), 2001. |
| [10] | FARADIP - THREE V9.2, Reliability Data Base, Technis, 26 Orchard Drive, Tonbridge, Kent, TN10 4LG, ISBN 0-951-65623-6.. |
| [11] | *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.* |
| [12] | “Hazard and Risk Analysis Document for PSS0 (ESS-0229506)”. |
| [13] | ESC, SIL Determination Rule Set: Document Ref. P001\_ID090.. |

# Appendix A: Hazard Register

The hazard register summarizes all initiating events and provides qualitative assessment of hazardous scenarios against a Conventional safety risk matrix. Figure 2 gives a step-by-step guide of filling in the Hazard register.

Figure 2: Systematic procedure of filling in the Hazard register.

Table 5 provides a brief description of the hazard register elements (columns), which follow IEC 61511 requirements on identification of hazardous events, their likelihoods and consequences.

Table 5: PSS0 Hazard Register elements.

| **PSS0 Hazard Register column** | **Description** |
| --- | --- |
| Hazard ID / IE ID | *PSS\_Hazard\_xxx* - PSS relevant hazard IDs are created to be consistent throughout this sheet and reports in all phases of PSS. The IE ID identifies the initiating event for given hazard. |
| Hazard | A definition of PSS relevant hazard.  Only one hazard is PSS0 relevant, but this field is kept to be consistent through all phases of PSS. |
| Initiating Event (IE) | An event that can lead to a hazardous situation.  Identified PSS0 initiating events are leading to a PSS0 hazard. |
| Consequences | Consequences as defined in the Conventional safety risk matrix and based on a qualitative evaluation of a initiating event scenario. |
| Likelihood | Evaluated probability of initiating event happening based on a qualitative evaluation of an initiating event scenario. |
| Barriers and procedures | A list of barriers and procedures that are in place to prevent and detect the initiating event and its consequences (without PSS0 safety functions in place). |
| PSS function required Yes/No | Is the PSS0 function required to reduce the risk to a tolerable region? |
| Protection and mitigation | A list of proposed PSS0 safety functions to reach a tolerable region. |
| Human actions | A list of human actions associated with the initiating event and PSS0 functions. |
| Risk reduction (with PSS functions in place and working) | Qualitative evaluation of how much the risk is reduced while considering PSS0 functions are in place and working. |
| Risk measures independent of PSS | Other risk measures independent to PSS0 but implemented in ESS overall design. |
| Recommendations and comments | Recommendations and comments from PSS team to be considered further. |
| Screening IN/OUT | Screened IN initiating events are considered for further analysis.  Screened OUT initiating events are analysed only qualitatively and not considered for further analysis. Justification for screening out will be described in this report. |

# Appendix B: SIL determination and verification

This appendix details the methodology used for determination and verification of SILs during the allocation of safety functions in the safety life-cycle (compare to section 2.1.2).

## General Concepts

### Risk reduction

The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency of the hazardous event and its specific consequences.

The tolerable risk will depend on many factors, including the severity of the consequences or injury, the number of people exposed to danger, and the frequency and the duration of the exposure. Important factors will be the perception and views of those exposed to the hazardous event.

Risk reduction is achieved by a combination of all of the available safety protective features, including any associated SIF. The necessary risk reduction to achieve the specified tolerable risk, from a starting point of the risk presented by the Equipment Under Control (EUC), is shown in Figure 2



Figure 2: The Concept of Risk Reduction

### Safety integrity level

Safety integrity applies to the Electrical / Electronic / Programmable Electronic (E/E/PE)safety instrumented system, other technology safety instrumented systems and external risk reduction facilities and is a measure of the likelihood of those systems satisfactorily achieving the necessary risk reduction. Once the tolerable risk has been set, and the necessary risk reduction is estimated, the safety integrity requirements for the SIFs can be allocated in terms of PFD or PFH. The PFD and PFH correspond to one of SILs specified in Table 5. These SILs specify the safety integrity requirements to be achieved by the safety instrumented system.

