Life Is On | Schneider Electric

Operational Safety Integrity – Closing the Safety Loop

by Sven Grone and Steve J. Elliott

Executive summary

Process safety management in the process industries has evolved beyond simple functional safety. Some companies are at risk because management and business process aspects are not integrated into the overall safety plan. Such gaps can impact both operational integrity and profitable performance. This paper explores the change drivers affecting plant process safety management and explains how operators can find, measure, and manage gaps to maintain safe conditions and improve profitability.

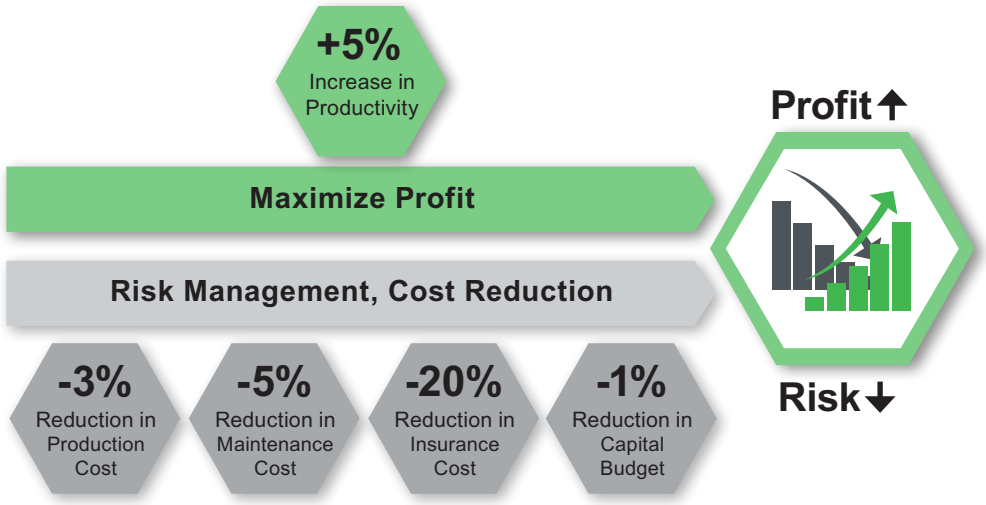
Introduction

Plant safety is high priority for most operators of industrial processes, with many operators publishing goals of zero incidents or accidents. Occupational safety includes procedures for protecting personnel from trips, spills, falls, handling hazardous materials, and working at heights. Functional safety arose from the need to avoid large-scale industrial disasters and involves the safeguards required to manage and mitigate hazards, assess possible consequences and risks, and determine a required level of protection. Today international standards such as IEC 61511, IEC 61508, ISA S84, and others are widely adopted and considered best practice in the industry. They provide a performance-based framework for the design, implementation, and operation/maintenance of automated safeguards, including safety instrumented systems (SIS) such as emergency shutdown systems (ESD), alarm functionality of the distributed control system (DCS), burner management systems, and other automation and control technology geared toward safe operations.

But regardless of how well-designed these safeguarding systems are, they can only ever be fully effective if operated and maintained according to their design criteria over the entire operational life of the plant. Growing awareness of this fact has given rise to a newer discipline of process safety management. Why pursue improvements in safety in addition to the fact that human life and health should be safeguarded at all times? Evidence is beginning to emerge that companies with good process safety realize significant direct cost benefits. **Figure 1**, for example, shows the results of research from the Center for Chemical Process Safety. Results indicate not only a 5% increase in productivity to the top line, but also improvement to the bottom line through reduced costs for production, maintenance, capital budget, and insurance.

Although these numbers will vary from industry to industry, end users reveal that they are seeing comparable trends. Process safety management is key to achieving such results.

This paper explores the change drivers affecting plant process safety and explains how manufacturers can find, measure, and manage gaps to maintain safe conditions and improve profitability.



Source: Center for Chemical Process Safety study found companies with good process safety reported significant direct cost benefits.

Figure 1
Process safety leads to both top- and bottom-line improvements.

