



Process safety: Blind spots and red flags

Improving safety for organizations involve more than technological solutions; understanding processes and plant interactions are a must

By: **Tom Shephard**, CAP, PMP, Mustang Engineering, LP

As Published in Hydrocarbon Processing, March, 2011

The Process Safety Management (PSM) regulation *29 CFR 1910.119* was developed in response to a series of major accidents. These same events led to the creation of the safety instrumented system (SIS) standard, *ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)*. Both provide a wholistic, lifecycle approach to the design, operation and maintenance of SIS and facilities. Plant safety improves when these programs are implemented, although accidents can still occur.

From studies of major accidents, most result from the simultaneous occurrence of multiple and seemingly minor errors and “incidents” that interact in complex and unforeseen ways.¹ PSM and ANSI/ISA 84.00.01 are similar in that both have interdependent elements that work together to reduce the likelihood of errors and hazards that can contribute to an accident. A failure or error in any element becomes the weak link. This article explores some of the hidden errors and conditions that can occur during the SIS or facility life cycle, and refers to them as “blind spots.” Examples of their varied modes and risks are highlighted. “Red flags” are a common prelude to a major accident. As an aid to revealing blind spots, an awareness of common red flags may be helpful. Examples from major accidents are listed.

“Blind spots” are often recognized as a significant contributor to a major accident. Those discussed here have hidden or unforeseen mechanisms that can degrade an SIS or a safety management program. Independent protection layers (IPLs) applied to reduce risk are methodically selected and implemented to reduce the probability of hazard occurrence to a tolerable risk. Typical IPLs include relief valves, alarms and SIS. Accidents can result if an IPL is inadequate, degraded or fails. Undefined hazards also exist and the associated hazard consequence and likelihood are unknown.

Project Execution

Today’s typical large-scale engineering projects have major teams that interact with many organizations and companies. In a relatively short time, they generate thousands of documents and a thousand-fold increase in project data that resides in many forms, formats, and systems. This information is communicated through many different media. Being a human endeavor, quality-checkpoints are added at key points. Schedule compression tends to increase error rate and challenge the quality check process. Compression is common to fast-track projects, and can occur with late design changes, delayed decisions and extended approval cycles. Quality checks become less effective if performed at the wrong time or under stress; thus, errors can be missed. A purchase order with a single digit error in a lengthy model number procures the wrong material. A person with essential technical knowledge misses a key meeting. An inspector misses an important detail at a factory check.

Undetected errors can occur in the engineering data exchange between companies if the data exchange protocols are not well defined or managed.

Construction projects have a higher number of personnel who work within a physically more hazardous environment. Onsite decisions are constant. Items don't fit, material cannot be located or a key person in the communication channel is taken ill. A missed or inaccurate positive material check on a case of bulk alloy fittings is not detected. If detected, the installed locations may be unknown. The transition from construction to pre-commissioning and startup involves handoffs of many documents and status reports - all opportunities for missed information.

Safety Assessments

Safety assessments such as hazard and operability studies (HAZOPS) identify hazards and quantify their respective risk. *A hidden deficiency in this process can result in risks that are underestimated so that the applied IPL's are inadequate. A hazard can be missed or incorrectly assessed if the team is missing key technical, operating or maintenance expertise.*² Combustion and process experts are needed to assess the complex impact of a major fuel gas drum swing on multiple fired vessels across the facility. Perhaps the burner data sheets no longer exist so it is not possible to verify the burners can operate safely with the current fuel-gas composition range. Expertise needed to identify and accurately assess hazards that are unique to rotating equipment, exothermal reactors and high-pressure equipment may also be missing. The assessment may fail to consider all modes of operation, common mode failures, process response time or the complex scenarios that can result when a major upset occurs in a shared utility system, e.g., steam, instrument air or cooling water.

A safety related alarm applied as an IPL may be invalid. This can occur if an operator cannot reliably respond to the alarm within the process response time (preferable half the time). Further, the alarm IPL is invalid if a common event generates multiple alarms that exceed the generally recognized operator alarm response limit of 10 alarms in a 10 minute period.³ The assessment may fail to explore this possibility. Finally, if the alarm is invalid, then the SIL assigned to an associated safety instrumented function may be insufficient.

Technology

New technology and new designs often create unforeseen "challenges". When the industry embraced open systems, the Microsoft® Operating System became a standard component in many control systems. The unforeseen risk was an ongoing urgency to install frequent software "patches" to correct security holes and software stability problems. Another is the increased exposure to destructive viruses of the type recently revealed as the Stuxnet virus.⁴ Computer servers require frequent replacement due to early obsolescence. Control-system vendors press users to upgrade application software and hardware to ensure future product support. These upgrades often have subtle and undocumented technical and performance differences. Implementing a change before it is fully tested introduces an unknown risk.

If a facility's software backup and recovery procedures are inadequate or not followed, the wrong program or an outdated version may be loaded in response to an unplanned emergency repair. Inadequate physical and administrative control of an engineering work station connected to a safety system can compromise system

integrity. Sensitive process control networks, thought to be isolated, may, in fact, connect to a business network or unprotected Internet connection and become a tempting target for computer hackers worldwide. Cross-connection of a process control system network to a business enterprise network opens the opportunity for a control system interruption or upset that may be caused by a routine business network administrative change or update.

