1

INTRODUCTION

Instrumented Protective Systems (IPS) implement protective functions that detect abnormal or unacceptable operating conditions and take action on the process to achieve or maintain a safe state. IPSs are used to reduce the process risk associated with health and safety effects, environmental impacts, loss of property and business interruption costs.

Safe operation cannot be achieved in isolation. The risk reduction strategy must also consider the owner/operator's business needs. Personnel are expected to operate process units to achieve target production rates, product quality, and cost performance. Balancing safety and production goals can be challenging when the IPS design and management does not adequately address the operational needs. The following can add significantly to this challenge:

- High initiating cause frequency results in frequent loss of control and process shutdown,
- High frequency of spurious IPS operation leads to:
  - Lack of trust in the IPS (leading cause of improper bypassing)
  - Frequent process equipment shutdown with subsequent process unit impact
  - Frequent process unit start-up which may have significant inherent risk
- High frequency of IPS equipment failure results in high operating and maintenance costs,
- Ignoring functionality requirements leads to an IPS design which does not adequately support the various process operating modes and potentially causes excessive IPS equipment bypassing, alarms, and shutdowns, and
- Ignoring maintainability requirements leads to inadequate maintenance resources and facilities and potentially failure of the mechanical integrity program.

It is well understood that plant productivity and operability improves when quality control processes are applied to process equipment operation. Given the potential problems associated with IPS implementation, it simply makes sense to apply the same quality control processes across the IPS lifecycle.

Quality control processes rely on the use of appropriate metrics to verify compliance with the work process expectations. For IPS design and management, these metrics are associated with core attributes that are considered essential for an instrumented safeguard to be classified as an IPS. Seven core attributes should be achieved by the IPS design and supported by appropriate management practices:

1. Independence,
2. Functionality,
3. Integrity,
4. Reliability,
5. Auditability,
6. Access security, and
7. Management of change.

These core attributes are periodically assessed to determine the degree to which they are being maintained and improved. Quality control processes, such as verification, assessment, auditing, and validation, are necessary to ensure the required attributes are achieved throughout the IPS life. The level of rigor employed in the quality control limits the performance which can be reasonably achieved by the IPS.

IPS implementation and continuous improvement involve the effort of many stakeholders, e.g., management, process safety, process, instrumentation and electrical, operations, maintenance, and manufacturers. Projects are often iterative processes requiring careful consideration of each discipline's needs and the core attributes.

This guidelines book intends to:

- Clarify the essential role of the various personnel responsible for IPSs,
- Establish a protective management system framework for IPS design and management,
- Provide the work processes to be followed for IPS development from risk assessment through its implementation and transfer to operations,
- Discuss essential on-going, day-to-day activities necessary to maintain the core attributes, and
- Challenge owner/operators to continuously evaluate opportunities for improvement.

1.1 PURPOSE

The process industry has made great strides toward improving process unit performance and safe operation. It has made and continues to make significant investment to address process risk using a variety of approaches aimed at identifying and controlling risk. These approaches often must fit within a regulatory framework, which relies on the use of recognized and generally accepted good engineering practices to define the minimum requirements.

Many governments (e.g., the United States of America, the European Union, the United Kingdom, Germany, The Netherlands, Korea, Taiwan, and Brazil) have regulations concerning the prevention of releases of hazardous chemicals that pose serious injury or life threatening consequences. Although each government uses unique terminology to describe such events, the concept of process safety management is well known throughout the world. It is widely supported even by governments that do not have specific regulations mandating its implementation. Most require, at a minimum, that an owner/operator demonstrate compliance with the good engineering practices applicable to the manufacturing process and its associated hazards.

The application of control and shutdown equipment to manage hazardous events was first discussed in *Guidelines for Safe Automation of Chemical Processes* (CCPS/AIChE 1993, referred to as *Safe Automation*). In particular, *Safe Automation* provided information for the design and implementation of the Basic Process Control System (BPCS) and the SIS. It established for the process industry many of the fundamental concepts used today, such as independent protection layer (IPL), safety integrity level (SIL), separation and diversity of the BPCS and SIS, access security, and fault tolerance.

Safe Automation was later referenced by the Instrumentation, Systems and Automation (ISA) society standard, ANSI/ISA 84.01-1996, *Application of Safety Instrumented Systems (SIS) for the Process Industry*. This standard provided good engineering practices for the SIS lifecycle, starting with the design phase and continuing through decommissioning.

The globalization of the process industry resulted in demand for international practices. Numerous good engineering practices, previously considered national or regional, are being modified, updated, harmonized, and issued as international practices. One such standard is IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, which expanded the requirements of ANSI/ISA 84.01-1996.

IEC 61511 is the first sector standard issued using the lifecycle framework established by IEC 61508, *Functional Safety of Electrical/ Electronic/Programmable Electronic Safety Related Systems* and covers the complete SIS lifecycle for the process sector. It was developed and is maintained

by the International Electrotechnical Commission (IEC) with volunteer support from organizations worldwide, including ISA and CCPS/AIChE.