Safety characteristics

Defining process safety

While functional safety has proven successful in reducing the probability of catastrophic events and recognizes the role of human factors, it does not explicitly address the key roles of management and business processes in maintaining the operational integrity and profitable performance of process plants over time.

By definition, process safety management (PSM) is the application of management systems to identify and control process hazards to prevent process-related injuries and incidents. The goal is to minimize process incidents by evaluating the whole process. PSM as an approach came into widespread use after the 1992 adoption of OSHA Standard 29 CFR 1910.119 Process Safety Management of Highly Hazardous Chemicals.

A further definition of PSM is "the proactive and systematic identification, evaluation, and mitigation or prevention of chemical releases that could occur as a result of failures in process, procedures or equipment."[1]

Process safety seeks to ensure that the functional safety safeguards and equipment are available and operating at peak performance. PSM includes enforcing routine maintenance procedures, keeping maintenance backlogs or records of the safety critical devices that manage those risks, and enforcing practices such as standard operating procedures. Lack of visibility into the operations and maintenance of functional safety equipment introduces significant uncertainty about the safety of the plant, and PSM has evolved as a discipline devoted to eliminating that uncertainty.

Measuring safety

Occupational, functional, and process safety share the need to measure performance, both for operational and for corporate reporting purposes. Occupational safety is the most mature and hence furthest along in this respect. It can be measured in lost time, injury frequency, injuries per million working hours, total recordable case frequency, and fatal accident rates. Attention to such clear and quantifiable measures has contributed to effect a steady improvement in plant safety. Industry groups have worked together, established standards, and shared best practices; and the workplace is much safer as a result.

However, despite the maturity of the occupational safety industry, its measures are only lagging indicators of danger, which can track historical performance but don't predict future safety. Occupational safety provides a baseline performance standard, which functional safety is beginning to emulate by measuring downtime, meantime between failures, and failures on demand; but these are lagging indicators as well. Whether a system will be ready tomorrow depends as much on whether it has been installed correctly, maintained properly, tested adequately, and evaluated in the context of its role in the company's broader processes.

Causes of safety gaps

The time factor

The passing of time, lack of visibility to degrading system and safeguards, and human complacency combine to deepen safety gaps (see **Figure 2**).

[1] OSHA, Process Safety Management Guidelines for Compliance

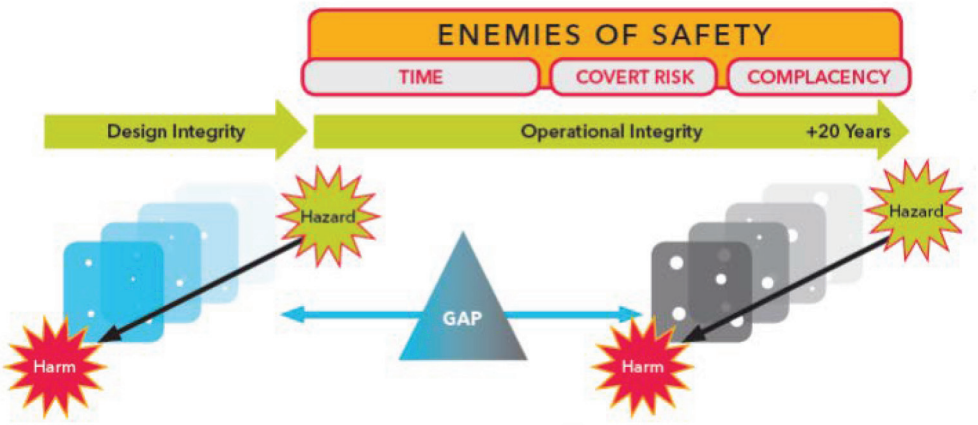


Figure 2
Drivers of today's heightened interest in plant safety.

Traditionally, almost all attention to safety gaps has been at the early phases of the safety lifecycle only, e.g., during the hazard and risk assessments, allocation of safety functions to protection layers, definition of the safety requirements, and full system specification. This detailed analysis can take six to 24 months, depending upon the size and complexity of the process, the plant, or the equipment. Resulting safeguards are typically operational for the next 20 or 30 years; however, the requirements for the life of an asset is now closer to 40 years. During that time, gaps start to appear in the safeguards during everyday operations and maintenance, and the real-world integrity of a system begins to vary from the original system design.

