A PROCESS ENGINEERING VIEW OF SAFE AUTOMATION

Angela E. Summers, SIS-TECH Solutions, LP

Published in Chemical Engineering Progress, December 2008.

This step-by-step procedure applies instrumented safety systems (ISS) to continuously reduce process risk.

Balancing safety and production investment can be challenging. When production improvement projects are executed, the return on investment can be verified numerically on a real-time basis with relative certainty.

In contrast, safety projects seek to prevent an event, such as an injury, and do not produce anything that can be measured in real-time. At a well-managed facility, significant hazardous events occur so infrequently that impact data are virtually meaningless for trending process operation. Worse yet, impact trending provides no opportunity for correction prior to the event. When trends can be detected, the systemic problems are generally extensive and run deep within the organization.

Some safety benefits are measurable, but many only report impact on key performance indicators with little acknowledgement of the loss prevention element. Loss prevention savings need to be tracked to demonstrate return on investment.

Sufficient theory and standards exist to ensure that process equipment can be operated safely. Risk can be successfully managed throughout the life of a process using safety systems that are demonstrated to meet documented requirements. A quality management system is required to sustain the safety system's integrity; otherwise, incidents occur when enough latent conditions accumulate. A proactive approach uses metrics to track behaviors, errors and failures that are precursors to hazardous events (1).

Instrumented safety systems (ISSs) are commonly used to achieve or maintain a safe process state when abnormal operation occurs. Over the years, many terms have been used to describe types or classes of ISSs to facilitate more rapid understanding of the system purpose (Figure 1). In some cases, industry practices dictate the requirements for specific classes or applications.

ANSI/ISA Standard 84.00.01-2004, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" (or simply ISA 84.01) (2) uses the term safety instrumented system (SIS) for an ISS designed to be separate and independent from the basic process control system (BPCS) in order to provide protection against postulated control system malfunctions. The risk reduction required of the SIS determines its target safety integrity level (SIL), which is a benchmark based on the probability of failure on demand (PFD):

- SIL 1: 0.01 < PFD < 0.1
- SIL 2: 0.001 < PFD < 0.01
- SIL 3: 0.0001 < PFD < 0.001

To be classified as achieving a specific SIL, an SIS must be designed and managed under a quality management system throughout its life. This article describes how ISSs and SISs are implemented as part of a successful risk-reduction strategy.

1. Define a risk-reduction strategy

A process engineer has cradle-to-grave responsibility for a facilities safe operation. The earlier a risk-reduction strategy is defined, the better it will work and the less it will cost. Identify process hazards early in the process design, so measures can be implemented to reduce or eliminate hazards through inherently safer design (3).

Once process design is complete, the remaining risk will need to be managed for the life of the process equipment. Although inherently safer design may increase the initial capital cost, it substantially reduces long-term risks. Safety systems should only be applied when inherently safer design becomes impractical, because safety equipment requires long-term investment in administrative, operating and mechanical integrity activities.

To develop the risk-reduction strategy, start with a process hazards analysis (PHA) and review the process design and its control, operation and maintenance practices. Select a multidisciplinary team with expertise in these areas, and use an accepted hazard-evaluation procedure (4), such as a hazard and operability (HAZOP), what-if, or checklist analysis, to determine how process deviations from intended operation lead to process hazards.

Identify the causes or conditions that lead to deviations. For example, low flow can be caused by the failure of the flow control loop. Events can be caused by a single failure or by multiple failures. Ensure that the identified causes are the minimum that will lead to the process deviation. The most common initiating causes are related to failure of:

- control loops within the BPCS
- humans to act as required
- mechanical equipment.

These events can happen multiple times over the life of the process, so if the consequence is significant, safety systems are generally required to address identified risk.

Estimate the severity of the consequence, taking into account likely event conditions. Occupancy during an abnormal event is typically not the same as during normal operation. If abnormal operation occurs, what are the responsibilities of the field operators or maintenance crew? If a safety alarm goes off, is the field operator expected to respond locally? The slower the event, the more likely there will be field response and higher occupancy, possibly including supervisory, operations and maintenance personnel.