IEC 61511 was accepted in 2004 by the European Committee for Electrotechnical Standardization (CENELEC) as EN IEC 61511 and the American National Standards Institute (ANSI) as ANSI/ISA 84.00.01-2004 Parts 1-3. In 2005, ISA published, *Guidelines on the Implementation of ANSI/ISA 84.00.01-2004*, to provide guidance to owners/operators concerning the application of the SIS standard to new and existing equipment. To recognize the contribution of both ISA and IEC to the documentation of good engineering practices for SIS, this book refers to the standard as ISA 84.01/IEC 61511.

ISA 84.01/IEC 61511 uses the SIL concept to benchmark the integrity of the instrumentation and controls used to achieve the required performance from the SIS. The required SIL is defined during a risk assessment process, which examines the process risk and identifies IPLs. ISA 84.01/IEC 61511 requires that the SIL be quantitatively verified using estimates of the random hardware failure rate of the SIS components in the intended operating environment.

Since ISA 84.01/IEC 61511 is an instrumentation and controls standard, it places a great deal of emphasis on the functionality and integrity of the hardware. The assignment and verification of SIL establishes a robust relationship between hardware design and risk reduction. It also provides justification for separation, fault tolerance, and proof test intervals. However, the SIS's capability to achieve or maintain a safe state is dependent on more than the sum of its hardware components.

Integrity and functionality are essential performance attributes, but excess attention on these can result in a loss of focus on other core attributes. While weak links in the hardware design may be identified during a numerical analysis of the SIS equipment, the ability of the installed SIS to achieve the SIL is generally limited by human performance against practices and procedures. Independence, reliability, auditability, access security, and management of change must receive as much, if not more, attention to detail.

The core attributes support the SIS throughout its life by ensuring appropriate focus on minimizing the potential impact of human error on the SIS performance. The absence of a rigorous management system can lead to discrepancies between the desired functionality and integrity and what is achievable in actual operation.

As process units become increasingly automated, integrated and complex, the deliberate and intentional act of implementing IPLs becomes more important. SISs are only one IPL of many that can be used to achieve and maintain safe operation. Other IPLs, such as relief devices and protective alarms, may be identified and should be managed appropriately. The management system ensures that protective equipment are designed, inspected, maintained, tested, and operated in a safe manner. Many incidents in the process industry have been caused by poor

management systems that allowed systematic errors to erode safe operation to the point of catastrophic release.

This book uses the seven core attributes, namely, independence, functionality, integrity, reliability, auditability, access security, and management of change, to define the required performance for the human and equipment systems necessary for safe operation. Following in the footsteps of *Safe Automation*, this book is intended for use by people who are familiar with the manufacture and use of chemicals. It expands the work processes to cover the major activities executed by the various disciplines supporting the SIS lifecycle.

With such an encompassing scope, no single book can possibly cover all of the detailed tasks required for safe and reliable operation. Instead, this book concentrates on the overall work processes, task intent, input information, considerations, and output deliverables. When necessary, the book provides references to other technical publications for greater detail and guidance on specific topics.

1.2 TARGET AUDIENCE

A performance-based management system relies on metrics to support prudent business decisions. Performance-based systems only work in a safety culture nurtured and directed by top management. Sustainable performance requires long-term vision, consistent focus and attention, and financial commitment from senior management. Consensus and participation of personnel are necessary to support the operational and strategic objectives, as well as foster a safe working environment.

The target users of this book are the various disciplines responsible for safe and reliable operation in the process industry. At any given facility, these disciplines may be represented by individuals, departments, or organizations. At some facilities, one person may be responsible for the activities listed for multiple disciplines. The site management system should specify the individuals, departments, or organizations responsible for work activities.

Table 1.1 provides the essential knowledge to be gained by reading this book for seven disciplines. Chapters 3 through 7 include a target audience section that identifies the essential tasks to be discussed for each discipline:

- **Management** includes personnel responsible for establishing policies related to safe and reliable operation and for oversight of the management system. Includes corporate and site organizations.

- **Process safety** includes personnel responsible for process safety management. Includes environmental, health, and process safety management organizations,

- **Process** includes personnel responsible for the process design and operation. Includes research and development, process, and process control.

- **Instrumentation and Electrical (I&E)** includes personnel responsible for instrumentation and control design and implementation. Includes I&E, process control and reliability,

- **Operations** include personnel responsible for the operation of the process. Includes process operations and operations management,

- **Maintenance** includes any personnel responsible for inspecting, testing, and maintaining IPS equipment. This may include personnel from maintenance, process control, I&E, and reliability (equipment), and

- **Manufacturers** include any entity that develops, markets, and sells a product for IPS use.

