CONTROL

Take Your Medicine

A Prescription for Practical
Process Safety

Take Your Medicine

A how-to prescription for practical process safety, using hazard identification, risk assessment, corporate risk policy, consistent implementation, thorough training and continuous revaluation—with help from harmonizing standards and new technical tools.

BY JIM MONTAGUE

OPEN WIDE. It isn't a spoonful of sugar. But doing process safety right doesn't have to be cod liver oil either.

For instance, planning to put safety instrumented systems (SISs) on hundreds of process heaters at 13 U.S. refineries and three in Europe might seem extremely difficult, if not close to impossible. However, engineers at ConocoPhillips (www.conocophillips.com) in Houston just did what they usually do and took on the problem step by step.

"We use the same approach as OSHA's PSM and ISA84 standards. Starting three years ago, we established an in-house standard and set a timetable for compliance by 2012," says John Campbell, principal instrumentation and controls engineer at ConocoPhillips. "So far, this project is going well. Most heaters are already in compliance, while others will need renovation and capital expenditures. It's not going as fast as we hoped, but we're getting there."

The U.S. Occupational Safety and Health Administration's (www.OSHA.gov) Process Safety Management (PSM) standard 29 CFR 1910.119 is available online. The International Society of Automation's (www.isa.org) ANSI/ISA84.01-2004 standard parallels the International Electrotechnical Commission's (www.IEC.ch) 61511 standard, except for a now-infamous grandfather clause that allows U.S. facilities with otherwise safe records to keep operating noncompliant processes.

"Our in-house standard covers requirements for how our refineries should shut down their process heaters, and so we tried to follow PSM at the 30,000-ft level, S84 for SISs at the 3,000-ft level, and the American Petroleum Institute's (www.API.org) 556 standard for process heaters at treetop level," explains Campbell. "We think involving all these levels gives our standard the best coverage."

One potential snag in ConocoPhillips' project is that each plant is responsible for its own process heater renovations, and each will be judged on a pass/fail basis in 2012. Campbell acknowledges that there's been some foot dragging, too. "This is why it's so important to have the man at the top say, 'This is your deadline, and you're going to be judged on whether you've met it or not.'"

Campbell adds that all the major oil, gas and other process industry players have faced these safety issues for years, and not just with instrumentation, but with all kinds of piping, valves, rotating equipment, vessels and other technologies. "I knew a guy in an ISA standards working group that had been dealing with process safety for awhile, and thought they had a good PSM culture. But then he walked into a plant for an audit, and the first thing the tech services manager asked was, 'Why are we doing all this safety stuff?'"

Just as equipment and systems need regular process safety check-ups, Campbell says process personnel need regular evaluations so anti-process safety prejudices and unsafe practices don't become widespread. "It takes plenty of manpower and time, but good PSM always relies on regular inspection and testing. Even if you repeatedly find nothing wrong and

Proper Process Safety Procedure and Planning

A useful process safety project includes several essential parts. Though they sometimes go by different names, here are the main steps included in most thorough safety evaluation, planning and implementation efforts.

1) Secure genuine commitment from top management to process safety effort.

2) Recruit and assign a cross-functional team with members from process engineering, process operators, mechanical and electrical staffers, instrument and controls people, the IT department and management as needed.

3) Go though hazardous operability (hazop) process and look at deviations from normal operations for each process unit and every covered process in the facility.

4) Whenever a credible cause and consequence of sufficient magnitude is found, conduct a risk assessment (RA) of it to evaluate its severity and frequency. RAs can use traditional qualitative methods, such as risk graphs, and/or semi-quantitative techniques, such as layer or protection analyses (LOPAs).

5) Use RAs and/or LOPAs in conjunction with company's corporate risk guidelines to establish acceptable risk levels for devices and processes, and assign safety integrity levels (SILs) for each applicable device, loop, process or application.

6) Check if existing safety functions are enough to handle RA issues and SILs identified. If they're sufficient, then document them. If they're inadequate, then identify gaps in existing safety system and seek to fill them.

7) Incorporate safety requirements into functional safety plan and specifications.

8) Seek to move beyond safety for individual devices to developing performance-, task- and life-cycle-based safety capabilities.

9) Install, maintain and continuously reevaluate and update process safety solutions according to a specific schedule.

think you can slack off, you still need to do it.

"My advice to other process safety folks is, if you're feeling overwhelmed, then find a smaller piece of your process that you can handle, do it and then move on to the next one."

Common Sense and Consistency

A practical approach to process safety begins with thinking about what you're going to do after an accident happens and what will be expected of you, according to Angela Summers, Ph.D, PE, president of Sis-Tech Solutions (www.sis-tech.com), a process safety consulting firm in Houston. "If you don't have an SIS in place, you'll be asked why after an incident occurs," she says.

