Session 15

Functional Safety Management Systems for Compliant and Efficient Implementation of Safety Instrumented Systems

Edgar C. Ramirez
Safety Systems Business Driver, ABB Inc. (Canada)

Stuart R. Nunns
Principal Safety Consultant, ABB Ltd. (UK)

Abstract

Statistics relating to the performance of major manufacturers are published internationally and incidents, especially those causing injury or death, make headline news. Recent inquiries into major incidents [1,2] have reinforced the importance of international standards IEC 61508 [3] and IEC 61511 [4] as a benchmark of acceptable good practice in the management, design, application and operation of safety-instrumented systems.

In today's world, manufacturers, engineering firms and producers face significant liabilities if they act in a socially irresponsible manner. Such liabilities include direct financial costs arising from the incident itself, from legal costs and fines if found guilty of breaking the law, damages paid to injured parties and damaged reputation, which can have far reaching implications on the business. The result is that safety, profitability and reputation are inextricably linked.

The industry environment can be summarized as follows:

- Increasing dependence on safety critical systems to achieve tolerable risk levels;
- Increasing need to demonstrate that you have achieved adequate levels of safety;
- Safety regulators using international standards as basis of what is reasonable;
- Maintenance of reputation in relation to safety a key business driver;
- Increasing formality of safety culture, management of functional safety, competence of the organization and personal competence.

Within hazardous industries effective risk reduction is sought through the use of safety protections designed and built according to the specific application requirements, and the more general compliance requirements in the Functional Safety standards IEC 61508 / IEC 61511. Compliance to Functional Safety standards is intended, amongst other things, to reduce/eliminate errors during implementation of safety instrumented systems (SIS). SIS consultants, engineering firms, Integrators and customers are responsible for ensuring that safety protection based on SIS are error-free and perform the intended safety functions. While the standards provide guidelines, the actual verification, documentation and validation actions required may not be evident until the

actual proof of compliance is sought. To deal efficiently with such requirements during project execution, a framework comprising organization, competency, resources, planning and implementation of activities required to ensure that functional safety objectives are met should be in place beforehand. Both SIS integrators and customers can be confident that they will fulfill safety integrity requirements when working under a Functional Safety Management System.

1 Introduction

There is growing awareness in the industry for the need to reduce risks and manage safety. In particular the international standards IEC 61508 and IEC 61511 are increasingly being used as a benchmark of acceptable good practice to both demonstrate compliance that (1) the required functional safety has been achieved and (2) that the legal requirements have been met. The adoption of these standards is not surprising given the increasing dependence on safety instrumented systems to achieve the required risk reduction targets. With heightened awareness to contractual rigor and the potential for litigation, should something go wrong, organizations need to demonstrate that their functional safety capability has achieved accepted good practice.

IEC 61508 and IEC 61511 are performance based standards that promote the concept of a safety lifecycle. The supply chain, in respect of a safety instrumented system, covers the specification, design, implementation and operation phases and demands effective functional safety management and competence throughout all phases of the safety lifecycle if functional safety is to be achieved.

The safety lifecycle can span many years in respect of the life of the plant asset and the asset's safety instrumented systems. In particular the safety lifecycle will involve many different organizations and a variety of client – supplier contractual relationships requiring clearly specified responsibilities, activities and deliverables. It is therefore essential that all those organizations involved in implementing phase(s) of the safety lifecycle take all necessary steps to demonstrate their competency and capability to implement the requirements of the relevant clauses of the relevant phase(s) of the standards.

Achieving the necessary organizational capability to effectively implement the requirements of IEC 61508 and IEC 61511 is not an easy task and will require all those organizations in the supply chain that have responsibilities for one or more phases of the safety lifecycle becoming fully conversant with these standards and mapping their areas of responsibilities against the relevant phases of the standards. Many regulatory authorities and process industry operators use, or are likely to use the standards as a benchmark of acceptable good practice and expect those in the supply chain to become sufficiently conversant with the requirements of those standards.

