Reprinted from
PHARMACEUTICAL ENGINEERING®
The Official Magazine of ISPE
September/October 2008, Vol. 28 No. 5

Functional Safety in the Life Science Industries

by David Hatch, Iwan van Beurden, and Eric W. Scharpf

This article presents an overview of functional safety within the life science industry based on international standards.

Introduction

For life science companies, the chemical safety of the process (plant design and operation) is as critical as the pharmacological safety of the products (drug quality). The use of flammable solvents, corrosive fluids, toxic gases, and explosive dusts present significant threats to the safety of production personnel, the local community, surrounding environment, and often expensive manufacturing equipment.

Functional safety contributes toward overall process safety and relies on the correct reaction (both action and speed) of automatic devices in response to actual or potential dangerous conditions, thus preventing hazardous events or mitigating harmful consequences.

Instrumented protective functions using electrical or electronic technologies achieve this via sensors to detect process deviations, logic solvers to evaluate the sensor data, and final elements to execute the required action to achieve or maintain a safe state. These Safety Instrumented Systems (SIS) have been widely used in the general process and pharmaceutical industries for many years, providing protection against deviations in pressure, temperature, level and flow, and other critical process parameters.

Correct management of the functional safety aspects of process plants is now globally recognized as the best way to reduce the inherent risks in hazardous industrial processes. International standards are driving major end users in the process industry to adopt the IEC61511[1] (ANSI/ISA–84.00.01[2] equivalent) lifecycle approach to safety. The aim of these standards is to make safety a priority throughout the entire life of any potentially hazardous plant or process.

Risk Reduction

Risk is a measure of the likelihood and consequences of a hazardous scenario when a process goes out of control or is otherwise compromised, leading to a loss of containment with the subsequent release of material and/or energy.

Companies have moral, legal, and financial responsibilities to limit the risk their operations pose to employees and members of the public to a level that is considered tolerable.

Determining whether a process plant is "safe enough" may sound easy, but in practice it means a very well thought out calibration of the As Low As Reasonably Practicable (ALARP) risk tolerability principle. ALARP has been documented by the UK Health and Safety Executive in their R2P2 publication,[3] which aims to provide a methodology for defining target frequency and severity (i.e., risk) of hazards to a minimum "tolerable" level.

The ALARP principle states that there is a level of risk that is "intolerable." Above this level, risks cannot be justified on any grounds. Below this intolerable level is the ALARP region where risks can be undertaken only if a suitable benefit can be achieved. In the ALARP region, risks are only tolerable if risk reduction is impracticable or if the cost of risk reduction is greatly outweighed by the benefit of the risk reduction that is gained. Below the ALARP region is the "broadly acceptable" region where the risks are so low that no consideration of them is warranted and detailed work is not needed to demonstrate ALARP because the risk is negligible. In addition, in this broadly acceptable region, risk is so low that no risk reduction is likely to be cost-effective, so a cost-benefit analysis of risk reduction is typically not undertaken.

In some countries, the law mandates tolerable risk levels whereas in others, such as the

United States, tolerable risk is determined by each company or organization and must be adopted consistently. Tolerable risk cannot be applied on a personal preference basis since everyone has their own view on what is tolerable (consider your own driving style for example).

Once an estimate is made on the likelihood of an unwanted event occurring, and the potential consequence of that event is calculated with a commercial value, the decision on whether to implement further protection measures is often a straightforward economical one. If the risk reduction is significant and the cost not prohibitive, then clearly the measure should go ahead. Conversely, if a measure is deemed to offer little impact on the overall risk reduction and it is prohibitively expensive, it is perfectly valid to consider the associated risk as "tolerable," assuming no other risk reduction measures are practical.

Safety Standards

IEC 61511 has been developed as a Process Sector implementation of the international standard IEC 61508:[4] which was prepared as an 'umbrella' standard from which industry specific standards (such as IEC 61511 for the Process Industry and IEC 62061 for the Machinery Industry) could be derived.

For end-users in the Life Science process industries (primary and secondary manufacture), IEC 61511 is applicable with the broader IEC 61508 limited to those who manufacture or supply Safety Instrumented System equipment or components. Hereafter we shall refer to IEC 61511 as 'the standard,' which has two key concepts that are fundamental to its application: the safety lifecycle process, and safety integrity levels which define required and achieved functional safety performance.