The process risk of a particular event is related to the likelihood that the event will occur and the severity of the consequences if it does. Compare the process risk to company risk criteria (5) to determine what is required to reduce the risk below the criteria (Figure 2). Residual risk represents a likelihood that an unacceptable consequence could occur, so drive it as low as reasonably practicable.

To lower risk, implement a defense-in-depth strategy in which one or more independent protection layers (IPLs) act to interrupt the event sequence, as illustrated in Figure 3. Independence is achieved when the IPL operation is not affected by the occurrence of the initiating event or by the failure of other IPLs. If

more than one function is allocated to the same IPL to prevent an identified hazardous event, the IPL must meet the overall functional and integrity requirement of all of its functions. Verify during the PHA that identified IPLs are properly classified and that available documentation clearly describes the IPL functional and integrity requirements. Seven core attributes of an IPL must be managed rigorously throughout the life of the process (6):

- independence
- functionality
- integrity
- reliability
- auditability
- access security
- and management of change.

In the past, it was common (and it still is common in small applications) for the safety alarms and controls to be separate from the BPCS. In recent years, some users have implemented safety alarms and controls in the BPCS when it is designed and managed to achieve the claimed integrity and reliability. Achieving safety integrity from the BPCS is not a trivial matter — it requires redundancy, diagnostics, and administrative controls that are beyond what is typically necessary for the control system.

In addition to addressing the process risk arising from identified initiating events (or process deviations) the risk-reduction strategy should also address secondary consequences associated with the operation of the IPLs, such as reduced production, shutdown, and flaring (Figure 4). Secondary consequences can be thought of as the side effects of the risk-reduction strategy — each time an IPL takes action, there is an effect on the process. Determine the cost of the spurious operation of IPLs to establish the maximum acceptable spurious activation rate. The final risk-reduction strategy should ensure that the side effects are acceptable or properly managed.

2. Implement the strategy

ISSs operate best when they are based on very simple logic. For example: “When the high-pressure alarm initiates, open the pressure control vent,” or “when high temperature occurs, close the feed valve.” This logic is simple enough that it can be implemented in hard-wired systems using trip amplifiers, alarm modules or relays.

Hard-wired systems are very cost-effective for systems of less than 10 functions. If more than 10 are involved, PLCs generally become more cost-effective. ISSs are not inherently complex systems, but they can become complex by design. Continue to focus on simple logic even in a PLC, where the ease of software programming encourages complex logic, increasing the likelihood for program errors.

PLCs are complex systems with the potential for large numbers of unidentified failures, including many systematic ones. Because of the unknown and unpredicted failures associated with PLCs, ISA 84.01 (Clause 11.5) requires the PLC to be safety-configured for SIS applications. Safety configuration addresses the widely known failure modes of the inputs, main processors, communications and outputs. This requires additional diagnostics and fault-tolerance capabilities that are not generally found in typical control systems, but that are available in systems marketed as compliant with IEC 61508.

ISA 84.01 (Clause 11.5) requires implementation of a user approval process to ensure that field equipment has sufficient prior-use history in a similar operating environment and that failure modes are understood and accounted for in the design, operation and mechanical integrity practices.

Facilities rely on ISS equipment to achieve or maintain safe operation. An ISS must be sufficiently robust to withstand environmental stresses and provide the required integrity and reliability. For each installation, define the environmental conditions that impact ISS equipment selection, such as:

- process composition, e.g., solids, salts, or corrosives
- process operating conditions, e.g., extremes in temperature, pressure, or vibration
- external conditions, e.g., winterization needs or hazardous area classification
- response time requirements related to available process safety time
- criticality, e.g., accuracy, drift, fire survivability and leak-tightness

The timely response of the ISS is critical to successful risk reduction. The process safety time starts when the process reaches the defined safe operating limit and ends with the loss of containment. The ISS should be capable of taking action on the process within one-half of the process safety time allocated to it. Final equipment specification requires an understanding of process dynamic response, instrument accuracy, and instrument loop response time.

