1 PROCESS SAFETY AND SAFE AUTOMATION

Chemical processing is an industrial activity that involves using, storing, manufacturing, handling, or moving chemicals. Chemical processing may be accomplished in a single vessel or a group of interconnected vessels and process equipment. Process operation poses different types of risk dependent on the hazardous nature of the chemicals, the quantity of chemicals processed, and the process operating conditions.

The process equipment can be designed using inherently safer strategies to assure safe operation under foreseen process upsets, such as specifying design limits above the maximum and minimum operating parameters that exist under emergency conditions. An inherently safer process is designed to eliminate the potential for loss events with features that are inseparable from the process equipment. When process equipment is not designed to inherently withstand abnormal operation, process safety is achieved through functional safety management. Safeguards, including process control and safety systems, are specified to reduce the process risk to the risk criteria.

Consequently, safe operation of chemical processes is achieved through a process safety management program supported by the twin pillars of inherently safer design and functional safety management (Figure 1.1). Most process designs incorporate aspects of both inherently safer design and functional safety management. Fundamentally, it is the owner/operator's responsibility to determine and document that the equipment is designed, maintained, inspected, tested, and operating in a safe manner, regardless of the means used to achieve this objective.

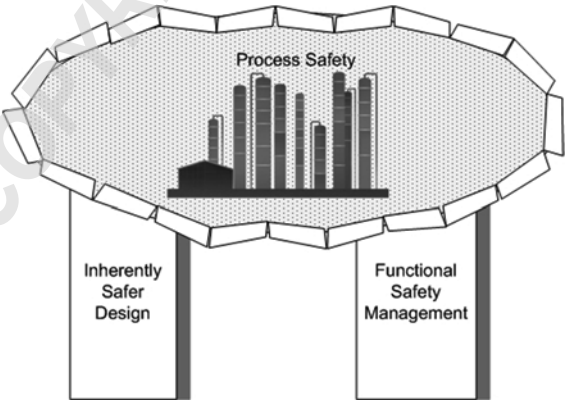


Figure 1.1. Process Safety Supported by Inherently Safer Design and Functional Safety Management

Inherently safer design involves making conscious choices to design and operate the process in a manner that avoids the hazard or minimizes the likelihood and consequence of the loss events. The word inherent means that the design feature is an essential constituent or characteristic of the process design; it becomes permanent and inseparable from the design. In contrast, functional safety management involves the addition of safeguards that act to achieve or maintain a safe state of the process when abnormal conditions occur. Safeguards can reduce the frequency and/or consequence of the loss event. Safeguards are specifically designed, maintained, inspected, tested, and operated to achieve the necessary risk reduction.

Process hazards can sometimes be reduced, or perhaps eliminated, during the design phase through inherently safer choices in process technology, equipment design, and operating parameters. When practicable, inherently safer design can minimize or eliminate the need for safeguards. Changes to the process design and operating plan should be considered as early as possible during the project life, since the relative cost of these changes typically escalates as the project progresses towards maturity (Figure 1.2). The particular means used to address risk is often influenced by the perceived effectiveness, availability, reliability, and sustainability of the protection relative to its lifecycle costs.

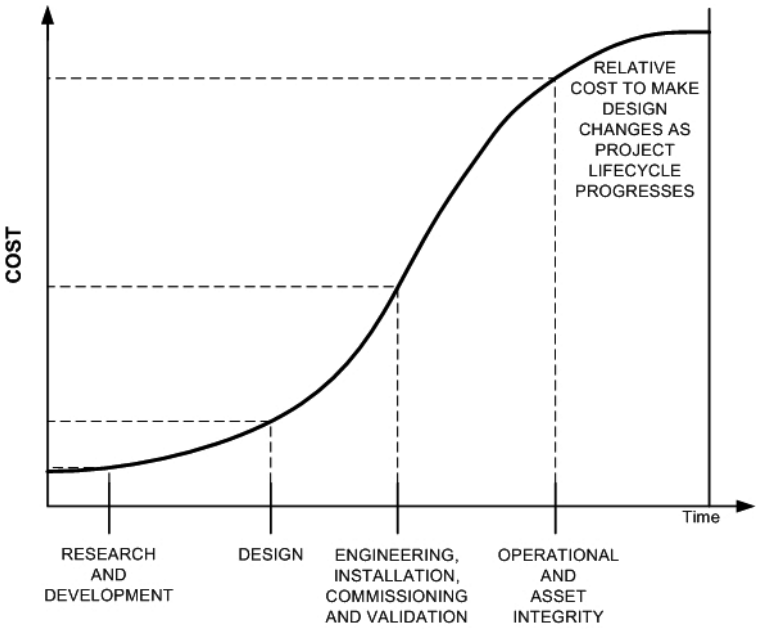


Figure 1.2. Relative Cost to Make Design Changes as a Function of Project Phase

Example: Designing a pipeline for maximum operating pressure

Consider a scenario where the maximum discharge pressure from a pump is sufficient to overpressure a pipeline. The team evaluates 2 inherently safer design choices: (1) lower the maximum discharge pressure from the pump or (2) increase the pipeline pressure rating. Lowering the maximum pump discharge pressure requires evaluation of the needed flows and pressures for the different process operating modes to ensure that the selected pump supports the intended operating plan. A different pump specification may result in a slight capital cost change for a new installation or perhaps a maintenance expense for retrofitting an existing pump. Designing the pipeline to withstand the maximum operating pressure typically requires more capital, because higher rated piping generally is more expensive due to increased wall thickness. When the higher rated piping is installed, there is only one item to maintain – the pipe wall thickness - to assure the pipeline integrity during the facility life. If the pipeline has not been built yet, the increased pressure rating is simply a specification change with increased capital costs. If the pipeline has already been built, the change of specification would require demolition and replacement of an existing asset with associated demolition and construction costs.