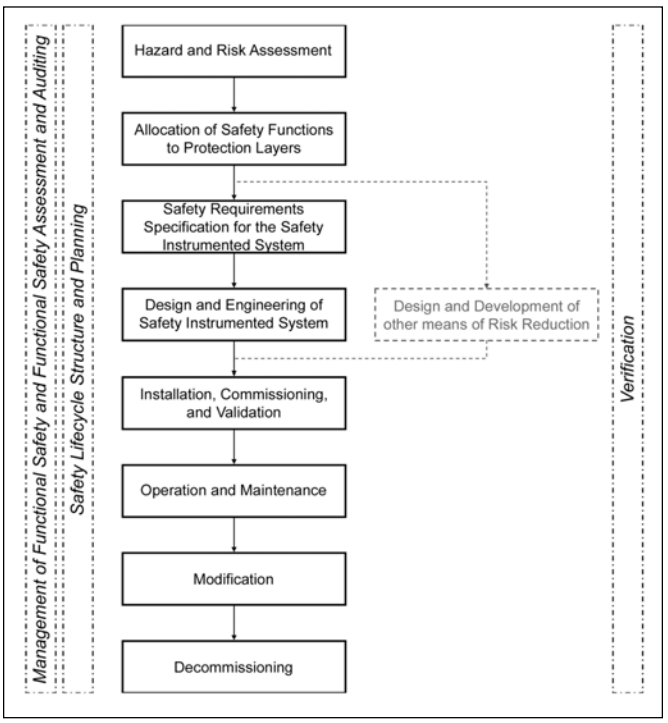

Figure 1. Functional safety lifecycle.

Safety Lifecycle

Similar to GAMP,[5] a lifecycle approach forms the central framework that links together the key concepts of the standard and is acknowledged good engineering practice for Safety Instrumented System implementation.

In order to achieve and sustain functional safety throughout the life of a facility (i.e., from initial conceptual design to final decommissioning), a number of technical and management activities must be performed, reviewed, and documented. Similar in many ways to the ISO 9000 quality process, the execution of the functional safety lifecycle is presented in Figure 1.

This lifecycle can be classified into three distinct groups of phases:

Analysis – How Much Safety is Required

Analysis focuses on identifying hazards and hazardous events, the likelihood that these hazardous events will occur and their potential consequences, the availability of layers of protection, as well as the need for any Safety Instrumented Functions (SIF) and their allocated Safety Integrity Level. The phase concludes with the development of the Safety Requirement Specification (SRS) to properly define the requirements for all Safety Instrumented Functions.

Implementation – How Much Safety can be Achieved

The implementation phases begin with a conceptual design of each Safety Instrumented Function based on equipment selection, architectural voting configuration, and periodic test interval to achieve the risk reduction defined in the Safety Requirement Specification.

These phases include detailed hardware design and build, software configuration, system integration, and testing prior to delivery to site. Implementation also includes advanced planning for installation, commissioning and validation, as well as long-term operation and maintenance.

Operation – How to Sustain Safety

The operation phases are the longest phases of the safety lifecycle and involve the validation of the Safety Instrumented System and all its Safety Instrumented Functions to confirm that it functions as per the requirements in the Safety Requirement Specification.

Following successful validation, the system is put into service and must be properly operated, maintained, and tested until permanently taken out of service. During this phase, all modifications must be fully evaluated and documented to ensure they do not compromise safety.

Management of Functional Safety

Like any execution process, functional safety management requires careful forward planning which defines the required activities along with the persons, departments, or organizations responsible to carry out these activities. The main purpose is to reduce the risk associated with systematic failures of specification, design, and procedure execution that

Executive Summary

Compliance with local, national, and international process safety regulations can be achieved efficiently and effectively by following established and well proven functional safety standards and principles. Best practice for achieving and sustaining functional safety has close parallels with pharmaceutical compliance.

can lead to harmful accidents.

Plans should be updated and related activities adjusted as necessary throughout the safety lifecycle to reflect any nonconformance, changes in scope, technology, or other influences. Regular independent monitoring and objective auditing is key to ensure that proper management is provided to support the technical execution of the project.

