Safety and Automation: Evaluating a Critical Relationship

Scott Hayes, Principal Engineer,
MAVERICK Technologies

When automation is inadequate or used incorrectly, it can cause serious incidents leading to loss of production, equipment damage, environmental releases, and harm to personnel. Here's how to prevent these potential catastrophes before they occur by applying proper safety standards and procedures.

Keeping a process plant operating effectively, efficiently and safely depends on a combination of people and automation. While many companies look for ways to train and develop their people, some consider their automation systems to be relatively static. Where systems function acceptably, they are often left alone and don't receive the attention they should.

Entropy takes its toll and the process operates with a tolerable level of deterioration: maybe a few instruments don't work as they should, maybe the operators can't see a reading or two in the control room, but life and production go on with just enough maintenance to avoid catastrophic failure...at least for now.

In these situations, a simultaneous deterioration of the automation and safety systems can take place, along with an erosion of personnel skills. It's subtle, but it can occur over time as a few instruments drift out of spec and a few key people may leave the company. Important personnel retire, find better jobs or get let go—and the result is a little less knowledge and experience on every shift.

The basic process control system (BPCS) is the first line of defense for safety. It should keep the process on an even keel to prevent upsets and react appropriately to abnormal situations. But if the BPCS isn't as good as it should be due to a lack of attention and maintenance, and if the people running the plant have lost some of their tribal knowledge and skill as well, the safety instrumented system (SIS) takes on greater importance.

When the BPCS begins to weaken, incidents escalate more frequently and the SIS is much more likely to see action. If the SIS is robust, it should protect the facility and its people, but routine reliance on this last line of defense is never a sound strategy.

These situations make it especially critical to keep the BPCS and the SIS functioning as intended. In many respects, this attention can compensate for inexperienced operators as they come up to speed on the facility and its processes. When the BPCS is sound and well maintained, the operators and safety systems have less to do. They still need to be there, but they will be called upon less frequently as the process becomes more stable. And when operators are needed, effective HMI (human machine interface) will make their jobs much easier.

Automate Before It's Too Late

Do situations really deteriorate as described to the extent of causing disasters? Unfortunately, yes. Let's look briefly at three well-documented incidents:

BP Texas City Refinery, March 23, 2005: Raffinate tower fire with 15 fatalities and 180 injuries.

Major causes included failures of multiple level instruments, poor HMIs in the control room and inexperienced operators trying to restart the unit manually without performing the required pre-startup safety review (PSSR). Had the PSSR been performed, the equipment would have failed the review, and the system would not have been restarted. There was not a single level instrument able to warn operators that they had filled the distillation tower, or when product was overflowing into the blowdown stack.

http://www.csb.gov/assets/1/19/CSBFinalReportBP.pdf

Effective Process Control is the First Safety Layer

Ultimately, we are trying to answer a key question: is the facility safe enough? This gets subdivided into a series of more specific questions:

- Have we identified the ways in which hazards could develop within our process?
- Have we drawn the line between tolerable and intolerable risks?
- Is the facility safely controlled by the BPCS and operations?
- Does the BPCS keep the facility safe and stable when running in automatic?
- Are the SIFs (safety instrumented function), as designed, able to protect from the intolerable hazards when used in combination with the other layers of protection?
- Are there standards relevant to our industry and processes that can help inform our decisions and guide our SIS design (See Sidebar 2)?
- Do all the elements of the facility's automation, safety systems and people work together to ensure safe operation?

Williams Geismar Olefins Plant, June 13, 2013: Reboiler rupture and fire, two fatalities, 167 injuries.

A change in the piping and valve configuration on a reboiler pair created a situation where an offline standby unit could be filled with liquid propane, and where heat could be applied while the unit was isolated from its overpressure relief device. Manual troubleshooting during a fouling blockage caused such an incident, resulting in an explosion and fire.

http://www.csb.gov/assets/1/7/Williams_Case_Study_2016-10-19.pdf

Bayer Crop Science, Institute, West Virginia, August 28, 2008: Methomyl unit explosion with two fatalities.

The unit was starting up for the first time since a major turnaround, including a new DCS (distributed control system) with all new operator HMI screens. The individuals performing the final PSSR were not qualified, nor were the operators adequately trained on the new system. Trying to start up the unit without a full safety check and poorly trained operators resulted in a reactor explosion.

http://www.csb.gov/assets/1/19/Bayer_Report_Final.pdf

Independent and Separate?

