22
Safety Instrumented Systems

Geoffrey S. Barnard

22.1
Introduction

Greater automation yields many benefits; however, advances in basic regulatory control system technology and the addition of advanced multivariable control systems are allowing for more complex and tightly integrated control schemes and, in many cases, continuous operation in more extreme portions of the process design envelope. Equally advanced automated safety systems are needed to respond to losses of control more quickly and reliably.

22.1.1
History

It has been common practice for decades to build certain protections into the basic process control system (BPCS) to help prevent equipment failures or human errors from resulting in unsafe process conditions, especially once programmable controllers had made this very simple and inexpensive. When a failure within the BPCS could result in an unsafe condition, electrical relay-based interlocks and later other programmable systems were frequently installed independently of the BPCS to provide a secondary means of shutting down the process. These independent systems have been known by a variety of different names: emergency shutdown systems, process safety systems, safety interlock systems, and others.

In response to several major disasters in the 1970s and 1980s, industry put a new focus on process safety and the use of automation to limit the influence of human error. Throughout the 1980s and 1990s much work was done by the European Workshop on Industrial Computer Systems (EWICS), the UK Health and Safety Executive (HSE), the German Institute for Standardization (Deutsches Institut für Normung, DIN), the American Institute of Chemical Engineers' Center for Chemical Process Safety (CCPS), the International Society of Automation (ISA) (formerly the Instrumentation, Systems, and Automation Society), and other industry groups around the world to address growing concerns about process safety through the use of technology.

Handbook of Loss Prevention Engineering, First Edition. Edited by J. M. Haight.

Today, both human errors and control system failures must be considered likely events. Physical separation between control and safety devices and functions must be considered to minimize the impact of common-cause failures. Other key changes in approach have been the recognition that process risk needs to be estimated more quantitatively, that risk-based criteria should be used to determine the necessary integrity of safeguards, and that ongoing maintenance requirements need to be specified to ensure integrity is sustained over time.

Functional safety is the component of overall safety that is based on the correct functioning of complex systems that take specific actions in response to specific conditions. The international community settled on the term *safety instrumented systems* (SISs) to describe functional safety systems in industrial process applications. An SIS will contain one or more safety instrumented functions (SIFs), each comprised of one or more sensors, logic solvers, final elements, and support systems; and each designed to protect against specific hazardous events.

22.1.2 Functional Safety Engineering Standards

The International Electrotechnical Commission (IEC) Working Group 65 was formed to deal specifically with issues surrounding industrial process measurement, control, and automation. This group, with broad international representation, developed the IEC 61508 standard, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. This seven-part standard defines the framework for the management of functional safety and the requirements for system hardware and software, but is not specific to any industry or application. It also defines the performance criteria for each safety integrity level (SIL), an order of magnitude expression of the risk reduction provided by an automated safety function. The standard's work process is built around a continuous *safety life-cycle* and a performance management model. The seven parts were initially approved and published between 1998 and 2000, and have since led to the creation of a series of international consensus engineering standards for a number of industries and applications where complex systems are used in safety-related service. IEC 61508 has since been revised and a second edition issued in 2010 (IEC, 2010).

One of the first application-specific standards developed under the umbrella of IEC 61508 was IEC 61511: *Functional Safety – Safety Instrumented Systems for the Process Industry Sector* (IEC, 2003b). This three-part standard provides the fundamental requirements for all aspects of SIS analysis, realization, and operation in process safety applications, and is the principle reference of this chapter.

Additional standards have been developed for other specific industries and applications such as IEC 62061 for machinery safety, IEC 61800-5-2 for variable-speed drives, IEC 61513 covering safety-related systems in nuclear power plants, ISO 26262 for automotive applications, EN 50128 for railway systems, and many others.

22.1.3 Regulatory Requirements

IEC 61511 is widely considered the *recognized and generally accepted good engineering practice* (RAGAGEP) for automated safety systems in industrial process applications. While compliance may not necessarily be explicitly mandated, the standard may still carry the force of law as observance of good engineering practice is a common benchmark for judging professional duty. It is important that both end-users and engineering contractors involved in the operation or design of hazardous chemical processes have a thorough understanding of the standard and its legal significance, in addition to any other applicable health, safety, and environmental regulatory requirements of the region where the facility is located.

22.1.4 Notes on This Chapter

Flexibility is a principle advantage of performance-based standards. As a result, every organization's approach will vary to a certain extent, using alternative terminology, methods, and even the specific sequence of activities. Other texts may present alternative strategies and viewpoints; your approach should be developed within the context of your particular facility (or project) and organization's culture and capabilities.

Many of the activities required for engineering and operation of SISs are not unique to SISs, but follow very closely the tenets of overall process safety management. It is unlikely that any functional safety management program will be successful without the presence of an effective overall process safety management program and a culture that encourages continuous improvement. As such, this chapter seeks to increase awareness of the specific considerations for SISs by concisely describing the basic stages and activities of the safety life-cycle, a cradle-to-grave approach to identifying, designing, and maintaining safeguards for process risk reduction, within the context of a typical engineering project and an overall process safety management program.

This text is not intended to repeat or replace the IEC 61511 standard, nor should reading this text be considered a substitute for a thorough understanding of the IEC standards and any applicable regulatory requirements. There are many books and countless technical papers devoted to various aspects and perspectives of SISs, several of which are listed as references here, such as Paul Gruhn and Harry Cheddie's *Safety Instrumented Systems: Design, Analysis, and Justification* (Gruhn and Cheddie, 2006), Ed Marszal and Eric Scharpf's *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis* (Marszal and Scharpf, 2002), William Goble and Harry Cheddie's *Safety Instrumented Systems Verification: Practical Probabilistic Methods* (Goble and Cheddie, 2005), and David Smith and Kenneth Simpson's *Safety Critical Systems Handbook: a Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards* (Smith and Simpson, 2011). The author encourages the reader to seek out additional

references that will address specific needs in greater detail. As with any engineering activity, SIS engineering requires judgments to be made based on knowledge and experience, and should not be undertaken without a suitably proficient leader in responsible charge.

22.2 Fundamentals

As a society, we accept certain risks in order to realize certain benefits. Risk can never be completely eliminated from any activity, but it is the responsibility of those who engineer and operate hazardous chemical and manufacturing processes to reduce the exposure to risks of on-site workers, off-site populations, and the environment to a level at or below what society considers tolerable. But how safe is safe enough?

The judgment of tolerability is complex. One approach, first put forth by the HSE, is the idea that there is a range of tolerable risk that above which cannot be justified in any circumstance, and below which is considered broadly acceptable where no further risk reduction effort should be expected. The region between these two levels is where risk should be considered acceptable only after being reduced *as low as reasonably practical* (ALARP). If suitable benefits can be realized, further risk reduction is not required once such efforts become impractical. Each process owner must determine the methods and the criteria for expressing tolerable risk for various risk receptors before any efforts to manage risk can be successful.

In any case, the more hazardous a process, the more critical it becomes to have reliable engineering and administrative controls to reduce the risk of hazardous events. Risk of a given hazard can be expressed as the product of the consequence likelihood and magnitude. Conversely, risk reduction can be accomplished by reducing an event's likelihood, consequence magnitude, or a combination of both.

Further explanation of ALARP and risk tolerance within the context of SISs can be found in Part 3 of IEC 61511 (IEC, 2003b), and *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis* (Marszal and Scharpf, 2002). *Safety Instrumented Systems: Design, Analysis, and Justification* (Gruhn and Cheddie, 2006) is also an excellent comprehensive reference for many fundamental tasks and considerations of SIS engineering.

22.2.1 Layers of Protection

No solution can ever be assumed to be 100% effective, therefore the most dependable risk reduction strategy will employ multiple diverse safeguards, or *protection layers*, that can each effectively reduce the severity or likelihood of hazardous events. In some cases, protection layers involve operator action, some may be automatic,

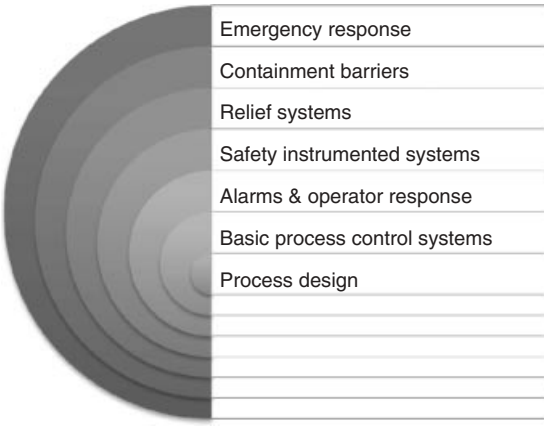

Figure 22.1 Typical layers of protection.

and others may simply lessen the effects of a loss of containment once it has already taken place, resulting in a more tolerable outcome.

Figure 22.1 illustrates common protection layers. *Preventive* layers are those that when functioning properly can stop a loss of containment from occurring, reducing its likelihood, whereas *mitigative* layers may lessen the magnitude of the consequence. Preventive measures are preferred, when possible. The effectiveness of mitigative layers may be difficult to quantify, and in some cases these may simply deflect the hazard – changing the consequence receptor. SISs are most often preventive in nature; however, instrumented fire and gas systems are mitigative and should be considered an SIS if credited with risk reduction.

Layers of protection can also be categorized as active or passive. *Active* layers include any devices or systems that must move or change state to be effective. This includes instrumented systems, relief devices and relief systems, and any responses involving human intervention. *Passive* layers are typically the strongest as they do not have moving parts that can fail, nor can they be easily removed. Passive layers include containment barriers such as dikes (bunds), blast walls, and flame or detonation arrestors, and may also include inherently safer process design, where equipment is engineered to specifications that exceed worst-case process conditions (CCPS, 2001).

SISs are important layers of protection for hazardous chemical processes because they may be the last layer that can prevent a loss of containment of material or energy. In some cases where a failure of the BPCS is the initiating cause of a hazard, the SIS may be only layer that can respond quickly enough to prevent a loss of containment. Well-engineered SIFs are also capable of achieving orders-of-magnitude lower probabilities of failure than many other protection layers (in some cases 1×10^{-4}or lower), which is why much effort and care are devoted to their design and maintenance.

22.2.2 Control Versus Safety

SISs share very similar construction and technology to BPCSs. Modern systems of each are microprocessor based, programmable, and use much of the same technology for sensors, final elements, field wiring, and digital communications. Both are typically designed to fail to a safe state, electrically and mechanically. Fundamentally, however, control and safety systems are engineered for different purposes with competing priorities, requiring many different considerations.