A key element of resource planning is to ensure that, according to the standard, "***Persons, departments, or organizations involved in safety lifecycle activities shall be competent to carry out the activities for which they are accountable.***"

This competence can be demonstrated with qualifications, experience, and qualities appropriate to their duties and should include:

- training to ensure acquisition of the necessary knowledge of the field for the tasks that they are required to perform
- adequate knowledge of the hazards and failures of the equipment for which they are responsible
- knowledge and understanding of the working practices used in the organization for which they work
- an appreciation of their own limitations and constraints, whether of knowledge, experience, facilities, resources, etc., and a willingness to point these out

Internationally recognized accredited schemes are available which formally establish the competency of those engaged in the practice of safety system application in the process and manufacturing industries.

Verification and Validation

Pharmaceutical validation is defined as "***Establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality attributes.***" Safety validation is synonymous with this principle and we could simply replace the word '*quality*' with '*safety*' to provide a mission statement for functional safety.

In common with pharmaceutical compliance, safety compliance adopts the proven principles of verification and validation. Very often these terms are misused as they define similar, but fundamentally different concepts.

Verification is defined as "***demonstrating for each phase of the safety lifecycle by analysis and/or tests that, for the specific inputs, the deliverables meet the objectives and requirements set for the specific phase***" and ensures that the final product meets the original design (low-level checking), i.e., you built the product right. This is done through procedural cross checks such as inspections, reviews, and audits.

Validation is defined as "***demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification***" and checks that the product design satisfies or fits the intended usage (high-level checking), i.e., you built the right product. This is done through dynamic testing and other forms of challenge or trial.

In other words, verification is an ongoing quality assurance activity throughout the lifecycle ensuring that the procedures have been followed and the Safety Instrumented System has been built according to the requirements and design specifications, while validation is a quality control activity at a specific point in the lifecycle, which ensures that the Safety Instrumented System actually meets the user's needs.

Information and Documentation Requirements

In common with process validation principles, accurate information and documentation underpin the implementation of a successful project and provide ongoing reference material for the support of operating processes.

An important aspect of functional safety management is to ensure that the necessary information is available, documented, and maintained in order that all phases of the safety lifecycle can be efficiently executed and that the necessary verification and validation activities can be effectively performed.

Process Hazard and Risk Analysis

Each process has its own inherent risk (i.e., potential to cause harm) by virtue of the chemicals handled (flammability and toxicity), the operating conditions (pressure and temperature), and the inventory (volume or mass), as well as the construction (materials), the location of the plant, and the occupancy (personnel exposure).

If we consider a typical pharmaceutical process, it often handles dangerous materials, but generally does not operate at extreme pressures or temperatures, and in common with other batch processes, has a limited inventory which is typically the reactor capacity – but the volume of storage tanks should not be discounted as these can often be significant. However, the threat often comes from the manual or semi-automatic nature of many processes which require some operator intervention and thereby exposure to the hazards of the process as well as the potential for human error.

Process Hazard Analysis (PHA) is an established activity in all process industries, including life sciences. Commonly known as a Hazard and Operability (HAZOP) study,[6] a PHA is only the start of the safety journey – identifying what can go wrong – now we must evaluate and address it.

Allocation of Safety Functions to Protection Layers

Overall risk reduction is achieved by combinations of independent layers of protection. These layers may take many forms – mechanical, instrument/electrical, procedural, etc., and the standard shows typical risk reduction methods in process plants in terms of these "layers of protection" which are presented in Figure 2.

The Safety Instrumented System is one of many potential measures that can be taken at the "Prevention" level, as opposed to "Mitigation" (cure). Once a "tolerable" level of risk has been established, an analysis of the layers of protection should allow a function-by-function comparison of the hazardous event frequency.

Assuming this hazardous event frequency is lower than what is considered tolerable, no additional layers of protection will be required. Conversely, if the frequency is higher than the tolerable level set, then additional independent layers need to be applied. One of these layers may be a Safety Instrumented System.

Safety Integrity Levels (SIL) are order of magnitude bands of risk reduction. There are four levels defined in the standard ranging from SIL1 with the lowest level of risk to SIL4 that provides the highest (and rarest) level of risk reduction. These levels are documented in Table A according to the risk reduction that they provide.