Historically, product certification has been considered a proof of functional safety management, and was originally undertaken to historical standards such as DIN 19250 or VDE 0801 and more recently to IEC 61508. With the wide-spread adoption of the IEC 61508 / IEC 61511 standards coupled with an increased awareness of the need for functional safety management and competency, at both an individual and organizational level, has seen a step change in direction to include the certification of the capability of an

organization to undertake specified functional safety activities. This would include the organization's functional safety management arrangements and procedures together with the organization's competence management system which would embrace personal competence in respect of the specific duties an individual has to perform.

Until now the development and implementation of functional safety management systems has taken place mainly within safety system vendor's organizations. However, it needs to be embraced by all organizations spanning the safety lifecycle and, in particular, end users who need to provide evidence to their regulatory authorities as a result of regulatory inspections/audits or in support of safety cases.

2 Risk reduction through compliant safety instrumented systems

The main objective of safety protective mechanisms is to achieve a determined level of risk reduction. In the case of safety instrumented systems this is sought by the specification of the safety instrumented functions and their associated safety integrity levels followed by the design and engineering of these safety instrumented functions so as to place and/or maintain processes in a safe state when demanded to do so [4].

The risk reduction capabilities of safety instrumented systems are measured in terms of their safety integrity[1]. The Safety Integrity Level (SIL) is required to be proportional to the risk that needs to be reduced. In IEC 61511 the requirements to achieve safety integrity are presented in clause Part 1, clause 11 "SIS Design and Engineering", and Part 1, clause 12 "Requirements for application software, including selection criteria for utility software".

SIS design and engineering activities include selection of the SIS logic solver components and field devices integrated into safety instrumented functions to fulfill safety integrity requirements. The SIS components need to satisfy both the hardware safety integrity and systematic integrity requirements.

It has been reported that an important contributory cause for failure of control systems is the improper selection of equipment based on its (claimed) safety integrity. The reasons for failing to select and use the proper equipment have largely been attributed to errors during specification, design or engineering [6]. There is, also unfortunately, a perception that in order to meet the target SIL for a safety instrumented function all that is required is the Probability of Failure on Demand (PFD) of the dangerous random hardware failures!

Hardware safety integrity requirements include various performance requirements such as system behavior on detection of a fault, PFD, and others. Some of these requirements are fulfilled by products tested and certified by internationally recognized bodies. For instance, SIS logic solver and instrumentation vendors are expected to demonstrate certification of their performance per standard IEC 61508. However such products have to be integrated, programmed and operated using interfaces to other systems,

[1]Average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a period of time [4]

communications, operations and maintenance facilities which constitute the safety instrumented systems. Thus the safety integrity requirements are extended to include SIS design and engineering activities and not only to products.

Application software development is discussed at length in IEC 61511 Part 1, Clause 12, due to the possibility for it to become a '*door to failures'* caused by errors. As in the case of other engineering activities, software errors may result in failures in the operation of the safety instrumented system. The use of application software coding techniques for reduction of faults, and the inclusion of verification stages are some of the IEC 61511 compliance requirements intended to help prevent software errors.

Problems during maintenance and modification activities have also been found to be important contributors to failures of control systems leading to serious incidents [6]. Procedures and facilities for the proper operation, maintenance, and modifications are an output from design and engineering of safety instrumented systems which need to be incorporated into the end users operations and maintenance regimes.

In summary, IEC 61511 requires mechanisms to be in place to prevent and detect errors during SIS design, engineering, and application software development. The ultimate intent is to prevent those errors from causing failures of the safety-related systems during their operation.

2.1 Compliance as a way to reduce systematic failures

Systematic failures[2] of safety-related systems can be caused by human errors during specification, design or engineering. An example of systematic failure causes are errors in software development. The effects of systematic failures depend on the phase where they are introduced [3], and can prevent effective risk reduction.

Systematic failures are especially relevant considering the many published reports of the high incidence of control system failures due to errors during specification and engineering.

It can also be difficult to demonstrate that systematic failures have been prevented – especially if there were no initial provisions to this end and the design or engineering activities have been completed! Therefore the best way to deal with them is to plan to use techniques or measures as a means of prevention.