BPCSs are active systems often providing *continuous, analog* control. In response to one or more input process variables, a BPCS control loop will seek to modulate its output to maintain a setpoint. Control loops are installed to optimize certain parameters in the process or piece of equipment. The systems are designed to aid the operator in maximizing throughput, product quality, material efficiency, energy efficiency, or any number of variables relating to process availability and profitability.

SISs are also active systems; however, they are typically *discrete* (on or off) in nature, and remain *dormant* until called to act. The SIS exists to shut down the process or piece of equipment, bringing it to a safe state when certain conditions are violated. This is accomplished most commonly by actuating valves or stopping rotating equipment by de-energizing control circuits. These systems are installed in order to protect people, the environment, or process equipment from dangerous deviations from normal operating conditions, and may take action in response to losses of control, human errors, or any number of external events.

SIFs are the individual logic functions programmed or configured within the SIS. A SIF is most typically designed to detect a specific process condition that is known to lead to one or more specific hazardous consequences, and respond by bringing the process to a safe state. Most often in continuous processes this is accomplished by a *trip* or a *shutdown* function that stops the addition of thermal or kinetic energy, or vents a product in an effort to stop the process quickly and prevent the progression of a hazard scenario. SIFs may also be designed to maintain a safe state through a change in operating modes in order to prevent a specific hazard. *Permissive* functions, for example, are frequently designed to enforce a particular order of operations, and are commonly used in batch processes, or to prevent resetting and restarting equipment out of the proper sequence.

22.2.3 Access Restriction

In order to accomplish its primary goal of allowing effective operation of the process, the BPCS must provide the operator a certain level of flexibility in decision-making. Systems must allow for the manipulation of certain aspects of the configuration such as control setpoints, automatic or manual control, and in certain circumstances PID (Proportional-Integral-Derivative) controller parameters

and alarm setpoints. This interaction is completely normal for the process control system, but would quickly render the SIS ineffective.

A critical characteristic of a reliable SIS is strict access control and a rigorous change management process. A well-designed SIS should require very little interaction. Normal human interfaces should be limited to predetermined commands configured as inputs to the program logic, such as manual shutdowns, resets, and overrides for maintenance and testing activities or to allow startup in certain circumstances. Any changes to program logic or trip setpoints while on-process should be rare, and must be very carefully planned and tested in an offline environment to ensure predictable behavior. Changes should never be made for operational convenience and, according to IEC 61511, should always follow a strict management of change (MOC) protocol including thorough planning, review, approval, and communication. It is also good practice to separate physically any computers and networks used with the SIS from normal BPCS operating consoles and control networks to limit the possibility of unauthorized or inadvertent change. Many SIS hardware manufacturers recommend configuring unique security credentials to ensure that only those individuals with proper training and authority can gain access to the systems.

22.2.4 Testing and Diagnostics

Failures of BPCS control loops are largely self-revealing. A loss of control will become obvious to the operator as the process does not respond or the deviation between setpoint and process variable fails to resolve. With many components in constant use, scheduled testing is usually unnecessary and preventive maintenance is often reduced.

Under normal operating circumstances, many SIS components are energized in a fixed position and may remain that way for months or years at a time. These characteristics present significant challenges for long-term reliability. Certain failure modes of all components will *not* be self-revealing, such as a valve sticking open or electrical contacts welding closed. Although minimizing unnecessary process interruptions is an important consideration for SIS designs, the priority is reliable safety performance. For this reason, periodic testing and preventive maintenance are required to confirm that all components in the system are capable of responding when needed.

Between functional proof tests, SIS hardware diagnostics are critical in detecting electrical faults and electronic malfunctions within individual components. Modern BPCS and SIS hardware are both equipped with extensive diagnostic capabilities covering both field devices and the programmable systems; however, their use in control applications is far less critical and may be implemented as a means for improving operability and process availability. The objective in a safety application is to detect the presence of critical failures before the system is required to act so that those components can be repaired or replaced. The type of diagnostics available and the actions that the system is designed to take in response to detected

failures may have a significant impact on the overall integrity. This will be evident using any of the calculation methods described in ISA TR84.00.02-2002, a five-part series detailing several SIL verification methods (ISA, 2002).

22.2.5 Redundancy and Fault Tolerance

Redundant equipment is frequently installed as part of both BPCS and SIS equipment to improve *fault tolerance*, the ability of the system to continue operating in the presence of a loss of capability in one of the components. The concept protects against negative impacts from *random failures* of the hardware by providing alternative pathways to detect process conditions, process and transmit information, or take action to influence the process.

The components of the BPCS that are most concerned with fault tolerance are typically those that deal with the availability of communication and display of information to the human operator. Control loops rarely make use of fault-tolerant sensors and even more rarely final elements.

SIS systems, on the other hand, are frequently designed to function with minimal human interaction or communication between logic solvers. Redundancy is important with all components from a standpoint of minimizing the likelihood that an undetected, *dangerous failure* prevents the system from functioning. Once the overall reliability of the system has been addressed, redundancy can also be added to reduce the frequency of *safe failures* spuriously shutting down the process. While components failing to a safe state are preferred to dangerous failures, such failures are usually not entirely safe. Emergency shutdowns and restarts are typically the most dangerous modes of operations, and it is good practice to engineer the SIS with enough redundancy and diagnostics to reduce spurious trips caused by safe failures, in addition to meeting the safety integrity requirements for dangerous failures.

22.2.6 Independence and Diversity

The BPCS helps maintain the process within its design limits and is one of first lines of defense against hazardous events. It is also common and good practice to have process-related interlocks within the BPCS that prevent human error and equipment failures from leading to hazardous process conditions. It should not, however, be the primary responsibility of the BPCS to detect and take action to prevent process hazards for several important reasons.

The BPCS is primarily responsible for basic regulatory control of the process. It is largely an open and flexible system that undergoes frequent changes, often with limited access control and only basic preventive maintenance. For these reasons, automated systems require separation of control and safety devices and functions. This is not due to any particular limitations of the technology, as modern control systems are highly robust and reliable, but it has to do with how the systems

are controlled and maintained, and the fact that combining control and safety responsibilities in a common system introduces many single points of failure that compromise both.

Minimizing the likelihood of *common-cause failures* is one of the highest priorities of SIS engineers. Common-cause failures occur when a single event renders two or more separate channels of a system incapable of functioning. BPCS sensors and final elements used for control should not be shared with SIS functions for safety, or a failure that results in a loss of control may also render the protection ineffective. But issues of common cause do not stop there. The SIS engineer must also consider the effects of *any* single failure that could impact both control and safety devices, or two or more redundant safety devices. This includes shared process connections, shared utilities, and support systems; not simply the primary devices themselves but all components of the system that effect their correct operation.

Two or more different means of accomplishing the same task are less likely to suffer from issues of common-cause failure. Diversity in sensor technology, sensor manufacturers, I/O module terminations, cable routing, and even testing and calibration schedules should be considered. Electrical power supplies and distribution, heat tracing, and instrument air supplies should all be designed and constructed in a way that minimizes single causes of multiple failures. This can require some effort and the cooperation of a number of disciplines, but will help reduce the impact of both safe and dangerous failures.

22.2.7 Integrated Control and Safety

Access control, fault tolerance, diagnostics, safe failure characteristics, regular testing, preventive maintenance, and independence all contribute to SISs being capable of providing several orders of magnitude better risk reduction than BPCS protection layers.

Nearly any modern SIS will provide process variables and alarms to the BPCS (often a distributed control system, DCS), and receive a limited number of inputs and commands from the BPCS. The operator console commonly provides a single *human–machine interface* (HMI) to display process and equipment health from both the BPCS and SIS. These characteristics alone do not necessarily compromise independence; however, as advances in technology and digital communication protocols make this increasingly seamless to both engineers and operators, control system vendors may advertise an integrated control and safety system (ICSS), including control and safety hardware designed according to the requirements of IEC 61508.

Although there would seem to be many obvious advantages in having a common platform, responsibility remains on the SIS engineer to approach such a solution cautiously and to ensure that the implementation conforms to the requirements of IEC 61511. The basic principle of independence must still be addressed in a way that is technically appropriate and not simply convenient or cost efficient. In some cases, a combined system may not qualify as a *demand mode* system,

meaning *continuous mode* rules for SIL determination and SIL verification may apply. Continuous mode systems are not discussed in great detail in this chapter, but the criteria should be understood before proceeding with an integrated design.

22.3 Planning and Management

Management of process risk reduction is not an isolated effort, and responsibility is not limited to a single individual or a single group within an organization. Success requires experienced leadership, stated goals, allocation of resources, and periodic review. Although it is the process owner who ultimately owns the risk of operating the facility, willing commitment and participation are required from all levels, especially those most exposed to risk.

Functional safety is just one aspect of an overall process safety management plan, but owing to the complexity of programmable systems and the infinite combinations of both physical and human elements, it is one that requires a high degree of care in order to achieve high levels of risk reduction. Requirements for the management of functional safety and the safety life-cycle process are described in both IEC 61508 Part 1 and IEC 61511 Part 1. Essentially, *what* is to be managed is defined by the standards, but the specifics of *how* each element will be addressed are up to the end-user to define and document.

Some effort is required to develop comprehensive procedures and quality control practices, but these are central components of the high risk reduction capability of SISs. These efforts are intended to ensure the ongoing integrity of the SIS, but will also lead to more consistent execution of projects and more effective overall management of process risk. These items are presented before the specific life-cycle activities because a management system should be fully developed before being put into practice.

The CCPS *Guidelines for Implementing Process Safety Management Systems* (CCPS, 2011) is an excellent reference for general process safety program development. ISA Technical Report ISA-TR84.00.04-2011 (ISA, 2011) provides specific guidance on the implementation of IEC 61511 (or ANSI/ISA 84.00.01, the American adoption of the international standard).

22.3.1 Functional Safety Life-Cycle Process

Functional safety standards cover more than just SIS design and engineering activities. They present an overall safety life-cycle which begins with a hazard and risk assessment (HRA) of the process design, and carries through the design, installation, operation, maintenance, and modification of all protection layers over the life of the process. While the standards do not cover specific requirements of all protection layers, performance requirements for each SIF are determined with consideration of the risks, the integrity of other protection layers, and within the

context of a facility's tolerance for risk. Changes to or removal of protection layers may have an impact on the requirements of the SIS and cannot be evaluated in isolation.

The standards present many requirements, not only for SIS hardware and application software, but also for planning, documentation, and competency of personnel involved throughout the life-cycle. The requirements are not prescriptive in nature where specific design constraints are placed on specific pieces of equipment. Rather, to be applicable to any chemical or manufacturing process, and any present or future instrument and systems technologies, the standards present a framework for making risk-based decisions, setting quantitative performance targets, and quantitatively verifying performance over time based on equipment reliability and other metrics.

