5 ways to improve safety and profitability, without disrupting operations

Process industries are inherently hazardous, and maintaining safety in processes and operations has become increasingly complex and costly. But too often, companies have difficulty demonstrating a clear return on investment in their safety activities. With both safety and financial concerns being a high priority, those in the process industry sometimes struggle to reconcile them.

In 1994, the world's regulatory environment was still reacting to the Bhopal, India gas leak that had occurred a decade before.

At that time, the American Institute of Chemical Engineers (AIChE) undertook a study to figure out how much emerging safety regulations actually cost. It concluded that, across all industry segments and plant sizes, the average U.S. industrial facility would start at 40 percent compliance and spend no less than $5.8 million over a decade to effectively achieve full safety compliance.

The return on investment (ROI)? The kind that gives financial executives gray hair: potential cost avoidance.

That was 27 years ago, and process safety management has since come a long way. First, ongoing investments are thought to be far higher than the AIChE had calculated – up to one-third to one-half, or even more, of the capital and operating costs of the new plant handling the hazardous operations,” declares an abstract for another old study: The Real Cost of Process Safety – A Clear Case for Inherent Safety, published in November 2003 by Process Safety and Environmental Protection, the journal of the European Federation of Chemical Engineering.

But also important: the ROI is now known to be far more tangible than the “what-if” costs of an avoided incident.

Even 10 years ago, safety processes and technologies were being viewed for their impact on Overall Equipment Effectiveness (OEE) and plant efficiency. According to the results of a study by the Center for Chemical Process Safety, as cited in a 2001 workshop report, facilities that embed safety into their daily operations typically achieve a 5 percent productivity increase, 3 percent reduction in production expenses, 5 percent reduction in maintenance costs, 1 percent savings in capital expenses and 20 percent reduction in insurance costs.

The timeline sends a clear message: While the cost of safety in process industries has far exceeded estimates from the dawn of the modern safety era, the benefits of safety are more tangible and substantial as well.
The simple assessment is that most companies can increase manufacturing flexibility, profitability and overall competiveness while improving safety, with little disruption and minimal capital expenditure.

These savings arise across the process safety area, but we will focus here on those related to process automation. Many companies have paid for these potential benefits with process automation capabilities that now exist in-house but are being underutilized or ignored.

The trick is knowing where these potential gains are hidden. Here, according to ABB Process Automation safety experts, are five areas where most companies can easily unlock improvements in safety and, quite possibly, profitability.

1. Utilization of existing automation

When a process is running, a well-designed automation system can deliver more reliability, repeatability and speed than any human being, according to David Huffman, a manager at ABB with background in chemical and process engineering. The control system can identify when processes change states, and can be programmed to act before those changes become critical.

“Chemical engineers like myself like to think you can put yourself at a steady-state process,” Huffman says. “But trust me, you’re never at a steady state. It’s a misnomer. Processes are always changing.”

Typically, an alarm management system is used to identify such changes, turning over the details of what to do about it to human operators.

Obviously, there are times when that must happen,” Huffman says. “But there are many other times when nothing is really going wrong. There are some changes that the automation system is capable of identifying and managing if it’s programmed properly.”

As an example, Huffman describes a distillation process that requires the product to move through one of three drying beds. The beds are rotated through primary, secondary and regeneration modes.

“So you’re running full and at the time you have to switch one bed offline, you find out there’s something wrong with another bed and you can’t put it back into service on time.”

The usual response is slowing down the distillation process while getting the troubled bed fixed. It’s a busy time for operators. “When you start scaling down a distillation tower, it loses efficiency, you lose product quality, and control loops don’t perform well at the reduced-rate condition. The operator is cutting flow rates, changing tower pressure, dealing with overhead systems, boiler systems etc. The more complex the tower is, the worse it gets. And the whole time, alarms are going off continuously.”

