Life-cycle Management of Safety Instrumented Systems

Dr. Bernd Schroers
Bayer AG, Leverkusen, Germany
University of Aachen, Germany
University of Kassel, Germany
D-51368 Leverkusen, Building 407

Abstract

General

Process and plant safety requires the implementation of a safety management system. IEC 61511 [1] and ANSI ISA 84 define rules for safety management. Every company in the process industry shall incorporate safety management into its corporate goals. A number of integrated management systems already exist, which simplifies the integration of an additional management component. The policy and strategy for achieving safety shall be described together with the methods for evaluating their achievement and shall be communicated throughout the organization.

All persons, departments, organizations or other units responsible for carrying out and reviewing each of the necessary activities involved in the implementation of safety measures (Safety Instrumented Functions, SIFs) in the form of a Safety Instrumented System (SIS) shall be identified and informed of the tasks for which they are responsible.

The core of safety management is the SIS safety life-cycle. The activities that shall be carried out must be defined in a safety planning process. This planning shall be updated as necessary throughout the SIS safety life-cycle and implemented on a detailed level of activity commensurate with the role of the individual or organization in the SIS safety life-cycle. As part of safety planning, the safety life-cycle shall be documented in the form of an SIS safety life-cycle plan.

Generally, the above requirements can be met by companywide regulations describing how and by whom (functional) safety assessments (FSA), design and engineering, maintenance, change etc. of SISs must be carried out, and which internal and external standards apply.
The objectives of the SIS safety life-cycle are:

- to define the phases and establish the requirements of the SIS safety life-cycle activities;
- to define and organize the technical activities into a SIS safety life-cycle;
- to ensure that adequate planning exists (or is developed) to ensure that the SIS meets the safety requirements.

Personnel

Persons, departments or organizations involved in the SIS safety life-cycle activities shall be qualified to carry out the activities for which they are accountable. This expertise can be achieved by internal and external seminars on the subjects of process and plant safety and/or by adequate work experience.

The following items shall be addressed and documented when considering the qualifications of persons, departments, organizations or other units involved in SIS safety life-cycle activities:

- engineering knowledge, training and experience appropriate to the process application;
- engineering knowledge, training and experience appropriate to the applicable technology used;
- engineering knowledge, training and experience appropriate to the sensors and final elements;
- safety engineering knowledge (e.g., process safety analysis);
- knowledge of the legal and regulatory functional safety requirements;
- adequate management and leadership skills appropriate to their role in the SIS safety life-cycle activities;
- understanding the potential consequences of an event;
- the SIL of the SIF;
- the novelty and complexity of the application and the technology.

Persons, departments or organizations involved in the functional safety audit and revision or verification activities, decisions or solutions in the various phases of the SIS safety life-cycle shall be independent and shall not be involved in work on the SIS. This requirement is generally met when there is no organizational link to the project or to the unit. The degree of independence is a question of acceptance by the controlling authorities or other legal institutions. Larger companies can generally meet this requirement by maintaining a central safety department.

Relevant failure types
One of the main tasks of a well-organized SIS safety life-cycle as part of a safety management system is to prevent SIS failures in design and operation. Failures can be either systematic or random. Systematic failures relate to pre-existing faults which occur consistently under particular conditions and can be corrected only by eliminating the fault by modifying the design, manufacturing process, operating procedures, documentation or other relevant factors. The failure rate can usually not be quantified using statistical / probabilistic methods. The majority of failures are caused by human error. If they cannot be prevented by life-cycle procedures (e.g. validation, preventive maintenance etc.), they can be taken into consideration as part of an evaluation of the possible/useful contribution of the layers of protection to the reduction of risk (e.g. by approximating systematic failures as random failures). Examples:

- Incorrect safe position of valve
- Unsuitable inlet material of field devices

The rest of the failures are categorized as random. Random failures occur at random times and are the result of a variety of degradation mechanisms in the hardware. The failure rate can usually be quantified using statistical / probabilistic methods. Within the scope of IEC 61511 random failures are assumed to occur after an exponentially distributed lifetime. Related causes (faults) derive from electronic components, e.g. resistors and capacitors. Wear-out effects are not distributed exponentially but can be approximated exponentially (e.g. electro- and electromechanical components). Examples:

