ELSEVIER

Journal of Hazardous Materials 130 (2006) 28–32

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

# IEC 61511 and the capital project process—A protective management system approach

Angela E. Summers *

*SIS-TECH, 12621 Featherwood Drive, Suite 120, Houston, TX 77034, USA*

Available online 24 October 2005

**Abstract**

This year, the process industry has reached an important milestone in process safety—the acceptance of an internationally recognized standard for safety instrumented systems (SIS). This standard, IEC 61511, documents good engineering practice for the assessment, design, operation, maintenance, and management of SISs.

The foundation of the standard is established by several requirements in Part 1, Clauses 5–7, which cover the development of a management system aimed at ensuring that functional safety is achieved. The management system includes a quality assurance process for the entire SIS lifecycle, requiring the development of procedures, identification of resources and acquisition of tools. For maximum benefit, the deliverables and quality control checks required by the standard should be integrated into the capital project process, addressing safety, environmental, plant productivity, and asset protection.

Industry has become inundated with a multitude of programs focusing on safety, quality, and cost performance. This paper introduces a protective management system, which builds upon the work process identified in IEC 61511. Typical capital project phases are integrated with the management system to yield one comprehensive program to efficiently manage process risk. Finally, the paper highlights areas where internal practices or guidelines should be developed to improve program performance and cost effectiveness.


*Keywords:* IEC 61511; Safety instrumented systems (SIS); Management system; Functional safety; Competence; Verification; Functional assessment; Configuration management; Auditing

## 1. Overview

The chemical industry has made great strides over the last 20 years toward improving process unit performance and safe operation. This improvement has been gained through a variety of approaches aimed at identifying and managing risk. Many countries (e.g., United States of America, the United Kingdom, Germany, and The Netherlands) have regulations concerning the management of process risk. Although each country has named the program differently, the concept of process safety management is well known. Over the last 20 years, the chemical industry has made significant investment in personnel, adding resources and specialized training, and in physical systems, adding protection layers to minimize risk.

The management system required in IEC 61511 [1], Clauses 5–7 uses a generalized framework, which integrates the various process safety management approaches that have been used successfully throughout the world. Proper planning and management of safety instrumented systems (SIS) will obviously improve process safety. One of the most exciting aspects of the standard is that its management system is very applicable to other protection layers. In fact, many companies have been applying this process to other instrumented systems for many years and have seen significant economic benefit, especially when applied to asset protection systems [2].

Economic benefit can be gained from appropriate investment in instrumented systems. It is now time to look beyond simple compliance with regulations directed at protecting workers, the community, and the environment. Many

* Tel.: +1 281 922 8324x14; fax: +1 281 922 4362.
*E-mail address:* asummers@sis-tech.com.
*URL:* www.sis-tech.com.

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.063

companies have long understood the importance of the assessment of business risk, process reliability, and process operability. Consequently, this paper will provide the framework for a generalized protective management system.

## 2. Requirements for an effective protective management system

The protective management system is applicable to the full lifecycle of any instrumented system used to mitigate process risk. Internal practices are developed to define the design and engineering requirements for the various classes of instrumented systems, such as basic process control systems, critical alarms with operator response, and protective instrumented systems, especially safety instrumented systems. The overall work process is based on the IEC 61511 lifecycle and includes the additional steps required for the non-SIS. Fig. 1 shows the work process and the following project phases that are covered by the protective management system:

- Hazard and risk analysis—perform hazard and risk analysis to define required functionality and integrity for each protective function and allocate each protective function to a protection layer.
- Design basis—develop a specification to achieve the required functionality and integrity while meeting plant targets for reliability, maintainability, and operability.
- Engineering, installation, commissioning, and validation—complete protective function implementation following design basis.
- Operating basis—define what is required to maintain safe operation for all operating modes, including start-up, normal operation, abnormal operation, and shutdown.