Detection lag and measurement error are generally quite small when instruments are properly installed and commissioned. Shutdown causes the most significant lag including the time required to shutdown (or start-up) and the retained mass and energy in the system after the safety function is completed (Figure 5). The process safety time can be long (seconds to minutes) or short (milliseconds), depending on process dynamics and equipment design. The allocation of process safety time affects whether an IPL can effectively operate prior to another IPL taking action or the occurrence of the hazardous event.

Assess potential common causes in the process support systems, such as power, communications, instrument air, cooling water and hydraulic power. Ensure that ISS support systems are designed to take the affected equipment to a specified safe state as necessary to achieve the required integrity. Approval of non-fail-safe design should consider the impact on the risk-reduction strategy assumptions, the type of ISS, the support system integrity, and alternative means to achieve a safe state. Human and cyber access to any ISS should be sufficiently restricted using administrative procedures and physical means to ensure that this access does not impact the ISS integrity.

Document an ISS design basis and maintain it under revision control as process safety information for the life of the system. All ISSs are unique in that each is designed to address a specific hazardous event associated with the process. Two ISSs may be similar, but no two are exactly the same. The ISS design basis should address the following:

- requirements for the detection of and response to potential hazardous events
- requirements for fault detection, such as diagnostics and proof testing
- requirements for fault tolerance against dangerous failures
- provisions for safe bypass for maintenance and testing, including the maximum length of time that the ISS can be in bypass before management of change (MOC) action is required
- provisions for safe operation when process equipment is operated with an ISS fault

- provision for safe shutdown if the SIS fails to take action when required
- requirements for start-up and shutdown.

The SIS design basis is covered by ISA 84.01 (Clauses 10 through 12). ISA Technical Report TR84.00.04 (7) gives extensive guidance on design requirements for the hardware and software used to implement SISs. Consider developing uniform practices for similar applications to promote consistency in ISS implementation, as well as to reduce training costs and the potential for human error (8).

ISA 84.01 (Clause 11.4) requires fault tolerance against dangerous failures for SIL 3, so redundant safety equipment should be provided for SISs of SIL 3. Fault-tolerance is not required for SIL 1 or SIL 2 when SIS equipment is selected based on previous use, is independent from the initiating cause, and implemented such that the dominant failure modes take the SIS equipment to a specified safe state.

ISA 84.01 (Clause 11.9) also requires that the SIS integrity be verified quantitatively. Ensure that the selected equipment is fit for use in the operating environment, that the subsystems meet minimum fault-tolerance requirements and that the system achieves the required functionality and integrity. ISA Technical Report TR84.00.02 (9) provides guidance on the verification of the SIL of SISs.

ISS equipment should be included in a mechanical integrity program (10) that seeks to maintain the ISS in the "as good as new" condition. Mechanical integrity includes a variety of activities, such as inspection, preventive maintenance, repair/replacement, and proof testing. Include the instrumentation and controls used by the operator to detect and take manual action. Maintain an equipment list that identifies ISS equipment by a unique designation and includes the required inspection and proof-test interval necessary to ensure the equipment remains fit for service.

The initial proof-test interval is determined based on offline test opportunities, relevant regulations, equipment history in similar operating environments, manufacturer's recommendations, and integrity requirements. When proof-testing is required more frequently than scheduled outages, online proof-test and repair facilities will be necessary.

If the online activity requires bypassing, document the compensating measures that provide equivalent protection to the lost ISS functionality. Assess bypass activities and potential hazards to define the compensating measures and the maximum allowable repair time. Implement bypass alarms when practical, and re-initiate bypass and safety alarms across shifts. Ensure that operators know the state of ISS equipment and what to do if a process deviation occurs.

3. Validate, start-up, operate and maintain the strategy

Validation has traditionally been referred to as a site acceptance test (SAT) because it represents the formal acceptance of the installed and commissioned ISS by the plant operations staff. The equipment is proven to work as required, and from this point forward, changes are reviewed and approved according to the plant's MOC practices. Validation is performed after instrument calibration and loop checks have been completed. A validation plan is developed to ensure orderly execution of the SAT and thorough documentation and resolution of any findings. ISA 84.01 (Clause 15) addresses validation of SISs.