Target Audience	Will Gain Essential Knowledge On
Everyone	Role and responsibility Risk criteria and affect on IPS requirements Core attributes of IPLs and IPSs Effect of IPS classification on design and management
Management	Management system and its fundamental features Activities, training, tasks, and systems required to support IPSs Communication of risk criteria and expectations
Process Safety	Activities, training, tasks, and systems required to support IPSs Risk criteria and affect on hazard and risk analysis and IPL requirements
Process	Protective requirements specification How functionality, operability, maintainability, and reliability affect design and operating basis Content of I&E requirements specification
Instrumentation and Electrical	Content of process requirements specification I&E requirements specification User approval of equipment How equipment selection, subsystem architecture, diagnostic capability, and proof test interval affect the integrity and reliability
Operations	Administrative procedures--access security management of change, bypass management, and event reporting Operating procedures--hazardous event description, failure response, compensating measures, when to execute a safe shutdown, and what to do when a shutdown fails
Maintenance	Administrative procedures--access security, management of change, bypass, configuration management, and failure reporting Maintenance procedures--hazardous event description, failure response, allowable repair time, inspection, preventive maintenance, and proof tests
Manufacturers	How functionality, operability, maintainability, and reliability affect safe operation

Table 1.1. Target Audience and Essential Knowledge.

1.3 BOOK ROAD MAP

The book is organized using a project lifecycle with six major phases:

- Planning,
- Risk Assessment,
- Design,
- Engineering, Installation, Commissioning and Validation,
- Operational and Mechanical Integrity, and
- Continuous Improvement.

These phases are shown in Table 1.2, which also provides a road map for the book listed by the target audience (see Section 1.2). An "X" is an indication that the chapter contains material that is important to that resource, e.g., a discussion of fundamental principles or specific task responsibility.

The protective management system discussed in Chapter 2 reduces the systematic errors through quality management processes and good engineering practices. Chapter 3 provides an overview of the risk assessment phase, which uses a variety of hazard and risk analysis techniques to identify and classify IPSs.

Chapters 4 and 5 address work processes for IPS design and implementation. Chapter 4 discusses the development of the design basis, which must achieve the intent of the risk assessment and the core attributes defined for each IPS. Chapter 5 covers the engineering, installation, commissioning and validation phase, where the design basis is turned into an installed and operational IPS.

Long-term operational and mechanical integrity is supported by an operating basis, discussed in Chapter 6, which addresses IPS operating and maintenance procedures and personnel training. Chapter 6 also discusses the importance of bypass management, compensating measures, periodic proof testing, and configuration management in achieving the core attributes. Finally, in Chapter 7, long-term performance is monitored and options for improvement are periodically considered.

Audience	Chapter 2 Planning	Chapter 3 Risk Assessment	Chapter 4 Design	Chapter 5 Engineering, Installation, Commissioning and Validation	Chapter 6 Operational and Mechanical Integrity	Chapter 7 Continuous Improvement
Management	X					X
Process Safety	X	X				X
Process	X	X	X	X		X
Instrumentation and Electrical	X	X	X	X	X	X
Operations	X	X		X	X	X
Maintenance	X			X	X	X
Manufacturers			X	X	X	X

Table 1.2. Road Map by Target Audience.

1.4 MANAGEMENT COMMITMENT

Management must make it a priority to develop a protective management system that ensures safe operation of their facilities. Management must support and approve the documentation of policies, practices, and procedures, which provide the work processes and metrics essential to effective risk management. Global competition also demands that the end result of these work processes yield reliable and cost effective IPS operation. Work processes should address significant classes of business risk, that is, safety, environmental, business interruption, and asset, to obtain the greatest value.

Many different management systems are used in the process industry to achieve safety and business risk goals. Consistent performance is directly related to the relevance of the prescribed practices to actual work tasks and the rigor employed to achieve quality workmanship.

In general, the management system should:

- Establish risk criteria and risk management philosophy,
- Verify work activities and associated documentation are in alignment with this philosophy,
- Establish processes to identify and classify IPS,
- Identify personnel or departments who are responsible for IPS work activities and specialists who support the management system elements,
- Verify competence of those assigned responsibility for the IPSs,
- Establish a process to evaluate whether existing IPSs meet applicable good engineering practices, and
- Verify that the behavior and actions of its personnel are consistent with a culture that encourages continuous improvement in IPSs.

Management must be fully committed and engaged in the development and implementation of the management system. Management responsibility includes establishing safe and reliable operation as a priority and providing the resources, tools and training required to get the job done. Successful execution requires decision criteria be clearly stated and consistently followed. For efficient implementation, these criteria should be embedded into each project and operational phase so that safety and reliability issues are considered a normal part of doing business. The best results are obtained when personnel who are responsible for safe and reliable operation:

- Understand their individual responsibility and authority within the management system,
- Understand the owner/operator risk criteria and how it is applied in the design and management of IPSs,
- Are expected to consistently apply internal practices related to safe and reliable operation,
- Feel support to do what is right (even if it requires changing the way things are done now),
- Have the competency and necessary resources to accomplish their assigned responsibilities, and
- Understand the boundaries of acceptable design, operation and mechanical integrity.