The underlying concept of an individual SIF and the larger SIS calls for layers of protection able to function independently—a given SIF must be able to do its job without dependence on any other system, such as the BPCS. The layers in a LOPA (layers of protection analysis) assume the BPCS is one layer, the SIS is another layer to back up the BCPS, and the dike holding the spill is a third layer standing by if both the BPCS and the SIS fail. This maintains independence between layers of protection, but the result can be a collection of small, uncoordinated operations scattered throughout the process.

Some companies try to practice this concept by making each SIF totally self-contained and disconnected from any other system. This "air gap" is intended as a means of protection and necessary to ensure independence. The same concept is often applied as a strategy for cyber security protection. If a system can't be reached, it can't be hacked.

This practice becomes problematic for two reasons. First, air-gapped systems are not usually as isolated as their proponents believe. So if there is no other means of protection, the system may be far more vulnerable than realized. Second, it loses the practical benefits of integration. An air-gapped system has no means to connect to larger networks, including historians, remote support or management visibility. These and other useful things are lost in order to provide protection which is ineffective, so it is a poor practice.

Some SIFs should be coordinated with the BPCS. The SIF needs to do its primary function independently, but operations may benefit if the action can have a response that mitigates the production disruption.

When they actually dig into the situation, many people are surprised at the extent of SIS integration with the BPCS when they look closely and realize how far it's gone in their facility. They often convince themselves that their systems are fully separated, when the reality is much different. Others embrace the advantages of integration and push it as far as possible without totally giving up required safety system independence. Each company needs to determine where it wants to be on the spectrum, and this question should be part of any major system analysis project.

Many people tend to compartmentalize process plants as they think about the different elements. The SIS is especially isolated in this regard, often viewed as totally independent both conceptually and mechanically. The reality is usually more nuanced (See Sidebar 1). While the ability of a SIF to do its job independently must be preserved, the safety hardware is probably more integrated with the BPCS than most people realize.

As mentioned earlier, for a facility to run well, the people and the automation systems must work together seamlessly.

The process should behave predictably in a steady state with the operators having a clear situational awareness of what's happening within the facility and its processes. Think for a moment of what is required for reactor operation:

- The mechanisms controlling feedstock flow into a reactor must be well controlled and stable to keep feed proportions and residence time correct for full and efficient reaction.
- Temperature control must be stable.
- The reactor must have sufficient capacity to meet process requirements, with some margin for safety.
- Burners and heaters need to start and stop reliably.
- Valves, manual and automatic, need to move positively and shut off completely when necessary.

The list could go on. These are all basic functions and the ability for each to operate as designed when required makes the difference between an efficient and productive operation and a potential accident site.

The bottom line is that an effective BPCS is the most important element for safety. A facility or unit unable to maintain steady-state control automatically during normal operation is an accident waiting to happen. Upsets can be triggered by an unexpected change in feedstock or some other equipment malfunction, but an effective BPCS should be able to automatically compensate for many of these abnormal situations. The intervention of an operator may be necessary, but knowing when this should happen and the correct steps to take should be very clear. Operators should not be left staring at the screens asking, "What just happened?" and "What should I do?".

When a production unit must depend on its SIS to handle routine upsets and frequently occurring abnormal situations, it's time to examine the BPCS. This will likely be obvious to everyone involved as frequent SIS trips will cause havoc due to corresponding production interruptions.

Safety Standards Relevant to Process Plants

When discussing safety systems, the topic of standards will invariably come up in the conversation. Some people resist the idea, considering standards to be in the same realm as regulations designed to make life more difficult. With the one exception explained below, this is usually the wrong way to look at things because standards are written by users to make implementations easier and more consistent. One of their primary intents is to help users sort through situations and solve problems without having to re-learn costly lessons.

As you begin your own discussions, here are several standards you should follow:

IEC 61508 — This is the broadest over-arching standard related to industrial safety in a wide variety of forms. It discusses both discrete and process manufacturing, so it covers a lot of ground. For process manufacturers, it defines devices which are used in SIFs, so it provides the qualifications to determine if, for example, a given pressure instrument is suitable in a safety application.

IEC 61511 and ISA 84 — These two standards started out separately but have merged. ISA 84 will soon become ISA 61511. This standard is very important for process industries and covers the most critical elements of SISs for process manufacturing facilities. It provides the most comprehensive picture of what a SIS needs to look like and how it should work. For example, when working through your LOPA, a SIF must prevent an incident (e.g., safety shutoff) and not mitigate the effects of an incident (e.g., fire suppression system). This standard is undergoing changes, so it is important to work from the most recent revision. Many of the changes relate to definitions of specific terms, but some take a deeper dive into some personnel issues related to the individuals involved in designing, building and evaluating safety systems. The standard stresses the importance of having a variety of people involved in the process to ensure the same set of eyes is not evaluating every element.