Summers explains that a check of past process incidents shows they don't occur in applications with a working SIS. "Incidents happen where an SIS wasn't put in, where it was broken or where it was defeated by its users," she says. "This generation believes its technology is better than it was 50 years ago, but back then, process technologies were simpler, more separated and less flexible, and so there were fewer potential failures. As these technologies continue to grow more integrated, we need to manage that integration more actively and aggressively."

Consequently, the first step in creating or renovating a process safety system is to look at the process application, identify any loss-of-containment events that could cause a fatality or serious injury, determine those events' initiating causes and frequency, look at available protection layers, examine how to reduce the frequency of any events, such as by implementing a well-designed and managed SIS [see "Proper Process Safety Procedure and Planning" sidebar.]

"Any place where an event like this could happen will need an SIS that's independent of the control system and part of a rigorous mechanical integrity program," says Summers. "Luckily, everything you need to implement an SIS is well within the expertise of any well-qualified process engineer."

While some users believe it's enough to have an SIS that complies with prevailing standards, Summers says that's not enough. "Standards can allow you to hang yourself if you don't recognize where your system is still vulnerable. So companies must also build their own prescriptive way of doing safety, make their SIS as idiot-proof as possible by ensuring that operators can't defeat it, and make certain that users test, maintain, report, respond and otherwise interact with it in the same way every time and in every setting."

Buddy Creef, vice president of sales at RTP Corp. (www.rtpcorp.com), adds it's vital for users to first do a hazardous operability (hazop) study and a risk assessment (RA), so they can be plotted against what risk levels user's organization is willing or not willing to accept. Next, a layer of protection analysis (LOPA) can help users' decide what protection they need, or indicate that they might need a dedicated safety system. "Users have a lot more safety options these days, but they still need to resolve the traditional tradeoff between availability and safety," says Creef.

Avoiding Overspills

One of the main causes of process safety accidents are overspill incidents due to loss of level control. Summers reports in her whitepaper, "Overfill Protective Systems—Complex Problem, Simple Solution," that these incidents caused the Esso Longford explosion that killed two people and injured eight in Australia in September 1998, the BP Texas City explosion that killed 15 people and injured 170 in March 2005, and the Buncefield explosion that injured 45 people in the U.K. in December 2005. Each tragedy was attributed to a combined lack of hazard recognition, underestimated likelihood of overfill, excessive reliance on operators, no defined safe-fill limits and inadequate mechanical integrity. Summers adds that catastrophic overfills are easily prevented by:

- Acknowledging that overfill of any vessel is credible regardless of time required to overfill;
- Identifying each high-level hazard and addressing risk in the unit where it's caused, rather than allowing it to propagate downstream;
- Determining a safe-fill limit based on mechanical limits of the process or vessel, measurement error, maximum fill rate and time required to complete action that stops filling;
- When operator response can be effective, providing an independent, high-level alarm at a setpoint that allows enough time for the operator to bring the level back into the normal operating range prior to reaching a trip setpoint;
- When the overfill leads to the release of highly hazardous chemicals or to significant equipment damage, design