While there are many individual tasks and many ways of representing the overall safety life-cycle, the simplest involves three primary phases: *analysis*, *realization*, and *operation*. Figure 22.2 shows all three primary phases executed from end to end, organized around a central plan and management system. The process will undergo periodic verification and validation activities, with documentation required throughout. The analysis phase begins with a conceptual process design. Risks of operating the process and process equipment are considered and safeguards are designed to address them. Specifications are developed to guide the detailed engineering activities taking place in the realization phase. Realization includes the engineering, procurement, installation, and commissioning activities. The

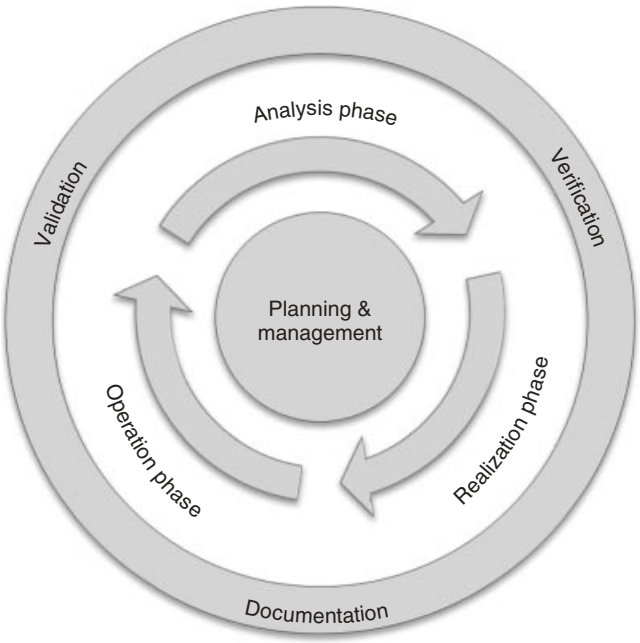

Figure 22.2 Simplified safety life-cycle process.

operation phase begins with the startup of the process, and involves ongoing maintenance and testing, in addition to the MOC, and the continuous monitoring of safety performance metrics. Changes to the process design and regular revalidations of the HRA will initiate new cycles until the facility's eventual decommissioning.

There is likely to be some overlap of activities from phase to phase, and information will need to flow between a variety of disciplines and organizations. This is why each facility or project must develop and document their own approach to the safety life-cycle, with roles and responsibilities assigned, and the inputs, outputs, and interfaces described for each activity.

Safety life-cycle requirements are contained in Clause 6 of IEC 61511 Part 1 (IEC, 2003b).

22.3.2 Policies, Procedures, and Documentation

For each major activity of the safety life-cycle, *policies* must be developed to guide decision-making and establish priorities for each element of the program. An effective policy will explain *what* the activity is and *why* it is being undertaken, acknowledging the requirements for compliance, defining the strategy for satisfying each requirement, and assigning responsibilities. Functional safety policies should be developed in alignment with, or as a component of, the overall process safety management program to ensure that common goals are established and that complementary and non-competing roles are served by various groups within the organization. The collection of policies may be contained in separate documents, may be combined, or may be contained within the larger process safety management policy documents. In any case, the collection of functional safety policies will be referred to in this chapter as the *functional safety management plan*.

Procedures must also be written for each activity to explain *how* it is to be performed, defining the steps required for completion and the criteria for success. Some activities such as system hardware design or application logic design may simply provide guidelines and best practices to allow for engineering judgment. Other activities such as field device maintenance, calibration, and testing may have very detailed work instructions and checklists to ensure completeness and consistency. Procedures should consider all information required for a particular task, including preparation and coordination activities, required tools, and required qualifications or training.

Policies and procedures alone do not make a management system complete. *Documentation* must be maintained to record activities throughout the program. Evidence must exist to demonstrate compliance with the program, to facilitate continuous improvement efforts, and to promote accountability. Records of activities may also provide valuable information for trouble-shooting or investigations following an incident. Policies and procedures should address what documentation is required, and also how and where documents are to be managed.

A document management system should be in use to cover the policies and procedures guiding the program, and also the documents and records generated through

its execution. This should include a hierarchical structure, a naming/numbering structure, and revision/approval control. Modifications should be very carefully controlled while still allowing open access for all to review.

Overall planning and management requirements are detailed in IEC 61511 Part 1 (IEC, 2003b) in Clauses 5 and 19. Specific procedures and documentation requirements are listed throughout IEC 61511 Part 1 (IEC, 2003b).

22.3.3 Roles and Responsibilities

Functional safety standards define many tasks that must be completed and documented as part of the safety life-cycle, but do not define who must be responsible or even to what organization those responsible must belong. Most projects and even routine plant maintenance activities may be performed with one or more contract engineering, construction, or maintenance service providers. Each organization and every individual involved must be informed of their roles in the overall safety life-cycle, in addition to their specific responsibilities.

A *senior experienced person* should be assigned by plant management as a champion for functional safety to oversee the entire program. This individual should be responsible for developing and maintaining the functional safety management plan, and ensuring that an appropriate technical approach is documented and executed in each iteration of the life-cycle. This person should have final review and approval authority over SISs and should ensure the competency of all individuals developing, leading, and carrying out the life-cycle activities. The specific qualifications for this role, or any other role, are not explicitly outlined by the IEC 61511 standard, but suggested criteria for evaluating individuals and organizations are listed in IEC 61511 Part 1, Clause 5 (IEC, 2003b).

Everyone involved must possess an adequate combination of knowledge, experience, and training in the area(s) for which they are responsible. Competency requirements and the criteria for evaluating individuals in various roles, including contractors and their organizations, should be developed as part of the planning activities. Appropriate training and qualification records must also be maintained by the process owner. End-user involvement and communication are critical. It should never be assumed that all participants understand their roles; these must be proactively communicated with periodic review and follow-up.

22.3.4 Performance Management

The functional safety standards are designed around a performance, or quality management model, commonly described with some variation of the *PDSA* (plan–do–study–act) model, which has its roots in the scientific method (Demming, 1986). Performance objectives are established, systems implemented, actual performance assessed, and objectives re-evaluated in an effort to enable continuous improvement. Activities described in this chapter are organized according to

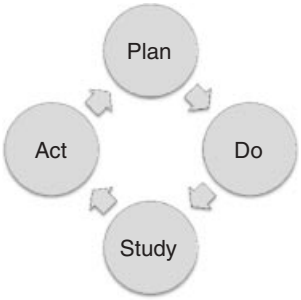

Figure 22.3 Performance management model.

major safety life-cycle phases; however, the performance model is a key component of each activity in the life-cycle as well as the overall management system (Figure 22.3).

Specific quality control activities are mentioned throughout IEC 61508 and IEC 61511. *Verification* in the context of the standards refers to a review or test to confirm a specific activity or deliverable has met its required objectives. Every activity and document generated should be subjected to some form of independent verification. *Validation* occurs when a SIF is physically tested and evaluated against the functional requirements in the safety requirements. *Functional safety assessments* may take place periodically during the life-cycle, frequently when approaching a major project milestone, with one being required immediately prior to startup. Such an assessment seeks to confirm that the collection of activities and deliverables as part of a specific project have met the objectives of the functional safety management plan and the requirements of IEC 61511. Finally, functional safety audits should be conducted periodically to evaluate the performance of the program overall, and may be conducted independently, or in conjunction with an overall process safety management system audit. The auditing process is described in great detail within the CCPS *Guidelines for Auditing Process Safety Management Systems* (CCPS, 2011).

All of these activities are designed to reduce the frequency and magnitude of *systematic* and *systemic failures*, and enable continuous improvement, thus improving functional safety. Systematic failures are those that result from incomplete or improper specification, failure to follow a specification or procedure, and any number of individual human errors that affect the ability of the SIS to function. Systemic failures are those that result from organizational or cultural issues that occur at a higher level, involving many individuals and patterns of behavior rather than isolated errors. Identifying both systemic failures, and systematic errors and omissions may be best accomplished with a certain level of independence between the reviewers and the practitioners to reduce bias and introduce other perspectives. The degree of independence may depend on the complexity or novelty of the design, the experience level of the team, and the level of risk reduction the system is designed to provide (IEC, 2010).

22.4
Analysis Phase

The basic control of risk will begin with the conceptual process design. At this stage, initial equipment specifications and basic process control schemes are developed. Often the risks associated with the process can be more easily anticipated by the conceptual design team and addressed more simply at an early stage using inherently safe design concepts.

Once the nature of the process takes shape, efforts can begin to engineer safeguards for containment of chemicals and energy. It would be good practice to begin a conceptual SIS design in parallel with the process control system design. Issues that may lead to common-cause failures between control and safety instrumentation, such as shared devices or process connections, should be avoided. Any applicable industry engineering standards or corporate guidelines that place design requirements on the process control or safety systems should also be applied at this time. Following an assessment of process risk, the performance requirements for SIFs can be determined and specifications documented.

22.4.1
Process Hazard Analysis

Both within the design stage of a project and regularly during a facility's operation, the process design should undergo a process hazard analysis (PHA), sometimes called a hazard and risk assessment. A PHA should be performed by a team of people familiar with the process and the equipment, with representation from process engineering, operations, and maintenance groups at a minimum, and often with additional support from mechanical, electrical, instrumentation, and controls engineering (CCPS, 2008a).

The basic objective is to identify hazards associated with the process and equipment so that steps can be taken to reduce their risk. This is frequently accomplished using the hazard and operability (HAZOP) methodology, which involves subdividing the process equipment into smaller, more manageable pieces, and systematically reviewing the causes and consequences that may result from process or procedural deviations. HAZOP is the most commonly applied, although there are alternatives.

The study should perform an in-depth review of the mechanical flow diagrams or piping and instrumentation diagrams, control system design, and often operational and maintenance procedures. Cause–consequence combinations or hazard scenarios should be qualitatively evaluated by assigning severity and likelihood rankings and safeguards or protection layers (including SIFs) should be identified that may lessen the consequence severity or likelihood of each. The risk ranking process helps prioritize areas of risk so that they can be further evaluated and addressed by a larger team outside the PHA.

A process deviation occurs when normal operating conditions are violated. This may or may not amount to a complete loss of control, but those situations that

could lead to a loss of containment should be prioritized. Most deviations have many possible causes, including process equipment failures, utility failures such as electrical power, control system failures, and human errors, among others. Even those causes that seem implausible should be recorded by the team so that it will be clear to others that they were considered.

The PHA plays a major role in shaping engineered safeguards such as SISs, and becomes the foundation for risk-based decision-making. The study may identify areas where new protection layers are needed or may simply allocate existing protection layers to particular hazard scenarios. In either case, one must begin to understand the specific hazards before safeguards can be designed to prevent them. The principles and various methodologies of PHA are covered in greater detail in Chapter 21 by Paul Baybutt, "Analytical Methods . . ." (hazard and operability (HAZOP), what-if (WI), fault tree analysis (FTA), etc.).