But, Huffman continues, “If you know this happens from time to time, you can record what the operator has to do and write a procedure around it for the automation to move the distillation process into a safer mode.”

There is an advantage in speed, which reduces product waste. And automating the routine around best practices means achieving the same results, even if the event occurs when your best operators are off-shift.

Most companies have dozens of examples like this, Huffman says – events that happen often enough to automate, but not often enough to have confidence that every operator is always going to be adequately trained and tested.

Admittedly, improving automation at this level isn’t easy or free. “You have to go through the pain and expense of understanding your routine states, defining them and putting in the programming code.”

Many companies overlook this step when implementing a new automation system. “There’s fatigue involved,” Huffman says. “The company gets tired of spending money, and the people get tired of the constant change; they want to get back to a steady state too.”

The good news, he says, is that it means you still have opportunity to make big improvements long after you’ve grown comfortable with an automation system.

Quantifiable benefits include reduced staffing, less wasted product, increased quality and faster adjustment of controls at a level of higher precision and repeatability. With respect to safety, it removes distractions from operators, making routine events out of occurrences that would previously have set off an alarm flood.

Often discussed in the industry as state-based environments, the discipline of improving automation across a wider array of recurring events is the subject of a new ISA committee. While ISA-106, focused on sequential process control, is a few years away from releasing its first set of standards, Huffman says the goal is to “educate companies that processes run in states and, in order to keep them safe and profitable, it’s OK to take things out of operators’ hands and let the automation system do a lot more work.

“There are big companies that are embracing this because they are convinced it’s not only safer, but you can make money with it,” Huffman says.

2. Rationalizing alarms

Here’s a simple way to know if your alarm management system is doing its job well: Count the total number of alarms that the system activates during the course of a month and divide it by the number of operator hours worked during the same month.

If the total comes in at much more than 6 alarms per operator per hour, there is an advantage in speed, which reduces product waste. And automating the routine around best practices means achieving the same results, even if the event occurs when your best operators are off-shift.

Most companies have dozens of examples like this, Huffman says – events that happen often enough to automate, but not often enough to have confidence that every operator is always going to be adequately trained and tested.

Admittedly, improving automation at this level isn’t easy or free. “You have to go through the pain and expense of understanding your routine states, defining them and putting in the programming code.”

Many companies overlook this step when implementing a new automation system. “There’s fatigue involved,” Huffman says. “The company gets tired of spending money, and the people get tired of the constant change; they want to get back to a steady state too.”

The good news, he says, is that it means you still have opportunity to make big improvements long after you’ve grown comfortable with an automation system.

Quantifiable benefits include reduced staffing, less wasted product, increased quality and faster adjustment of controls at a level of higher precision and repeatability. With respect to safety, it removes distractions from operators, making routine events out of occurrences that would previously have set off an alarm flood.

Often discussed in the industry as state-based environments, the discipline of improving automation across a wider array of recurring events is the subject of a new ISA committee. While ISA-106, focused on sequential process control, is a few years away from releasing its first set of standards, Huffman says the goal is to “educate companies that processes run in states and, in order to keep them safe and profitable, it’s OK to take things out of operators’ hands and let the automation system do a lot more work.

“There are big companies that are embracing this because they are convinced it’s not only safer, but you can make money with it,” Huffman says.

2. Rationalizing alarms

Here’s a simple way to know if your alarm management system is doing its job well: Count the total number of alarms that the system activates during the course of a month and divide it by the number of operator hours worked during the same month.

If the total comes in at much more than 6 alarms per operator per hour, then your system is running at an unnecessarily high level of risk and inefficiency.

That rule of thumb (6 alarms per operator hour) is just a guideline, warns Ken Praprost, alarm management optimization engineer at ABB. It’s far simplified from ISA-18.2, a new standard released in 2009 that addresses alarm management in process industries.

“During an “alarm flood” period, you may get alarms at five or ten times that rate,” Praprost says. But six per hour per operator is one metric let you know if there’s a reason to go back to work on the alarm management system.