Table 5. SIL Specified PFD

| **SIL** | **Low Demand (PFD)** | **High or Continuous Demand (PFH)** |
| --- | --- | --- |
| SIL4 | ≥ 10-5 to < 10-4 | ≥ 10-9 to < 10-8 |
| SIL3 | ≥ 10-4 to < 10-3 | ≥ 10-8 to < 10-7 |
| SIL2 | ≥ 10-3 to < 10-2 | ≥ 10-7 to < 10-6 |
| SIL1 | ≥ 10-2 to < 10-1 | ≥ 10-6 to < 10-5 |
| SILa | ≥ 10-1 to < 1 | N/A |

“SILa” indicates that although additional mitigation is required, the necessary level of risk reduction is below the SIL1 range and is thus outside the remit of IEC 61511 [1]. If, however, an instrumented system is implemented to address a PFD target of greater than 0.1 (i.e. “SILa”), the UK Health and Safety Executive (HSE) requires said function to be subject to the following provisions [7]:

* the persons who have responsibilities for the instrumented system shall be suitably competent;
* clear, precise and unambiguous specification of the safety function;
* independence between control and safety functions wherever reasonably practicable;
* accurate, accessible, controlled and easily understood engineering documentation showing the component parts of the instrumented system and how they are configured. Examples of engineering documentation include loop or circuit diagrams, equipment data sheets and records of parameter settings;
* periodic inspection of the instrumented system, for example visual or more detailed inspection to reveal evidence of deterioration or unexpected modifications;
* periodic maintenance of the instrumented system, for example calibration, cleaning or flushing;
* periodic proof testing of the instrumented system for the purpose of revealing dangerous undetected faults;
* management of change, including control of access to software functions and backing up of software-based systems.

### Risk Targets

In the UK, the HSE guidance on tolerable levels of risk (Reducing Risks, Protecting People [8]) defines the following risk boundaries:

* “*Individual risk of death of one in a million per annum* ***[1.0E-06/yr]*** *for both workers and the public corresponds to a very low level of risk and should be used as a guideline for the boundary between the broadly acceptable and tolerable regions*”
* “*Boundary between the ‘tolerable’ and ‘unacceptable’ regions for risk entailing fatalities […:] as individual risk of death of one in a thousand* ***[1.0E-03/yr]*** *per annum […] for workers*”.

Given the inherent inaccuracies in the data applied in SIL determination studies, it is deemed prudent to set the tolerable risk as an order of magnitude lower than the ‘tolerable risk boundary’; i.e.1.0E-04/yr. For SIL targeting purposes, this value is typically reduced by a further order of magnitude to account for other, non-process risks of fatality (i.e. slips, trips and falls) to which the hypothetical employee may be exposed.

In SIL studies for PSS systems, a more stringent target risk of 1.0E-06 per year is applied as the target for a single employee fatality.

## LOPA

The LOPA technique used for assignment of SIL targets is described in [1] and the American Institute of Chemical Engineers (AIChE) CCPS LOPA 2001 [9].

### LOPA for low demand SIFs

This section details the steps of the LOPA to determine the SIL for each of the SIFs. Note that steps 1 to 4 are part of the Hazard and Risk Analysis (see section 2.1.1), and are expected inputs for the allocation of safety functions to protection layers (see section 2.1.2 done by PSS.

1. Identify hazards (which can be addressed by the implementation of a SIF) using a suitable Process Hazard Analysis tool (e.g. Hazard and Operability Study - HAZOP);
2. Rank the severity of the consequences of the specified hazard. **It is important that existing protection layers are disregarded at this stage.** Compare this with the corresponding risk target in Section 7.1.3;
3. Identify initiating events and estimate their frequency using operating experience where applicable, data sources such as FARADIP [10] and engineering judgement;
4. Identify Conditional Modifiers / Post-Event Mitigation. For example, occupancy, probability of ignition and vulnerability;
5. Identify Independent Protection Layers (IPLs), which prevent the hazardous event from occurring;
6. Determine the likelihood of occurrence (Total Mitigated Event Frequency);  
   This is calculated by applying equation ( 1 ):

|  |  |
| --- | --- |
|  | ( 1 ) |

where:

|  |  |
| --- | --- |
|  | is the calculated frequency of consequence *C* summed over all relevant initiating events and with credit taken for all relevant protection layers and conditional modifiers/post-event mitigations: “Total Mitigated Event Frequency” |
|  | is the frequency of initiating event *i* leading to consequence *C*. |
|  | is the probability of failure on demand of the jth protection layer that protects against consequence *C* for initiating event *i.* See “Independent Protection Layers” |
|  | is the probability that conditional modifier *k* will allow consequence *C* to occur for initiating event *i*. See “Conditional Modifiers” |

1. Compare the Target Risk Frequency with the likelihood of occurrence (Total Mitigated Event Frequency) to determine the required PFD for the SIF under consideration. This is calculated by applying equation ( 2 ).

|  |  |
| --- | --- |
| , | ( 2 ) |

where:

|  |  |
| --- | --- |
|  | is the Target Risk Frequency |

1. Determine the SIL requirement of the SIF under consideration by comparing the calculated PFD requirement with Table 5.