22.4.2 Layers of Protection Analysis

One of the failings of qualitative assessments of risk is that human judgment tends to underestimate the possibility of unexpected, random events, especially events caused by multiple concurrent failures. Major process accidents rarely occur due to a single cause, so it is precisely these low-frequency, high-consequence scenarios that should attract attention through more precise quantitative likelihood analysis.

Often done in conjunction with or immediately following a PHA, a LOPA seeks to semiquantitatively refine the qualitative assessments of the PHA risk ranking. This is done in order to reduce the subjectivity in scenario likelihood estimations, and either to confirm the adequacy of existing protection layers or to ensure that additional protection is installed to meet or exceed the owner's tolerance of risk.

LOPA is based on the concept of an event tree, a fault propagation modeling technique which begins with a single initiating event and carries through a series of intermediate or branch events, each with multiple possible outcomes. Typically, initiating events and final outcomes are expressed as a frequency, such as events per year. At each particular branch, the outcomes are generally considered complementary or mutually exclusive. The frequency of a particular final outcome depends on the initiating event frequency and the probability of each branch event in the series (Figure 22.4).

A LOPA scenario is essentially a simplified analysis of a single path through an event tree diagram. Each intermediate event represents a protection layer with two complementary, mutually exclusive outcomes – true or false, success or failure. Additional factors such as scenario enablers, time-at-risk factors, and other conditional modifiers may also be accounted for in terms of a probability. Commonly, the LOPA team or analyst will only be concerned with the worst-case outcome of each scenario in order to determine the maximum risk posed by a single initiating event, although when there are multiple possible consequence receptors (on-site injuries, off-site injuries, environmental impacts, asset damage, production downtime, etc.), it may be useful to examine each independently to ensure that

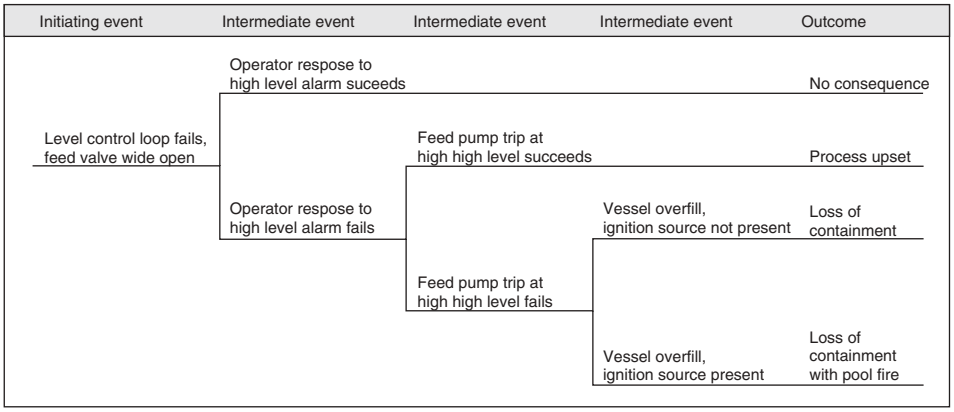

Figure 22.4 Example event tree diagram.

adequate protection layers are in place for all outcomes, or that protection layers do not create secondary hazards. Effective protection layers may also vary by consequence receptor. A LOPA diagram such as that in Figure 22.5 may be used to visualize the process.

Variations of the process are possible, but in general, probability multiplication is used to evaluate the initiating event frequency, scenario enabler and conditional modifier probabilities, and the probability of failure of each protection layer to yield a mitigated event frequency. LOPA requires that safeguards be evaluated according to certain criteria in order to qualify as *independent protection layers* (IPLs). In order to qualify as an IPL, a safeguard must be:

- **Independent** – from all components of the initiating cause and other protection layers;
- **Effective** – in preventing the hazard or reducing its severity on its own at least nine times out of 10; and
- **Auditable** – in terms of design, maintenance, and integrity requirements.

In order for the LOPA results to be valid, each protection layer must be independent. Dependences between protection layers or with the initiating event are not readily addressed with simplified mathematical analysis, nor can dependent

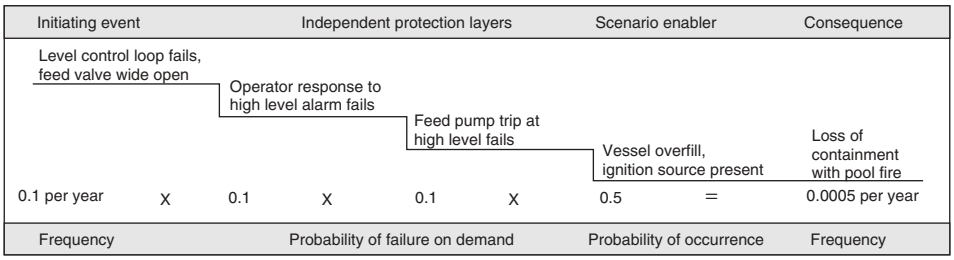

Figure 22.5 Example LOPA diagram.

protection layers be considered effective in preventing a hazard if the device on which they rely is already known to have failed.

Whether or not the mitigated event frequency is considered tolerable by the process owner will depend on the estimated magnitude of the consequence and the consequence receptor. It is necessary to establish certain criteria in advance for evaluating tolerance to risk, which should also be expressed in terms of frequency. If the mitigated event frequency is greater than what is tolerable, the difference represents the additional risk reduction required from additional IPLs.

LOPA may also be utilized within the framework of the ALARP principle by establishing certain maximum levels of tolerable risk, as well as more conservative *target* or minimum levels of risk. Unless such a strategy is employed, LOPA should *not* be used as a means to justify removal of protection layers. SIS functions not requiring a specific SIL are common, and this does not imply that they should simply be removed.

In summary, the LOPA technique provides the analyst or analysis team with a framework for determining which safeguards qualify as IPLs. This ensures that safety does not depend too heavily on items with common causes of failure. The LOPA technique aids in focusing attention on the areas of highest risk, more precisely and consistently applying effective safeguards. The LOPA technique is discussed in detail in the CCPS texts *Layer of Protection Analysis: Simplified Process Risk Assessment* (CCPS, 2001), *Guidelines for Independent Protection Layers and Initiating Events* (CCPS, 2012), and also in chapter 23 by Paul Baybutt, ''Layers of Protection Analysis''.

22.4.3 Safety Integrity Level Determination

A SIL is an order-of-magnitude expression of the availability of a SIF to carry out its designated actions to prevent a particular hazardous event. A SIL-1 SIF can be counted on to be successful at least nine times in 10 opportunities, which equates to at least 90% availability, or an average probability of failure on demand (PFD_{avg}) of less than 0.1. Likewise, a SIL-2 SIF must be successful at least 99 times out of 100 opportunities, at least 99% available, and with PFD_{avg} less than 0.01.

There are four distinct SILs according to IEC 61508 and IEC 61511 (Table 22.1). Each level represents an order of magnitude greater risk reduction that the previous one, will generally also require an order of magnitude greater care in design and maintenance, and likely has greater costs of installation and maintenance due to requirements for higher reliability, redundancy, and fault tolerance.

The quantitative result from a LOPA can be readily used to assign SIL. Using the table 22.1, risk reduction requirements can easily be translated to a SIL. Although there are four SILs, it is generally thought that risk reduction is best accomplished through multiple IPLs. Relying too heavily on a single system or solely on instrumented layers is not good practice no matter how reliable or fault tolerant because the systematic failure potential will begin to outweigh the random failure potential. A project team finding a gap of 1×10^{-3} or greater for a

Table 22.1 Safety integrity levels.

Risk reduction required	Acceptable safety integrity level (SIL)	Acceptable average probability of failure on demand (PFD_{avg})
$\geq 1 \times 10^{-1}$	1	$< 1 \times 10^{-1}$
$\geq 1 \times 10^{-2}$	2	$< 1 \times 10^{-2}$
$\geq 1 \times 10^{-3}$	3	$< 1 \times 10^{-3}$
$\geq 1 \times 10^{-4}$	4	$< 1 \times 10^{-4}$

given situation after applying all available non-SIF IPLs should begin to assess the possibility of a more inherently safe process design or other forms of administrative control of risk.

Risk graphs and risk matrices are simplified, qualitative SIL determination methods. Although these methods can be calibrated to account for greater or less risk tolerance, they are more subjective in nature. These techniques do not directly account for the reliabilities of other safeguards or protections layers and are more likely to lead to over- or under-designed systems. It is the author's belief that these methods are generally inadequate for estimating required risk reduction for SISs and do not offer a significant savings in the level of effort required to complete an analysis. Because much effort is devoted to verifying quantitatively the resulting SIL of SIFs, failure to assign a SIL target quantitatively may lead to a system that is more expensive than necessary, requires more frequent testing and maintenance than necessary, or one that simply does not provide a level of protection adequate for the actual risk.

Guidance for determining SILs can be found in Part 3 of IEC 61511 (IEC, 2003b).

22.4.4 Safety Instrumented Function Design and Safety Requirements Specifications

Preliminary SIS design may have begun prior to the PHA or, in some cases, needs for new SIFs may have been discovered during the PHA. In either case, it is important for the SIS engineer to ensure that each SIF is specifically designed to detect the hazardous condition(s) in question and stop the progression of the hazardous event(s). For example, preventing overpressure of a reactor will likely require pressure sensors, and their locations on the vessel must be appropriate for the best, most direct measurement of the hazard. Inferring high pressure through some other process variable, or too far upstream or downstream in the process, may not always be effective or provide an adequate response time.

The SIS engineer must also consider the actions that a SIF must take to prevent the hazardous event. If the scenario that results in vessel overpressure is caused by a runaway reaction, simply removing external heat sources may slow the reaction but will likely not prevent overpressure – meaning that the SIF would be ineffective in preventing the hazard and will not qualify as a protection layer for the scenario.

Once the actions required for safety have been determined, there may be additional actions a that SIF should take to address secondary hazards. This may include tripping additional SIFs protecting upstream or downstream equipment, or may simply involve operability issues, such as setting a BPCS controller to close its control valve. Further still, entire logic functions may be specified for secondary purposes to take advantage of existing SIS instrumentation for operability reasons, but will not necessarily be called for by the PHA or assigned a SIL. Whether or not these functions are designated as SIFs or some other name will depend on the preferences of the end-user. Rationale should be documented in the functional safety management plan to guide engineers and provide distinctions for auditors.

