BRIDGING THE SAFE AUTOMATION GAP

PART 1

Angela E. Summers, Ph.D., P.E, President, SIS-TECH Solutions, LP

"Bridging the Safe Automation Gap Part 1," Mary Kay O'Conner Process Safety Center, Texas A&M University, College Station, Texas, October 2001.

"Bridging the Safe Automation Gap Part 1," Hydrocarbon Processing, April 2002.

The Chemical Process Industry has rapidly adopted automation to improve product quality and production rates, to reduce the potential for operator error, and to decrease manpower requirements. Process industrial automation includes process controls, alarms, safety instrumented systems (SIS), and consequence mitigation systems. While these systems require less manpower once they are implemented, they require more effort and attention during specification and design. Well-implemented automation leads to safe operation. Poorly implemented automation can lead to significant hazardous incidents, involving impact to people, the environment, and assets.

Much has been done to encourage, guide, and regulate safety through identification and control of procedures and systems installed to achieve safe automation. While industry is indeed safer from a personnel injury risk (i.e. falls, burns, cuts, etc.), significant events continue to occur at an alarming rate. Incident causes can be viewed as safe automation gaps, which must be bridged if a company desires to move from where it is now to safer operation.

This topic is divided into two parts. Part 1 discusses safe automation on a broad perspective examining safety culture, organization and hazards analysis issues. Part 2 focuses on instrumented systems and discusses specification, implementation, operation, maintenance, and management of change.

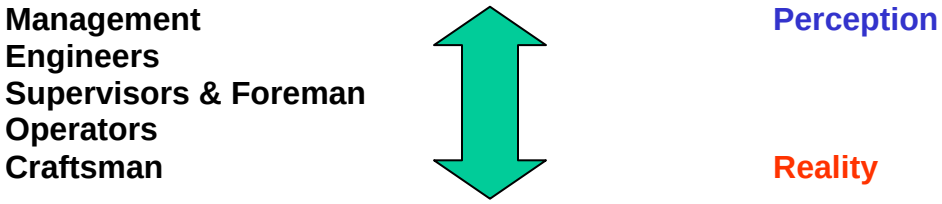
SIS-TECH

12621 Featherwood Drive • Suite 120 • Houston, Texas 77034
Tel: (281) 922-8324 • Fax: (281) 922-4362
www.SIS-Tech.com

PART 1: SAFETY CULTURE, ORGANIZATION, AND ANALYSIS

Problem 1. Perception versus Reality

When discussing safe automation with plant personnel, there is often a significant difference of opinion, depending on the level of the person in the organization. As the discussion progresses from management to the craftsman level, the context changes sharply. The management dialog of "Safe operation is our mission" is changed to "Safe operation as long as it does not get in the way of production."



Many production units are running significantly above boilerplate capacity, resulting in these units being run close to the alarm and trip points. This has led many operators to become "cowboys," taking the responsibility for safety and bypassing the automatic controls in order to stay on-line and ride out the upset.

Developing a safety culture requires that values and policies are converted to practices and behaviors. There must be a continual audit of actual practices and behaviors to ensure that the policy, guidelines, and procedures are being adhered to (1). There must be clear communication that safe operation is rewarded and that "cowboyism" will not be tolerated.

Problem 2. Ownership and Accountability

Due to restructuring, the responsibility for safe automation has been scattered across departments to many different individuals. With no one in a leadership role, it is easy for things to deteriorate into an "Anybody but me" philosophy where it is always someone else's responsibility to ensure that the devices are running. Operations is often made responsible for production, while maintenance is responsible for testing and inspection. If operations does not allow access to the devices for testing, due to the fear of a process upset or shutdown, who is responsible for the functionality of the devices?

A good safe automation culture can only exist when operations is responsible for safe operation. Performance of the operations management must measured by the number of instruments on back-log for

testing and inspection, by the number of near misses, and by the safety attitudes of personnel working under their supervision.

Problem 3. Procedures

Ask yourself the following questions about your procedures:

- Do the right procedures exist?
- Are procedures effective or understandable
- Do people follow procedures?

There seems to be fear that detailed procedures result in greater risk of being found in violation of a procedure if an incident occurs in a unit. This is simply not true. Well-written procedures decrease the frequency of process excursions by providing consistency to plant operation. Poorly written or non-existent procedures essentially guarantee that human error will occur. Achieving safe operation requires that experienced personnel continuously improve procedures and that management allocate the necessary resources to get the job done right.