### LOPA for high demand or continuous SIFs

1. Identify hazards (which can be addressed by the implementation of a SIF) using a suitable Process Hazard Analysis tool (e.g. Hazard and Operability Study - HAZOP);
2. Rank the severity of the consequences of the specified hazard. **It is important that existing protection layers are disregarded at this stage.** Compare this with the corresponding risk target in Section 7.1.3;
3. Identify Conditional Modifiers / Post-Event Mitigation. For example, occupancy, probability of ignition and vulnerability;
4. Identify Independent Protection Layers (IPLs), which prevent the hazardous event from occurring;
5. Determine the Target Risk Frequency (/hr).  
   This is calculated by applying equation ( 3 ):

|  |  |
| --- | --- |
|  | ( 3 ) |

where:

|  |  |
| --- | --- |
|  | is the probability of failure on demand of the jth protection layer that protects against consequence *C* for initiating event *i.* See “Independent Protection Layers” |
|  | is the probability that conditional modifier *k* will allow consequence *C* to occur for initiating event *i*. |
|  | is the Target Risk Frequency |

1. Determine the SIL requirement of the SIF under consideration by comparing the calculated PFH requirement with Table 5.

### Independent protection layers

In order for an IPL to be considered valid (in accordance with IEC 61511-3 [1], the following criteria must be met:

1. **Effectiveness** – an IPL reduces the identified risk by at least a factor of 10;
2. **Specificity** – an IPL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL;
3. **Independence** – an IPL is independent of other protection layers if it can be demonstrated that there is no potential for common cause or common mode failure with any other claimed IPL;
4. **Dependability** – an IPL can be counted on to do what it was designed to do by addressing both random failures and systematic failures during its design;
5. **Auditability** – a protection layer is designed to facilitate regular validation of the protective functions.

In order to help achieve and maintain the Auditability criteria (item 5 above), a database of all IPLs applied in the LOPA study for a PSS system shall be attached to the SIL Assessment Report of a PSS system. For the purposes of PFD estimation, it is assumed that all stated IPLs are tested at a proof test interval stated in the Assumption in the SIL Assessment Report.

## Hardware reliability assessment

The hardware reliability of a SIF is expressed in terms of either its Probability of Dangerous Failure on Demand (PFD) or of its Average Frequency of a Dangerous Failure per Hour (PFH[[2]](#footnote-2)), depending on the frequency of demands made upon it.

The frequency of demand (‘mode of operation’) on the SIF falls into three categories:

* low demand mode (IEC 61511-1: 3.2.29 [1]) – where the safety function is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year; or
* high demand mode (IEC 61511-1: 3.2.29 [1]) – where the safety function is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year; or
* continuous mode (IEC 61511-1: 3.2.29 [1]) - where the safety function retains the EUC in a safe state as part of normal operation.

Note that compliance with IEC 61511 can be achieved by following IEC 61508 regarding hardware reliability assessment.

### Probability of Failure on Demand

For low demand SIFs (refer to section 7.3), IEC 61508 [11] requires calculation of the PFD of each complete SIF loop according to equation (4) (IEC 61508-6: B.3.2.1 [11]):

|  |  |  |
| --- | --- | --- |
|  |  | ( 5 ) |

where:

|  |  |
| --- | --- |
|  | is the probability of failure on demand of a safety function for the electrical/electronic/programmable electronic safety-related system; |
|  | is the probability of failure on demand for the sensor subsystem; |
|  | is the probability of failure on demand for the logic subsystem; |
|  | is the probability of failure on demand for the final element or final element subsystem. |

The overall PFD of the complete SIF is compared with its PFD target to determine whether sufficient risk reduction is provided.

### Failure rate, λ

To calculate the PFD and PFH, it is first necessary to introduce the term ‘failure rate’.