High-integrity pressure protective systems (HIPPS) are increasingly being used to reduce project cost or increase production. A well-designed and managed HIPPS offers safety benefits, but is also a “high-tech” solution that replaces a low-tech solution that is well understood. Management of HIPPS and other SIL 3, high-integrity safety systems require a mature, disciplined and technically talented organization for the duration of the system’s life cycle. Most of the blind-spot failures discussed here can degrade this system. Because a SIL 3 system is typically implemented to mitigate a high-consequence safety hazard, its failure or degradation can result in a major accident.

Human Factors

Humans will always make mistakes regardless of age, training and level of experience. A well-designed system, organization or procedure integrates humans into activities and processes where they are known to perform well, and it avoids or minimizes activities that humans are known to perform less reliably. If this is not the case, the expected error rate will be higher, and the resulting errors may be overt, hidden or unforeseen. Human error in any type of process or activity increases when humans are under tasked, over tasked or placed under stress.⁵

Human error is not random, but it is now understood to be systematic. The error is biased by the systems, culture and environments in which humans operate. Under high stress, the perception of time can become distorted. During a plant emergency, the actual elapsed time as experienced by a stressed individual may be significantly longer than perceived. When presented with a problem, humans tend to develop a mental model of what is happening and select data that supports that model. Data that does not support the model is often ignored, a condition that has contributed to major accidents. On the positive side, humans are essential because they provide the only means available to mitigate or manage a hazard that was previously unknown and has no other safeguards.

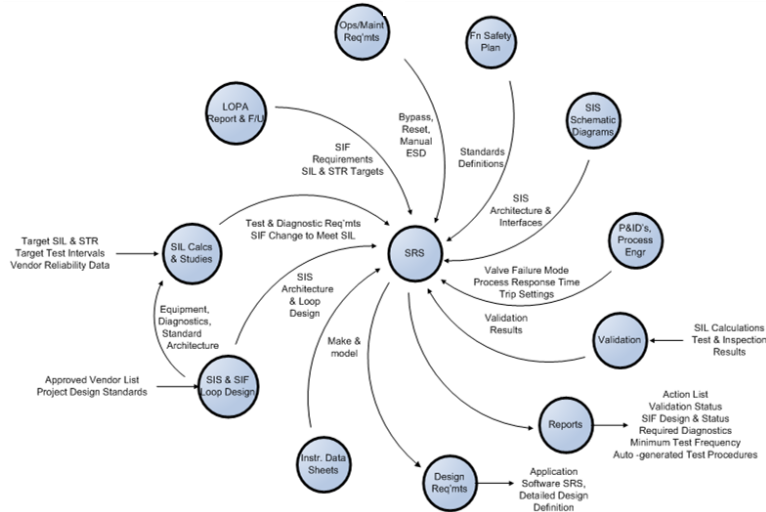
Organization

High-performance organizations of the type needed to manage high-integrity safety systems and successfully merge the PSM and ANSI/ISA S84.00.01 are not at a natural state; the laws of entropy apply. *Organizations undergo continuous change, whether desired or not.* The organization affects the other listed modes in positive and negative ways, which means it contributes to blind spots. A seemingly subtle change in priorities, staffing, training, work process, safety culture, age, technical expertise or tools can significantly affect process safety as it interacts with other listed modes.

When SIS progresses through its life cycle, the safety requirements specification (SRS) provides the essential foundation document needed to define and maintain system integrity. Figure 1 summarizes the information included in this document. An inadvertent change in any item can degrade or disable one or more safety

instrumented function residing in that safety system. Mapping each datum element to the department, technical discipline or organization charged with its creation or management provides an indication of the potential challenge. The opportunity for hidden errors and changes increase when elements are distributed across organizational boundaries.

Figure 1- Safety Requirements Specification (SRS)



If the group charged with managing a PSM program operates like a regulatory organization, then the expected safety management culture and practices are probably not being fully realized, though “full compliance” may be what’s listed in company reports. Current organizational structures may be an impediment when attempting to merge the requirements of ANSI/ISA S84.00.01 into the existing organization. How organizations integrate this standard with their PSM program appears to be an early work in progress for many. Until this process is complete and the “bugs” are worked out, mistakes will happen.

Operations and Maintenance

Operating modes may exist that are “below the radar” and, therefore, not assessed from a safety and risk perspective. A facility may regularly have a manual bypass valve open around a control valve to increase throughput. Others may operate a fired process heater when a forced draft fan has failed. A damper is opened and the heater is operated in a natural draft mode that was not considered in its original design. An operator tweaks a mechanical stop on a fuel gas valve, changing a process heater’s minimum firing rate. Use of safety system bypasses may become a common and casual act. The duration that a safety function is bypassed may be increasing, but is not tracked and goes unnoticed.