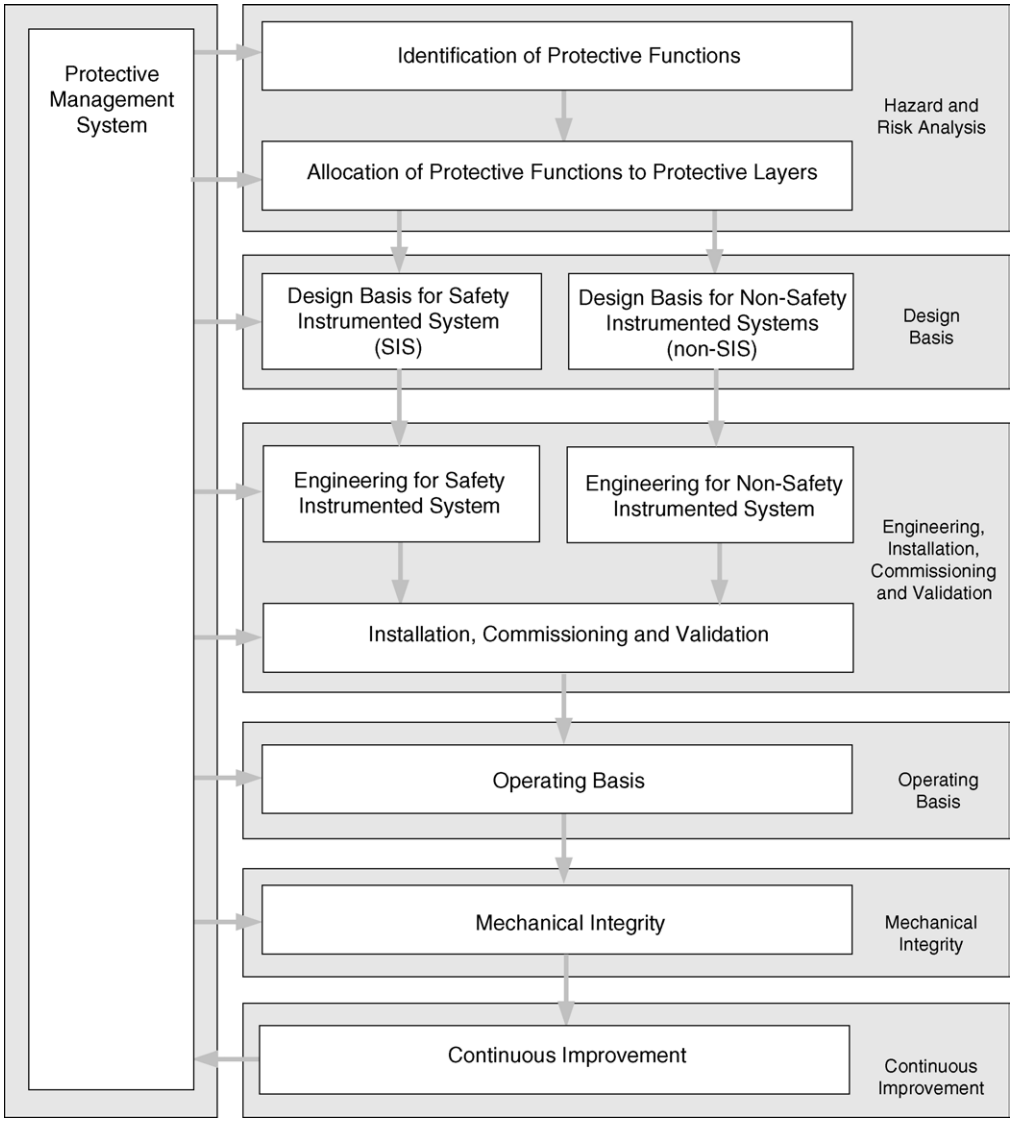


Fig. 1. Overview of the protective management system showing project phases.