Failure rate is denoted by *λ* and defined as the *number of failures per unit time.*

#### Failure Modes

In order to calculate the PFD of the sensor, logic or final element subsystem using *λ*, its failure modes must first be examined. The number of failures is apportioned into safe and dangerous failure modes, where:

* A **dangerous failure** (IEC 61511-1: 3.2.11 [1]) is defined as a failure which impedes or disables a given safety action. When fault tolerance is implemented, a dangerous failure can lead to either
  + a degraded SIF where the safety action is available but there is either a higher PFD (demand mode of operation) or a higher likelihood of initiating a hazardous event (continuous mode of operation); or
  + a disabled SIF where the safety action is completely disabled (demand mode of operation) or the hazardous event has been induced (continuous mode of operation).
* A **safe failure** (IEC 61511-1: 3.2.62 [1]) is defined as failure which favours a given safety action. When fault tolerance is implemented, safe failure can lead to either:
  + operation where the safety action is available but with a higher probability of success on demand (demand mode of operation) or a lower likelihood to cause a hazardous event (continuous mode of operation); or
  + a spurious operation where the safety action is initiated.

It follows that the total failure rate, *λ*, is equal to the sum of the safe and dangerous failure rates:

|  |  |
| --- | --- |
| , | ( 6 ) |

where:

 is the dangerous failure rate per hour and;

 is the safe (or spurious) failure rate per hour.

#### Diagnostic Testing

The dangerous failure rate is further apportioned into dangerous detected and undetected failures, where:

* A **detected** failure (overt) [IEC 61511-1 3.2.13 [1]] is defined as a failure, in relation to hardware and software, which is not hidden because it announces itself or is discovered through normal operation or through dedicated detection methods.
* An **undetected** failure (covert) [IEC 61511-1 3.2.85 [1]] is defined as a failure, in relation to hardware and software, which is not detected or overt.

The relationship can therefore be described by:

|  |  |
| --- | --- |
| , | ( 7 ) |

where:

 is the dangerous detected failure rate per hour and;

 is the dangerous undetected failure rate per hour.

### PFD and Mean Down Time

The PFD of a single subsystem - for instance, a single detector - is found by multiplying the dangerous failure rate, *λ*D (refer to Section 7.3.2.1), by the Mean Down Time (MDT):

|  |  |
| --- | --- |
| , | ( 8 ) |

where MDT is the time taken to repair a fault and is, itself, defined as the Mean Time To Repair (MTTR), plus the time taken to detect it. It is assumed that, on average, a fault will occur at the mid-point of the test interval and, thus, the time taken to detect a fault is equal to half the test interval, . Therefore:

|  |  |
| --- | --- |
| , | ( 9 ) |

#### PFD for Detected Failures

In general, for failures that are detected by the diagnostic tests of a subsystem (refer to Section 7.3.2.2), the test interval (termed as ‘diagnostic test interval’), Td, is typically less than one hour (refer to IEC 61508 [11]: Part 6, Annex B ) and, thus, the time taken to detect a fault, Td/2, is considered small in comparison with the MTTR. That is:

, and thus:

|  |  |
| --- | --- |
| , | ( 10 ) |

where MTTR is measured in hours.

#### PFD for Undetected Failures

For undetected failures (refer to Section 7.3.2.2), i.e. failures revealed only by manual proof testing, the MTTR is considered small in comparison with the time taken to detect a fault, i.e. the mid-point of the proof test interval, Tp/2; therefore:

,

and thus:

|  |  |
| --- | --- |
| * , | ( 11 ) |

where Tp is the proof test interval in hours.

#### PFD for Subsystem

The overall PFD of a single subsystem (sensor, logic or final element subsystem), comprises the PFD for undetected faults and the PFD for detected faults:

|  |  |
| --- | --- |
| . | ( 12 ) |

#### PFH for Subsystem

The PFH of a single subsystem - for instance, a single detector - is equivalent to its dangerous undetected failure rate, *λ*DU (refer to Section 7.3.2.2).

|  |  |  |
| --- | --- | --- |
|  |  | ( 13 ) |

### Voting configuration

When a subsystem (sensor, logic or final element) consists of several components, such as sensors in a two out of three (2oo3) voting configuration, the combined PFD of the whole subsystem must be calculated. The PFD for subsystems in different configurations are found using the formulae presented in [11].

The reliability analysis for subsystems in redundant configurations is conducted using the FTA.

### Common cause failure (CCF)

When assessing the reliability of a subsystem in a redundant configuration, IEC 61508 requires that the effect of CCFs is taken into account. A CCF is defined as: a *failure that is the result of one or more events, causing failures of two or more separate channels in a multiple channel system.*

An example of a CCF would be freezing weather conditions causing identical level transmitters in a 1oo2 voting configuration to fail simultaneously.