Moreover, the passing of time without a process incident is not necessarily an indication that all is well. All systems degrade over time. Without proper maintenance, systematic calibration, or ongoing proof testing, safeguards can ultimately degrade to the point at which they lose effectiveness.

Lack of visibility

The more exactly manufacturers know when the safety systems move off spec, the more effectively they can know what to do to get them back on track, which underlies the second contributing element in safety gaps: lack of visibility into the risk. Risk is covert; it emerges from the least expected places. It is often difficult for management to know the quality and health of PSM systems. It is not just the passing of time that causes safety integrity gaps; it is the inability to visualize and see where the risks are and from where the next incident may originate.

Evolving Workforce

The workforce of today is very different to that even 20 years ago. Working at the same company or plant for 20+ years is no longer the norm. The accumulation of skills and knowledge within operational staff is ever decreasing. The modern workforce is more reliant on technology to make decisions than ever before. As the workforce becomes more mobile, staff turnover increases, and with the imminent retirement of the baby boomer generation, much of the accumulated knowledge, skill, and experience of the plant will also retire. Management needs to recognize the potential safety impact of gaps in workforce experience.

Human complacency

The third major contributor to safety integrity gaps is human complacency. As time passes without a visible incident, people may become complacent and drop their guard. In the upstream oil and gas industry, for example, where there's a high dependency on contracting staff, contractors may move frequently from company to company. They may bring with them habits from one company that may not be acceptable in another. For instance, a company might find it unacceptable to bypass alarms for 12, 24, or 48 hours, while another might be more willing to accept the related risk. But the contractor may just accept the riskier approach as standard and apply it to all companies, sometimes without ever being conscious of the habit.

Drivers for change

Increased awareness, regulations, and collaboration

Today, greater public awareness of safety incidents is a strong driver for the heightened interest in improving plant safety. In this age of pervasive communication and social media, likelihood of containment of any incident is minimal. As a result, the cost to the company of a serious incident has grown exponentially, to the point where a single major incident could cause the failure of the entire company.

Financial Cost

The Deepwater Horizon oil spill of April 2010 has had a financial impact close to USD $60 billion and counting. The operators' share value lost more than 50% within 60 days after the incident.

Public awareness also contributes to the second development that is heightening plant safety activity and increased regulation. Today's regulatory activity has shifted from passive to predictive and preventive. Recent updates to international safety standards such as IEC 61508 and associated (impending) updates to IEC 61511 have seen "informative" language become "normative" In other words, advisory recommendations have now become mandatory requirements within the standards. Requirements such as periodic validation of safety instrumented function (SIF) performance against design criteria, and the need for personnel working on safety systems to have the required training and competence are now mandatory.

In parallel, associated industry bodies are also calling for the modification and update of regulatory standards such as OSHA's PSM framework, with the US Chemical Safety Board adding the modernization of process safety management regulations to its list of "Most Wanted Safety Improvements" list.

Where regulators once showed up only to investigate after an accident, today they are very much involved pre-incident, working with operating companies to mitigate risk by identifying and managing leading indicators.

The third driver for change is increasing collaboration among oil and gas, chemical, energy, and other industries that run higher risk processes. While operating companies all have welldeveloped safety and related maintenance risk management programs in place, they are collaborating in the creation of a common framework that will shape best practices.

Safety standards

Recommended safety practices

The fourth driver is the maturing of safety standards, safety practices, and safety communities. The International Association of Oil and Gas Producers (OGP), for example, now annually reports safety performance metrics of more than 45 operating company members so that these companies can benchmark themselves against each other. One of their recommended practices was around Process Safety Key Performance Indicators (Report No. 456 Process Safety – Recommended Practice on Key Performance Indicators), which provides guidance on the establishment of leading and lagging indicators to strengthen risk controls (barriers) and prevent major incidents.

This builds upon the ANSI (American National Standards Institute) / API (American Petroleum Institute) standard on Process Safety Performance indicators for the Refining and Petrochemical Industries recommended practice API 754, published in April 2010.