The concept of designing a process to be inherently safer is covered by the Center for Chemical Process Safety (CCPS) publication, *Inherently Safer Chemical Processes: A Life Cycle Approach* [2009b]. A report issued by CCPS [2010a] to the Department of Homeland Security stated, "A technology can only be described as inherently safer when compared to a different technology, including a description of the hazard or set of hazards being considered, their location, and the potentially affected population." Inherently safer design involves the use of four strategies:

- **Minimize**—reducing the quantity of material or energy contained in a manufacturing process or plant
- **Substitute**—replacing the material with a less hazardous substance; the replacement of a hazardous material or process with an alternative that reduce or eliminates the hazard
- **Moderate**—using materials under less hazardous conditions; using less hazardous conditions, a less hazardous form of a material, or facilities which minimize the impact of a release of hazardous material or energy
- **Simplify**—designing facilities which eliminate unnecessary complexity and make operating errors less likely and are forgiving of errors that are made

Inherently safer design becomes integral to the operating plan and process design basis. The design strategies typically are incorporated into customary practices, or "*the way things are done*," at a site, so people come to expect certain types of design and management depending on the equipment classification. Inherently safer design involves design choices that make the process and its equipment less susceptible to human error and dangerous

failure during the facility life, but the installed equipment is still subject to degradation mechanisms that over time can erode the inherently safer assumptions. For example, what was an inherently safer design for the process equipment 30 years ago could now be a degraded foundation, vessel, or piping network in need of replacement.

Once the process design is complete, the risk of process operation generally can be further reduced through the implementation safeguards. These safeguards are implemented in protection layers (Figure 1.3) that are not inherent to the process design; they are added to the process to ensure functional safety. IEC 61511-1 clauses 3.2.23 [2015] defines functional safety as "part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers." Using the terminology and scope of *Guidelines for Safe Automation of Chemical Processes 2nd Edition* (referred to as *these Guidelines)*, functional safety is part of the overall safety plan relating to the process and its control system, which depends on the correct functioning of the safety controls, alarms, and interlocks (SCAI) and other protection layers.

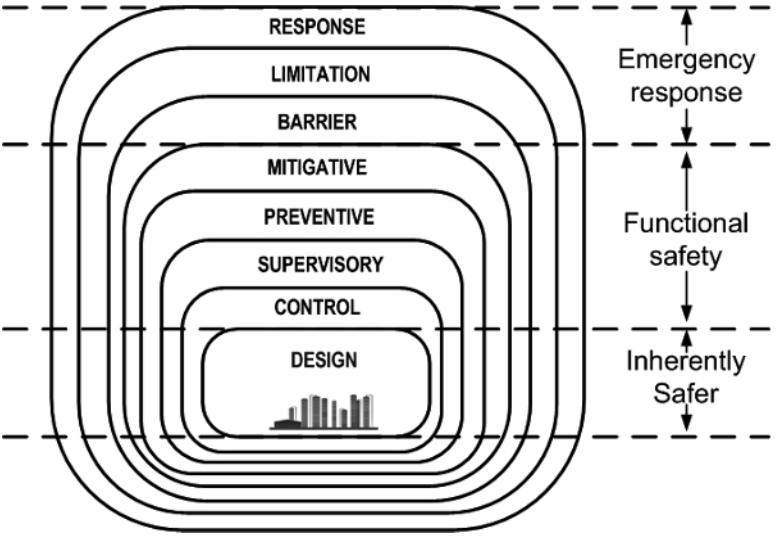


Figure 1.3. Protection Layers Used as Means of Risk Reduction

Example: Designing safety interlock to protect piping

For the overpressure example above, if inherently safer design cannot eliminate the overpressure risk, a safety interlock could be used to detect excess pressure and isolate the pressure source when abnormal conditions occur. A safety system, or specifically safety instrumented system, may require less capital than the higher pressure rating pipeline, but typically requires substantial attention and effort to ensure its integrity and reliability.

Automated systems, whether in manual or automatic mode, are complex systems where many different devices must work successfully to achieve the desired functionality and therefore require many different skill sets and planned activities to ensure that the systems work as desired when required.

The need for functional safety management is determined by analyzing how abnormal operation propagates to loss events. Protection layers can reduce risk to an acceptable level but these functional safety features can be impacted by human error during the equipment life starting with conceptual design and ending with equipment replacement. Achieving sustainable safe operation requires a safety culture (Table 1.1) that is proactively looking for problems with the process equipment, protection layers and intended process operating plan and taking action to ensure that risk is reduced as low as reasonably practicable.