SIF design is highly dependent upon the chemical or manufacturing process, and may require significant input from process engineering, operations, and other disciplines to ensure that the correct actions are taken in the correct sequence and within an acceptable amount of time. The *process safety time* is the amount of time between the initial detection of the process deviation and the point at which the hazardous event can no longer be prevented. This means that the available process safety time is dependent upon the trip setpoint selected and will need to be carefully coordinated with the parameters of other protection layers.

A SIF's *response time* includes the sensor lag time, the logic solver system's processing time, any delay timers included in the logic, the time it takes physically to actuate the output device(s), and the time it takes for these actions to impact the process. This time depends on many factors and may vary from minutes to fractions of a second. It is critical for the SIS engineer to coordinate with other disciplines in selecting appropriate trip setpoints that will initiate each SIF with sufficient time to act before the process safety time is exceeded, and to ensure that appropriate devices are selected and sized to be capable of meeting the requirements. It is customary to ensure that a SIF's response time is less than half of its process safety time. The actual SIF response time should be used to judge success or failure during commissioning and subsequent proof-testing over the life of the system; meaning that adjustments to setpoints may be required, or components may need to be replaced if the response time is too long or begins to grow over time. The setpoint determination methods and the relationships to other protection layers and their setpoints should be maintained as part of the process safety information and examined carefully when any changes are proposed.

All issues relating to the proper design, engineering, installation, operation, maintenance, and modification of a SIF should be documented in a safety requirements specification (SRS). This document or collection of documents is intended to record the extensive list of issues relating to the correction functioning of a SIF for two critical audiences. First, the SRS will communicate specific requirements to the team involved in a project's detailed engineering, installation, and commissioning activities. This may include measurement technology and instrument selection criteria, the quantity and architecture (e.g., voting) of field devices, logic requirements, diagnostics and alarms, on-process testing facilities, interfaces to the BPCS, HMI, or other third-party systems, among many other items. It also serves as a critical reference for the end-user during operation and maintenance

of the system. The SRS will record any specific operational requirements and maintenance and proof-testing requirements, and will provide a record of the intended purposes of the SIF and the scenarios that it is designed to prevent. This information is extremely valuable for those not involved in the original design for either supporting or rejecting future changes to the equipment over the life of the system.

IEC 61511 Part 1 provides a detailed list of SIS hardware-related items to be documented in an SRS in Clause 10, with application software-related items detailed in Clause 12.2. There are no specific requirements for how the information must be presented, so each end-user may choose a format for narrative descriptions, SIF specification data sheets, or some combination of the two. In practice, there are many items that are simply documented in tabular form such as trip setpoints, response time requirements, and proof-test intervals, but many others may require some effort to explain in more detail, such as requirements for reset and restart. The level of detail required in an SRS may depend heavily on the amount of standardization called for in corporate or facility-level SIS policy and procedure documents. Often hardware and software design guideline documents or a global SIS design basis document will detail many specifics about how the system should be designed and how logic should be constructed, making some portions of SRS development much simpler and less repetitive. The IEC standards do not require that all aspects of the SRS information be contained within a single document, provided that there are clear and traceable references to all other sources.

It is also important to appreciate that some aspects of the SIS design will be iterative and certain details may need to be developed in the later stages of a project. The SRS should never be so rigid that it forces unnecessary complexity; however, care must be taken to ensure that the intents of the conceptual design are recorded in the SRS and understood by the detailed engineering team. As is common with many engineering design documents, a project team should consider producing as-built documents to capture additional detail along with any approved changes upon completion of the project.

The author believes that it is good practice to document the entire contents of an SIS in some way within an SRS, even if many elements or functions are considered ancillary and not directly credited with risk reduction. The SRS begins as a design and engineering tool, but later provides critical information to those responsible for operation and maintenance, and for future PHA revalidations and the MOC process. Failure to document the purposes and intents of all devices and functions may result in their misuse or removal over time.

22.4.5 Safety Integrity Level Verification

For each SIF assigned a SIL target, a quantitative verification must be performed to confirm that the combination of instrument redundancy, diagnostics, and testing specified is suitable for the required SIL and can reasonably be expected to meet or exceed the requirements for PFD_{avg}.

We rely on assumptions of PFD for all IPLs that are based on the histories of similar devices and simple systems in similar service, which can typically be validated through direct measurement. Each SIF, on the other hand, is its own complex system of devices – unique combinations of sensors, logic solvers, final elements, and support systems for each particular application – and all must function simultaneously in order to be effective. We can make assumptions about individual components based on their historical performance, but predicting SIF performance requires a much more thorough analysis.

In order to determine the suitability of devices and subsystems that comprise an SIF, the SIS engineer must first define the purpose of the function and the criteria for success. This will determine what components will be included within the boundaries of the model, and also what failure modes are of interest. For subsystems that are not designed as de-energize to trip, support systems required to actuate the final elements must be included, such as electrical power and instrument air or hydraulic pressure. All subsystem required to reach a safe state and their boundaries should be clearly identified in the SRS.

Once the boundaries have been set, the physical arrangement or architecture of devices and subsystems can be modeled. While constructing the model, each subsystem within the model should be examined for adequate fault tolerance. IEC 61511 lists specific requirements for hardware fault tolerance for sensor, logic solver, and final element subsystems based on the assigned SIL. A fault tolerance requirement of one, generally required for SIL-2 service, implies that no single device experiencing a dangerous failure should be able to render the SIF inoperable. This requires parallel redundancy through each subsystem and voting that does not require all components to agree, such as 1oo2 (one-out-of-two) or 2oo3 (two-out-of-three). IEC 61508 has similar requirements, although some flexibility exists in determining fault tolerance requirements based on the safe failure fraction of the subsystem components.

Fault trees and Markov models are two commonly used quantifiable modeling techniques for SIL verification. Fault trees begin with a defined undesirable, or *top event* (e.g., dangerous SIF failure) within a system, and expand through the logical relationships between subsystems and components using AND and OR logic gates (Figure 22.6). *Basic events* (e.g., dangerous component failures) are defined at the lowest level. Top event probability can be solved using rules of probability mathematics for the combinations of *fault* or *intermediate events* at each logic gate.

Markov models illustrate systems in various operating *states* connected by *state transitions*. Certain failures of individual components will not immediately result in a complete system failure. Markov models are very useful for modeling complex and repairable systems with many possible intermediate states of degraded operation. State transitions are quantified by assigning failure and repair rates, and models can be solved using matrix multiplication (Figure 22.7).

Regardless of the modeling technique used, it is important to include all factors that may influence both failure and repair, including issues of common-cause failures between like or related devices. The model should include all means specified for detecting component failures within each subsystem, such as diagnostics,

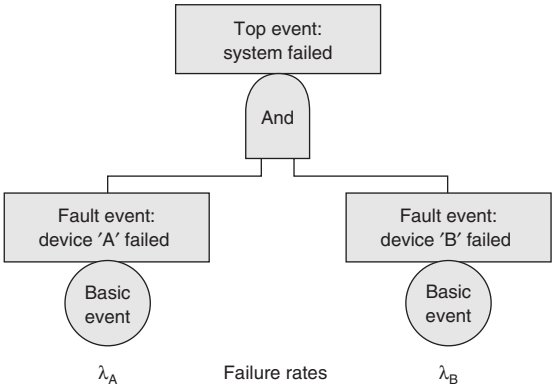

Figure 22.6 Simplified fault tree for a parallel system.

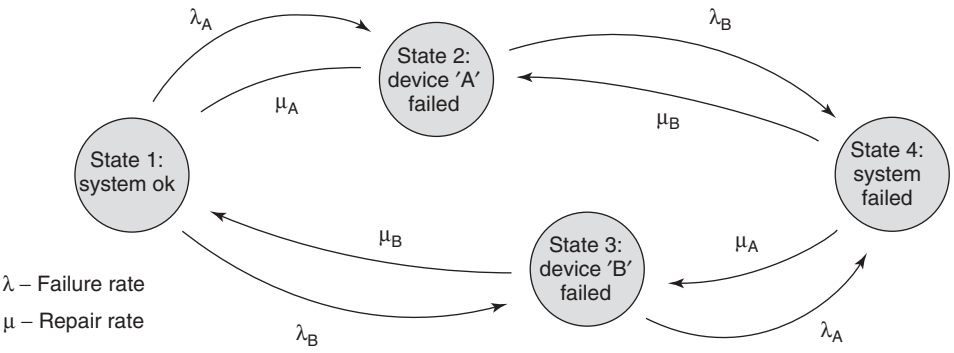

Figure 22.7 Simplified Markov model for a parallel system.

online testing, offline testing, how often each will take place, and how effective each is expected to be in uncovering all critical modes of failure. Each will have certain failure modes that can be uncovered, and those that cannot. Even offline testing and repair will not be able to restore all components to an as-new condition, hence an end-of-life replacement schedule may also be considered. When online testing takes place, or if a failure has been detected while the unit is operating, the model must also consider the mean time to restore proper operation of the component, as the time to test, calibrate, repair, or replace a component may mean that the device or the entire system remains unavailable or in a degraded state for some time. All of these factors will impact the overall integrity of each SIF.

The final step is to quantify the model and solve. Since the primary interest is in obtaining an average PFD, data should be gathered for devices in terms of their rates of dangerous failures. Obviously, more reliable devices will result in a smaller PFD_{avg}, but the coverage factors of diagnostics and testing, and also their frequencies, will also influence the overall PFD_{avg}. The best data to use in SIL verification studies are those collected from within your own facility. These

naturally account for the particular models of devices in use, how they are used, common installation and maintenance practices, and the conditions inside and outside the process. If a sufficient sampling of data is not available for each particular device, generic industry data are available from a variety of sources. All data used in SIL verification should be sufficiently conservative, or of high confidence to avoid under-designed and under-maintained SIFs with higher than anticipated PFDs.

PFD_{avg} is most generally a measure of a function's availability to act in the presence of a demand. Whereas a SIF's availability may be influenced by both random and systematic failures, the SIL verification process typically relies only on the statistics of random failures. The calculation seeks to demonstrate the capability of each unique combination of hardware to meet or exceed the PFD_{avg} requirement for the given SIL.

The probability of systematic and systemic errors leading to individual device or SIF failures is not easily quantified. If such items could be specifically identified and measured, they could most certainly be eliminated through more complete specifications or more appropriate work practices. The possibilities for such errors are real, but are generally addressed through qualitative means, such as thorough and independent reviews of specifications, and detailed work instructions in maintenance and testing procedures, and not necessarily quantitatively in the SIL verification. Attempting to include an overall safety factor or systematic failure factor may yield conservative results, but likewise may disproportionally impact functions with higher SIL requirements, leading to over-design or unnecessarily frequent proof-test intervals – neither of which will reduce the actual rate of systematic failures. At some point, the rate of manual testing becomes impractical, reducing system availability and actually increasing the PFD_{avg}. Manual proof-testing also involves human intervention which in turn increases the opportunity for human error. Human factors must certainly be considered throughout the safety life-cycle, but attempting to do so quantitatively in the SIL verification process is not likely to provide meaningful results.

