| Safety Requirement Specification | SIF specification form ver: 1.0 |
|---|---|
| SIF ID: | **SIF name:** |

This form 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.

| A. Document issued for: |
|---|
| **Project:** |
| **Company:** |
| **Process:** |
| **Plant / Site:** |

| B. Document source: | | |
|---|---|---|
| Risk assessment by: | Organization: | Date: |
| SIF specification issued by: | Organization: | Date: |
| SIF specification examined by: | Organization: | Date: |
| SIF specification approved by: | Organization: | Date: |

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



SafeProd
Functional safety in complex products
**www.sp.se/safeprod**

C. Related documents:

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

D. Document history:

| Date: | Rev: | Change description: | Sign: |
|---|---|---|---|

| 1. Functional description: |
| --- |
| Description of hazardous event, consequences and protection: |
| Defined safe process state: |
| Operative demand: |

| 2. Primary actions / sequence (for bringing the process to the defined safe state): |
| --- |
| |

| 3. Secondary actions / sequence (for operational reasons): |
| --- |
| |

| SIF ID: | SIF name: | |
|---|---|---|

| 4. Demand rate and Safety integrity: | |
|---|---|
| Estimated demand sources: | Est. demand rates |
| Estimated SIF demand rate:<br>Used likelihood analysis method: | |
| Low Demand, High Demand or Continuous mode of operation: | |
| Established target SIL (Safety Integrity Level):<br>Used SIL-selection method: | |

| 5. Trigging / Tripping: | |
|---|---|
| Automatic trigging and trigging detection: | **Yes/No?** |
| Manual trigging: | **Yes/No?** |
| Trigging response and delay time requirements: | **Max. response time:** |

| 6. Reset / Restart: | |
|---|---|
| Automatic reset and reset detection: | **Yes/No?** |
| Manual reset: | **Yes/No?** |
| Reset response and delay time requirements: | **Max. response time:** |

| 7. Overriding, Inhibiting and Bypassing: | Yes/No? |
|---|---|
| Description of Overriding, Inhibiting and Bypassing functions: | |

| 8. Spurious trips and reset failures: | |
|---|---|
| Maximum allowable spurious trip rate: | |
| Estimated consequences of nuisance trips: | |
| Maximum allowable reset failure rate: | |
| Estimated consequences of reset failures: | |

| 9. Final elements description: | | | | | |
|---|---|---|---|---|---|
| Description of output actions: | | | | | |
| Defined fail-safe positions of final elements: | Fail-safe position OPEN/CLOSED? | | | | |
| Justification of the defined fail-safe positions: | | | | | |
| Final elements specification: | TAG-name: | Equipment type: | Req | Actuator action: | |
| Requirements for successful operation of final elements: | | | | | |

| 10. Fail-safe process output description: | | | | |
|---|---|---|---|---|
| Digital fail-safe outputs: | | | | 1 |
| **Digital output description:** | I/O-name: | Device: | Req | Trip action: |
| | | | | **ENERGIZE/ DE-ENERGIZE?** |
| Output circuits requirements: | | | | |

| 11. Fail-safe process input and trip limit description: | | | | |
|---|---|---|---|---|
| Digital fail-safe inputs: | | | | 6 |
| **Digital input description:** | I/O-name: | I/O-voting | Req | Work. circuit |
| Analogue fail-safe inputs: | | | | 3 |
| **Analogue input description:** | I/O-name: | I/O-voting | Req | Trip limit: |
| Input circuit requirements: | | | | |

| 12. BPCS and other systems interface: | | | | |
|---|---|---|---|---|
| Digital outputs (non fail-safe): | | | | |
| **Digital output description:** | | I/O-name: | To system: | Action: |
| Digital inputs (non fail-safe): | | | | |
| **Digital input description:** | | I/O-name: | From system: | Action: |
| Other type of output interface signals: | | | | |
| **Other type output signal description:** | Type: | I/O-name: | To system: | Action: |
| Other type of input interface signals: | | | | |
| **Other type input signal description:** | Type: | I/O-name: | From system: | Action: |

| 13. Requirements for proof test intervals: | |
|---|---|
| Desired full proof test interval: | |
| Full proof test possible during operation: | Yes/No? |
| Partial proof test possible during operation: | Yes/No? |
| Special proof test design requirements: | |

14. Relationship between process inputs and outputs:

Logical description:

**Trigging and reset:**

**Actuating:**

15. Operator interfaces (HMI):

Panels / Buttons:

Graphics:

Generation of alarms:

Generation of events:

Alarm and event logging:

| 16. Requirements for protecting the SIF from special environmental conditions: |
| --- |
| Requirements: |

| 17. Requirements for protecting the SIF from major accidents: |
| --- |
| Requirements: |

| 18. Consequential hazards (due to implementation of the SIF): |
| --- |
| Discovered consequential hazards: |
| Hazards due to concurrently occurring events: |
| Possible risk reducing measures: |