TABLE 1.1. Features Associated with A Positive Safety Culture (CCPS Human Factors [2007c])

Hardware	Good plant design, working conditions and housekeeping Perception of low risk due to confidence in engineered systems
Management systems	Confidence in safety rules, procedures and measures Safety prioritized over profits and production Satisfaction with training Good job communication Good organizational learning
People	High levels of employee participation in safety Trust in workforce to manage risk High levels of management safety concern, involvement and commitment
Behavior	Acceptance of personal responsibility for safety Frequent informal safety communication Willingness to speak up about safety A cautious approach to risk
Organizational factors	Low levels of job stress High levels of job satisfaction

Inherently safer strategies can be applied to automated systems. One might argue that the application of these strategies to a protection layer can only make a process safer, rather than inherently safer. However, when such strategies are applied systematically across the site, the resulting design and management practices become part of "*the way things are done*" and result in an inherently safer process operation. The inherently safer strategies can be applied to automation systems as follows:

- **Minimize**—reducing the use of automation features that tend to increase the failure mechanisms that result in system failure
- **Substitute**—replacing an automation feature with an alternative that reduces or eliminates the frequency of dangerous failure
- **Moderate**—using automation features to facilitate operating the facility under less hazardous conditions; using automation features which minimize or limit the impact of dangerous failure of the automation system on the process operation
- **Simplify**—designing automation in a manner that eliminates unnecessary complexity, makes operating and maintenance errors less likely, and is forgiving of errors that are made

For example, use the principle of substitution to select devices that fail to the safe state on loss of any utility, such as power or instrument air, instead of devices that require energy to take action. This example illustrates what is often referred to as fail-safe design. Unfortunately, fail-safe is sometimes erroneously interpreted as inherently safe where all failures result in the safe action. As with the equipment design, it is rarely possible to design an automated system to be inherently safe. Instead, *these Guidelines* use the term *inherently safer practices* to describe a way of thinking about the design of the automated system that focuses on the elimination or reduction of the failure mechanisms that result in system failure.

Many types of systems are used to implement safeguards within the process industry. Examples of systems often identified as safeguards are illustrated in Figure 1.4. The size of each bubble represents the relative risk reduction provided by the system. The bubble location is related to the relative ease of sustaining the system's risk reduction and reliability. Sustainability of these systems can be significantly different even when they are designed and managed to provide similar risk reduction. The process control system, safety alarm system, and SIL 1 SIS may achieve similar risk reduction from a hardware integrity standpoint, but the resilience of the SIS to systematic failure is higher due to its more rigorous design, verification, and validation processes. This makes the SIS performance more sustainable long-term. A pressure relief valve and a check valve are both mechanical devices, yet the pressure relief valve achieves much higher risk reduction with greater sustainability. *Choosing protection layers that are more resilient to systematic failures is an inherently safer practice.*

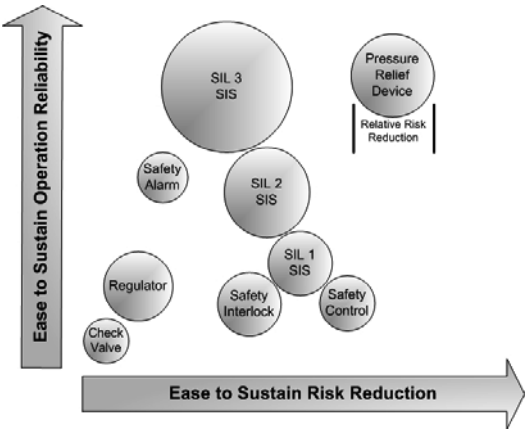


Figure 1.4. Protection Layers Showing Relative Risk Reduction, Reliability and Sustainability

Example: Considering manual versus automatic response

Consider the choice of an alarm versus a SIS. While the alarm appears to be an easy option, the sustainability of the layer is much more difficult due to the number of operators and worker turnover. It only takes one poorly trained operator to cause a failure of an alarm system. In contrast, the SIL 1 SIS is more predictable in its operation and thus more sustainable when it is well maintained.

These Guidelines cover the use of any automation system to assure safe operation of the process, whether implementing a safety control, alarm, or interlock. These systems take action to achieve or maintain a safe condition of the process in response to specified abnormal conditions.

1.1 OBJECTIVE

The subject of designing and managing automated systems is addressed by numerous standards and practices. In the 1990s, CCPS issued the 1st edition of *Guidelines for Safe Automation of Chemical Processes* [1993]. Although over two decades old, *Safe Automation of Chemical Processes* has remained a foundation book for safely and reliably applying automated systems to the control of chemical processes. The 1st edition was sponsored as a part of a continuing effort to improve the safety performance of the chemical processing industry through education of engineers and others who design, start-up, operate, maintain, and manage chemical processing plants. In the last 20 years, numerous standards and practices by other industrial organizations around the world have been written and updated based on the concepts and approaches established in *Safe Automation of Chemical Processes*.

The challenges posed by the implementation of programmable equipment in control and safety applications resulted in the instrumentation and controls

community developing standards and practices throughout the world to identify and reduce the potential of hardware and software failure. The first standard ISA S84.01-1996 [ANSI/ISA 1996] accepted as an American national standard in 1997 was followed by an international standard, IEC 61511 [2003a], in 2003. *These Guidelines* make reference to latest version of IEC 61511, which was released as final draft international standard (FDIS) in 2015. The FDIS represents the pre-publication draft of the standard and is considered a technically complete document. However, some minor editorial changes may be noted between *these Guidelines* and the final standard.