- Analog sensor signal stuck at x%
- Valve stuck in open position

Figure 1: Relevant failure types (qualitative)
Experience has shown that incidents occur in the field of process and plant safety with the following distribution of failures:

- 60% of incidents occur due to deficiencies in hazard identification and evaluation (12+33+15);
- 70% of failures are already present in the system at commissioning (12+33+15+11);
- 34% of incidents can be traced back to human error following the correct identification of a suitable safety measure during HAZOP (23+11);
- only 6% relate to technical failures.

The reduction of systematic technical and organizational failures requires testing and verification in all phases of the managed SIS safety life-cycle.

![Figure 2: Relevant failure distribution](image)

**Engineering**

Nowadays most companies prefer to hire third party contractors to provide engineering services. This approach simplifies the requirement for independence but not the task of verification and validation. A precise task description (contract document/design specification) with all the necessary technical information is the necessary basis for the start of outside engineering work. Otherwise the engineering result will only reveal any inaccuracies in the task description.

A great deal depends on how much of the detail work the customer wants to allocate to contractors. In the end, the customer may gain no new expertise but retains full responsibility.
The interfaces (see Figure 3) between customer and contractor must be well-organized to avoid systematic failures. Audits during engineering work or tracking results may be helpful, but not in the sense of allocating work to external partners. Therefore after the engineering work is completed, the customer must still conduct a full verification of the result.

Figure 3: Safety management system and interfaces (dotted lines)

Especially after installation and/or commissioning, the safety requirement specifications defined and documented in the hazard and risk assessment shall be tested and approved.

**Operation and maintenance**

The engineering phase of an SIS safety life-cycle has the shortest timeline in comparison with the operation phase. The tremendous effort required for the definition, conception, design and SIL verification stands in sharp contrast to the monotonous routine work during the operation and maintenance phase. The need to perform recurring procedures diverts attention and motivation away from safety-related work, although the operation phase is the important period during which the customer acquires increasing experience with the implemented SISs.

Customers are able to improve the statistical preconditions of the SIL verification by collecting failures and failure rates of the implemented safety instruments continuously over the full SIS safety life-cycle. Customers will be able to declare instruments as having a history "of prior use"
if these instruments fulfill certain criteria over a specified number of operating hours (e.g. 100,000 hours per instrument in a single application or 10,000 hours per 10 instruments in similar applications).

All these activities must be carried out as part of a safety management system during the SIS safety life-cycle while normal maintenance, repair and inspections are ongoing. Special effort is required to guarantee verification by independent persons, departments or organizations. A key principle is the 4-eyes-principle in which, for example, maintenance activities are monitored by a second person, department or other organization. In many cases the necessary independence is not available within the maintenance organization. However, the analysis of operation and maintenance activities reported to independent persons, departments or organizations makes it possible to create key performance indicators (KPIs) e.g. for proof-test discipline. These key performance indicators, together with others such as the analysis of proof-test results and the reliability data collected make a good starting point for the independent control of operation and maintenance within a safety management system.

**Documentation**

The backbone of a safety management system is well-organized documentation of all scheduled and unscheduled activities in the different phases of the SIS safety life-cycle. These days, paper documents are being replaced by electronic information compiled in data bases or individual files. Nevertheless the requirement that such information must be easy to locate is at least as strict as for paper documents. No standard document forms are required, merely a set of information gathered in a form such as a Safety Requirement Specification (SRS) or similar document. Of prime importance is the quality of information, which must be:

- unique,
- up to date,
- understandable,
- traceable,
- identifiable and
- immediately locatable.

**Conclusions**

A safety management system controls the SISs safety life-cycles of a process plant. The integration of a safety management system may be simplified if other management systems already exist. Monitoring activities are considered to be independent if independent persons, departments or organizations have their own independent procedures. All verifications and life cycle activities shall be documented to establish the life-cycle management of safety instrumented systems.
Reference