In Praprost’s experience, most companies deliver too many alarms, falling into three categories:

- Nuisance alarms: Those that go on and off so routinely that they eventually get ignored, like an alarm that sounds whenever process temperature rises above a threshold, even if the process generally takes care of itself before operators intervene. Praprost has frequently seen operations where there are so many standing alarms that they can only be viewed on multiple screens. “And many of these may be for equipment that’s not even in use. The flow is zero, which sets off an alarm that the operators simply have to look at.”

- Standing alarms: Those that remain in an active alarm state for a significant period of time.

- Non-alarms: Many alarms are really just events or data that someone in the organization had wanted recorded.

In all three instances, operators struggle to identify important

alarms, especially when alarms are not prioritized – a common condition everywhere.

Fixing it can improve safety and potentially improve plant performance, Praprost says. “If we can get the alarm system so it’s not providing useless information that operators don’t need to know, the operators can do a better job running the plant. They can avoid lost-production events simply because they didn’t pick out the right alarm from a long list of alarms that all look the same.”

The main steps to improving an alarm management system are:

- Evaluate documentation and interview operators, engineers and supervisors: Investigate whether the systems operate as required and if personnel know why each alarm is triggered, precisely how to respond to it, and how easy is it to interact with the system interface.

- Performance assessment: A review of alarm data over an appropriate period of time (usually a few weeks to a month) to determine the rates, frequency of individual alarms, and response times to alarms.

- Benchmarking: Comparison of results with industry guidelines.

- Recommendations for improvement.

- Plan and implement an improvement program.

- Establish an appropriate monitoring and review process.
“One thing we’ve learned is that people like to put an alarm on anything. If we investigate further, we can reclassify many of the alarms as events so they don’t occupy space on the list. Then we reprioritize to identify the true high-priority items,” Praprost says.

There are also strategies for dealing with nuisance alarms, vastly reducing how often they trip while assuring that they do appear when intervention is required.

Evaluating such issues is a process independent of the type of system being used. While it requires some cost, it can be conducted with minimal interruption and meaningful improvements in the way processes are managed. It not only brings significant improvements in plant safety; alarm rationalization can make a significant impact to the bottom line by reducing unnecessary plant trips.

3. Consider human factors

If alarm management tends to place too much reliance on people, human factors explore the issues created by the fact that people are the most fallible part of a safety system.

Human factors typically include such areas as the design of interfaces and displays, lighting, noise management, staffing, safety-critical communications, ergonomics and, as already discussed, alarm management.

“In human factors, a key issue is that people are overloaded with information. When something goes wrong, the system is not well-enough designed to allow time for reaction. It doesn’t direct people where to look for the information they need,” says Chris Greaves, business manager at ABB Consulting. “While that is obviously relevant to alarm management, it also applies to the other human factor areas.”

As an example, Greaves says it’s common practice for work permits in a facility to be managed in the control room. “The argument is that if people want to get work done, they need to check in with the process superintendent.” The commotion related to issuing work permits can be a safety distraction to operators, Greaves argues, but he has seen instances where lighting was used to minimize the disruption, by darkening that part of the room where permits are issued when lighting is not required.

Other human-factor techniques can include providing different audible tones for different types of alarms, or automated redirection of lighting to focus on the correct displays during alarm bursts. Ventilation – maintaining a temperature that keeps people comfortable but alert – is a common challenge in many control rooms, Greaves says.

“As with anything, you can quickly get into a project that suddenly would have people writing large checks for fancy displays and ergonomic chairs,” he notes. “There are certainly times when that is justified and prudent, but if you’re talking about ways to improve operations and reduce safety risk, you simply cannot overlook these human factors. The control room is your last line of defense, and for many companies, it would be very easy and affordable to find multiple opportunities to change the environment in a way that helps the people who work there to do a better job.”