Some of the recommended measures to avoid or control systematic failures during SIS design and engineering can be found in IEC 61508-2 Table B.2:

- Observance of guidelines and standards
- Documentation
- Structured design

[2] Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors [4]

- Use of well tried components
- Checklists

Compliance with the functional safety standards IEC 61508 / IEC 61511 is one bench mark that has been recognized within the global safety market to achieve safety integrity in safety instrumented systems. However one issue that remains is how to operate efficiently whilst maintaining compliance with functional safety standards given the need to implement more specific activities than for standard process control applications?

3 Compliant and efficient implementation of SIS?

Compliant safety instrumented systems require additional activities over and above those used for control systems, focused on ensuring that the required safety integrity is achieved and maintained. If numerous SIS projects are to be executed by an organization it very soon becomes evident that efficient execution requires an appropriate organizational infrastructure. Within this infrastructure, several elements need to be aligned and managed: competent personnel, relevant supporting resources such as templates, databases, development tools, methods and procedures, and an engineering and design framework should all be put in place to allow for subsequent projects to take advantage of previous work and experience.

The operation and maintenance of safety instrumented systems need to be managed and supported throughout the safety lifecycle to ensure that safety integrity is maintained to achieve the risk reduction targets.

In the next section a Functional Management System implemented to achieve safety integrity during safety instrumented systems project execution is described.

3.1 Safety Lifecycle

The safety lifecycle[3] concept presented in IEC 61511 is a mechanism that helps maintain consistency and focus on safety integrity through the life of safety instrumented systems. The relevance of the safety lifecycle resides in the permanent window it provides to visualize and plan for the activities that are needed to maintain safety integrity.

Definition of a safety lifecycle is a compliance requirement during SIS projects.

During the safety lifecycle definition the SIS projects technical activities are organized into phases that refer to the different project stages. For each phase the required inputs and outputs, technical activities and verification activities need to be defined. Planning of the means to complete technical activities and achieve the SIS safety requirements for each phase leads to selection of relevant criteria, techniques, measures and procedures. Many of the Quality Management System processes can be used in the safety lifecycle model.

[3] Necessary activities involved in the implementation of safety instrumented functions occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use

The development of the SIS safety lifecycle for specific projects can be done by mapping the relevant phases of the IEC 61511 safety lifecycle (Figure 1). Process operators need to consider most of the phases in the lifecycle, while SIS integrators need to be concerned mainly with the phase related to SIS design and engineering (e.g. Phase 4).

Due to the criticality of the development of SIS application software, IEC 61511 requires that a safety lifecycle is defined for application software development and integrated to the SIS safety lifecycle to ensure that requirements are satisfied. For each phase in the software lifecycle the inputs, objectives, activities, and outputs are to be defined. This in turn allows for verification of each (sub) phase, also a requirement.

The adoption of the safety lifecycle model can contribute to a reduction in effort when subsequent SIS projects are executed without comprising on functional safety.