- Mechanical integrity—test and inspect installed equipment to ensure that it functions as intended and that it achieves the target integrity and reliability.
- Continuous improvement—review data collected during the hazard and risk analysis, plant operation, and maintenance activities to determine whether changes are needed to maintain or improve protective functions.

Each phase is supplemented with internal guidelines and procedures to ensure compliance with the company's risk management philosophy, to support project engineering and on-going plant maintenance, to serve as a training tool, and to capture lessons learned.

The management system, therefore, is intended to:

- Define an engineering approach to prevention of process incidents, especially those that involve the release of hazardous chemicals or significant damage to equipment.
- Outline the essential criteria for the various decision-making processes that occur throughout the life of a process unit.
- Provide a clear definition of risk criteria in terms of safety, environmental, and economic protection.
- Incorporate process reliability goals, allowing a balance between process risk mitigation and process reliability.
- Identify key resource needs, whether expertise, skills, knowledge, tools, or work process-based, to ensure the resources are available during the execution of normal day-to-day tasks, as well as for capital projects. The identification of key resources ensures effective employee involvement in the management system.
- Outline the general work processes and deliverables that are required to properly manage risk.

The protective management system will be different at each company for many reasons, including variations in safety culture, resource loading, process age, and personnel experience. Fig. 2 shows the delicate balance that must be sought between the management system and site personnel capability. The horizontal or "*x*-axis" is the degree of rigor applied in the management system. The far left would represent no written management system, while the far right would represent a highly prescriptive system. The vertical or "*y*-axis" is a measure of the site personnel capability to manage the risk themselves. The bottom corner would represent little experience/training on the activities necessary to achieve safe and reliable operation. The top corner would represent a high level of understanding, where a high percentage of people know exactly what they need to do.

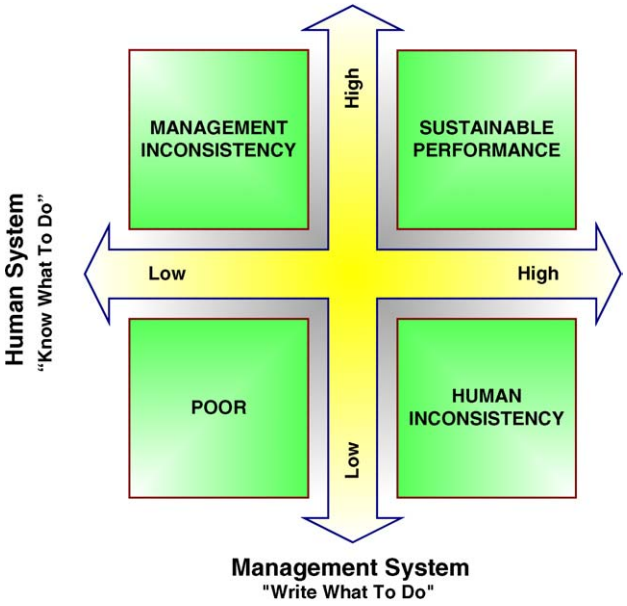


Fig. 2. Consistency of performance related to human systems and management systems.

The diagram is divided into four quadrants that are explained in Table 1. All of the quadrants except the one labeled "sustainable" represent a combination of skill and documented processes that often yield inconsistent performance with relation to the implementation of protection layers. Sustainable performance is achieved when important work processes are documented, personnel are trained on the work processes, and compliance is expected and audited.