For example, to achieve a tolerable risk of one death in 1,000,000 years (indicative value for illustrative purposes only) from a residual (i.e., with all other protection measures credited) risk of one death in 50,000 years, the Risk Reduction Factor (RRF) would be 20 (i.e., 1,000,000 ÷ 50,000) which lies in the SIL1 band. Therefore, we would require a Safety Instrumented Function with this integrity to achieve the required risk reduction.

Risk Reduction Factor	Safety Integrity Level
10000 – 100000	4
1000 – 10000	3
100 – 1000	2
10 – 100	1

Table A. Risk reduction and safety integrity levels.

Note that the standard suggests that applications which require the use of a single safety instrumented function of SIL 4 are rare in the process industry and that they shall be avoided where reasonably practicable by reviewing the process design to implement more reliable and (wherever possible) inherently-safe non-instrumented protection measures.

There are various methods of determining the Safety Integrity Level for a particular hazardous scenario and these are generally classified into two types:

- Qualitative
- Quantitative

Qualitative methods group numerical targets into more broad categories of risk reduction, while Quantitative methods give specific numerical targets for risk. Often qualitative methods are used for quick initial screening with quantitative meth-

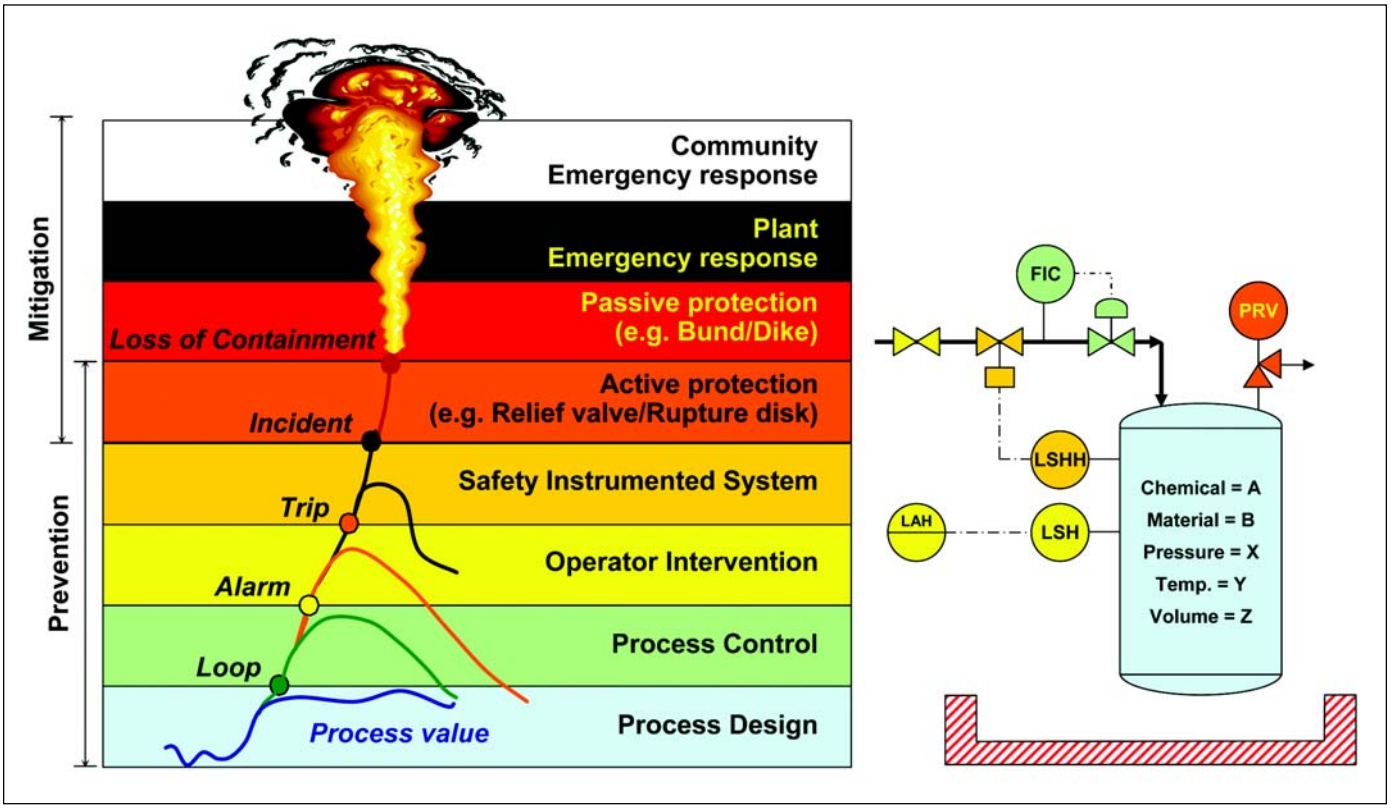

Figure 2. Typical protection layers.