IEC 61511 also requires spurious trip rate targets be specified and verified for SIFs. Unnecessary shutdowns can be both costly and dangerous, and often small changes in device architecture or application software can have a significant impact on their likelihood. What constitutes a spurious trip will depend on the architecture of devices just like the dangerous failure model. Although the physical architecture of devices is the same, the original dangerous failure model is likely to require some changes. For example, 1oo2 (one-out-of-two) voting will require both devices to fail dangerously to render the subsystem ineffective when examining PFD_{avg}; however, only one safe failure may result in a spurious trip. The analyst may also choose to draw different boundaries when components contribute to safe and dangerous system failures differently. When creating a second model for estimating spurious trip rate, each logical relationship should be re-examined, in addition to the failure rates, test coverage factors, and diagnostic coverage factors.

As is common in the process industry sector, this section explores the considerations for SIFs in a *demand mode*, which simply requires separation between

control and safety, and that a SIF failure will not result in a hazard being realized unless a failure also occurs in the BPCS. In other words, a *demand* for the SIF to act is assumed to be very infrequent, less than once per year, and a failure in the SIF is more likely to be discovered by a periodic proof-test than by a hazard being realized. This is a key assumption that allows us to perform SIL determination and SIL verification in terms of average PFD. There are additional considerations for SIFs in *continuous mode*, requiring analysis in terms of probability of failure per hour (PFH). Current versions of IEC 61508 and IEC 61511 differ in how these systems are classified, and both standards should be consulted if the requirements for demand mode do not hold true.

Reliability engineering is a complicated field of study, especially when dealing with complex systems of both electronic and mechanical components. Understanding failure is critical due to the dormant nature of SISs. Once the SIS is deployed in service, it could be several hours or several years before a SIF is called upon to act. SIS engineers must take steps in the design process to ensure that appropriate technology and maintenance are specified to keep the system in good working order at all times.

There are many books and other resources available covering topics of SIL verification and the methods mentioned above, including *Safety Instrumented Systems Verification: Practical Probabilistic Methods* (Goble and Cheddie, 2005) and ISA Technical Report ISA-TR84.00.02-2002 Parts 1–5 (ISA, 2002).

22.4.6 Justification

SISs may be installed for a variety of needs: personnel safety, environmental stewardship, protection against asset damage and business interruption, even lower insurance premiums, or combinations of these. Certain improvements or additions of instrumentation may be evaluated from a financial perspective once the basic requirements for safety have been met. It is possible that a lower PFD, providing a high-risk reduction factor, may easily pay for itself by reducing more risk on an annualized basis than the cost to install and maintain. Such cost–benefit studies are common when examining risk in the ALARP region. Of course, such evaluations should be used to justify improving risk reduction, and not reducing it.

Additional instrumentation may be justified even more simply when designed to reduce the rate of spurious trips. Spurious trip rate calculations as part of the SIL verification can be used to compare instrument architectures and optimize a design that simultaneously provides high levels of safety integrity and process availability. The reduction of one unplanned outage in some cases could be shown to justify the cost of an entire project.

Safety Instrumented Systems: Design, Analysis, and Justification (Gruhn and Cheddie, 2006) further explores SIS justification from both risk reduction and business interruption perspectives.

22.5 Realization Phase

The realization phase of the safety life-cycle corresponds to the detailed engineering, procurement, construction, and commissioning portions of a project. Although there is likely to be some overlap of activities within the analysis and realization phases, the conceptual design requirements are generally determined in the analysis phase by a smaller team and then executed in the realization phase by a much larger team. A larger team means more people who were not involved in the original design specifications, who will not have the benefit of knowledge developed in the analysis phase, and who may not completely understand the goals.

Projects of any size will likely have one or more engineering firms, construction contractors, control systems integrators, and many specialized disciplines that must coordinate information and communicate requirements. It will always be critical for the owner's senior representative(s) to remain engaged throughout the process to ensure that design specifications are followed, that all organizations maintain effective quality control practices, and that every individual understands their role in ensuring safety.

22.5.1 Hardware

When selecting hardware for safety-related applications, it is important to have a clear understanding of each component's characteristics, failure modes, and intended purposes, ideally through prior experience. Safety logic solver systems, and often many sensors and actuators, are being designed specifically for applications in SISs according to the requirements of IEC 61508. Such devices may be required by IEC 61511 to provide a *safety manual* that details any particular requirements for installation, operation, or maintenance. It is critical that these instructions are followed to ensure that the system as a whole will perform as expected.

A safety device will often undergo an independent assessment to ensure compliance with IEC 61508, including a *failure modes, effects, and diagnostics analysis* (FMEDA). Data can be used to determine the expected safe and dangerous failure rates, and a *safe failure fraction*. Devices with sufficiently high safe failure fractions can reduce the need for fault tolerance in higher-SIL applications according to the IEC standards. Such devices may be called "SIL-capable" and may come with a certificate of compliance of some sort. It should be noted that there are no testing agencies granted specific authority to certify devices for safety applications, nor is such a certificate required by IEC 61508 or IEC 61511. All devices should be appropriately evaluated by the purchaser for the intended application and the specific requirements listed in the SRS and Clause 11 of IEC 61511 Part 1.

Hardware procurement, especially for logic solver systems, may have to begin very early in the project, possibly before all of the design requirements and

I/O quantities have been fully determined. It is good practice to include significant spare capacity throughout the system to allow for modest growth as the project progresses and even during operation to avoid costly shutdowns for small expansions.

22.5.2 Application Program

Application program logic should be developed with careful consideration of the requirements defined in the SRS, cause and effect diagrams, and any logic narratives. Although the specific steps for system configuration and programming will vary by manufacturer and model, most modern systems are designed to follow one or more of the limited variability programming language specifications in IEC 61131 Part 3. The most popular include function block diagram and ladder diagram because of their flexibility and ease of use. Some systems offer options for sequential function chart, instruction list, and structured text. The method chosen should be appropriate for the application, and should always consider how the system will respond to unexpected combinations or sequences of inputs.

Priority must be given to considerations of human factors in logic design. Rules for consistent use of logic and internal documentation should be developed, not only for the benefit of the project team, but also more importantly, for those who will be responsible for future modifications and trouble-shooting. The use of custom function blocks and logic templates is an effective way to speed the application software development process while enforcing rules of consistency across large programs and even multiple systems in a facility. A single library of carefully designed, tested, and managed logic templates can greatly reduce the likelihood of programming errors and other systematic failures; however, a poorly managed or untested library will simply ensure the propagation of errors, magnifying their impacts. The concepts of performance management, including verification and validation, should be applied to the application software development process. An isolated development and testing stage for logic templates should take place before the application program development begins.

In order to ensure predictable behavior, all logic solver systems must be designed to detect and respond to various faults and abnormal system conditions. Diagnostic logic and fault handling for sensor inputs and feedback from final elements is especially critical in SIS functions. Any component required for safety should be promptly repaired or the system shut down appropriately when faults are detected that impact the overall integrity. Appropriate facilities for operational and maintenance overrides should also be provided. The requirements for fault handling and appropriate overrides may depend on both the SIL and the architecture of devices; how the application for each SIF must be designed to handle these items should be documented in the SRS.

Clause 12 of IEC 61511 Part 1 (IEC, 2003b) addresses SIS application software and the software life-cycle requirements.

22.5.3 Interfaces

The SIS should be designed to bring the process to a safe state without relying on inputs from external systems; however, there will undoubtedly be multiple interfaces required to operate a modern SIS effectively. Required system interfaces must be determined early in the engineering process as they will impact both the hardware and software designs.

The first consideration will likely be the programming and configuration interface. If a permanent network is installed for program changes, this network should be completely isolated from the process control networks and any outside business networks to prevent remote access and limit network traffic. Any workstations connected to this network should have strong access control to prevent unauthorized bypasses or program changes.

The SIS will also likely need to have a permanent interface to the BPCS for display of process variables, process alarms, system health, and diagnostic alarms, in addition to a limited number of inputs from the operators such as manual shutdown commands and trip reset commands. It is common for the SIS and BPCS to share a common HMI for graphical displays and annunciation of alarms. This does not necessarily violate the principle of independence between control and safety provided that the SIS is designed to carry out its safety functions without this interface, should a failure occur.

There are many advantages to making available to the operator the additional process variables through a common HMI. The BPCS may also provide additional diagnostic capabilities by monitoring the SIS health, in addition to discrepancy or deviation alarms between control and safety measurements of the same process variable. When designing SIS logic that requires commands from the BPCS or HMI, always consider how the system will react if the communication is suddenly lost. Consider hardwiring any interfacing signals that are critical for operation or process availability. Interfaces that are required for safety should be redesigned to ensure that the SIS can operate independently. The same is true for any connections to third-party systems, such as compressor control or vibration monitoring systems. Equipment that must be tripped by the SIS, but is primarily controlled by another system, should have a separate hardwired signal and separate relay installed in the control circuit to ensure that a failure of the control system does not impact the ability to stop the equipment from the SIS.

22.5.4 Fabrication and Installation

Throughout the conceptual design and detailed engineering stages of a project, many drawings are created to illustrate how the control systems hardware should be physically constructed. This includes piping and instrumentation diagrams, system cabinet layout drawings, input and output signal termination drawings, electrical power distribution drawings, instrument and junction box location plans,

instrument cable routing plans, instrument installation details, network architecture diagrams, and control building layout plans. While developing these drawings, special care should be exercised to ensure physical separation between control and safety, and compliance with any the specific requirements of the SRS. When control and safety sensors measure the same process variable, shared process connections should usually be avoided. The same is also true when redundant safety sensors are installed. Such single points of failure have the potential to negate the benefits of separation and redundancy.

Engineers and designers should consider whether redundant safety sensors and actuators should be wired to separate I/O modules, terminated in separate junction boxes, on separate instrument cables, and even with alternative cable routing. Issues of common-cause failure should first be analyzed for dangerous SIF failure potential, but also for the possibility of causing a spurious trip.

22.5.5 Integration and Factory Acceptance Testing

Upon completion of the control system panels or cabinets, integrated testing may begin to test and trouble-shoot interfaces between control and safety systems and with additional third-party devices. This may also be the first opportunity to run and debug the application software, and verify the correct functioning of the HMI displays.