## 3. Specific topics

Various policies, practices, and procedures must be developed to support the protective management system. The degree of management system rigor should be sufficient to support the required performance of each protective layer. For example, the modification of a safety instrumented

Table 1
Achieved performance within the labeled quadrant

| Achieved performance (label) | Explanation |
|---|---|
| Poor | Personnel experience is low and there are few documented requirements. |
| Management inconsistency | High level of fundamental understanding among personnel, yet there are few documented requirements. Performance is uncertain, because staff turnover could result in the loss of internal practices. |
| Human inconsistency | The management system is highly prescriptive, but personnel are not trained on it and have difficulty understanding and implementing it. Performance is uncertain, because the inconsistent application of the management system may cause many problems. |
| Sustainable performance | Personnel understanding of the principles behind safe and reliable operation is high and the work processes are documented to maintain consistency of implementation. |

system will often be covered by a more rigorous management of change procedure than a protective instrumented system installed to protect against asset risk only. The following provides an overview of six key topics that should be addressed for each protective layer:

- competence of individuals;
- verifications;
- functional assessments;
- configuration management;
- auditing;
- requirements for independent resources.

### 3.1. Competence of individuals

The personnel responsible for various protective management system activities must have the fundamental education and experience necessary to perform their assigned responsibility. Personnel should be trained in the work processes associated with the protective management system and they must understand how to execute the tasks that are assigned to them. This ensures that operators, maintenance personnel, process engineering, I&E engineering, and project management personnel understand what is expected of them or how their actions affect the operation of the IPS.

As procedures are developed to support the protective management system, key skills and knowledge considered important for the execution of the work processes and procedures should be identified. These procedures can be used to retain essential information, which is often kept informally by key individuals, within the organization. When staffing resources change, procedures are often the only means of communicating the requirements and activities.

When project assignments are made, the required skills and knowledge should be compared to the individual's capabilities. Lack of necessary, specific experience should be addressed through training or mentoring programs. Competent trainers and mentors should be identified and formally assigned to monitor project or plant personnel activities, as necessary. Specialized training should be considered, as necessary, to focus on responsibilities and activities at the discipline or department level.

### 3.2. Verification

Verification activities are quality control checks typically conducted by alternate members of a project team, department, or company. Documentation should be comprehensible and prescriptive enough for all personnel to understand. Anyone responsible for a verification activity should have sufficient skills and experience to review the information collected and documentation generated to ensure work is consistent with expectations. For SISs, verifications would be performed during the execution of each work process step shown in Fig. 1.

The degree of documentation review and the number of required verifications depends on the scope of work, including the protection layer complexity, personnel familiarity with the hardware and software systems, and the expertise of the project team members.

### 3.3. Functional assessment

IEC 61511 recommends that functional safety assessments be executed at five stages of the SIS lifecycle. The Stage 3 assessment, which is after installation, commissioning, and validation but prior to the introduction of hazards into the process, is required by IEC 61511 and overlaps with the pre-start-up safety review that is required by many countries, including Germany, the United Kingdom, and the United States.

Functional assessments should be considered at similar transition points in the protective management system to verify completion of the following phases: (1) design basis; (2) engineering; (3) installation, commissioning and validation; (4) operation basis; (5) modification. These assessments are essentially quality control checks intended to reduce systematic errors by assessing available information and documentation against the original design premise.

The degree of independence of the assessor is typically based on the complexity of the function and the integrity requirement. For safety instrumented systems, at least one person should be assigned to the assessment team who has experience in hazard and risk analysis, inherent safety, process safety and SIS design, operation, and maintenance. This person should be independent of the project team and obtain operations' and/or management approval of the assessment team's findings, i.e., that the found risk is tolerable to the company.

Deficiencies discovered during the functional assessment should be prioritized and remedied in a timely manner. The prioritization often varies dependent on the process risk, required engineering time, and opportunity for access to the equipment.

### 3.4. Configuration management

Controlling configuration at this level requires not only a detailed procedure, but also the expertise to make the replacement-in-kind assessment. For example, when a replacement transmitter is purchased, it is likely that the software, and perhaps even, the hardware have been modified. The transmitter may have the same root model number, but the version has changed. The original transmitter may no longer be available, but the manufacturer has a recommended substitute. Configuration management requires a knowledgeable person to review the changes associated with the transmitter to ensure that these changes will not affect the functionality, integrity, or reliability of the device in the installed application. This review includes assessment of the transmitter itself and assessment of the devices that the transmitter is

connected to, especially those devices that are relying on a signal from the transmitter. Manufacturers can assist with this assessment by reporting how changes to the device affect the functionality, integrity, or reliability.