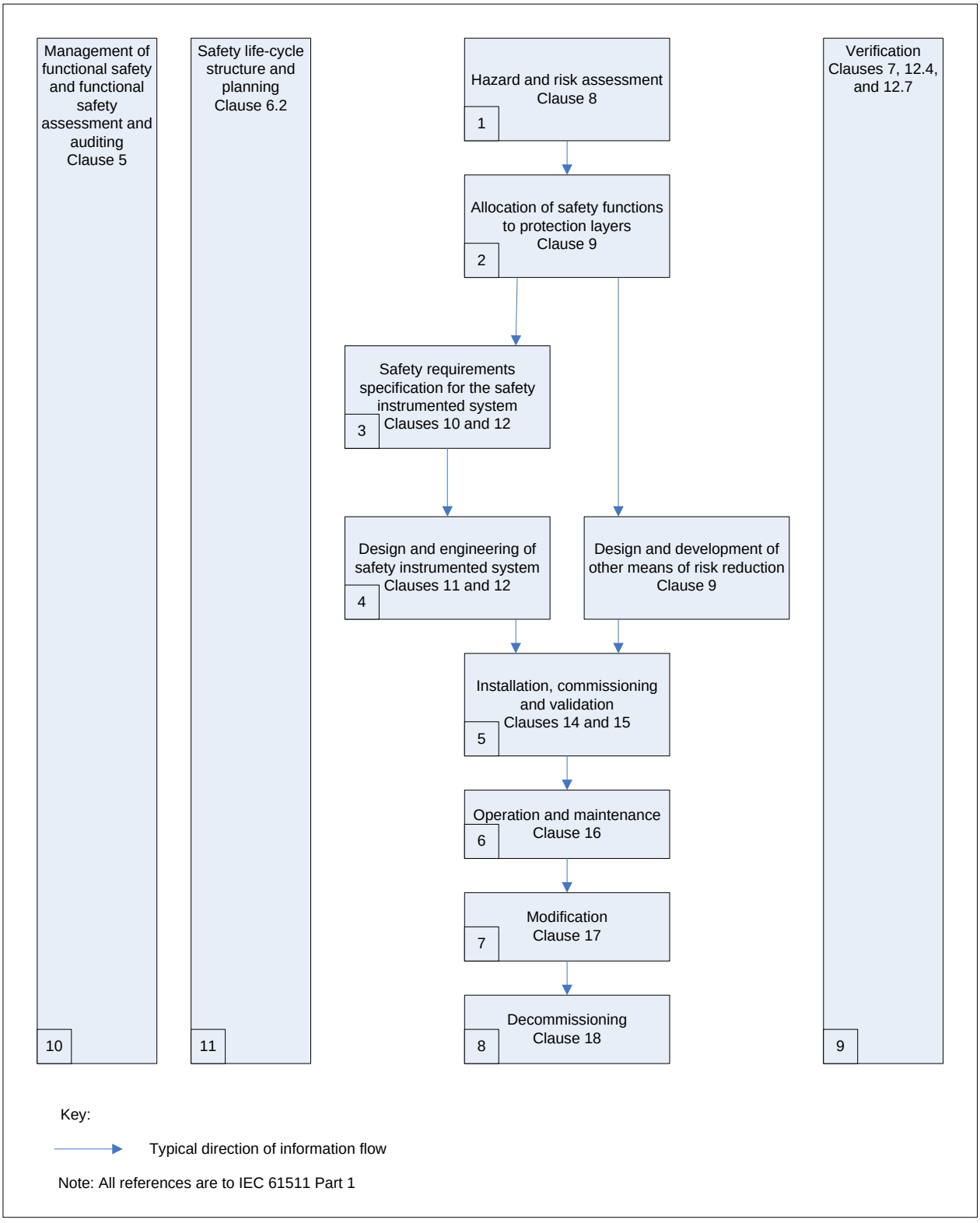


Figure 1. IEC 61511 SIS Safety Lifecycle

3.2 Competency requirements

One of the requirements for organizations that wish to execute SIS projects is to ensure that competent personnel are assigned to take responsibility for the various activities in the safety lifecycle.

Competency requirements include training, knowledge, qualifications, and experience adequate for the tasks defined. Formal descriptions of personnel competency requirements and evidence of personnel qualifications need to be available as part of the SIS design and engineering information. Specific processes to manage competence requirements are and integral part of the Functional Management System, to ensure compliance and to make this process available for use on subsequent projects.

3.3 Realization of technical activities

The SIS safety lifecycle phases summarize the technical activities required from hazard and risk assessment to decommissioning of the SIS. For instance, SIS design and engineering - IEC 61511, Phase 4 activities include a functional design description, application coding, factory acceptance tests, and others. Management of the activities and resources is needed to ensure that the functional safety objectives are met [4].

The overall effort to secure competent resources, generate procedures, produce documentation, and accomplish all activities required for SIS projects is usually more than the effort required for implementation of similarly sized non-safety related control systems. In corporations that engage repeatedly in SIS projects it can be very advantageous to create a framework management system that encompasses the safety lifecycle, procedures, methods, techniques, and documentation required. This set of resources is denominated a Functional Safety Management System (FSMS).