Validation demonstrates that the ISS operates according to the design basis as installed and commissioned. Validation is an input-to-output test of the ISS that also proves that the ISS equipment interacts as intended with other systems, such as the BPCS and operator interface. The SAT also provides

an opportunity for a first-pass validation of the operating and maintenance procedures. Validation must be completed prior to the initiation of any operating mode where a hazardous event could occur that would require the operation of a new or modified ISS. Some users require that validation be performed after any major process outage or shutdown.

Complete a pre-start-up safety review (PSSR) to verify that:

- new or modified ISS equipment is installed and demonstrated to operate per design intent
- adequate procedures are in place to ensure required functionality and risk reduction
- appropriate hazard analysis or MOC reviews have been conducted and their recommendations addressed
- training of affected personnel has been completed.

Additional information about the PSSR can be found in Ref. 12.

Clearly define the safe operating limits in the operating procedures, and the proper action to take when these limits are exceeded. The operator's response to an indication, alert, alarm, or incident is dictated first by procedures and training and then by experience. Audit the operator's response to ISS diagnostic and safety alarms. ISA 84.01 (Clause 16 and 17) addresses operator and maintenance procedure requirements for SISs. Procedures should include:

- a description of the hazardous events being prevented
- a description of the ISS
- the appropriate operator response to detected ISS equipment failure and provisions for operation with detected faults (i.e., compensating measures)
- conditions under which it is safe to reset an ISS
- use of start-up bypasses and the process conditions to be monitored during start-up
- the expected operator response when safety alarms are received and the setpoints for those alarms
- trip setpoints, the expected safe state when a trip is completed, and the form of trip notification (if provided)
- expected operator actions if a safe state is not achieved
- the "never exceed, never deviate" process conditions that require manual shutdown.

Installed safety equipment is subject to the same operational stresses as control equipment, and it can fail at any time. Safety equipment typically operates in demand mode, i.e., it is not supposed to act until the abnormal condition occurs. When the ISS fails, it may not be readily apparent, as would a failure in a control application. Equipment often demonstrates a failure rate over time that follows a so-called bathtub curve (Figure 6).

Early failures are caused by manufacturing, assembly, test, installation and commissioning errors. Many early failures are the result of rough handling, improper pre-installation storage, poor installation practices, or sloppy construction practices. Rigorous inspection, commissioning and validation activities are necessary to identify and correct these failures.

The wear-out period is characterized by an increasing failure rate over time. Poor mechanical integrity has been cited as a primary cause of equipment failure. Preventive maintenance can extend

equipment useful life and improve its reliability. Mechanical integrity records provide data that equipment is being maintained in the "as good as new" condition and justify its continued use. Consequently, maintenance personnel must be trained on the activities necessary to ensure equipment integrity.

Periodic proof-tests should be performed at a frequency sufficient to detect the transition from the useful life period to the wear-out period, so that the need for equipment replacement or upgrade can be identified and planned. Equipment failure should be investigated using root-cause analysis to reduce or eliminate failure causes. The proof-test interval should be periodically evaluated based on plant experience, hardware degradation, demonstrated software reliability, etc., and in the event of repeated failures, the interval should be shortened as necessary to ensure expedient failure detection.

Execute proof-tests using operation and maintenance procedures that ensure the test is completed correctly, consistently and safely. Proof-tests should determine the "as-found/as-left" condition for all defined operating modes. Documentation should be traceable to the procedure, equipment, and person performing the test. Identify and assess deviations from the design basis and equipment specification, e.g., incomplete MOC or accelerated degradation. Then, use the proof-test to train personnel on expected ISS functionality and to verify procedures clarity & completeness.

Real-world risk-reduction is demonstrated by mechanical integrity data. The records associated with any ISS must show that the equipment can operate as specified during all intended operating modes. This is especially true for the SIS, which often provides the last chance to bring the process to a safe state.

Failure tracking and analysis is essential to close the safety lifecycle. Repeated failures likely indicate that the installed equipment is not capable of meeting the performance requirements. Use root-cause analysis to determine why metrics are trending in the wrong direction, in order to implement action plans that improve the management system, equipment, procedures, and personnel training. Identify special and previously unknown failures and communicate these to personnel, ensuring that lessons learned are not hidden in mechanical integrity records.