A factory acceptance test (FAT) will typically take place at the completion of a hardware vendor's or control systems integrator's project scope. Depending on divisions of scope there may be multiple FATs for individual work packages; however, a fully integrated BPCS and SIS FAT should be scheduled near the completion of the overall engineering effort to ensure that the combined system functions as required in a simulated environment. Facility operators should be encouraged to attend to ensure that control loops and safety functions will allow the unit to operate as designed. All systems should be exhaustively checked against their design documents, including piping and instrumentation diagrams, cause and effect diagrams, control narratives, logic narratives, and SRSs.

At a minimum, the tests to be performed on the SIS should be determined in advance and a detailed written test plan developed for all aspects of the system. Any significant changes to design that occur during the FAT should be carefully evaluated and verified against the requirements in the SRS. Items that do not satisfy their requirements must be corrected and completely retested. A test log and punch-list should be kept current throughout the testing activities to ensure that all items are addressed, and strict MOC should be enforced following the conclusion of the FAT.

Integrated testing and the FAT may be the first and only opportunity for the entire team to witness tests involving all of the systems together before being installed on-site. It is critical that the hardware and software be fully tested and proven together, covering both normal and abnormal conditions, to avoid reconfiguration

delays during later commissioning stages where it will become much more costly. Detailed requirements can be found in Clause 13 of IEC 61511 Part 1 (IEC, 2003b).

22.5.6 Maintenance and Testing Procedures

General mechanical integrity (MI) requirements are discussed in the section covering the safety life-cycle operation phase; however, testing and maintenance requirements must be determined during the realization phase, and detailed testing and maintenance procedures compiled prior to commissioning.

The nature of the testing and maintenance activities will be based on the published requirements of the equipment selected (contained within each device's safety manuals or other documentation provided by the manufacturer), the requirements for system performance recorded in the SRS, past experience of maintenance personnel with similar devices, and good engineering practices. All items that impact the successful operation of the SIF must be tested and maintained to original specifications for each mode of operation, requiring detailed procedures addressing the capability of devices, process connections, logic design, HMI and alarm system design, and any specific tools or training required to complete the procedures.

General system-level procedures should be developed to detail the standard operation, routine maintenance, and inspection activities required for the logic solver system, and also procedures and protocols for modifying the configuration and application program.

Each device related to the SIS will have one or more testing frequencies specified in the SRS and confirmed through SIL verification. If testing or calibration may be required more frequently than planned unit outages, an on-process test procedure will be required that may be very different from what can be done while the unit is not operating.

Because the SIS is often designed to shut down or interrupt the process, certain testing while on-process will obviously be disruptive and potentially unsafe if not specified properly. On-process testing and maintenance are frequently limited to one device at a time, rather than an entire SIF or SIS. Such testing is acceptable provided that it fulfills the intended purpose of revealing dangerous modes of failure. Procedures should cover not only the testing activities to be performed, but also coordination with operations, provisions for ensuring safety while devices are out of service, instructions for recording results, and instructions for judging and reporting failures.

Complete functional proof-test procedures, sometimes called system validation procedures, should also be developed. These procedures should be exhaustive, systematically testing all aspects of the entire system: process connections, sensors, logic solvers, application logic, diagnostic logic and alarms, actuators, final elements, support systems, and interfaces to the BPCS, HMI, and other applicable systems. These procedures should be executed every time the unit or facility is offline and cleared, allowing the full capability of each SIF and the SIS overall to

be completely validated. The primary objective is to discover dangerous random failures within the system, and instructions for recording results and the criteria for judging success or failure should be included in the procedures. The system validation process also aids in uncovering systematic failures in equipment selection, programming, or maintenance practices that may not normally be discovered by isolated testing one device at a time.

While the basic requirements of the testing and maintenance procedures should be developed from the SRS and not the program logic, the procedures themselves must be comprehensive, meaning that certain details will likely need to be developed in the later stages of the realization phase in parallel with the program logic. All systems will undergo some level of change through the integrated acceptance testing process. Any changes that may impact the accuracy of the testing and maintenance procedures will need to be captured and reflected in the final versions.

A FAT plan or procedure should not be considered a substitute for maintenance and testing procedures for MI, as the objectives are very different. Although there will undoubtedly be similar steps involved with testing logic and interfaces, field devices are typically simulated in a FAT but must be addressed directly and exhaustively in testing and maintenance procedures.

22.5.7 Commissioning and Site Acceptance Testing

The commissioning of SIS components should follow a written plan, carefully coordinated with the overall construction schedule. Efforts should concentrate on areas where major mechanical construction operations are complete to avoid the possibility of damage or disconnection of instruments after they have been checked.

Proper installation of each device should be confirmed according to the manufacturer's and project team's requirements. Proper wiring of each field device should be proven, followed by calibration and functional testing. Record keeping is very important in this process, often called loop-check, to ensure that each of the hundreds or even thousands of devices are ready to operate. Properly testing and confirming functionality in isolation will facilitate subsequent integrated testing.

Following mechanical completion and loop-check, an integrated site acceptance test (SAT) must be performed to verify the correct functioning of the complete control and safety systems, hardware, and software, with the associated field devices and mechanical equipment. During this stage, the requirements of the SRS should be completely validated; including total SIF response time to ensure that all actions can be completed well within the process safety time. Testing should include, but may not be limited to, the system validation/proof-test procedures. The SAT will mark the first full system functional test, and any exceptions noted during testing must be promptly resolved. This is the team's final opportunity to confirm the system operates as designed before hazardous chemicals and energy are introduced.

Clauses 14 and 15 of IEC 61511 Part 1 (IEC, 2003b) provide requirements for installation, commissioning, and validation activities.

22.5.8
Pre-Startup Safety Review

A pre-startup safety review (PSSR) marks the end of the engineering and construction activities of a project and the transition of responsibility to facility operations. The process typically involves a complete inspection of all design documents, including P&IDs (Piping and Instrumentation Diagrams), the PHA report and worksheets, equipment specifications, and other process safety information, in addition to walk-downs to verify proper installation and construction in the field according to design specifications, and that applicable codes and engineering standards have been followed.

There should also be a complete review of all operating, maintenance, and emergency response procedures for the entire unit, and training should be verified for all workers involved with the unit. The review should also consider any approved changes that have been completed.

Regardless of project schedule, a thorough PSSR is imperative to confirm that all aspects of the facility and those responsible for safe operation are prepared before hazardous chemicals enter the facility. Any findings or recommendations should be promptly resolved prior to startup.

Guidelines for Performing Effective Pre-Startup Safety Reviews is a comprehensive text on the subject (CCPS, 2007a).

22.5.9
Functional Safety Assessments

As part of the safety life-cycle's ongoing verification activities, periodic assessments should be made of the overall conformity with the project requirements, the requirements of the functional safety management plan, and of IEC 61511. This should involve complete inspection of all project documentation and deliverables to ensure traceability of SIFs to the hazard scenarios they protect against, that all hazard scenarios are effectively mitigated, and that functional safety will be appropriately achieved.

The assessments should be carried out by a team of suitably experienced individuals independent of the project team. Greater independence is intended to lead to a more objective assessment, provide the team an opportunity to benefit from outside perspectives, and reduce systematic and systemic failures and their impacts.

Functional safety assessments may be carried out at any number of various stages of a project. The benefits may depend on the project complexity, scope, schedule, and the size and experience level of the project team. At a minimum, a functional safety assessment must be carried out following the completion of the SAT, prior to the introduction of chemicals to the facility. This may be done in conjunction with a PSSR or handled independently; however, the results and resolution of recommendations will need to be coordinated with the overall PSSR team.

22.6
Operation Phase

SISs are largely dormant systems, but this does not imply that they can be installed and forgotten. The operation phase of the safety life-cycle requires no less care than the analysis or realization phases. Long-term success of the SIS depends on continuous and proactive inspection, preventive maintenance, and testing activities, in addition to strict MOC. Those involved with routine maintenance, testing, and modification of SISs must be suitably trained and experienced, and a senior experienced person at the facility must remain in responsible charge of SIS operation.

Many of the activities in the operation phase will follow very closely the activities required for other classes of equipment within a process plant, and therefore it is strongly recommended that efforts to manage SIS operation be fully harmonized with the facility's overall process safety management program.

22.6.1
Inspection, Maintenance, and Proof-Testing

An MI program is a fundamental element of overall process safety, assuring the ongoing performance of equipment involved in the storage and processing of hazardous chemicals. SIS equipment should be closely monitored for signs of degradation and maintained in as-good-as-new condition; including process connections, sensors, logic solver system components, actuators, and final elements. The MI program must also cover the systems supporting the SIS, such as electrical power, instrument air, heat tracing, and even some aspects of the interfacing systems such as the BPCS and HMI.

SISs are completely customized for each application; therefore, there can be no single collection of predetermined requirements for maintenance and testing. Determining, documenting, and executing the required activities for long-term reliability of the system require coordination throughout the entire safety life-cycle, not simply in the operation phase.

SIFs and their subsystems are designed according to integrity requirements determined in an analysis of process risk. A number of variables, including frequencies of periodic functional testing, are specified and confirmed qualitatively in the analysis phase. Accommodations for testing and detailed full-function proof-testing procedures are developed in the realization phase once each SIF and each SIS have been fully designed.

At a minimum, all routine inspections and calibrations should take place according to the manufacturer's guidelines and suggested schedules contained in the safety manuals or other published documentation. The purpose is to replace parts designed to wear out, and detect conditions of degraded performance so that devices can be repaired or replaced before complete failures occurs.

All maintenance and testing activities should be proactively scheduled and resources devoted to ensuring timely completion. Those involved should be specifically trained in the specific requirements of all devices and systems, the tools

required for maintenance and testing operations, the MI program policies and procedures including permitting requirements and safe work practices, and their roles and responsibilities in the overall safety life-cycle.

Forms and procedures should detail the steps of all work required, and also criteria for evaluating the condition of devices and their suitability for continued use. The as-found and as-left conditions of devices should be recorded and described in detail so that trends can be identified in the population of similar devices and appropriate corrective actions taken. This may require increasing inspection and calibration frequencies, decreasing the intended service life, or revisiting design specifications to evaluate changes in the device technology or materials of construction to be more compatible with the chemicals and process conditions.

General MI program considerations are addressed in the CCPS *Guidelines for Mechanical Integrity Systems* (CCPS, 2006). Specific requirements for SISs are provided in Clauses 16 of IEC 61511 Part 1 (IEC, 2003b), with guidance and examples provided in much greater detail within the ISA Technical Report ISA TR84.00.03-2012 (ISA, 2013b).