An essential initiator is senior management commitment.

Functional Safety Management Systems are in use in organizations where the following benefits have been observed:

- Demonstration of due diligence
- Establishing an efficient, repeatable safety management system
- Reduction in pre-contract discussions
- Reduced time for proposal preparation
- Best in class performance

The above are relevant for SIS consultants, EPCs, integrators and users. Certification of the FSMS by an accredited third party is a good measure to find inconsistencies and ensure that the overall framework is compliant with the functional safety standards.

As industry becomes more mature in its understanding of IEC 61508 / IEC 61511 and the specific details of what product compliance means, it is apparent that many claims currently being made for the achievement of SIL of a product will not meet the full requirements of the standard in respect of:

- The requirements for hardware safety integrity comprising:
  - Architectural constraints; and,
  - Probability of dangerous random hardware failures
- The requirements for systematic safety integrity comprising:
  - The avoidance and control of systematic failures; or,
  - Evidence that the equipment is “proven is use”

3.4 Functional Safety Management System for SIS Integrators

As an example consider the case of implementation of an IEC 61511 compliant functional safety management system for a SIS Integrator.

The safety lifecycle for the SIS integrator is typically focused on the SIS design and engineering activities - Phase 4 in the IEC 61511 SIS safety lifecycle. Other aspects covered in the SIS safety lifecycle which are relevant for SIS integrators include management policy and commitment, competency, management of change, verification, validation, functional safety assessments and audits.

The following steps were taken during implementation of the Functional Safety Management System:

1. Secure senior management commitment, internal funding and resources

2. Benchmark current practice. A gap assessment of the existing safety management system against the requirements of IEC 61511.

3. Development of the safety lifecycle. A safety lifecycle model was developed mapping the relevant phases and activities of IEC 61511 against those of the system integrator. The lifecycle considered and utilized the existing certified Quality Management System. See the safety lifecycle model in Appendix 1.

4. Establish individual competencies. The intent was to ensure that personnel with responsibilities in safety-related projects have training, knowledge, experience and qualifications appropriate to the tasks for which they are responsible. Competency databases are used to record and provide the competency profiles and data of all personnel.

5. Development of procedures, templates, and documentation framework used to execute the technical activities in the safety lifecycle. This set of documents and resources was denominated the Functional Safety Management System (FSMS).

When this FSMS was first implemented by the organizations project execution group, its implementation was independently validated, audited and assessed.

Some of the efficiencies derived from the implementation of the safety lifecycle and the Functional Safety Management System include:

- The creation of procedures reduces the design effort for future projects.
- Documentation templates reduce documentation generation times
- After initial validation of the FSMS resources, future projects have reduced needs for validation of procedures and documentation.

In addition to the compliance and efficiency benefits, this SIS integrator choose the option to achieve certification by an accredited third party based on the compliant FSMS and evidence of its use on projects.

The use of the FSMS is a proven approach to comply with IEC 61511 requirements for SIS integrators. While there are several ways to achieve compliance on projects, the formal use of a certified lifecycle and FSMS promote efficiency and consistency for future projects.

The benefits of certification of an organization's FSMS are:

- Providing independent assurance that the organizations FSMS has achieved accepted good practice;
- Limiting the risk exposure to potential liabilities;
- Demonstrating due diligence;
- Professionalism;
- Establishing an efficient, repeatable safety management system (procedures, techniques, tools etc);
- Reducing unnecessary pre-contract discussions (a benefit to all parties)
- Cost effective proposals;
- Reducing requirements for bespoke project safety procedures;
- Gaining a competitive advantage.

The Functional Safety Management System scheme described has been implemented by several ABB units globally. After implementation of the FSMS its framework became the main mechanism to ensure compliance to functional safety standards during SIS project execution. It has also enabled certification by accredited third party bodies.

4 Functional Safety Management Systems for Process Operators

Process operators have the responsibility to ensure that safety instrumented systems maintain their safety performance over the life of the process plant/asset.