Problem 4. Documentation

After initial startup, resources and priority are rarely allocated to creating or maintaining as-builts. When documentation is incomplete, it is illogical to expect employees to be diligent about reporting and examining planned changes to the control logic, procedures, or installation. The lack of documentation sends a message to employees that these systems are not important enough to warrant the time and money expenditure for accurate documentation.

Problem 5. Hazard Analysis

During a HAZOP, the team discusses each process deviation and forecasts a worse case scenario. The team then lists the safeguards that prevent the incident from yielding the worse case scenario. Once the safeguards are listed, the team determines whether there is sufficient protection against the incident. In many HAZOPs, no attempt is made to determine whether a listed safeguard truly provides any measurable reduction in the frequency or consequence of the incident. The desire to balance the worse case scenario with the appropriate number of safeguards leads the team to list safeguards that are often inadequate for mitigating the incident. The following are common errors made in evaluating safeguards:

Lack of separation/independence of safeguards

Failure of a process control loop is often an initiating cause for an incident. Yet the devices used in a process control loop are often listed as a safeguard – the control transmitter will be used for alarm and shutdown or the control valve will be used for alarm and shutdown response. If the control transmitter has failed, the incident will begin to propagate, no alarm will be initiated, and no safety response or shutdown will be taken. The safeguards must be examined to ensure that there are a sufficient number of independent safeguards, i.e. the failure of one safeguard does not result in the failure of other safeguards.

Procedures protecting procedures

Operation and maintenance errors are examined as potential initiating causes for incidents. After all, accident investigations show that human error causes 70 to 90% of all industrial accidents (2). Some companies believe that using strict administrative procedures and training are sufficient to prevent

hazardous events. Consequently, the HAZOP team will list these items as safeguards and weigh them heavily when considering whether additional safeguards are necessary. However, even with extensive procedures and training, basic human error cannot be completely eliminated. Procedures must not be used as a substitute for good design. Procedures supplement good design.

Equipment protection

Check valves. Check valves are often listed as the sole means for prevention of reverse flow. However, it is well known that check valves do not always check, especially in dirty services. In most companies, check valves are rarely inspected and never tested (unless a reverse flow demand occurs). Check valves can be viewed as reducing reverse flow, but the HAZOP team should not rely on a single check valve to prevent reverse flow.

Run/Status. Run/status indication for pumps and agitators are listed as a safeguard for loss of flow or loss of agitation, respectively. However, in both cases, run/status only indicates that power is supplied to the device. It does not provide information on whether the pump is pumping or that the agitator is mixing. Safeguards should detect the process deviation of concern. For the pump, the concern is loss of flow. For the agitator, the concern is no agitation.

Process control system

In the HAZOP, instrumentation often enters a perfect world where known instrumentation problems are ignored. Process control loops function normally and respond rapidly in spite of known lag times. Further, the team will not discuss the fact that many of process control loops are actually operated in manual, requiring operator intervention to respond to process changes. If operator intervention is required, the incident propagation rate must be examined to ensure that the operator has sufficient time.

Overall system performance is limited by how changes to the process control system are managed. Optimization of process operation leads to many software changes, which can negatively impact the operation of the critical functions. Moreover, the team will list multiple process control loops, alarms, and interlocks that reside in the same process control system. Therefore, the amount of risk reduction assumed by many HAZOP teams is substantially more than can reasonably be expected from the basic equipment hardware.

Alarms

When examining a specific risk, it is easy to state that the operator will understand the relationship between the alarm and the initiating cause for the incident. However, when the alarm shows up on the HMI, the operator does not see a specific risk. The operator sees an alarm. The HAZOP should ask the following:

- How are alarms managed,
- What is the alarm priority,
- How much time does the operator have to respond, and
- What should the operator do when this alarm is received?

How are alarms managed? Unfortunately, many plants are operated by responding to alarms. Process control loops are run in manual due to poorly tuned loops. The operator adjusts outputs on the control elements based on input signals. The operator is accustomed to receiving alarms and taking a control action. To facilitate this operational strategy, the process control interface allows the operator to

change the alarm setpoints to his/her operating envelope. This is unacceptable for management of safety critical alarms, since it is unknown whether the alarm will be available at the time of process excursion. No alarm should be listed as a safety critical alarm, unless the team is willing to make it a protected alarm.