Primary Process Safety Organizations and Websites

International Society of Automation
www.ISA.org

U.S. Occupational Safety and Health Administration
www.OSHA.gov

Center for Chemical Process Safety
www.AIChE.org/ccps

U.S. Chemical Safety and Hazard Investigation Board
www.chemsafety.gov

Mary Kay O'Conner Center Process Safety Center
process-safety.tamu.edu
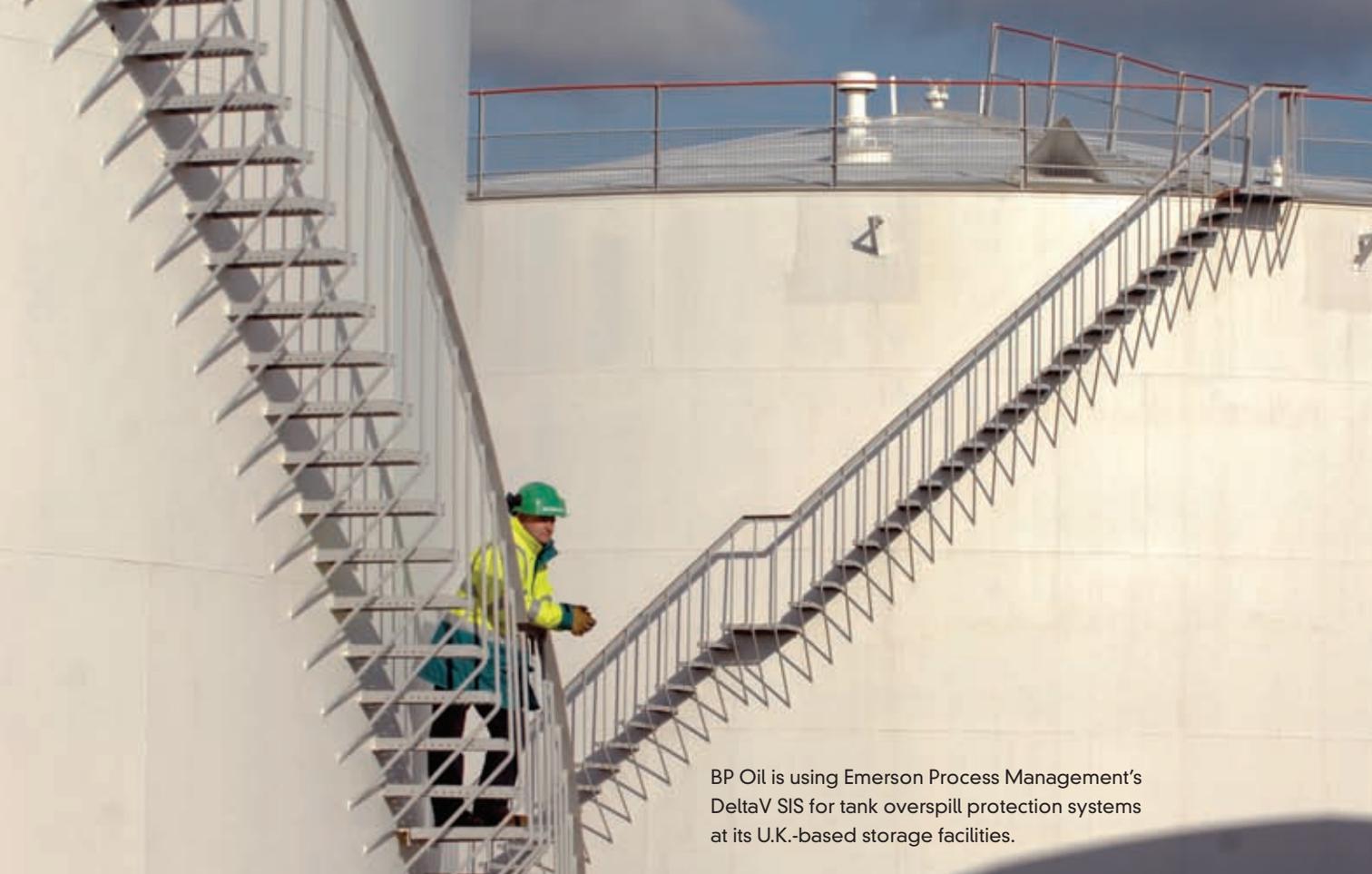
American Petroleum Institute
www.API.org

Voluntary Protection Programs Participants' Association
www.VPPPA.org

TÜV Rhineland
www.us.TUV.com

BP Oil is using Emerson Process Management's DeltaV SIS for tank overspill protection systems at its U.K.-based storage facilities.

and implement an overfill protection system that provides an automated trip at a setpoint that allows sufficient time for the action to be completed safely. Risk analysis, such as LOPA, should be used to determine the SIL required to ensure that overfill risk is adequately addressed. While there are exceptions, most overfill protection systems are designed and managed to achieve SIL 1 or SIL 2.

• Determine the technology most appropriate for detecting level during abnormal operation. The most appropriate technology may be different than the one applied for level control and custody transfer.

• Provide means to fully proof test any manual or automated overfill protective systems to demonstrate the ability to detect level at the high setpoint and to take action on the process in a timely manner.

To address some similar issues, BP Oil recently contracted with Emerson Process Management (www.emersonprocess. com) to add its DeltaV SIS to BP's tank overspill protection systems at fuel storage and distribution sites across the U.K. (Figure 1) These updated protection systems will monitor tank levels and automatically shut off feeds if levels reach a high cut-off limit. DeltaV's SIS uses predictive diagnostics to monitor each tank's whole safety loop, and its logic solver communicates via the HART protocol with smart devices to diagnose faults before they cause spurious trips.

Performance, Tasks and Life Cycles

While process safety and risk assessment begin with qualita-

tive judgment, they don't stay there. The quest to improve RAs and safety inevitably lead to evaluating and measuring process performance, operator tasks and interaction with it, and indeed the entire timespan in which that process and its equipment functions.