Continued on page 5

Because the BPCS is the first line of defense in a properly designed and maintained facility, most SIFs are specifically designed to be low demand, with frequent use to be avoided. For example, SIL2 (safety integrity level) indicates probability of failure on demand (PFD) of 0.01 to 0.001, meaning failure is expected once out of every 100 to 1000 times it is called upon. There is a significant difference between calling upon a SIF once or twice a year as it was designed to handle, versus calling upon it every day.

Even if the BPCS is working as designed, there are still times when the safety systems will be called upon, and their proper operation is critical in these circumstances.

A Comprehensive, Coordinated Approach

Looking at a facility or production unit with the purpose of improving the SIS must take all the operational elements into consideration. Once the process, feedstocks, reactions and other steps are understood, it's time to work on the daily operation in greater depth.

How well is the process running now, and what has been happening over the last year?

- Number of times it started up and shut down intentionally—Is operation continuous for long periods or subject to regular stops?
- Number of times it shut down unintentionally—What things happened that caused it to stop due to an upset, equipment malfunction or SIS trip?
- Maintenance history—Is all the instrumentation working and in calibration? Are routine repairs handled quickly, or do they end up deferred for cost reasons? Is diagnostic information used to guide maintenance planning?
- SIS trip history—How often did a SIF activate to shut down some or all the unit?

How effective is the BPCS?

- Ability to run in automatic—Does the BPCS operate effectively by itself, or do significant parts of the facility run in manual?
- Instrumentation—Are there enough transmitters? Are they measuring the right variables in the right places? Are they sized and ranged appropriately for the specific application?
- Startups and shutdowns—Are these procedures automated or handled manually?
- Alarm management—Are operators flooded with alarms, more than they can respond to? Are there "stale" alarms? Are some regarded as nuisances and disabled or ignored?

Safety Standards Relevantto Process Plants *Continued*

API — There are many standards under the American Petroleum Institute umbrella and they frequently serve as commentary on how to implement some of the specifics of IEC 61511 within the oil and gas industries—particularly for offshore installations, pipelines and product storage. For companies not working with bulk volumes of flammable products, these standards are effectively irrelevant.

OSHA Process Safety Management Standard, 29 CFR 1910.119 — Here's the exception: this is a government regulation and carries the force of law. It defines what safety systems are supposed to do, so there are many "Thou shalt..." kinds of statements. However, it does not discuss how to implement the rules. Those decisions are left to the other standards and the company's judgment.

Obviously these comments are intended simply as pointers toward areas where you should be doing much deeper research. Any safety system design must take the appropriate standards into consideration, so any outside consultants working with you need to bring a high degree of familiarity to the discussion.

How well do the operators understand and do their jobs?

- Situational awareness—Do the operators have a good idea of what's happening, or is the process a black box in some instances? Can they respond to abnormal situations?
- Life in the control room—Do the operators see what they need to see on the HMIs? Are the graphics well laid out to deliver critical information? Do they keep to a few familiar screens when problems occur, or do they have to jump between rarely used views to see what they need?

Once these basic operational questions are answered, it's time to start digging into the SIS itself and its history:

- How old is the HAZOP (hazard and operability study) analysis on which the SIS was built?
- Is the facility still configured as it was then, or has it been updated? Have the HAZOP analysis and SIS been updated to stay current? Is there a good sense of how management of change is supposed to work?
- Was the SIS built in accordance with any specific safety standards?
- Have the experiences of the facility over the years reflected the expectations of the original HAZOP, or have different kinds of incidents happened which were not anticipated?
- Do the individual SIFs get tested as frequently as they should?

These are not trivial questions with simple answers, and launching an analysis of a working facility or unit is a major undertaking. Some companies try to limit this analysis to the safety system alone, working with specialists to delve into LOPA (layers of protection analysis) and HAZOP analysis, and how the individual SIFs work together. This is fine as far as it goes, but the SIS does not exist in isolation. A more complete evaluation looks at the larger automation picture, and how people work within the context of its operation.

One thing missing from the list is cyber security. While related to the issues discussed so far, it needs to be examined on its own. Suffice it to say, the BPCS can come under attack either directly from the outside or via the corporate networks. If control is disrupted, the facility may have to depend on the SIS to protect it. At the same time, with growing integration of SIS functions, these can also be attacked. If anything, cyber threats emphasize the need for the BPCS and SIS to work together in a coordinated effort to protect the facility.

Doing the Detective Work

An effective safety audit and analysis should begin by looking at the operational history for at least a year, looking for the causes that could have created incidents, not just ones that did. This is similar to near-miss reporting for personal safety. The incident occurred when a worker slipped on a spill and broke his arm, but the blame rests with the ten people who stepped over the spill and didn't report it.