A Functional Safety Management System should therefore be implemented by process operators to provide the support framework for execution of their activities in the SIS safety lifecycle. Furthermore, current industry models for project execution are such that different parties (e.g. risk consultants, EPCs, SIS integrators, etc.) take execution responsibility for different phases in the safety lifecycle, contributing to SIS implementation in support of process operators who have the overall responsibility. Indeed all parties would benefit with the use of FSMS, just like QMS are a standard requirement for all.

Process operators need to have visibility and control over the whole SIS safety lifecycle. For example the plan and programme for functional safety assessments. There are advantages provided by compliance and the potential to improve efficiency in SIS implementation when having a repeatable process that leads to compliant safety instrumented systems. For instance, during execution of a phase such as “safety requirements specification of the SIS” (see phase 3 in Figure 1) the safety requirements specification document would be available as a template whereby the safety instrumented functions would be described according to inputs from the previous phase (e.g. phase 2, Allocation of Safety Functions).

Such reuse of engineering procedures and documentation leads to more efficient use of resources. There may also be significant potential for efficiencies for process operators that deploy and operate many safety instrumented systems as part of their continuous operations.

Management commitment is of course very much needed to ensure that the FSMS is developed and adequately maintained/modified should there be changes to international, national or corporate standards and regulatory requirements.

Functional safety management systems can help process operators achieve functional safety beyond the implementation of a SIS. Effective safety protections need to be engineered, operated and maintained according to functional safety requirements.

- Safety protections need to be validated after construction to ensure that they meet risk reduction requirements

- Operation and maintenance of safety protections, including proof testing regimes, need to ensure that safety integrity is maintained

A FSMS can provide some of the detailed definitions needed to achieve and maintain safety integrity of instrumented functions, which are one among the various types of safeguards used in processes.

Within the process industries there are increasingly more cases of process operators that are implementing functional safety as part of an overall process safety management scheme. Some of these cases have been observed among chemical and oil & gas companies that have a record of compliance and adherence to functional safety standards, plus some cases of companies that are adhering to functional safety requirements recently. Some of the initial results indicate that the FSMS and SIS implemented are considered defendable and best practices that are planned to be used in other sites.

In one of the cases observed a corporate manager promoted and is overseeing implementation of a Functional Safety Management System in the corporation. After a first project other projects are also being executed under the FSMS approach. An initiative to use the FSMS on a corporate level provides support for future projects.

In a second case a SIS and functional safety management were implemented as part of a project. However there is no commitment yet to implement the FSMS in the corporation. In this situation the responsible personnel, the implemented SIS and supporting procedures are more isolated in the

organization and there exists the risk that as time passes the safety integrity requirements are left behind.

6 Summary

The use of safety instrumented systems compliant with functional safety standards is widespread and recognized as the best practice when instrumented safety protections are required. Most attention is paid to SIS hardware requirements but industry reports show that errors in design and engineering activities have significantly contributed to failures leading to incidents. SIS engineering and design also need to be compliant with IEC 61511 requirements to ensure that the risk reduction targets are accomplished.

The framework provided by a SIS safety lifecycle and a Functional Safety Management System help implementing compliant SIS. Efficient implementation is enabled for organizations that need to build several SIS.

Senior Management commitment is fundamental for implementation of a FSMS. There needs to be understanding and acceptance of the obligations that the corporations will undertake. The benefits that can be obtained should outweigh initial reservations.

References

1. "Recommendations on the design and operation of fuel storage sites"; Buncefield Major Incident Investigation Board

2. "The Report of the BP US Refineries Independent Safety Review Panel" (concerning the Texas City incident).