The design and management aspects of electrical, electronic, and programmable systems have been addressed in many other publications from ISA, IEC, API, ASME, NFPA, etc. CCPS published *Guidelines for Safe and Reliable Instrumented Protective System* (CCPS IPS) [2007b] to provide guidance on the implementation of instrumented protective systems in safety, environmental, and asset protection applications. These documents focus on the hardware and software choices from a lifecycle perspective. *These Guidelines* follow a similar framework and describes the activities that should be performed during each lifecycle step to properly specify, install, commission, operate, and maintain the process control and safety systems.

One of the major changes over the years has been the increased awareness of the impact of human error, especially systematic ones, on functional safety. Technology evolution, the increasing complexity of equipment hardware and software integration, the wide range of implementation strategies including centralized, distributed, and hybrid systems, and the ever expanding variety of communication between and interconnectivity of control systems, business enterprise systems, and the Internet has introduced new sources of human error that must be dealt with effectively to ensure safe automation. "*The way things are done*" may not be good enough when practices haven't kept up with technology.

In the instrumentation and controls community, this awareness has given birth to the safety lifecycle and functional safety management, which includes a myriad of activities, intended to identify and prevent human errors that impact system effectiveness. These activities include competency assessment, verifications, functional safety assessments, configuration management, management of change, audits, and metrics. Proper management of these systems requires a strong safety culture that applies the rigor necessary to maintain equipment integrity and reliability. Maintaining management focus and support while experiencing success is a continuing challenge.

These Guidelines provide guidance on how to develop and implement an effective functional safety plan for ensuring safe and reliable performance. It discusses the need for management rigor in defining the organizational structure, competency, and work quality expectations supporting functional safety, and the significant differences between the systems typically used in process control and safety applications. It provides guidance for the design and management of the systems that are used for normal control of chemical processes and those used to reduce the risk of loss events. Finally, *these*

Guidelines propose key performance indicators that demonstrate safe operation and proactively manage system reliability.

1.2 SCOPE

These Guidelines are directed not only toward those responsible for the design, installation, use, and maintenance of process control systems, but also to the broader community of management, engineers, and technical professionals who are responsible for the safe design, operation, and management of chemical processes. Over the years, process operation has become increasingly automated and the systems involved in the automation have become more diverse and complex, resulting in the potential for many unknown (or not yet experienced) system interactions and conflicts. It is more important than ever for process design and control system specialists to understand each other's disciplines, and to work together to provide facilities where the instrumentation and control system design and process design are closely integrated.

These Guidelines provide considerations and recommendations on how to implement and improve process safety performance of new and existing systems in process control and safety applications. The complete control system is covered including the field-mounted process sensors, the logic processor, the operator interfaces, and the final elements. For the logic processor, the primary emphasis is on application of electrical, electronic, and programmable electronic systems (E/E/PES), but the principles may be applied to all types of control systems, such as pneumatic or hydraulic systems. Electrical and electronic systems are non-programmable and are available in many types of discrete control systems, such hardwired systems, electromechanical relays, motor-driven timers, and trip amplifiers. The term PES applies to all types of programmable controllers, such as single loop controllers, distributed control systems (DCSs), programmable logic controllers (PLCs), digital relays, and other microprocessor-based equipment.

1.3 LIMITATIONS

The discussion of safety issues in *these Guidelines* is limited to the direct or indirect application of safeguards relying on instrumentation and controls. The primary focus is on loss events leading to process safety impact, but the principles can be applied to the prevention of losses related to business interruption and property damage as well.

These Guidelines are not intended for the nuclear power industry. In the United States, the Department of Energy has recommended the use of IEC 61511 [2015] for the design of safety significant instrumented systems in nuclear facilities for processing of nuclear material or nuclear wastes.

The special safety concerns related to discrete parts manufacturing industry, materials handling industry, or packaging industry are not addressed in *these Guidelines* even though they may have some applicability in the process industry. *These Guidelines* also do not cover the special requirements for effective fire protection systems.

These Guidelines do not provide detailed guidance for the identification of loss events or for the design of risk reduction means that do not involve automation. *These Guidelines* follow a typical lifecycle process to determine whether or not a safety system is needed and to provide recommendations for how to design and implement the system when it is needed.

The reader is referred to other CCPS publications for additional guidance, namely:

- *Guidelines for Engineering Design for Process Safety* [2012b]
- *Guidelines for Hazard Evaluation Procedures* [2008a]
- *Inherently Safer Chemical Processes: A Life Cycle Approach* [2009b]
- *Guidelines for Chemical Process Quantitative Risk Analysis* [2012a]
- *Layers of Protection Analysis: A Simplified Risk Assessment Method Analysis* [2001]
- *Guidelines for Initiating Events and Independent Protection Layers* [2014b]
- *Guidelines for Safe and Reliable Instrumented Protective Systems* [2007b]

These Guidelines were written by a group of knowledgeable people who are leaders in the safe automation of chemical processes. More than a dozen companies and organizations that support CCPS have peer reviewed and provided feedback on *these Guidelines*. The resulting publication represents a spectrum of the current practices on the specification, design, implementation, operation, and maintenance of control and safety systems.

1.4 TARGET AUDIENCE

The target audience is anyone assigned responsibility for a lifecycle activity associated with the instrumentation and controls. The seven roles typically assigned responsibilities for lifecycle activities are listed below and in Table 1.2, which also includes a high level summary of the essential knowledge gained from reviewing *these Guidelines*.