### 3.5. Auditing

After the protective functions have been turned over to plant operations, an audit should be conducted to verify that the installed equipment is performing as intended during operation and that the procedures are understood and being used consistently. The initial audit should be conducted within a short period of time after project completion to gather lessons learned and to finalize the update of the operating and maintenance procedures. Then, audits should be conducted at a frequency established by the owner/operator based on the protective system complexity, the required integrity, and the number of changes made to the protective system. The audit frequency should also take into account the site safety culture. Those sites that show poor performance related to the protective management system should be audited more frequently to serve as a focal point for compliance improvement.

### 3.6. Requirements for "independent" resources

Throughout the life of the protective systems, verifications, functional assessments, and audits will be performed. At times, independence of the reviewer from the project team, unit management, plant management or facility management should be considered to ensure the practices being used are appropriate for the required risk reduction.

As previously stated, verifications generally involve review of project documents by an alternate member of the project team, department, or company, who has an overall understanding of the requirements. Verifications evaluate the consistency of the input (scope) documents and the output (deliverables). Project documents are reviewed to determine whether the scope for the specific work process step was met, e.g., does the engineering design package meet the established design basis.

In contrast, functional assessments are higher level reviews of the overall risk management strategy being implemented at the completion of a major project phase (e.g., front-end loading or detailed design) to determine whether it is consistent with the hazard and risk analysis and operational needs. Likewise, audits determine whether the practices and procedures documented in the design and operating basis are appropriate for the process risk. Functional assessment and audits often involve an independent reviewer, i.e., someone who is not part of the project team and does not report to project team management. This independent reviewer can be an employee of the company or a contracted third-party, as long as the reviewer understands the process hazards, the protective management system, and the fundamentals of appropriate design, installation, operation, maintenance, and testing.

## 4. Why a protective management systems makes good business sense

Protective management systems make good business sense, because they are the most efficient way to achieve consistent, predictable results from the process unit. An effective management system uses a systematic approach to manage the entire protective layer lifecycle. Most companies have policies and procedures already in place for many of the lifecycle phases. The purpose of the overall system is to tie all of these policies and procedures into a comprehensive program that streamlines the processes and eliminates duplication of effort.

Using this approach, the process design, protective layer design, operation, and maintenance procedures, training program, change management, and continuous improvement activities are considered appropriately at each stage of the project lifecycle and the operating process life. When the management system incorporates quality control checkpoints, verifications, and validations, the owner/operator has greater assurance that the design and construction of the process achieves risk management goals and regulatory compliance. Thus, the implementation of a management system should have a positive effect on the process operation and offer significant benefits to owners/operators.

Achieving safe and reliable operation requires resources to create a sustainable management system, to audit performance, and to initiate improvement in the management system or in personnel training, when necessary. It requires commitment from the top to provide the resources necessary for the effort and commitment from the bottom to make it work.

For more information on Protective Management Systems, look for "*Guidelines for Designing Safe and Reliable Instrumented Protection Systems*" Spring 2006 from the Center for Chemical Process Safety [3].

## References

[1] International Electrotechnical Commission (IEC), IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Sector, Geneva, Switzerland, 2003.

[2] Instrumentation, Systems, and Automation Society (ISA), IEC 61511, ISA TR84.00.04, Guidelines on the Implementation of ANSI/ISA 84.00.01-2004, Research Triangle Park, NC (2005).

[3] Center for Chemical Process Safety, American Institute of Chemical Engineers, Project #159 Book, Guidelines Designing Safe and Reliable Instrumented Protective Systems (tentatively titled, anticipated publication date Spring 2006).