KLM Technology Group
#03-12 Block Aronia,
Jalan Sri Perkasa 2
Taman Tampoi Utama
81200 Johor Bahru
Malaysia

INSTRUMENTATION SAFETY REQUIREMENT SPECIFICATIONS (SIL)

(PROJECT STANDARDS AND SPECIFICATIONS)

TABLE OF CONTENT

SCOPE

This Project Standard and Specification is intended to to identify and present the safety requirements for the Safety Instrumented Functions.

DEFINITIONS AND TERMINOLOGY

Basic Process Control System - 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 safety integrity level.

Safety Instrumented Function - 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.

Safety Integrity Level - discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

Safety Instrumented System - instrumented system used to implement one or more safety instrumented functions. A safety Instrumented System is composed of any combination of sensor (s), logic solver (s), and final elements(s).

Safety Requirements Specification - specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems.

SYMBOLS AND ABBREVIATIONS

SYMBOL/ABBREVIATION	DESCRIPTION
BPCS	Basic process control system
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

GENERAL SRS REQUIREMENTS

The requirements need to be documented during the safety planning. The SRS is created after the hazard and risk analysis and the allocation of safety functions to protective layers in the safety life cycle. See figure 1.

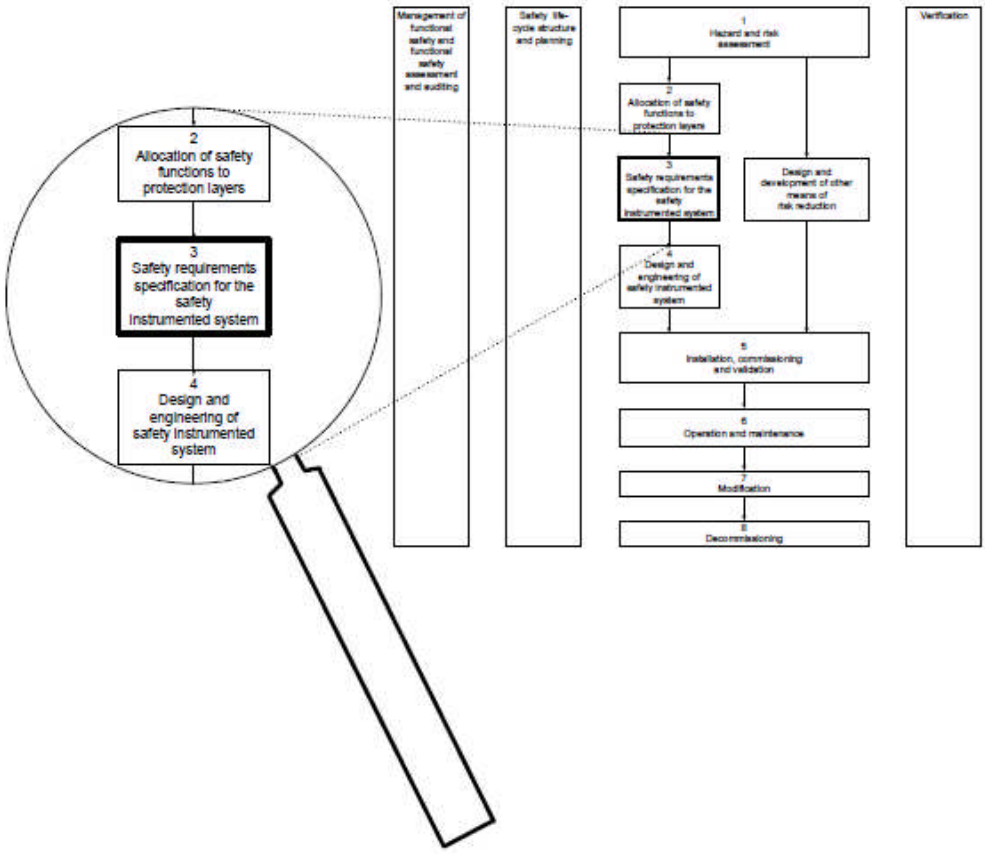

Fig.1 - SIS safety life-cycle phases

The safety requirements shall be derived from the allocation of safety instrumented functions.

Documentation

The requirements regarding the SRS documentation may be developed by the Hazard and Risk Assessment team or the project team.
It is important that the documentation covers all safety aspects to be addressed during the safety lifecycle. The need of documentation depends on the

complexity of the application. Typically, a SIS safety requirements specification includes requirements for:

- design and architecture
- reliability (nuisance trip rate)
- availability (SIL)
- support systems
- installation, testing and maintenance
- hardware specification
- software development, Security
- human machine interface

SRS Personnel

The development of the SRS is an iterative process carried out by e.g. the instrument engineer in co-operation with the plant design team and any associated safety specialists.

SRS Format

The requirements for the SRS format could be divided in three components:

- general requirements
- functional requirements
- safety integrity requirements

The input information and general requirements are applicable on all SIFs included in the SIS. Each SIF must fulfil specified functional requirements and integrity requirements.