Event Likelihood				
	High	2	3	4
	Moderate	1	2	3
	Low	–	1	2
		Minor	Serious	Extensive
		Hazardous Event Severity Rating		

Table B. Risk matrix (EXAMPLE).

ods reserved for higher risk scenarios that require more detailed investigation and evaluation.

Two basic types of qualitative Safety Integrity Level selection are commonly used in the process industry:

- Safety Matrix
- Risk Graph

The Safety Matrix example in Table B considers the severity of a specific hazardous event (X-axis) against the likelihood that the hazardous event will occur when all other credited protection layers have failed (Y-axis). The intersection of severity and likelihood gives a grade of risk reduction (or Safety Integrity Level) that the Safety Instrumented Function (specific to this hazard) must achieve.

The Risk Graph is a development of the safety matrix with a similar severity (Consequence) grading on the Y-axis and then consideration of three elements (Exposure, Avoidance, and Demand) that make up the likelihood X-axis of the hazardous event. Both safety matrix and risk graph methods produce a Safety Integrity Level, not a specific Risk Reduction Factor.

Quantitative methods are more powerful, but require more information. They enable the user to perform sensitivity analysis on all the risk reduction measures, allowing them to identify the weaker protection layers, which may require more attention.

One of the most common quantitative methods of Risk Reduction Factor determination (and therefore Safety Integrity Level selection) is Layer of Protection Analysis (LOPA) as shown in Table C.

This method is used to calculate the risk reduction factor for a specific hazard based on the unmitigated risk of the hazard severity and initial likelihood, which is then reduced by taking credit for appropriate and independent protection layers, each with their own probability of failure (lower probability of failure means more reliable), to yield a residual risk which is then compared to the target tolerable risk. The strength of this method relies heavily on having adequate, appropriate, and accurate (not necessarily exact) data, preferably from the users own experience.

Further guidance on the determination of Safety Integrity Level is given in the ISA publication Safety Integrity Level Selection[7] as well as part 3 of IEC 61511 and the AIChE CCPS publication Layer of Protection Analysis.[8]

Safety Instrumented System Safety Requirements Specification

The concept of a User Requirement Specification (URS) is well understood by pharmaceutical companies who follow the principles of Good Automated Manufacturing Practice (GAMP). It is a document (or set of documents), which defines clearly, concisely, and unambiguously what the user requires and is provided to the supplier as the definitive statement of what the system must do. The URS details functional and non-functional requirements with the emphasis on the requirements themselves (i.e., what) and not the method of implementing these requirements (i.e., how).

The implementation of Safety Instrumented System is similarly documented in a Safety Requirement Specification (SRS), which defines the requirements for the Safety Instrumented Function(s) within the Safety Instrumented System. These requirements must cover the following three key areas of each function:

- Functionality – what it does
- Reliability – how well it does it
- Performance – how quickly it does it

The UK Health and Safety Executive conducted a survey[9] of failures of computer-based systems and the causes of these failures are summarized in Figure 3.

The findings show two key issues. First, nearly 60% of failures are already "in" the system before it even arrives on site. Second, failures can occur at any time within the lifetime of a system, it is not just problems that occur due to maloperation or wear and tear during service. Ironically, it is the initial stage of the lifecycle where one may expect more 'educated' personnel to be involved that is the weakest.

The Safety Requirement Specification captures what needs to be done to achieve functional safety and is often a contractual document, which is passed from the User to the Supplier who is responsible for implementing the Safety Instrumented System.

Safety Instrumented System Design and Engineering

A Safety Instrumented System is a system composed of sensor(s), for example, pressure transmitters, logic solver(s),

Hazardous Event	Severity	Initiating Cause	Initiating Likelihood	Protection Layers				Residual Risk	Tolerable Risk	RRF	SAFETY INTEGRITY LEVEL
				BPCS	*Alarms*	*Relief*	*Other*				
Reactor rupture	1 death	Loss of cooling water	0.05/year (1 in 20 yrs)	0.1	0.5	0.01	1	2.5×10^{-5} (1 death in 40,000 yrs)	1×10^{-6} (1 death in 1,000,000 yrs)	25	1

Table C. Layer of protection analysis (EXAMPLE).