4. Manage changes to the strategy

Deming believed that 85% of a worker's effectiveness is determined by the system he works within and only 15% by his own skill (11). A successful risk-reduction strategy accepts that humans are involved in every aspect of an ISS's lifecycle. Therefore, the integrity claimed for any ISS is limited by the quality management system that identifies and seeks to eliminate flaws in the system. Human error must be reduced to the point where it does not significantly impact system integrity (12). Assurance of personnel competency is key.

Knowledge evolves over time as research and development yields operational enhancements to process facilities. Events involving abnormal operation identify weaknesses in the risk-reduction strategy, leading to the need for more safeguards and improved performance metrics. New ideas identify ways to lower risk further.

Periodically evaluate existing ISS against current criteria and industry practices to determine whether equipment is designed, maintained, inspected, tested and operating in a manner that would hold up to public scrutiny. Use a MOC procedure to initiate, document, review and approve changes to ISSs other than replacement-in-kind. Evaluate changes to the process and its equipment to determine their

potential impacts on the approved ISS design basis prior to implementing the change. Personnel need to understand what triggers a MOC review and why tracking changes is important.

Update documents to "as-built" status, incorporating changes made since the last formal drawing/document revision. Maintain documentation under revision control for the life of the equipment. Documentation should be traceable to the process hazards analysis and should be auditable.

Final thoughts

An effective management system uses a systematic approach to manage the risk throughout the process equipment's life. With the continuous involvement of process engineering, the risk-reduction strategy can be tailored to meet operating, maintainability and reliability goals. A strong, sustainable strategy ensures that the process design, ISS design, and operation and maintenance procedures are rigorously managed to achieve high integrity and reliability with minimum opportunity for common-cause failure. Over the life of the equipment, this approach will have a positive effect on the process operation and offers significant benefits to users.

Literature Cited

1. Overton, T., and S. Berger, " Process Safety: How Are You Doing?" *Chem. Eng. Progress*, 104 (5), pp. 40–43 (May 2008); the full metrics report is available on the CCPS website, www.aiche.org/ccps/knowledgebase/measurement.aspx.
2. International Society of Automation, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector," ANSI/ISA 84.00.01-2004, ISA, Research Triangle Park, NC (2004).
3. Center for Chemical Process Safety (CCPS), "Inherently Safer Processes," Second Edition, American Institute of Chemical Engineers, New York, NY (Dec. 2008).
4. Center for Chemical Process Safety (CCPS), "Guidelines for Hazard Evaluation Procedures," Third Edition with Worked Examples, American Institute of Chemical Engineers, New York, NY (2008).
5. Center for Chemical Process Safety (CCPS), "Guidelines for Developing Quantitative Safety Risk Criteria," American Institute of Chemical Engineers, New York, NY (expected 2009).
6. Center for Chemical Process Safety (CCPS), "Guidelines for Safe and Reliable Instrumented Protective Systems," American Institute of Chemical Engineers, New York, NY (2007).
7. International Society of Automation, "Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511)," ISA TR84.00.04, ISA, Research Triangle Park, NC (2005).
8. Gentile, M. and A. Summers, "Cookbook Versus Performance SIS Practices," *Process Safety Progress,* 27 (3), pp. 260-264 (2008).
9. International Society of Automation, "Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques," ISA TR84.00.02, ISA, Research Triangle Park, NC (2002).
10. Center for Chemical Process Safety (CCPS), "Guidelines for Mechanical Integrity Systems," American Institute of Chemical Engineers, New York, NY (2006).
11. Deming, W. E., "Out of Crisis," MIT Press, Cambridge, MA (1986).
12. Gentile, M. and A. Summers, "Random, Systematic, and Common Cause Failure: How Do You Manage Them?" *Process Safety Progress*, 25 (4), pp. 331–338 (2006).

13. Summers, A. E. and W. H. Hearn, "Quality Assurance in Safe Automation," *Process Safety Progress,* 27 (4), pp. 323-327 (2008).