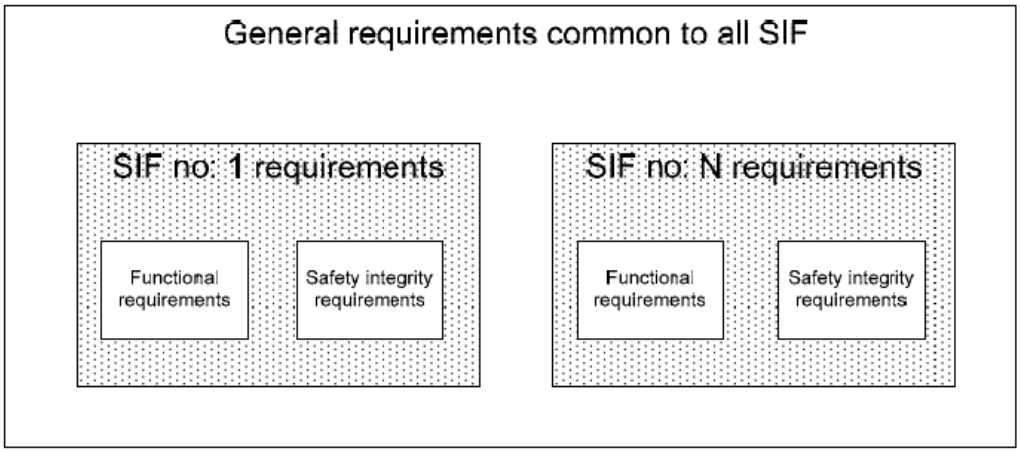

Fig. 2 – Requirements

SRS input information

The safety requirements specification is carried out after SIL selection in the safety life-cycle. In order to create a comprehensive SRS it is important that the required information is accessible for the personnel dealing with the SRS documentation. A typical set of input information includes:

1. Process information and process conditions

   The process itself shall be described in order to give detailed information regarding the process parameters to the personnel dealing with the SRS documentation. Drawings that support the description of the process itself are useful. Later on this process information is important for the personnel dealing with implementation of SIS and SIF. Specific process conditions that are important for the safety must be addressed.

2. Process and hazard report (PHA)

   The PHA report is needed. This report gives valuable information about the hazards and the hazardous events for the intended Safety Instrumented System. Important information are also the hazard frequencies and hazard consequences.

3. Required Safety Instrumented Systems

   A specification of the required Safety Instrumented Systems

4. Required Safety Instrumented Functions

   A specification of each individual Safety Instrumented Function.

5. Target SIL

   The target SIL shall be defined for each SIF.

6. Regulatory requirements

   If there are any regulatory requirements that affect the design of the SIS, the SRS shall include these requirements.

7. Common cause failures

   The possibilities of common cause failures must be taken in account. These failures could reduce or eliminate the redundant safety measures applied in the SIF or SIS. Sometimes it is tricky to find the common cause failures that affect the safety measures. The personnel involved in the design of the SIS or SIF must identify possible common cause failures.

GENERAL REQUIREMENTS

Safe State

The safe state is defined as “state of the process when safety is achieved”. In order to set a process to a safe state the knowledge of the process is very important. In some cases the safe state exists only if the process is continuously running, in other cases the process may have to go through a number of states before the process enters the final safe state.
Actions necessary to achieve or maintain a safe state in the event of detected fault(s) shall be described. The relevant human factors that can affect the safe state shall be taken in account.
The description shall address safe state details regarding process actions needed e.g.:

- sequential shutdown
- which process valve(s) is needed to perform a specific action during the safe state.
- which flows should be started or stopped
- stop, start or continue operation of rotating elements (motors, pumps etc)

Proof Test Intervals

The proof-test interval shall be defined. It is important that the proof-test interval is taken in account during the design of the process application since the proof-test interval affects the design of the application. The proof test idea is to test the function as far as possible. It is more advisable to perform a proof test is when the process (factory) is stopped.
Important activities:

- describe the proof test procedures
- investigate if additional safety measures (monitoring, redundancy etc.) has to be adapted during the proof test interval.
- investigate if human aspects (forgotten bypass etc) could affect the safety during the proof test especially if the consequences could be catastrophic if the proof test goes wrong
- specify the required proof tests during the life-cycle
- the proof test activity shall be documented (the final result of the proof test)

Response Time

The response time requirements for the SIS, to bring the process to a safe state, shall be stated. Parameters that affect the response time are:

a. Process related
   - time constants in the process itself
   - dead time in process response

b. Control system (electrical)
   - time delay in control system
   - the sampling time of the controller

c. Other (mechanical)
   - Inertia
   - Friction
   - Wear

Reset

The reset after shutdown shall be defied.

Spurious trips

Define the maximum allowable spurious trip rate.

SIS Process Measures and Trip Points

Describe SIS process measurements and their trip points. Information regarding the inputs to the SIS, a description of:

- every measurement circuit
- the architecture
- number of inputs
- type of input
- range of measurement
- accuracy of measurement
- trip levels

SIS Process Output Actions

Describe SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves.
Information regarding the outputs from the SIS, a description of:

- every measurement circuit
- the architecture e.g. block and bleed