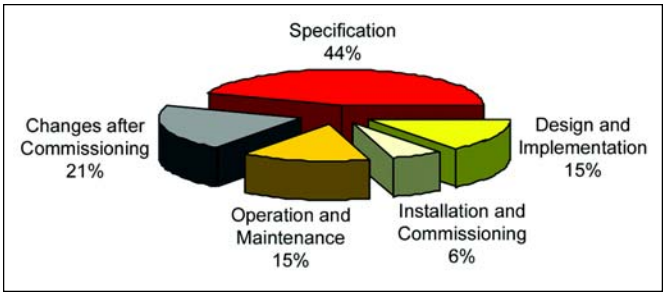

Figure 3. Failures of computer-based systems.

Risk Reduction Factor	Safety Integrity Level	Probability of Failure on Demand	Safety Reliability
10000 – 100000	4	0.0001 to 0.00001	99.99% to 99.999%
1000 – 10000	3	0.001 to 0.0001	99.9% to 99.99%
100 – 1000	2	0.01 to 0.001	99% to 99.9%
10 – 100	1	0.1 to 0.01	90% to 99%

Table D. Safety integrity levels and probability of failure on demand.

for example, Programmable Logic Controllers (PLC), and final element(s), for example, actuated valves, designed in such a way as to implement Safety Instrumented Functions.

The Safety Instrumented Functions are specified with a particular Safety Integrity Level in order to achieve a certain risk reduction for a defined hazardous event. This in turn sets the requirements for both hardware and software safety integrity of the sub elements in the safety loop by means of a target probability of failure.

We cannot predict exactly what will happen when, but we can make educated and well informed judgements regarding what is likely to happen both in terms of hazardous events and protective equipment failures. We consider that the worst-case scenario of a hazardous event occurring at the same time as the safety equipment is unavailable has a probability and that the greater this probability, the greater the likelihood of harm.

In order to address this challenge, we must aim to reduce the frequency of the hazardous event occurring and reduce the probability of the protective equipment failing. Everything will fail; some will fail sooner than others, but even then most 'reliable' equipment has the potential (however small) to fail when you really need it most.

If we develop Table A into Table D, we see that the higher the required risk reduction (i.e., the more 'unsafe' the process) then we require a Safety Instrumented Function with a higher safety reliability (i.e., when we place a demand on the Safety Instrumented Function, there is increased confidence that it will do what is required).

Although the determination of required safety may be determined qualitatively (as a Safety Integrity Level) or quantitatively (as a Risk Reduction Factor), the determination of achievable safety can only be determined quantitatively as a probability of failure. These probability calculations are performed using a variety of techniques, but all are based on the following three basic considerations:

1. Reliability – the quality of the equipment used within the Safety Instrumented Function in terms of failures
2. Redundancy – the quantity of equipment used within the Safety Instrumented Function in terms of voting and diversity
3 Repairability – how often and how thoroughly each Safety Instrumented Function is tested and faults repaired

Therefore, to achieve a Safety Instrumented Function with the lowest probability of failure, we should use the best equipment with multiple combinations and test it as often as practical. This obviously has a commercial impact, as the best equipment will often come at a higher price and frequent testing involves significant maintenance costs as well as production interruption with the associated loss of revenue.

Very generic sources of equipment failure data have existed for years in the oil and gas industries, but more manufacturer data is now being collected, assessed, and published by independent evaluation companies and bodies. The most accurate failure data comes from your own plant records that reflect actual devices in actual processes under actual maintenance regimes.

Further guidance on the confirmation of Safety Integrity Level and reliability calculations is given in the ISA publication Safety Integrity Systems Verification.[10]

Safety Instrumented System Installation and Commissioning

Installation and Commissioning of a Safety Instrumented System is similar to a system within a pharmaceutically validated process.

Installation Qualification (IQ) is defined as "***the documented verification that all aspects of a facility, utility or equipment that can affect product quality adhere to approved specifications and are correctly installed.***"

For Safety Instrumented Systems, we could simply replace "product quality" with "process safety" and then consider the IQ to include aspects such as undamaged delivery to site, mechanical completion, and cold (power off) loop checking.