4. Don’t purchase unnecessary redundancy

Redundancy is not equivalent to safety, and safety does not require redundancy. “People get the two confused,” laments ABB’s Huffman. “People get locked into thinking that if they’re going to have a safety system, it has to have full logic solver redundancy, often to 3x or 4x levels, in order to be safe.” That means they have to invest in a second set of equipment that is going to require regular testing and maintenance, and if all goes well they’re never going to use it.

“It’s not a true statement” Huffman says. “You can have single-element safety systems that can be certified up to SIL 3 levels.”

When a single-processor system detects a process problem that justifies tripping the plant, then it’s designed to lead the plant through a safe shutdown. In the case of an internal fault, it will also shut down the process safely, per SIL 3 safety requirements.

“In that case,” Huffman says, “I’ve lost the process, not because of a process problem, but because of a fault in the system. If you want to keep the process running, then redundancy is a matter of maintaining uptime, but not process safety.”

Sometimes, keeping the process running is important for personnel safety, Huffman says, because certain startups and shutdowns can put people at risk. But that’s a different decision than the process safety itself.

Huffman’s point is that companies pay for logic solver redundancy in cases where the investment might have more impact elsewhere, whether in other areas of safety or in operating efficiency.

His recommendation is that companies pay to put at least one person, who is respected at the executive level, through some level of basic safety education, such as the ISA’s EC50 course on Safety Instrumented Systems (SIS). Then use that education as part of the decision-making process around investments in safety and process automation. Having this knowledge can help with making system selections based on key performance requirements rather than the redundancy architecture of the logic solvers.

5. Map the competence of people

One well-worn, under-attributed statistic in process safety automation is that machinery is typically the cause in 10 percent of failures; the other 90 percent of the time, human error is to blame.

Lack of a source for this statistic notwithstanding, few people seem to argue the point that human error is the least predictable and more common source of breakdowns in safety.

With that in mind, John-Erlend Stromme, Service Manager, ABB Oil, Gas and Petrochemical Business Unit, suggests that any company would benefit from a routine and systematic review of the way safety competence is built and maintained among its people.

“Competence is simply being aware that you are doing things right. A small mistake can start the ball rolling, and anytime we, as an industry, find ourselves looking at a major accident, it seems that’s ultimately how it started,” Stromme says.

Competence, however, is not simple. It’s a combination of having the right technical knowledge, knowledge of work processes and experience for whatever situation an individual may face.

“It’s not just knowing what you’re doing, but knowing how to follow procedures so you can avoid making an error you didn’t know about,” Stromme says.

Facets in mapping competence include documenting the type of education each worker has received, and what kind of experience, detailed to specific tasks and technologies.

Requirements and certifications in specific work environments are considered as well.

More difficult but equally important, he notes, is to map an individual’s attitude to reducing risk and conducting high-risk work. “People around him will know whether he’s someone who tends to make a situation more or less safe. Whether you can get that information or not goes to the culture of the company: Do they dare to tell you,” he says, “or do they dare not to tell you?”

“When you take seriously this process of understanding the competence of each worker, as an individual, that says a lot about the importance of safety in an organization,” Stromme says. “You’ll get the level of information that you have earned, based on past experiences that your people have. If you demonstrate an open mind and attitude – that people won’t be punished, and that information will be used to help everyone become better and safer at their job – you are already doing a very good job of reducing risk in your operation.”

Summary

There is no avoiding the need to make ongoing investments in all aspects of safety: equipment, processes, systems and people. But not all investments are the same. While some require long-term planning and capital budgets, others are small and fast. And still others have already been made, and are waiting to be utilized and optimized.

By focusing on these five areas:

− Increasing utilization of automation
− Decreasing utilization of alarms
− Considering human factors
− Understanding the role of redundancy
− Mapping the competence of people

most process companies can unlock hidden safety improvements, and in many cases increasing operating effectiveness, without disrupting ongoing operations or making large investments.