On the maintenance side, off-the-books repairs and undocumented software changes may be implemented in response to a problem that occurs during an unscheduled event, holiday weekend maintenance callout. Spare parts used may not actually meet the “replacement in kind” requirement of PSM or the more rigorous requirements in ANSI/ISA S84.00.01. Changes may be made without applying the “Management of Change” process (from PSM), or perhaps the process is not sufficiently controlled or transparent.

Risk Acceptance Creep

Individual risk tolerances can shift when the person is faced with an immediate decision on whether to proceed (e.g., maintain production) or revert to a known safe state (e.g., shutdown). Risk acceptance appears to increase or perhaps, risk denial occurs. For example, a difficult new unit startup is nearing completion. A safety event occurs, forcing the person in charge to decide on whether to proceed or shut down. The risk associated with proceeding is not immediately clear or understood. The time-sensitive decision increases stress and may offer little time to consult others who may understand the risk. (Perhaps the person who understands the risk is not in a position to affect critical decisions.) The decision to proceed or shut-down reflects the attributes of the decision-makers and how they have internalized their understanding of the company's management expectations, safety culture, priorities and training. The decision to proceed is made, and the situation improves, worsens or remains unclear. This may be followed by another decision to proceed and it follows the well worn adage, "in for a penny, in for a pound." This phenomenon, in a slightly different form, can occur during the engineering phase of a project when a tight schedule conflicts with the time needed to finish a safety-critical assessment or quality check.

Accident Investigations

Analyzing and identifying the root cause of a near miss or accident is an essential element in a safety management program. Past theory and practices for accident investigations took an approach that often cited "operator error" as the root cause. The new theory, which takes a much wider view, will often trace the root cause to a management failure or a failure of the organization or system in which humans function.⁵ Those applying the old approach (still commonplace) are not aware of where the true weakness in their systems exists, so similar accidents may reoccur.

Management and Leadership

All organizations, whether they are project teams or operating facilities, face the dichotomy of balancing process safety with production, cost and schedule demands. By words, actions and examples, management and safety leaders demonstrate their expectations. Subordinates interpret this message and bias their actions and attitudes accordingly. Given the challenges of communications in large and complex organizations, a few misunderstood words or an ambiguous or conflicting message may degrade the process safety attitude of employees.

For example, the appearance of an overriding priority on production may bias an operator's belief that a unit shutdown button should only be used if the hazard is certain and imminent. The systematic bias may be to delay a safety response when it conflicts with production. A downsizing that lays off a key technical expert who provides maintenance support for a highly technical safety system places that system at risk. Management and safety leaders may not be aware of the possible limitations in their safety management program. Many companies are implementing behavior-based safety programs that have been very effective at reducing injuries and accidents. These same programs may be less effective at revealing or mitigating errors caused by technology or project execution blind spots. An assumption that a given safety program sufficiently encompasses the full breadth of the safety management challenge may be a serious blind spot.

Red Flags

Several blind spot modes have been discussed. Many others exist, including training, standards and procedures, physical environment and regulatory environment, to name a few. A complete listing of possible blind spots within each mode can fill volumes. To limit their accident contribution, an awareness and acceptance that blind spots exist is essential. Another important element in a safety management program should include an awareness of the red flags that often precede a catastrophic accident. Management and safety leaders should give pause when they hear several important words; they may have just arrived at “that point, that last chance” when a critical failure can be prevented;

- Experience says that will never happen. (most catastrophic accidents)^{6,7}
- We need to reduce maintenance, staffing and training to cut costs (Bhopal MIC release)⁷
- “So we are all in agreement, RIGHT” (Shuttle Challenger and Columbia Disasters)⁶
- We don’t have time for that (most catastrophic accidents)^{6,7}
- Prove to me that it is not safe (Shuttle Challenger and Columbia Disaster)⁶

References:

- ¹ Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* New York, Basic Books Inc., 1999.
- ² Tom Shephard and David Hansen, “IEC 61511 Implementation – The Execution Challenge” *Control* magazine, May 2010.
- ³ Peter Bullemer and Doug Metzger, “CCPS Process Safety Metric Review: Considerations from an ASM Perspective” ASM Consortium Metrics Work Group, May 23, 2008.
- ⁴ Nancy Bartels, “Worst Fears Realized” *Control Engineering* magazine, September 24, 2010.
- ⁵ Sydney Decker, *The Field Guide to Understanding Human Error*, Surrey UK, Ashgate Publishing Ltd., reprint 2010.
- ⁶ Brigadier General Duane W. Deal, USAF, “Beyond the Widget: Columbia Accidents Lesson Learned Affirmed” *Air & Space Power Journal*, Summer, 2004.
- ⁷ G. Joseph, M. Kaszniak, L. Long, “Lessons After Bhopal: CSB a Catalyst for Change,” *Journal of Loss Prevention in the Process Industries*, Volume 18, Issues 4-6, July-November 2005.

Tom Shephard is an automation project manager at Mustang Engineering. He has 28 years of control and safety system experience in the oil and gas, refining, marketing and chemical industries. Mr. Shepherd is a Certified Automation Professional (ISA) and a certified Project Management Professional (PMI). He holds a BS degree in chemical engineering from Notre Dame University.