Operational Qualification (OQ) is defined as "***the documented verification that all aspects of a facility, utility or equipment that can affect product quality operate as intended throughout all anticipated ranges.***"

For Safety Instrumented Systems, we could consider the OQ to include aspects such as hot (power on) loop checking to ensure that individual sensors can sense/measure correctly and individual final elements function correctly.

Safety Instrumented System Safety Validation

Safety validation of the Safety Instrumented System is vital to ensure that all the Safety Instrumented Functions perform as required to achieve the necessary risk reduction. This activity is also known as Site Acceptance Testing (SAT) or a

Pre-Start-up Acceptance Test (PSAT).

Performance Qualification (PQ) is defined as "***the documented verification that all aspects of a facility, utility or equipment that can affect product quality perform as intended meeting predetermined acceptance criteria.***"

The acceptance criteria for PQ of a Safety Instrumented System would typically include the confirmation of:

- logical relationships between sensors and final elements (e.g., a deviation detected by a specific input initiates a response from a related output)
- time of response between initial detection and final action (albeit in initially clean/ideal service on day one)

Safety Instrumented System Operation and Maintenance

Safety validation of the Safety Instrumented System must be completed before the hazards are introduced and the system is put into service. This demonstration that the Safety Instrumented System can reduce risk is only the first step in a journey that may last for decades to ensure that the risks are reduced to the defined tolerable level while the facility and its protected processes and equipment are in operation (and therefore continue to present a threat of harm to personnel).

Regular maintenance of equipment is vital to ensure that the Safety Instrumented Function is available and capable as and when required and this involves routine inspection and cleaning as well as properly executed proof testing.

The purpose of the proof test is to find component failures that are otherwise hidden and make any repairs to restore the Safety Instrumented System to its fully functional state. It is often assumed that if it works properly, it has not failed and a conventional approach is to check to see if the Safety Instrumented Function operates and the equipment has not failed. This is only true for the most part since many proof test procedures do not completely test all of the equipment used in the Safety Instrumented System.

Regular and effective proof testing is a key element in sustaining functional safety and should be considered as early as possible within the design of each Safety Instrumented Function.

Safety Instrumented System Modification and Decommissioning

As with all quality aspects of regulated facilities, proper management of change is vital to ensure that safety is not compromised by uncontrolled or unevaluated modifications to the physical (hardware) or functional (software) attributes of a Safety Instrumented System.

Since the purpose of a Safety Instrumented Function is to reduce risk, any change to the risk it must reduce or its capability to reduce that risk will affect the safety it provides. It is important to note that these changes must include differences between the performance of equipment estimated during the analysis and design phases relative to its actual performance in the field.

- Hazard severity – If effects are worse than predicted, the risk reduction requirement is greater.
- Hazard likelihood – If more frequent than predicted, the risk reduction requirement is greater.
- Equipment reliability – If equipment fails more frequently than assumed, the risk reduction capability is less.
- Equipment redundancy – If equipment redundancy is reduced, the risk reduction capability is less.
- Equipment repairability – If equipment is tested less frequently than declared, the risk reduction capability is less.

Any of these changes must be properly evaluated, documented, and implemented to ensure that the functional safety protection is not weakened or eliminated.

The multi-product nature of many pharmaceutical facilities means that the same equipment may handle a variety of chemical regimes with process pressure and temperatures that change according to the recipes and production phases used. Therefore, it is essential that the risk reduction requirements and capabilities are properly evaluated for each plant and processes within that plant.

Decommissioning a Safety Instrumented Function or a complete Safety Instrumented System is an extreme form of modification. The key consideration for decommissioning is to assess the effects of removing some or all of the risk reduction and to ensure that other Safety Instrumented Function or non-instrumented protection layers are not compromised or expected to provide a greater level of risk reduction than they are capable of.

Conclusions

Functional safety mirrors the principles of process quality and can be summarized as follows:

- What can go wrong? (HAZOP or PHA)
- How bad can it be? (Risk Analysis)
- What can be done about it? (Safety Integrity Level Selection and Safety Requirement Specification)
- How reliable will it be? (Safety Integrity Level Verification)
- How do I stay safe? (Safety Integrity Level Sustain)

It is vital to know how much safety is actually required and what measures are available to achieve it before embarking on the expensive implementation of Safety Instrumented Systems, which may actually be unnecessary.

