How to Evaluate and Mitigate Process Control Safety Risks

Scott Hayes,
MAVERICK Technologies

Introduction

Automation and safety systems protect us from accidents that 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 procedures and standards.

For a process facility to operate effectively, efficiently, and safely depends on two factors: people and automation seamlessly working together. Many companies find ways to train and develop their people. On the other hand, automation systems are often considered relatively static. They function acceptably, so little attention is paid to them. Entropy takes its toll, and the process operates with a tolerable level of deterioration: maybe a few instruments don't work properly, maybe the operators can't see a reading or two in the control room, but production goes 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 key personnel retire, find better jobs or get let go—resulting in a little less knowledge and experience on every shift. In light of these issues, how can we mitigate risk and ensure our process control system is operating effectively?

Think for a moment of what is required for reactor operation

- People who support the existing DCS are close to retirement.
- 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.
For all these basic functions to operate as designed when required makes the difference between an efficient and productive operation and a potential accident site.

The First Safety Layer

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 resource tribal knowledge and skill are lacking, 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 will be called on less frequently as the process becomes more stable. And effective human-machine interfaces (HMIs) will make an operator's job much easier.

Ultimately, to ensure effective process control, we need to ask, "Is the facility safe enough?", which prompts more specific questions:

- Have we identified enough of the ways hazards could develop with 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 safety instrumented functions (SIFs), 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 Understanding Safety Standards on Pg 6)?
- Do all the elements of the facility's automation, safety systems and people work together to ensure safe operation?

Many people tend to compartmentalize process facilities 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 complex (see Independent and Separate on Pg 7). 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 and the pressures to integrate the BPCS and SIS continue to increase.

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.

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.

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. In the process industries low demand is defined as no more than once per year. There is a significant difference between calling upon a SIF once a year as it was designed to handle versus 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 happened to cause 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?

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 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. 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 cybersecurity. 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, as SIS functions are also now being integrated, they 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. On the positive side, there is updated information in the IEC standards to help you protect these critical systems.

Dig into Historic Roots

To perform an effective safety audit and analysis, look at the operational history for at least a year, and dig into 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 10 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 at what could have caused incidents or prompted near misses. Safety incidents are disruptive to production and therefore expensive, but they also tell a lot about a facility's condition, its automation systems and people.

How often does the SIS trip and cause a shutdown? Each of those incidents should be examined in 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.

Understanding a Complex Picture

The safe and effective operation of facilities and processes has many facets. No single element can ensure success, but it only takes one to cause failure. Facilities should be evaluating their operations constantly looking for ways to improve production or solve problems.

To start, companies often look first at the SIS and realize they need help from a third-party expert – someone who can bring a fresh set of eyes to the situation. Often, different individuals bring new insights and a broad experience base to bear on potential problems. Getting third-party 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.

An experienced consultant can bring deep domain experience on all fronts, tying together all the factors involved in your operation. By combining and applying process knowledge, automation depth and SIS expertise, facility operation can be improved and incidents avoided. But it's not just about the mechanics, it's also about people.

Safety doesn't happen by chance. All the elements must work together to make it happen correctly. Just remember, with intentionality from management, the right help from external experts, and automation and people working together seamlessly, you can mitigate safety risks and ensure an effective process control system.

Understanding Safety Standards

STANDARDS RELEVANT TO PROCESS PLANT

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 and 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., re 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.

IEC 62443 and ISA-99 — These cybersecurity standards are for industrial control systems. A lot of recent work has gone into the technical reports that define cybersecurity lifecycle and safety zones.

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. For any safety system design, consideration must be given to the appropriate standards, so any outside consultants working with you need to bring a high degree of familiarity to the discussion.

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 if the BPCS fails, and the dike holding the spill is another layer standing by if both the BPCS and the SIS fail. This maintains independence, but the result can be a collection of small, uncoordinated operations scattered throughout the process.

Some companies try to make 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 cybersecurity 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 and for management visibility. Useful things are lost to provide protection, which is ineffective and thus 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.

ABOUT THE AUTHOR

Scott Hayes (scott.hayes@mavtechglobal.com) is a Program Manager at MAVERICK Technologies. He has more than 20 years of experience in process control. He is a licensed Control System Engineer and a TÜV certified function safety engineer.

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