API 754 defines leading and lagging indicators in the four-tier pyramid illustrated in **Figure 3**. The tip of the pyramid represents incidents which have the greatest consequence but which are the lowest in frequency as contrasted with the base of the pyramid, representing incidents that occur most often but have least serious consequence (when considered in isolation). Left unchecked, Tier 4 incidents can aggregate and advance to become dangerous Tier 1 events.

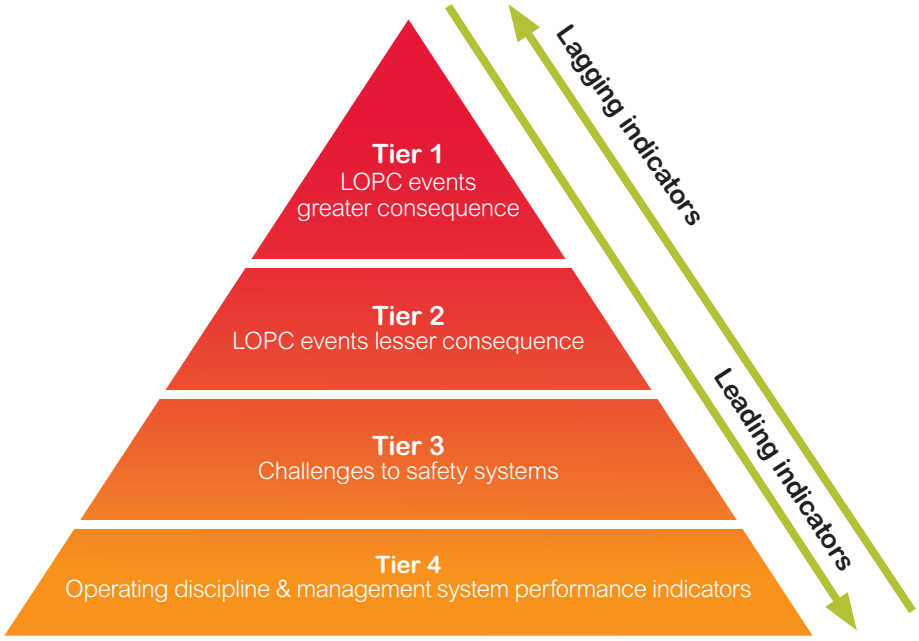


Figure 3
Process Safety Indicator Pyramid (API RP 754).

The four tiers are expressed as a triangle to emphasize that statistically larger data sets are available from the KPIs in the lower tiers. This approach mirrors the Occupational Safety Indicator personal accident pyramid (**Figure 4**).

Figure 4
Occupational Safety Indicator Pyramid.

The bottom tier of the pyramid is largely within the company's' domain of control, because these incidents often result from factors such as breaches in operating discipline or ignorance of performance indicators. These can be addressed through management and technology improvements in areas such as monitoring, communications, and training. Small steps taken here can avoid a major catastrophe down the road.

The higher up the pyramid, the less control there is over prevention and prediction, and a manufacturer may enter into the realm of damage control. At Tier 3, for example, most of the control is relegated to the safety instrumented system (SIS) that is in place to manage or mitigate those risks identified during the design phase. Some companies stop at that, assuming the SIS will continue to do its job of protecting the plant from threats.

But API 754 also calls for continuous monitoring and analysis of threats to the SIS. Companies with more safety maturity, for example, might consider a challenge to the system as a near miss and investigate it as such. They would want to understand what caused it, what could have happened if left unchecked, and what might have happened if the SIS didn't work exactly as defined. With this level of attention, challenges to the system can become leading indicators of future problems, which can be managed through operations and maintenance improvements.

Evolving standards

API 754 is one of a number of safety standards or recommended practices that has emerged to help manufacturers to improve, benchmark, and maintain regulatory compliant operations. The following are among the most important standards impacting plant process and functional safety:

- IEC 61508 covers safety-related electrical and electronic programmable systems
- IEC 61131 provides the standard for programmable controllers
- IEC 61511 is the standard for safety instrumented systems for the process industries
- ISA SP84 is another standard that affects programmable electronic systems used in safety

But while adherence to such standards can lead more companies toward meeting a zeroincident goal, most were not in place or being implemented 10 or 15 years ago. Many of these standards are now going through a period of update. For example, IEC 61508 was updated in 2010 and IEC 61131 has been updated to specifically address functional safety. IEC 61511 and ISA SP84 standards are being redrafted.

