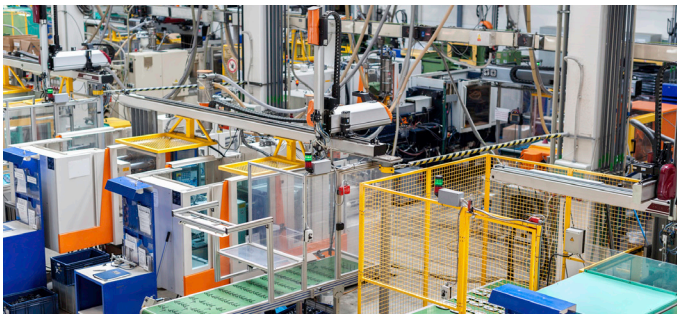
hargrove | Safety Requirements Specification



Within the machine safety lifecycle, a Safety Requirements Specification (SRS) tells the designers how a machine should be built to meet the requirements from the Safety Risk Assessment (SRA). The SRS captures all the details necessary and provides the required design and operational criteria for each safety function. This critical document is used to create a safer, more efficient facility. Below are the key components of an SRS.

Learn More

csia CERTIFIED

Hargrove's certified TÜV Rheinland Functional Safety Engineers have years of experience and can help you ensure hazard risk reduction at your site.

Key components of an SRS

Results of the Safety Risk Assessment (SRA) including:

- Each Hazard / Task Combination
- All Safety Functions (SF) necessary for the reduction of risk for each hazard
- Associates interacting with the hazards and their response time requirements

Machine operating characteristics:

- Modes of operation of the machine
  - Description of the safe state
  - Example: if the machine requires a certain safe state to perform maintenance
- Cycle times of each safety function
- Response time performance
- Environmental conditions
  - Examples: electromagnetic immunity, temperature, humidity, dust, chemical, mechanical vibration & shock
- Working processes
  - Interactions of persons (Maintenance, Operations, Cleaning, Setting, Etc.)
- Any manual activities
- Local modes
- Automatic modes

Safe distance calculations

- Affects of the response time of the machine safety

Excepted Usages (Frequency)

- Including: Rate of operating cycles, duty cycle, demand of operation

An overall safety input/output matrix for all SFs

Each Safety Function (SF) should have:

- The Performance Level Requirements (PLr)
- Detailed requirements of each SF for each Input-Logic-Output block (I-L-O)
- A description including the trigger & effected elements
- Functional Requirements Specification
  - How the SF should operate in normal conditions
  - Description of the interfaces with other machines or safety functions
- Fault reaction functions
  - How the SF should operate in a fault condition
  - How should the SF be reset?
  - Are there any constraints?
- Required Stop Categories
  - In the event of an fault, how should the SF stop?
  - Category 0 Stop – Immediately remove all power
  - Category 1 Stop – Controlling certain functions to as safe speed then remove all power
  - Category 2 Stop – Remove all power except for certain functions where removing power would result in further risks
- A Fault Tree Analysis to make it easier to spot Common Cause Factors (CCF)
- Priority order
  - Some SFs can simultaneously activate whereas others may cause conflicts so priority should be identified if needed.