What is the alarm priority? The HAZOP team will often list several alarms as separate safeguards even though the same operator will be responding to these alarms in some undefined manner based on the perceived alarm priority and relevance. The HAZOP team should remember, "One operator equals one response. Excess alarms equals wrong response."

How much time does the operator have to respond? The probability that an operator will respond correctly to an incident is directly dependent on the amount of time available for response. For total mitigation response, the diagnosis must be turned into an operator response. Consequently, an assessment of the response time must be made. Then, the total diagnosis and response time must be compared to the speed of incident propagation. The evaluation of incident propagation requires process engineering support and an understanding of the process dynamics.

What should the operator do when this alarm is received? When the operator is asked what he/she does in response to alarm, the response is "Troubleshoot and correct the problem" or "Execute a shutdown, if necessary." When asked for a more detailed response, such as "Troubleshoot based on what?" or "What determines if shutdown is necessary?" the operator does not have a response. The answer to the first question is a drilled response with little substance.

Experienced operators and plant engineers must be tapped to document their procedures, so that experience is retained and passed on within the organization. When completed, these procedures should be an important part of new operator training and should be available for review. As new lessons are learned, they should be included in the documentation.

Pressure Relief Valves

Pressure relief valves (PRV) are frequently listed on the HAZOP for mitigation of overpressure events. Many HAZOP teams assume that if a PRV is present on the vessel or pipeline that the overpressure is completely mitigated and that no other safeguards are necessary. However, PRVs do not work perfectly every time they are challenged. Table 1 provides industry data from "Guidelines for Process Equipment Reliability Data" by the Center for Chemical Process Safety (4), showing the general availability information for a single PRV. The mean value for a pilot operated PRV is no better than a SIL 2 safety system.

Table 1. Pressure Relief Device Failure to Open on Demand

Pressure Relief Device Type	Failure to Open on Demand		
	Lower	Mean	Upper
Spring Operated	7.90E-06	2.12E-04	7.98E-04
Pilot Operated	9.32E-06	4.15E-03	1.82E-02

Furthermore, there are many cases where PRVs are incapable of mitigating the overpressure, such as reactive or plugging services (5). The failure rate data shows that PRVs should be considered as a layer of protection, not necessarily the only required layer of protection.

Safety Instrumented Systems

HAZOP teams often treat all safety instrumented system design as equal. For a high pressure event, the team identified a high pressure trip and moves on with the analysis. However, the actual SIS design may not be capable of achieving the performance expectation. The SIS must be examined from the inputs to the outputs to ensure that the SIS functions to mitigate the incident.

The SIS performance expectations should match the actual design. Calculations are not necessarily required. At some point the SIS integrity should be determined more quantitatively, but for HAZOP purposes, many times a simple comparison of the SIS design to current design practices will provide enough information. For example if the installed SIS logic is performed by a 1960 vintage pneumatic switch system, perhaps it is time to consider a SIS upgrade.

A Long Way To Go

The process industry has made tremendous progress toward providing a safer working environment. However, the process industry is pushing production beyond design limits, right-sizing employees down to minimum levels, and adopting management systems that require tremendous resources to implement. It is during these times that mistakes happen, precipitating disaster.

Policies must be translated into effective procedures and design practices. Safe automation systems must be examined closely to see if these systems are good enough to warrant our trust. Design analysis must be performed on the safe automation level, asking what needs to be measured, what system is making the decision on the measurement, what action is to be performed, and what performance level will be required. Then, operations can assure that all employees have a safe working environment, even when running at full blast, by right-sizing the safe automation design and establishing maintenance management systems for testing and inspection.

References

Dowell, A.M., "Getting from Policy to Practices: The Pyramid Model (or, what is this standard really trying to do," South Texas Section AICHE Process Plant Safety Symposium, Houston, TX (1992).

"Guidelines for Preventing Human Error in Process Safety," 1st edition, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York (1994).

"Guidelines for Chemical Process Quantitative Risk Analysis," 2nd edition, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York (2000).

"Guidelines for Process Equipment Reliability Data," Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, New York (1989).

"Using Instrumented Systems for Overpressure Protection," Chemical Engineering Progress, November 2000.