One obvious area of concentration is examining all the circumstances surrounding unscheduled shutdowns. But the digging must go deeper to look for causes that could have caused incidents, or prompted near misses. Safety incidents are disruptive to production and therefore expensive, but they also tell a lot about the condition of a facility, its automation systems and people.

How often does the SIS trip and cause a shutdown? Each of those incidents should be examinedin detail to identify the cause. If it's related to poorly configured process equipment, a quirk of the automation system,or an improper procedure or work instruction, it needs to be fixed.

Let's return to our three incidents cited earlier and consider what effective analysis could have shown. Such analysis may be written off as "20/20 hindsight," but many of these causes could and should have been spotted before the problems escalated.

The BP Texas City incident has been studied in every conceivable way and the range of problems leading up to the explosion is mindboggling. While there were multiple violations of procedures and too few qualified operators on the site at the time of the incident, one of the most glaring problems with the unit was a total absence of working level instrumentation in the tower and blowdown drum. Operators in the control room read a liquid height measurement in the column of 8.4 feet when the level had actually reached about 98 feet. Although a failed level instrument was a primary cause of this specific incident, the blame rests with a culture capable of allowing an instrument to fail and not get fixed, then another to fail, and another until finally an incident occurred. Also, a more extensive HAZOP analysis might have realized there was no mechanism to detect or sound an alarm when the tower was beginning to fill.

The Williams incident was spawned by a combination of poor equipment selection, poor HAZOP analysis and lack of instrumentation. The reboiler that exploded was in standby mode. It was supposed to be isolated from the propylene fractionator by a closed gate valve and pressurized with nitrogen. There was no pressure instrument or other sensor able to determine pressure, or the presence of liquid propane. Over time and unknown to the operators, the unit had started refilling with liquid propane. Moreover, access to the relief valve protecting the unit was blocked. When the heated quench water was turned on and started warming the unit, it quickly over-pressurized and exploded, releasing the propane. A thorough HAZOP analysis would have cited the pressure relief shut-off and probably would have called for some type of pressure instrument. The valves isolating the unit when in standby mode should have been replaced with a more positive closing design and equipped with position detection of status.

The Bayer Crop Science incident is different than most because it happened in the midst of a significant automation upgrade. The plant had just finished a seasonal outage during which it had replaced the methomyl unit's DCS. Given that the plant had made a similar change on another unit with great success in the previous year, this should have been a positive DCS migration experience. Unfortunately, the plant was in a hurry to resume methomyl production, which caused management to accelerate the schedule. Final safety inspections were left to unqualified individuals and the operator training that was so critical to the smooth startup in the previous year was skipped almost entirely. Operators were left to self-study for all practical purposes. As a result, startup of the unit, which was tricky under the best circumstances, fell apart and disaster followed.

Asking for Expert Help to Understand a Very Complex Picture

Sometimes seeing a new side of the situation requires a fresh set of eyes coming from the outside in the form of expert assistance. No single element can ensure success, but it only takes one to cause failure. The lessons here tell us that safe and effective operation of facilities and processes has many facets. Facilities should be evaluating their operations constantly looking for ways to improve production or solve problems. Getting outside help is important since different individuals bring new insights and a broad experience base to bear on potential problems.

Companies often start this approach by looking first at the SIS which results in a realization that they need expert outside help. As mentioned earlier, getting expert help for SIS analysis and improvements is important since it requires specialized knowledge. However, given the linkage between the SIS and BPCS, studying either in isolation is short sighted. Both systems should be examined together, even if they are not fully interconnected.

MAVERICK can bring deep domain experience on all fronts, tying together all the factors involved in your operation. By applying a combination of process knowledge, automation depth and SIS expertise—operations can be improved and incidents avoided. But it's not just about the mechanics, it's also about the people. Our consultants can handle the training so all the individuals in your facility understand their part in the larger safety picture.

Safety doesn't happen by chance and all the elements making it happen correctly must work together. Maintaining the critical relationship between automation and people requires intentionality from management and can often benefit from the help of outside experts.

MAVERICK is uniquely positioned to help producers in many process industry verticals become more effective in day-to-day operations, and much safer. Some of the leading verticals where MAVERICK possesses deep domain expertise include chemical, oil and gas, food and beverage, life sciences, power, pulp and paper, high-tech manufacturing and mining.

MAVERICK TECHNOLOGIES
A Rockwell Automation Company

MAVERICK Technologies, LLC
265 Admiral Trost Drive | Columbia, IL 62236 USA
+1.888.917.9100 | Fax +1.618.281.9191
info@mavtechglobal.com | mavtechglobal.com