22.6.2 Management of Change

A MOC program is another fundamental element of overall process safety that plays an especially important role in the operation of SISs. While changes large and small are unavoidable in process plants, it is paramount that even minor changes are investigated for their potential impacts across the facility, and the details of the change are communicated to those who may be affected. Any proposed modifications (other than a true replacement-in-kind) to the process equipment, process conditions, or chemicals, whether temporary or permanent should initiate a thorough evaluation process involving all disciplines and stakeholders.

MOC procedures should address potential process hazards associated with the change, or how the change impacts existing evaluations of risk made in the PHA and/or LOPA studies. Changes influencing previous assessments of risk or the applicability of safeguards may require a PHA team to be reconvened to consider the risk formally. The entire safety life-cycle will also restart on a smaller scale, triggering a re-analysis of the integrity requirements of safeguards and IPLs, the SRSs, and SIL verification. Any modifications found to be required to the SIS configuration or programming will require complete documentation, thorough testing in an offline simulated environment, and updated maintenance and testing procedures. Only after all documentation and offline testing have been completed and verified should formal approval be granted for the changes to proceed. Records of changes should always be maintained with a formal change log.

What changes are possible while on-process will often depend on the limitations of the logic solver system, and should be understood and considered while evaluating the timing of a change. If a unit shutdown is required to implement a physical equipment change, a full functional test of the entire SIS should also

be considered to take advantage of the outage and identify dangerous failures that could not normally be discovered during operation.

Over time, advances in technology or equipment approaching the end of its design life will require SIS logic solver systems to be upgraded, migrated to entirely new systems, or permanently decommissioned. Such projects must also follow the same MOC process and reconsider the entire safety life-cycle to ensure no gaps in safety are created. Diligence in maintaining SIS documentation, such as the SRS with traceable ties to PHA scenarios, will aid in this process. Before decommissioning an SIF or SIS for any reason, adequate documentation must exist to show that the process hazard(s) that each SIF was designed to prevent are no longer present, or are sufficiently mitigated through other means.

MOC for process safety is explained in the CCPS *Guidelines for the Management of Change for Process Safety* (CCPS, 2008b). Specific requirements for SISs are listed in Clauses 17 and 18 of IEC 61511 Part 1 (IEC, 2003b).

22.6.3 Performance Monitoring and Continuous Improvement

Effective performance management requires periodic assessments of past results to allow future improvements. This often requires re-evaluating the results of past decisions, taking advantage of hindsight to refine assumptions. As mentioned in earlier sections, functional safety requires continuous verification activities throughout the individual safety life-cycle stages, including both qualitative and quantitative evaluations. Similar continuous and periodic evaluations should be carried out at the program level to ensure appropriate measures of quality are established and controlled.

Enabling a highly reliable and cost-efficient functional safety program will depend on collecting various quantitative measures, such as equipment failure rates, SIF demand rates, and instrument failure rates, including dangerous and safe, detected, and undetected. These measured values can then be used to validate previous assumptions and to develop more appropriate and effective functional specifications aimed at reducing future rates of failure. Such data collection is aided by computerized databases, including maintenance management systems and process data historians, capable of reporting various statistics for use in calculating both leading and lagging metrics.

PHA studies should be revalidated periodically, as this is often a requirement of governmental process safety regulations. It is recommended that an SIS analysis revalidation takes place soon after a PHA revalidation. Such an effort should consider actual performance data collected in evaluating the assumptions of the original study.

The most effective data for use in SIL verification comes from plant-specific records. Actual measured rates of failure will directly account for the specific installation, maintenance, environmental, and process conditions to which each device is likely to be subjected, and also the characteristics of the particular manufactures and models of equipment in use. Studies involving generic data

will rarely be able to account for these factors accurately. Without reasonable confidence in the data, the results of SIL verification have the potential to lead to costly, over-designed systems requiring excessive human intervention to test and maintain, or dangerously under-designed systems that are ill-suited to providing adequate risk reduction. PFD_{avg} should be re-examined using in-service data and compared with previously estimated results.

Obviously, as an industry we cannot judge safety performance by simply measuring the rate of major incidents. Similarly, the lack of past incidents does not necessarily indicate a healthy process safety program. To facilitate the periodic qualitative evaluations of program performance during operation, certain quantitative metrics may be established and tracked based on the collection of certain data. *Lagging metrics* measure actual past events, such as device or SIF failures, as a way to compare rates of occurrence. Failure rates may be compared with other periods of time within the facility's history to identify trends, or other facilities within the industry to gauge relative performance. *Leading metrics* are those which look at conditions that could be expected to contribute to failures, seeking to identify weaknesses before failures occur. Leading SIS metrics might include quantity and duration of SIF bypasses, quantity and duration of overdue proof-tests, mean time to repair or restore, and many others. Both leading and lagging metrics are valuable in continuously or periodically appraising actual performance, and may indicate that current practices are either succeeding or failing to improve functional safety.

Both the UK HSE and the CCPS have published recommended practices for developing and interpreting process safety metrics (HSE, (2006); CCPS, 2009b).

22.7 Conclusion

As the operations workforce declines in size and experience, dependence on computer-based process automation will grow. Whether due to ethical, legal, or financial necessity, investment in automated safety technology is growing at a substantial rate. An equally knowledgeable and passionate workforce will be required to keep pace. The author encourages further study and recommends the publications already cited in the text and additionally CCPS (1993, 1996, 1998, 2007b,c, 2009a), Charlwood, Turner, and Worsell (2004), HSE (2007), IEC (2003a, 2005), ISA (1996, 2001, 2004, 2008, 2012a), Johnson, Rudy, and Unwin (2003), Kletz (2009), Nunns (2002), and Smith (2011).

References

CCPS (Center for Chemical Process Safety) (1993) *Guidelines for Safe Automation of Chemical Processes*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (1994) *Guidelines for Implementing Process Safety Management Systems*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (1996) *Guidelines for Writing Effective Operating and Maintenance Procedures*,

American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (1998) *Guidelines for Improving Plant Reliability Through Data Collection and Analysis*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2001) *Layer of Protection Analysis: Simplified Process Risk Assessment*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2006) *Guidelines for Mechanical Integrity Systems*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2007a) *Guidelines for Performing Effective Pre-Startup Safety Reviews*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2007b) *Guidelines for Risk Based Process Safety*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2007c) *Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2008a) *Guidelines for Hazard Evaluation Procedures*, 3rd edn, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2008b) *Guidelines for the Management of Change for Process Safety*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2009a) *Guidelines for Developing Quantitative Safety Risk Criteria*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2009b) *Guidelines for Process Safety Metrics*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2011) *Guidelines for Auditing Process Safety Management Systems*, 2nd edn, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2012) *Guidelines for Independent Protection Layers and Initiating Events*, American Institute of Chemical Engineers, New York.

Charlwood, M., Turner, S., and Worsell, N. (2004) *A Methodology for the Assignment of Safety Integrity Levels (SILs) to Safety-Related Control Functions Implemented by Safety-Related Electrical, Electronic and Programmable Electronic Control Systems of Machines*, Health and Safety Executive, Norwich.

Demming, W.E. (1986) *Out of the Crisis*, MIT Center for Advanced Educational Services, Cambridge, MA.

Goble, W.M. and Cheddie, H.L. (2005) *Safety Instrumented Systems Verification: Practical Probabilistic Methods*, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

Gruhn, P. and Cheddie, H.L. (2006) *Safety Instrumented Systems: Design, Analysis, and Justification*, 2nd edn, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

HSE (Health and Safety Executive) (2006) *Developing Process Safety Indicators: a Step-by-Step Guide for Chemical and Major Hazard Industries*, Health and Safety Executive, Bootle.

HSE (Health and Safety Executive) (2007) *Managing Competence for Safety-Related Systems, Parts 1 and 2*, Health and Safety Executive, Bootle.

IEC (International Electrotechnical Commission) (2003a) IEC 61131-3. *Programmable Controllers – Part 3: Programming Languages*, 2nd edn, International Electrotechnical Commission, Geneva.

IEC (International Electrotechnical Commission) (2003b) IEC 61511. *Functional Safety – Safety Instrumented Systems for the Process Industry Sector, Parts 1–3*, International Electrotechnical Commission, Geneva.

IEC (International Electrotechnical Commission) (2005) IEC 62061. *Safety of Machinery – Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*, International Electrotechnical Commission, Geneva.

IEC (International Electrotechnical Commission) (2010) IEC 61508. *Functional Safety of Electrical/Electronic/Programmable*

Electronic Safety-Related Systems, Parts 1–7, 2nd edn, International Electrotechnical Commission, Geneva.

ISA (Instrumentation, Systems, and Automation Society) (1996) ANSI/ISA-S84.01-1996. *Application of Safety Instrumented Systems for the Process Industries*, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

ISA (Instrumentation, Systems, and Automation Society) (2001) ANSI/ISA-91.00.01-2001. *Identification of Emergency Shutdown Systems and Controls that are Critical to Maintaining Safety in Process Industries*, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

ISA (Instrumentation, Systems, and Automation Society) (2002) ISA-TR84.00.02-2002. *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques, Parts 1–5*, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

ISA (Instrumentation, Systems, and Automation Society) (2004) ANSI/ISA-84.00.01-2004 (IEC 61511 Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Parts 1–3*, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

ISA (International Society of Automation) (2008) ANSI/ISA-TR96.05.01-2008. *Partial Stroke Testing of Automated Block Valves*, International Society of Automation, Research Triangle Park, NC.

ISA (International Society of Automation) (2013a) Draft ANSI/ISA 84.91.01-2013. *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interiors in the Process Industry*, International Society of Automation, Research Triangle Park, NC, in press.

ISA (International Society of Automation) (2013b) Draft ISA-TR84.00.03-2013. *Mechanical Integrity of Safety Instrumented Systems (SIS)*, International Society of Automation, Research Triangle Park, NC, in press.

ISA (International Society of Automation) (2011) ISA-TR84.00.04-2011, Part 1. *Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*, International Society of Automation, Research Triangle Park, NC.

Johnson, R.W., Rudy, S.W., and Unwin, S.D. (2003) *Essential Practices for Managing Chemical Reactivity Hazards*, American Institute of Chemical Engineers, New York.

Kletz, T.A. (2009) *What Went Wrong?: Case Histories of Process Plant Disasters and How They Could Have Been Avoided*, 5th edn, Butterworth-Heinemann, Oxford.

Marszal, E.M. and Scharpf, E.W. (2002) *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis*, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

Nunns, S. (2002) *Principles for Proof Testing of Safety Instrumented Systems in the Chemical Industry*, Health and Safety Executive, Bootle.

Smith, D.J. (2011) *Reliability, Maintainability and Risk*, 8th edn, Butterworth-Heinemann, Oxford.

Smith, D.J. and Simpson, K.G.L. (2011) *Safety Critical Systems Handbook: a Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards*, Butterworth-Heinemann, Oxford.