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

ANGELA E. SUMMERS, PhD, is president of SIS-TECH (12621 Featherwood Dr., Suite 120, Houston, TX 77034; Phone: (281) 922-8324; E-mail: asummers@sis-tech.com; Website: www.sis-tech.com) and has 20 years of experience in safety instrumented systems (SIS), process engineering, and environmental engineering. She is a licensed professional engineer in Texas, is a member of AIChE, ISA, IEC and ANSI, and is an active participant in industrial standards committees. She has published over 50 papers, contributed chapters to engineering handbooks, and edited technical reports and books on topics related to process safety and instrumented system design. Summers received the 2005 ISA Albert F. Sperry Award and was inducted into the 2007 Process Automation Hall of Fame for her contributions to safe automation in the process industry. She received her PhD in chemical engineering from the Univ. of Alabama, MS in environmental engineering from Clemson Univ. and BS in chemical engineering from Mississippi State Univ.

Figure 1. Various terms are used to classify instrumented safety systems.

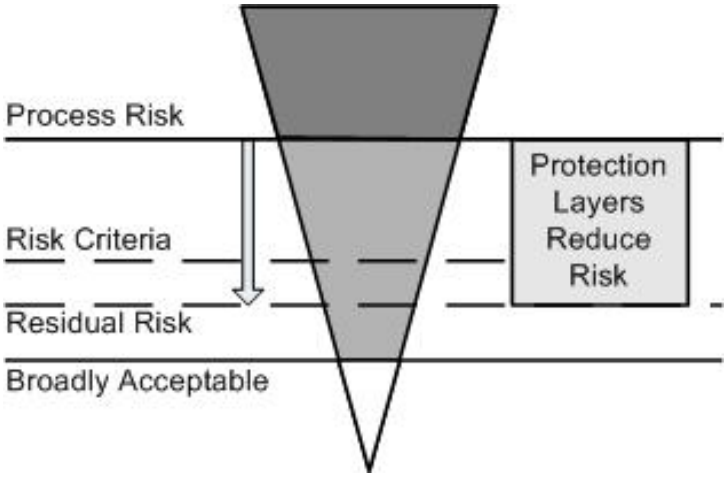

Figure 2. Comparing the process risk to company risk criteria helps determine what is required to reduce the risk as low as reasonably practicable.

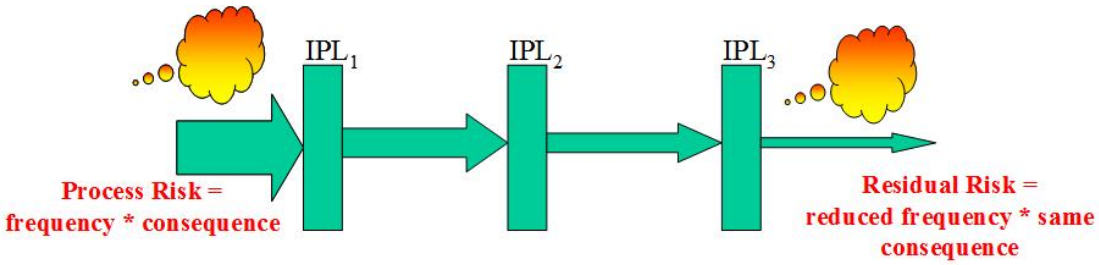

Figure 3. Process risk is reduced by three independent protection layers.