- **Management**—personnel responsible for establishing policies related to safe and reliable operation and for oversight of the management system.
- **Process Safety**—personnel responsible for process safety management.
- **Process Specialists**—personnel responsible for the process design, automation, implementation, verification, and validation. This includes research and development, process engineering, and process control.
- **Instrumentation and Electrical (I&E)**— personnel responsible for instrumentation and control design and implementation.
- **Operations**—personnel responsible for the operation of the process.
- **Maintenance**—personnel responsible for inspecting, testing, and maintaining process control and safety system equipment.
- **Manufacturers**—personnel who work for an entity that develops, markets, and sells a product for process control and safety system use.

In any given organization, individuals or departments may support the listed roles. User personnel, specialty consultants, engineering contractors, or other suitably competent parties on project teams may support these roles when implementing new or modified systems. At some sites, one person may be responsible for the activities listed for multiple roles. The functional safety management system specifies the individuals or departments responsible for various lifecycle activities.

TABLE 1.2. Target Audience and Essential Knowledge

Target Audience	Will Gain Essential Knowledge On
Everyone	Role and responsibility Risk criteria and effect on control system requirements Core attributes of control systems Effect of control system classification on design and management Lifecycle concepts Relationship between control and safety systems
Management	Management system and its fundamental features Activities, training, tasks, and systems required to support control systems Competency and resource needs Communication of risk criteria and expectations Establishing a safety culture
Process Safety	Activities, training, tasks, and systems required to support control systems Risk criteria and effect on hazards and risk analysis and independent protection layer (IPL) requirements
Process Specialists	Process requirements specification How functionality, operability, maintainability, and reliability affect design and operating basis Content of safety requirements specification
Instrumentation and Electrical	Content of process requirements specification Safety requirements specification User approval of equipment How equipment selection, subsystem architecture, diagnostic capability, proof test effectiveness, and proof test interval affect the integrity and reliability Instrument and electrical reliability requirements
Operations	Administrative controls – access security management of change, bypass (and manual operation) 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 controls – 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 Instrument reliability assurance
Manufacturers	Role and responsibility in ensuring safe and reliable application of their products How functionality, operability maintainability, and reliability affect safe operation

1.5 INCIDENTS THAT DEFINE SAFE AUTOMATION

The 1st edition of *Guidelines for Safe Automation of Chemical Processes* was published in 1993. In the decade leading up to its publication, the process industry suffered significant loss events that brought worldwide attention to process safety management.

Since 1993, additional loss events have occurred that brought renewed effort in defining the requirements for safe automation on a global scale. Numerous standards and practices, which are referenced in *these Guidelines*, have been published to address different aspects of instrumentation and controls from basic electrical safety through performance-based standards for alarm management, SCAI and SIS.

To emphasize the importance of safe automation, case studies of previous incidents (Table 1.3) have been placed throughout *these Guidelines*. There are typically many lessons to be learned from these incidents, and some of these incidents have become synonymous with certain safety issues, e.g., Texas City 2005 related to siting of temporary and permanent structures. *These Guidelines* do not make any attempt to replicate these previous lessons learned, but instead focuses on the contribution of inadequate design, installation, testing, maintenance, and operation of the process control and safety systems.

The case studies have more than high cost and significant impact in common. The attributed causes are similar. Each process had been subjected to multiple assessments of the likelihood and consequence of significant events. The assessments involved different methods, were conducted by different individuals, and were often supported by independent consultants. The hazards were known and accepted, as "*the way things are done,*" with the pervasive belief being that the event was highly unlikely to occur. There was little acknowledgement or planning for event escalation, so when the event began to unfold, personnel who had the greatest opportunity to stop the incident were overwhelmed.

In contrast to the common single cause-consequence paradigm, multiple causes and latent conditions were usually present in these case studies, although a primary root cause was identified for each specific accident. In most cases, the accident was not a sudden failure occurrence, but an evolving set of conditions that lined up in a dangerous manner: instrumented systems relied upon for control and monitoring did not work properly, and operators misinterpreted or ignored available data. Plant personnel often suspected abnormal operation, but investigation and correction were delayed.

TABLE 1.3. Incidents That Define Safe Automation

Case #	Location and Date	Process type	Unit	Consequence
1	Sunray, Texas; February 16, 2007	Refinery	Propane deasphalting (PDA)	Propane Fire; 4 Injured Direct loss $50 million
2	Mexico City, Mexico; November, 19 1984	LPG terminal	LPG terminal	Explosion and fire; Over 500 fatalities Over 7000 injuries; 200,000 evacuated
3	Hebei, China; February 28,2012	Pesticides and Pharmaceutics	Reactors	Explosion; 25 fatalities; 46 injured
4	Point Comfort, Texas; October 6, 2005	Plastics	Olefins	Propylene Explosion; 16 injured; Unit heavily damaged One school evacuated
5	Belle, West Virginia; January 23, 2010	Chemical	Small lots manufacturing	Toxic Chemical Release; 1 fatality
6	Institute, West Virginia; August 28, 2008	Pesticide	Methomyl-Larvin insecticide	Pressure Vessel Explosion; 2 fatalities; 8 injured; 40,000 residents sheltered in place/evacuated
7	Pascagoula, Mississippi; October 13, 2002	Chemical	Mono-nitro-toluene	Explosion and fire 3 injured
8	Bhopal, India; December 3, 1984	Pesticide	Methyl isocyanate (MIC)	Release of MIC; Over 100,000 fatalities Tens of thousands injured
9	Petrolia, Pennsylvania; October 11, 2008	Chemical	Oleum transfer	Oleum release; 1 injured; Plant evacuated; 2500 people from 3 nearby towns evacuated
10	Milford Haven, Wales; July 24, 1994	Refinery	Flare system	Explosion, 26 injured; plant and nearby homes damaged, 4.5 months downtime, 10% UK capacity