CCFs in redundant systems are accounted for using the **model, which assumes a fixed proportion of failures are caused by a common cause. This proportion, termed **is estimated based on:

* the degree of channel separation;
* design with common cause awareness;
* diagnostic coverage;
* self-test frequency and other factors.

The CCF rate, according to the **model, is calculated as follows:

|  |  |  |
| --- | --- | --- |
|  |  | ( 14 ) |

and, thus, the overall PFD due to dangerous CCFs is given by:

|  |  |  |
| --- | --- | --- |
|  |  | ( 15 ) |

## Architectural assessment methodology

### Hardware fault tolerance (HFT)

In addition to the hardware reliability assessment (refer to Section 7.3), there are also minimum architecture requirements to be met. Each subsystem within a SIF must meet the minimum HFT for the required SIL. That is, the sensor, logic and final element subsystems must all individually meet the overall SIL requirement for the SIF. To determine the level of HFT (or redundancy) required in a SIF using the Route 1H approach detailed in IEC 61508-2: 7.4.4.2, the Safe Failure Fraction (SFF) must be calculated for each subsystem.

### Safe failure fraction (SFF)

The SFF is essentially the proportion of random failures in a subsystem that either result in a safe state, or a dangerous state that is revealed by automatic diagnostic tests. SFF is calculated using the following formula (IEC 61508 [11]: Part 2, C.1.h):

|  |  |  |
| --- | --- | --- |
|  |  | ( 16 ) |

where:

 is the dangerous detected failure rate per hour;

 is the dangerous undetected failure rate per hour;

 is the safe (spurious) failure rate per hour.

### IEC 61508 architectural constraint (Route 1H)

Table 6presents the (Route 1H) maximum allowable SIL given minimum HFT and SFF for Type A and Type B components respectively. The maximum SIL is determined by the component type (Type A or B), its Safe Failure Fraction (SFF, usually determined by an FMEA, available on its certificate) and the Hardware Fault Tolerance (HFT).

For a component to be considered Type A, all the following criteria must be met:

* Failure modes are well defined and;
* Behaviour under fault conditions is well defined and;
* Failure data is available.

If a component fails to meet any of these criteria, it is considered to be Type B. Type B components typically contain complex microelectronics, commonly found in Programmable Logic Controllers (PLCs) and smart sensors. Simple devices, such as valves and relays, are typically considered to be Type A.

Table 6. HFT for Type A and Type B Components

| **SFF** | **Minimum HFT for Type A Component** | | | **Minimum HFT for Type B Component** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **SIL for simplex** | **SIL for m+1** | **SIL for m+2** | **SIL for simplex** | **SIL for m+1** | **SIL for m+2** |
| **(HFT=0)** | **(HFT=1)** | **(HFT=2)** | **(HFT=0)** | **(HFT=1)** | **(HFT=2)** |
| <60% | 1 | 2 | 3 | Not allowed | 1 | 2 |
| 60-90% | 2 | 3 | 4 | 1 | 2 | 3 |
| 90-99% | 3 | 4 | 4 | 2 | 3 | 4 |
| >99% | 4 | 4 | 4 | 3 | 4 | 4 |

# Appendix C: Applicable safety regulations

Table 7 lists the three main voltage categories described in the Swedish standards and regulations.

Table 7: Swedish authority voltage hazard categories.

|  |  |  |
| --- | --- | --- |
| Swedish | English | Accelerator PSS |
| Klenspänning | Extra-low voltage | U < 50V AC (or 120V Ripple Free DC) |
| Lågspänning | Low voltage | U < 1000V AC (or 1500V DC) |
| Högspänning | High voltage | Above "lågspänning" |

# Document Revision history

| Revision | Reason for and description of change | Author | Date |
| --- | --- | --- | --- |
| 1 | First issue | Meike Rönn | <<YYYY-MM-DD>> |
|  | <<Keep only full number revisions when approving document>> |  |  |
|  |  |  |  |

1. Equipment Under Control (EUC) is a concept from IEC 61508 [11], and the equivalent concept in IEC 61511 [1] is a process. In this document and all related PSS0 documentation we will use the term EUC to denote a process. [↑](#footnote-ref-1)
2. The term “probability of dangerous failure per hour” is not used in IEC 61511 [1] but the acronym PFH was retained. When it is used, it means “average frequency of a dangerous failure [h-1]" [↑](#footnote-ref-2)