If they are necessary, then Safety Instrumented Functions must be appropriately designed, implemented, installed, operated, maintained, and regularly tested in order to optimally achieve and continue to achieve the required risk reduction throughout their life.

Appropriate management must be exercised with competent personnel, accurate data, and proven methods to support the analysis, realization, and sustainment of functional safety.

References

1. IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector (2003).
2. ANSI/ISA–84.00.01–2004 (IEC 61511–1 Mod): Functional Safety: Safety Instrumented Systems for the Process Industry Sector (2004).
3. UK Health and Safety Executive R2P2: Reducing Risks, Protecting People (2001).
4. IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (1998).
5. ISPE GAMP: Good Practice Guide – Validation of Process Control Systems (2003).
6. IEC 61882: Hazard and Operability Studies (HAZOP Studies) – Application Guide (2001).
7. ISA Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis (2002).
8. AIChE CCPS: Layer of Protection Analysis – Simplified Process Risk Assessment (2001).
9. UK Health and Safety Executive out of Control: Why Control Systems go Wrong and How to Prevent Failure (2003).
10. ISA Safety Instrumented Systems Verification – Practical Probabilistic Calculations (2005).
11. AIChE CCPS: Guidelines for Safe Automation of Chemical Processes (1993).

About the Authors

David Hatch is a Partner with Exida and has more than 20 years of design, commissioning, operating, and consulting experience in the life science, energy, and chemical industries. This experience covers blue-chip operating companies, major multinational engineering contractors, and control and safety system suppliers. He has a BSc (Hons) in chemical and process engineering from the University of Strathclyde (UK), is a Chartered Engineer and Fellow of the Institution of Chemical Engineers in the UK, and an IChemE Registered Safety Professional. He is a Certified Functional Safety Expert, a member of the IChemE Safety and Loss Prevention Subject Group, and a specialist in process automation, hazard analysis, and alarm management; authoring and presenting papers on these key subjects. Hatch is an active member of ISPE, the Instrument Systems and Automation Society (ISA), and is currently contributing to the development of an international standard for alarm management. He can be contacted by telephone: +44-7909-973719 or by email: david.hatch@exida.com.

Exida, Epic House, Eliot Park, Barling Way, Nuneaton, CV10 7RH, United Kingdom.

Iwan van Beurden is the Director of Engineering at Exida and previously worked for Yokogawa Industrial Safety Systems in Apeldoorn, the Netherlands. He worked both in the R&D and in the Operations Department as a safety assessment specialist. He was involved with the implementation of IEC 61508 within Yokogawa Industrial Safety Systems dealing with SIS reliability calculations and the safety education of engineers. He is a Certified Functional Safety Expert, a member of the Instrument Systems and Automation Society (ISA), and has published various papers and magazine articles. He holds a Master of Science degree from Eindhoven University of Technology in Eindhoven, the Netherlands, where he majored in reliability engineering and graduated cum laude. He can be contacted by telephone: +1-215-453-1720 or by email: vanbeurden@exida.com.

Exida, 64 N. Main St., Sellersville, Pennsylvania 18960, USA.

Dr Eric W. Scharpf is a Partner with Exida and is based out of Port Chalmers, New Zealand. He has more than 10 years of professional experience in the chemical processing industry. Scharpf is recognized as an expert in chemical process efficiency analysis and improvement. He developed several of the cryogenic gas processing and separation techniques currently used for hydrogen, synthesis gas, and power generation. He was most recently a lead process chemical engineer with a Fortune 200 gas and chemical processing company. Principal work responsibilities have included engineering research and development, project execution, safety and risk analysis, and operations/manufacturing efficiency and reliability improvement in the bulk gas and specialty chemicals industry. He has authored more than 10 US and international patents as well as several journal articles and conference publications. Currently, he teaches process optimization and energy management at the University of Otago in Dunedin, New Zealand. He has a BChE from the University of Delaware and a PhD in chemical engineering from Princeton University, both in the USA. He can be contacted by telephone: +64-3-472-7707 or by email: escharpf@exida.com.

Exida, 278 Blueskin Road RD1, Port Chalmers 9081, New Zealand.