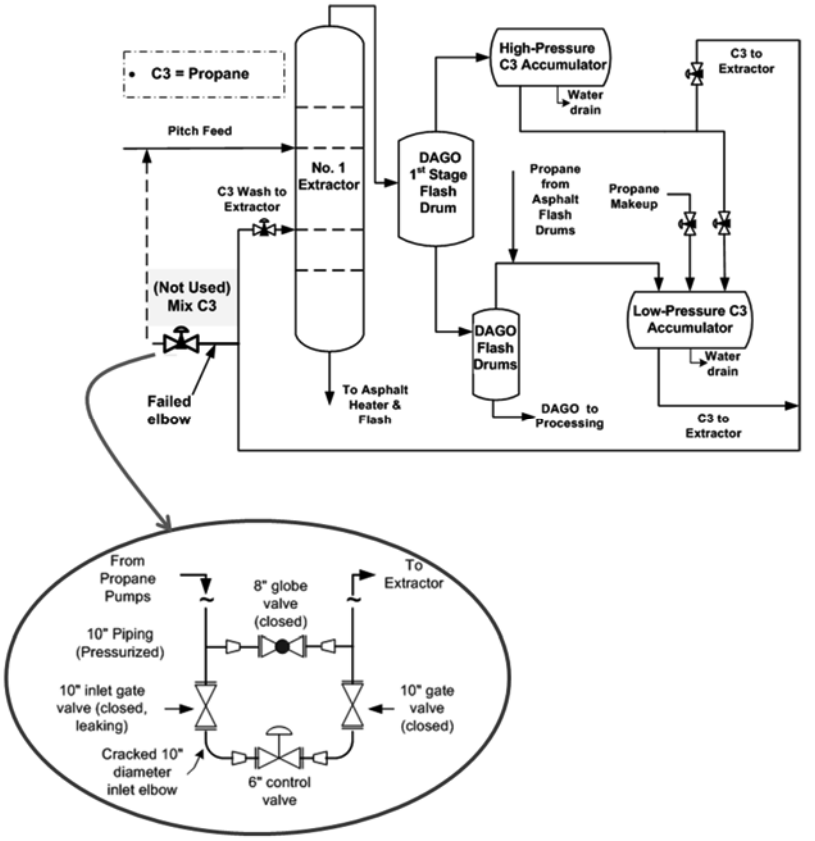
Case #	Location and Date	Process type	Unit	Consequence
11	Longford, Australia; September 25, 1998	Natural gas	Lean oil absorption	Gas explosion and fire; 2 fatalities; 8 injured Estimated Loss A$ 1.3 billion Gas supply affected for 2 weeks
12	Valley Center, Kansas; July 17, 2007	Chemical	Storage Tank	Explosion; 12 injured; Facility extensively damaged; 6000 people evacuated
13	Bayamon, Puerto Rico; October 23, 2009	Tank farm	Storage tank	Overfill, fire and explosion; 3 injured; 17 tanks burned; Almost 300 homes damaged
14	Channelview, Texas; July 5, 1990	Petrochemical	Waste water storage tank	Fire and Explosion; 17 fatalities; An area the size of a city block was destroyed
15	Pasadena, Texas; October 23, 1989	Chemical	Polyethylene reactor	Explosion; 23 fatalities; 130 injured Estimated loss over $750 million
16	Illiopolis, Illinois; April 23, 2004	Plastics	Polyvinyl chloride	Vinyl chloride explosion; 5 fatalities Facility heavily damaged; 150 people evacuated
17	Texas City, Texas; March 23, 2005	Refinery	Hydrocarbon isomerization	Explosion; 15 fatalities; 180 injured More than $ 1.5 billion loss
18	Ontario, California; August 19, 2004	Chemical	Ethylene oxide	Ethylene Oxide Explosion; 4 injured Facility extensively damaged Neighboring facilities were evacuated
19	Hemel Hempstead, England; December 11, 2005	Oil storage depot	Storage tank	Fire and Explosion; 43 injured; 2000 people evacuated; Significant damage to both commercial and residential properties Estimated Loss 1.2 billion British Pounds
20	Macondo, Gulf of Mexico; April 20, 2010	Offshore oil exploration	Offshore drilling platform	Blowout and explosion; 11 fatalities; 17 injured; Biggest spill in USA; Tens of billions of dollars

Case 1 **Location:** Sunray, Texas

Process: Propane Deasphalting Unit (PDA) **Date:** February 16, 2007

Impact: 4 injured; total refinery evacuation; 2 month refinery shutdown; 1 year reduced capacity

Process Flow Diagram and Control Station Detail:



Summary:

Before the accident, a leaking, but closed, valve allowed water to accumulate in a low point of a control station that had been out of service for 15 years. Cold weather caused freezing, likely fracturing an elbow in the control station. When warmer weather melted the ice, pressurized propane was released. Plant workers heard a noise and saw vapor blowing from the elbow. The vapor cloud travelled to the boiler house and ignited, causing a flash back to the leak source. The jet fire spread rapidly and caused widespread equipment and structural failures.