The continued evolution of these standards will have a marked impact on operating companies. Standards are evolving to include more target-based quantitative measures, which will require greater monitoring and analytic capabilities.

Closing safety gaps

Business integrity

Improving plant safety requires closing gaps in design, operations, maintenance, and financial integrity. Managing business integrity starts at the very top of the organization with leadership, compliance, and culture. Assurance of the integrity of an organization's operations requires visible leadership and accountability at all levels of the organization. Management must lead by example – it is no longer acceptable for senior management and leadership to just "talk about safety." Effective PSM requires the proactive involvement of the entire safety leadership and can no longer be relegated to the technical domain.

Certainly, companies are in business to make a profit, and cost reduction is one strategy for doing that, but cost reduction does not necessarily go hand in hand with plant safety improvement. Cutting costs in safety management could have a huge, negative impact on profitability in just a single preventable incident.

Design integrity

Design integrity focuses on risk identification and assessment, identifying the risks inherent within a plant and process, understanding the potential causes of the risks, the consequences of the risk — economic, environmental, or safety — and then implementing the methods to manage and reduce risks to an acceptable level. It is guided by international standards, corporate standards, and company- or site-specific standards. These then lead to the safeguards that might be designed, built, tested, and implemented to mitigate or manage risks to ensure operational integrity. Once implemented, it is then up to operations to execute these safeguards and maintenance to keep them in running order for the life of the plant.

"Though risk can never be eliminated through design, a variety of methods can balance desired safety outcomes with day-to-day business imperatives and pressures."

Though risk can never be eliminated through design, a variety of methods can balance desired safety outcomes with day-to-day business imperatives and pressures. It starts with application of standards and performance analyses such as Hazard and Operability (HAZOP) studies, which can identify risks. Once hazards are identified, Layer of Protection Analysis (LOPA) can suggest ways of reducing the risks to acceptable levels, which provide the basis for safety targets such as "Safety Integrity Levels" and required safeguards, which should then roll up into a "Safety Requirements Specification."

At that point, simulation tools and techniques can assist with the design by modeling the risks, enable "what if" analysis, and prove the value of risk reduction safeguards before they are actually implemented. Such models can also be carried forward into operations to use for operator training, enhancing the skills and competencies of the operator's ability to respond to abnormal conditions or situations where the process is deviating from the normal safe operating state into a potentially unsafe condition.

Design analysis and simulation information can define the systems that would be put in place to mitigate the design risks, including selection of safety integrity level (SIL)–certified instrumentation and a wide range of control systems for functions such as emergency shutdown, burner management, fire and gas detection, and high-integrity pressure protection.

Operational and maintenance integrity

Once safeguards are in place, it is the job of operations and maintenance to use them effectively. Operational and maintenance integrity involves the people and procedural aspects — where people are, what they are doing, how they are doing it, what skills and competencies they have to do their jobs, and the practices and procedures that they follow. It looks also at the equipment they use to perform their jobs as well as the physical plant equipment they touch.

This begins with monitoring the real-time performance of the safety systems against potential risks identified during the design phase. Any divergence from design limits is flagged, displaying dashboards of appropriate safety metrics and leading indicators and then alerting the appropriate safety personnel to any issues detected. In effect – "closing the safety loop" (see **Figure 5**).

This approach might, for example, involve tools such as HMI-based visualization systems that support the application of inhibits and bypasses, supports workflows in accordance with IEC 61511, and complies with the ISA S18 standard for annunciators and sequences.

Figure 5
Closed loop safety.

The challenge for many companies has been how to do this automatically and persistently without expending unsustainable engineering effort and manpower. Many companies utilize data collection software, historians, and other methods of collecting data. However, the automated real-time analysis and validation processes still tend to be done manually.