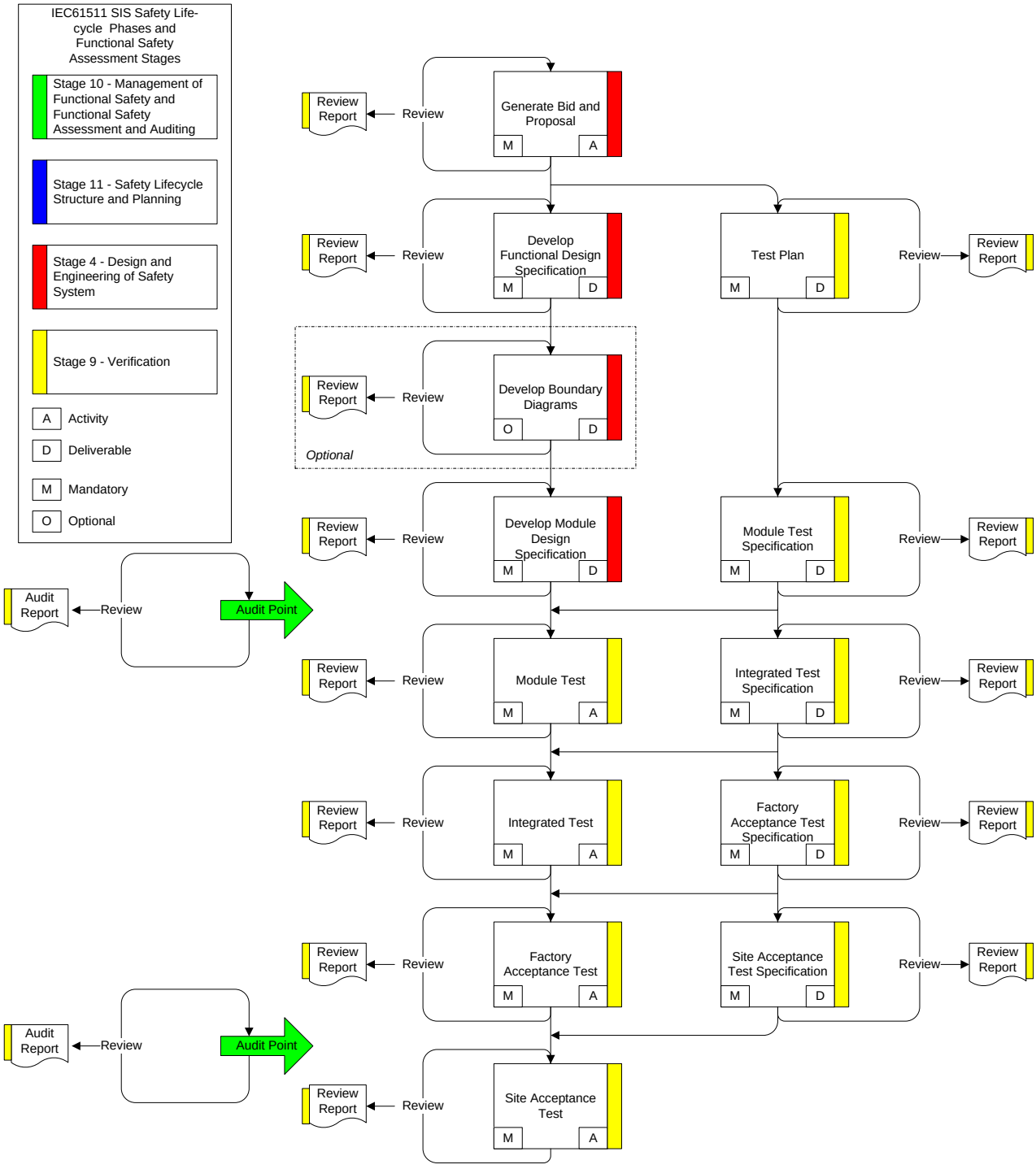
3. International standard IEC 61508. Functional safety of electric / electronic / programmable electronic safety – related systems. Parts 1 – 7.

4. International standard IEC 61511. Functional safety – Safety instrumented systems for the process industry sector. Parts 1 – 3.

5. Nunns S.R., Prew R., Achieving organisational functional safety certification to IEC 61508. ABB Review, 2007

6. Health and Safety Executive, Out of Control – Why control systems go wrong and how to prevent failure, 2003.

Appendix 1 Safety Lifecycle Model for ABB Safety Execution Centres



Appendix 1 Safety lifecycle model for ABB Safety Execution Centres (continued)