Key Automation Learning Point:

Valves should not be relied upon for long-term isolation. The differential pressure across the valve will continue to apply stress on the valve seat, which will lead to a failure eventually, especially when the valve is not being routinely inspected, tested, and wearable parts rebuilt or replaced. Decommissioning of instrument installations should be reasonably prompt to avoid leaving extraneous piping for pressure, process contaminants or byproducts to accumulate. [ISA 2012e]

Instrumentation and Controls Gaps:

- PHA failure to identify the hazard: control station design with dead leg collects entrained water
- Failure to conduct an MOC review when use of the control valve was discontinued but not isolated from the process
- Failure to heat trace the control valve station
- Lack of remotely operable shut-off valves as recommended by insurers and required in company standards
- Incorrect closure of 1996 PHA recommendation to install remotely operable shut-off valves as completed when these were never installed

Sources:

- CSB. 2008. *Investigation report - LPG fire at Valero – Mckee refiner.* Report 2007-05-I-TX. Washington, D.C.: U.S. Chemical Safety Board.

Unsurprisingly, there was a strong belief that the control and safety systems were capable of preventing extensive harm. However, this belief was unfounded because the alarm, shutdown, and emergency isolation systems proved to be inadequate when the event unfolded.

In every event, competent people with knowledge of the process, equipment, process operation, and operating history did not acknowledge that the conditions for failure could be (or were) present. Is this a case of confirmation bias, where the team only looks deep enough to confirm the belief that everything is ok as is? A lack of understanding of how abnormal operation occurs or a refusal to accept that harm is possible inherently limits the capability of responsible personnel to correctly assess and manage risk. Process safety risk is not addressed by a big list of poorly managed safeguards or a list of nothing; it is addressed by the right list of rigorously designed and managed safeguards [Summers 2008, 2009].

1.6 OVERVIEW OF THE CONTENTS

Each of the five chapters following this introduction addresses an aspect of the automation work process. While some elements of sound process control and automation are presented as a starting point, primary emphasis is on specific issues that impact safety, rather than general operability and reliability of the process unit. *These Guidelines* discuss choices that affect the operability, maintainability, and reliability of the instrumented systems in process control and safety applications.

There are many good references addressing considerations in the selection of instrumentation and their application to the control of processes. References are listed at the end of each chapter. The reader is encouraged to use additional sources in applying sound engineering practices to the application of instrumented systems.

1.6.1 Chapter 2—The Role of Automation in Process Safety

The process industry is in transition due to worldwide competition, increasing governmental regulations, and customer demands for greater traceability and connectivity. These changing conditions require the use of more automation and less dependence on humans for routine operation. Rapid technological changes in control systems are also introducing additional challenges and opportunities. Change management, effective deployment of system upgrades, and new equipment impacts the safety and reliability of automation.

Process control and safety systems play important roles in reducing the frequency of loss events, so considerations related to selection, design, and implementation are briefly covered in Chapter 2, with detailed guidance provided in Chapters 3 through 5. The long-term performance of automation systems depends on the quality and rigor of the management systems. Robust management systems reduce the likelihood of human errors, particularly systematic ones, leading to process control or safety system failure. Administrative controls are addressed in detail in Chapter 6.

A functional safety lifecycle is used to depict the different activities and work processes necessary to properly specify and implement process control and safety systems. The lifecycle emphasizes the need for conducting hazard analysis, performing risk assessments, and identifying the various means used to reduce the risk of loss events.

The concepts of the protection layer and an independent protection layer (IPL) are introduced. Guidance is presented for identifying and evaluating whether protection layers qualify as IPLs using a set of specific criteria. Once the protection layers are defined, the required performance is determined based on risk criteria. The need for each company to develop specific criteria in this area is emphasized, since these design decisions involve judgments of risk acceptability.

Readers are cautioned to satisfy their own company's practices or other application criteria when identifying and classifying systems, as well as complying with good engineering practices.

1.6.2 Chapter 3—Automation Specification

The chapter addresses the importance of understanding the overall functional requirements for the control and safety systems and how faults (or failures) of system devices contribute to a system failing to operate when required. It also covers the various techniques that can be utilized to minimize the impact of these failures on the overall safety of the process.

Proper application of control systems improves safety of chemical processes by reducing the frequency of abnormal operation and demands on the safety layers. The use of modern technology offers additional enhancements if properly applied. Chapter 3 offers guidance on accomplishing this for the process control system and safety controls, alarms, and interlocks. Guidance is provided to determine the appropriate separation of process control and safety systems in terms of hardware, software, personnel, and function. Safe and secure integration of these systems is paramount to achieving desired functionality and operability.

1.6.3 Chapter 4—Design and Implementation of the Process Control System

Chapter 4 gives guidance in the application of control system technology, field instrumentation (process sensors and final elements), operator/control system interface considerations, and process controllers.

Safety considerations in applying single-loop controllers (pneumatic, analog, discrete, and programmable) and multi-loop control systems (DCS and PLC) are discussed. The application of varying types of process sensors and final elements (e.g., control valves) is also presented. Emphasis is on the safety aspects rather than on general application and selection practices, since these can be found in other texts and references.