There is a need therefore to turn the data collected into knowledge that can form the basis of good decision-making. Putting context around the data to provide the right information to the right people in the right timeframe is critical to ensure that both lagging and leading indicators are trustworthy and delivered to those that need them in a timely fashion.

Operating manuals and procedures, standard operating procedures (SOPs), process and operational status monitoring, and handover documentation are also instrumental in closing operational and maintenance integrity gaps. Management of operational interfaces, management of change, operational readiness, and process start-up also come into play here, as do emergency preparedness, inspection and maintenance, management of safety critical devices, work control, permits to work, task risk management, and the selection and management of contractors and suppliers.

All of these systems contribute information to a plant's risk profile. Such profiles can be used to characterize risk through dedicated HMIs that might display risk across the enterprise, populating decision support tools, executive dashboards, performance reports, etc., which help show in real time the trade-offs between plant safety and plant profitability. Managers, operators, and engineers alike can make critical decisions in the context of the associated safety risk.

An important step in closing the safety integrity gaps is continuous review and improvement — organizations should regularly review compliance and ensure that they learn from investigational findings. Incident reporting and investigation, together with audits, assurance management review, and intervention are vital to ensure that performance meets defined targets.

The challenge for the automation technology community is to enable companies to meet this higher level of scrutiny without jeopardizing profitability or the safety of the operations themselves.

Metrics for analyzing risk

Developing process safety metrics is essential for managing and addressing the specific concerns of each functional area of a plant, from equipment to the overall plant and corporate level. Process safety metrics can guide personnel in different functions, such as maintenance supervisors, technicians, and operators who are responsible for tactical actions and performing tasks at the right time. For executives, metrics can roll into a trending view of a plant's safety level.

Once such information is visible, the next step is to articulate the value at risk, adding a dollar value to the performance. With that information, plant officials can then look at an individual asset, determine its value in terms of its contribution to both the risk profile and the revenue, and evaluate any piece of equipment or process, based on both its contribution to the risk profile and to the bottom line. A manufacturer can then determine an action plan for improving or maintaining safety levels.

Conclusion

By measuring and identifying appropriate KPIs and monitoring procedures, manufacturers can begin to close gaps in process safety.

A successful process safety management program is the sum of the best people, plus the best practices and procedures, plus the right technology, collaborating in real time to minimize the gaps between the acceptable design and what actually happens in day-to-day operations and maintenance activities.

This formula provides a framework for building a holistic and systematic approach to balancing economic performance, production performance, quality performance, and safety performance.

For companies large and small, the principles of balancing relationships among people, processes, and technology is critical to closing the safety integrity gaps and business performance loops.

References

Center for Chemical Process Safety (CCPS): Guidelines for Process Safety Metrics

Energy Institute (EI): High Level Framework for Process Safety Management

Health and Safety Executive (HSE): Developing process safety indicators – A step-by-step guide for chemical and major hazard industries.pdf

International Association of Oil and Gas Producers (OGP): Process Safety – Recommended practice on key performance indicators (report No. 456)

Organization for Economic Cooperation and Development: Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response

About the author

Steve Elliott is Senior Director, Offer Marketing - Process Automation for Schneider Electric, globally responsible for future direction and go-to-market strategy. He is a TÜV certified functional safety engineer with more than 20 years experience in the process control and automation industry and has extensive experience in safety systems and the safety lifecycle. Steve regularly blogs on process safety related topics: https://blog.schneider-electric.com/author/selliott/

Sven Grone is a Safety Services Practice Leader for Schneider Electric's EcoStruxure Triconex safety and critical control systems and solutions. He is responsible for the development and implementation of safety lifecycle services within Asia Pacific and Middle East regions. He is a TUV Certified Safety Engineer with 13 years' experience in safety systems and the safety lifecycle and more than 25 years' experience in the automation and controls industry.

For information on EcoStruxure Triconex Safety Systems visit: www.schneider-electric.com

Schneider Electric
70 Mechanic Street, Foxborough, MA 02035 USA Telephone: +1 877 342 5173 schneider-electric.com/processautomation

PN SE-998-20241665_GMA-US Rel. 03/18