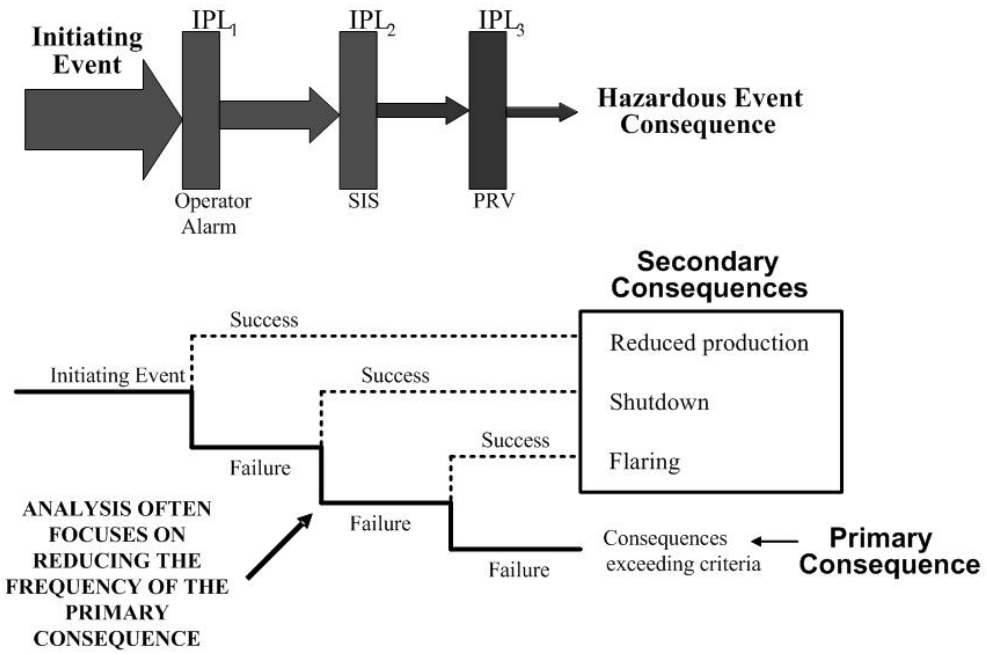

Figure 4. An event tree illustrates primary and secondary consequences of an initiating event.

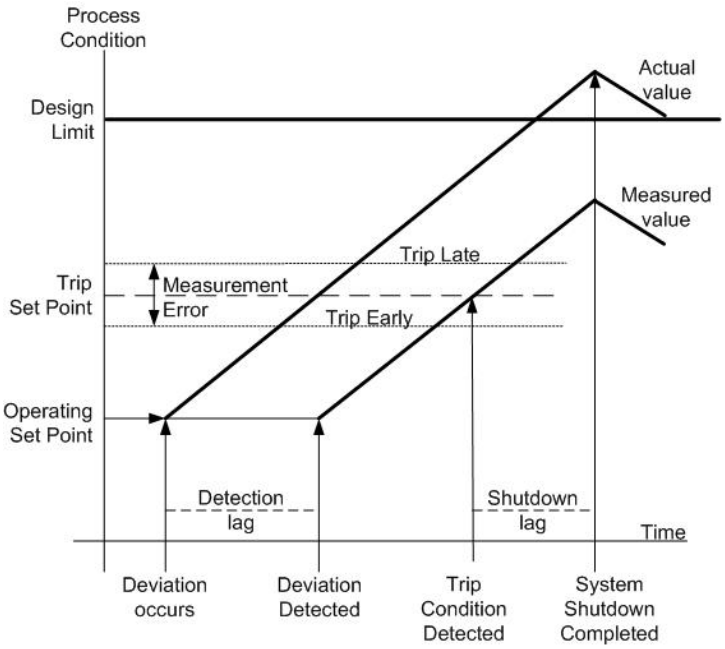

Figure 5. ISS effectiveness is related to detection lag, measurement error, and shutdown lag (8)

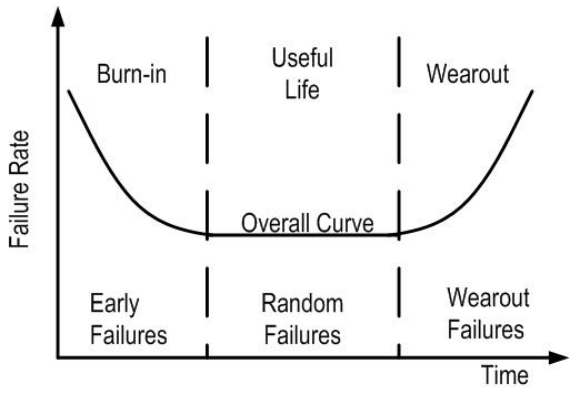

Figure 6. The failure rate over time of most safety equipment can be represented by a bathtub curve.