Operator interface considerations are covered from the viewpoint of information overload or adequacy of information available to the operator. Work processes and considerations are presented for selecting and supporting various types of hardware used for process control.

Information is also provided relating to safety concerns in power supply, grounding and distribution systems, installation of specific components, communication considerations between systems, and the use of advanced control techniques.

1.6.4 Chapter 5—Design and Implementation of Safety Controls, Alarms, and Interlocks (SCAI)

Chapter 5 addresses the specific issues related to safety controls, alarms, and interlocks (SCAI) that may be required to ensure safe operation and to meet company risk criteria. The potential for systematic failure is addressed with rigorous design work processes that ensure thorough analysis and documentation of the system requirements. Examples are given of *inherently safer practices*, which can be applied to SCAI. A method of selecting the most appropriate hardware for a given system is presented, along with criteria to follow in the system design. Special requirements for the application program are also discussed.

Communication considerations that may be required to maintain integrity, reliability, and security are covered. The concepts of separation, redundancy, and diversity are presented with discussions of their impact on the overall system integrity. Methods for integrating the reliability and availability requirements to obtain acceptable system performance are discussed.

1.6.5 Chapter 6—Administrative Controls and Monitoring

This chapter addresses both the need for and the types of administrative controls and actions that may be required to maintain any control system in a safe operating condition for the long term. It describes the content of procedures related to documentation, maintenance, operation, security, testing, bypassing, and other areas that apply to instrumented systems.

Special emphasis is given to the management of changes to the system design and functional logic. Suggestions are presented for minimum levels of administrative control procedures. The use of engineered systems versus administrative controls is addressed. There is an emphasis on the need for written procedures rather than verbal instructions, ensuring the consistency of work execution and the ability to audit.

The use of simulation techniques is briefly discussed in this chapter. Also covered is a discussion of the types of personnel, competencies, and skills required to support the lifecycle. Finally, the need for independent verifications

and assessment of deliverables to avoid systematic failure across the automation system lifecycle is emphasized.

1.6.6 Other Information

In addition to the information already described, *these Guidelines* contain a glossary, a list of acronyms and abbreviations, and references at the end of each chapter. An index is included for quick reference to specific topics within the book.

Appendices are included with information on several subjects that expand upon the material in a specific chapter. These provide additional reference materials for the user in applying the principles outlined in *these Guidelines*.

1.7 KEY DIFFERENCES

In the years since the original publication of *Safe Automation of Chemical Processes* [CCPS 1993], numerous CCPS guidelines, international standards and application practices have been published. Each publication has addressed the fundamental requirements of functional safety lifecycle from management system concepts to specific applications of instrumentation and controls. Some terminology has changed such as the use of safety instrumented system rather than safety interlock system. Yet most of these changes are barely perceptible from a technical perspective.

More importantly, there is a stronger emphasis on the organizational discipline and safety culture necessary to support safe and reliable instrumented systems. Functional safety involves the systematic implementation of tasks and activities to ensure equipment is properly designed, installed, and working in accordance with its specifications and remains fit for purpose until it is removed from service. When process safety is achieved through functional safety, the organization accepts the burden of assuring that the process is designed, maintained, inspected, tested, and operated in a safe manner.

REFERENCES

ANSI/ISA. 1996 (Replaced). *Application of Safety Instrumented Systems for the Process Industries, S84.01-1996*. Research Triangle Park: ISA.

CCPS. 1993. *Guidelines for Safe Automation of Chemical Processes*. New York: AIChE.

CCPS. 2001. *Layers of Protection Analysis: Simplified Process Risk Assessment*. New York: AIChE.

CCPS. 2007b. *Guidelines for Safe and Reliable Instrumented Protective Systems*. New York: AIChE.

CCPS. 2007c. *Human Factors Methods for Improving Performance in the Process Industries*. New York: AIChE.

CCPS. 2008a. *Guidelines for Hazard Evaluation Procedures, 3rd Edition*. New York: AIChE.

CCPS. 2009b. *Inherently Safer Chemical Processes: A Life Cycle Approach*. New York: AIChE.

CCPS. 2010a. *Final Report: Definition for Inherently Safer Technology in Production, Transportation, Storage, and Use*. New York: AIChE.

CCPS. 2012a. *Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition*. New York: AIChE.

CCPS. 2012b. *Guidelines for Engineering Design for Process Safety, 2nd Edition*. New York: AIChE.

CCPS. 2014b. *Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis*. New York: AIChE.

IEC. 2003a (Replaced). *Functional safety: Safety instrumented systems for the process industry sector - Part 1-3,* IEC 61511. Geneva: IEC.

IEC. 2015. *Functional safety: Safety instrumented systems for the process industry sector - Part 1-3*, IEC 61511. Geneva: IEC.

ISA. 2012e. *Mechanical Integrity of Safety Instrumented Systems (SIS)*, TR84.00.03-2012. Research Triangle Park: ISA.

Summers, Angela E. 2008. “Safe Automation Through Process Engineering,” *Chemical Engineering Progress*, 104 (12), pp. 41-47, December.

Summers, Angela E. 2009. “Safety Management is a Virtue” *Process Safety Progress*, 28 (3), pp. 210-13, September. Hoboken: AICHE.