Kevin Klein, Center of Reliability Excellence (CORE) for instrumentation at Celanese Chemicals (www.celanesechemicals.com) in Houston, says his firm's RAs start with a traditional, qualitative, judgment-based process hazard analysis (PHA), but then move to include a semi-quantitative, data-driven method. "We do a hazop to identify the hazard and conduct a qualitative assessment of it. Then we do the semi-quantitative RA to make sure we have the right protection in place or learn what we need to add," says Klein. "We perform these assessments routinely and continuously to check new equipment, or when we change equipment, or to reexamine existing applications every couple of years. For instance, if we have a storage tank with a flammable liquid that could auto-polymerize, we do a semi-quantitative RA to decide if it needs SIL 1, 2 or 3. A semi-quantitative study is based on numbers, so it the takes the emotion out of our decisions."

Also, because Celanese makes regular acquisitions, Klein adds, it uses its continuous RA method to evaluate its new companies, and bring them up to speed on Celanese's safety policies. "A Yugo or a Cadillac will get you where you want to go, but we don't want either. We just want to get in line with what everybody else in our industry is doing, and that means IEC 61511," says Klein. "The best way to improve

your own process safety is to get involved and join one of the many organizations that can answer your questions and help you get the knowledge you need. You don't have to go it alone. I found that when I joined a process safety committee, its members were struggling with the same problems that I was. So I was able to quiz them about their solutions, and we could compare experiences and come up with a better solution together. Sharing information and benchmarking is a very effective way to judge where you are."

Standards Harmonizing

Historically, process safety systems had to meet the rules for the nation or region where they were going to be used, and manufacturers had to adapt and readapt their equipment to comply. This situation is still true for many technologies in many places. However, some standards organizations are bringing their standards together and harmonizing them to produce some truly global standards. This harmonization is already making it easier for process control and automation manufacturers to sell into new areas.

Perhaps the best known harmonization so far is ISA84's adoption as IEC 61511. Likewise, the national API 610 standard for centrifugal pumps was recently adopted as international ISP 13709 standard.

Besides coordinating standards, other organizers are beginning to coalesce around common, globally available sets of process safety data that can be used to assist individual safety efforts. Scott Berger, executive director of the Center for Chemical Process Safety (www.aiche.org/ccps), reports that CCPS started a project in 2006 to develop a set of lagging process safety metrics to help companies push improvements and monitor progress in process safety programs. "We're seeking help from many members, external stakeholders, U.S. trade associations and international groups to adopt these metrics as a harmonized approach to improve industry benchmarking and transparency of industry performance," says Berger. Besides lagging metrics, CCPS also plans to seek leading metrics and near-miss reporting definitions.

"The process safety metrics that CCPS is putting together are so valuable because no one has been collecting this kind of historical performance information," says Bert Knegtering, global business development manager for Honeywell Process Solutions' (hpsweb.honeywell.com) safety consulting services. "For example, if you have a DCS in a particular application that's out of control, how much change do you need to bring it to a safe condition? This is the kind of experience you can add to these metrics and then use for future RAs."

Changing Minds

Once an audit, hazop study, risk assessment and safety plans are approved and implemented, then the real work can begin—instructing managers to give them more than lip ser-

vice and training staff to use them consistently.

"The ISA84 standard can walk you through the safety life cycle, and you can follow it and understand your process. However, the real challenge is getting users to consistently follow a safety plan, because doing it can seem overwhelming at first," says Charles Fialkowski, national process safety manager at Siemens Energy and Automation (www.sea.siemens.com). "Users say, 'I've got to make product,' and so any safety effort is initially seen as a drag on the process."

Bob Adamski, principal at RA Safety Consulting (www.ra-safetyconsulting.com) in Loudon, Tenn., adds that process safety systems must be automatic because people are too reluctant to initiate a plant's safety system on their own. "Humans will not push that big red button in a process application because when they do, someone always gets punished and fired," says Adamski.

Of course, this is a pretty clear indication of the prevalence of the tendency to put profit before safety.

"We've come a long way, but we still have a long way to go," says Dr. Sam Mannan, director of the Mary Kay O'Connor Process Safety Center (process-safety.tamu.edu) at Texas A&M University in College Station, Texas. "Industries and governments have a lot of process safety rules in place, and they're developing better tools, establishing real penalties and encouraging the culture change needed for process safety to make more gains," says Mannan. "However, it's still pretty scandalous how little data collection and metrics we have for process safety. Industry and government track all kinds of economic indicators at local, state and national levels, but there's no tracking of process safety issues that could help save people's lives and prevent injuries by holding companies accountable for making continuous safety improvements. I think firms should report safety performance data to stakeholders and the public because process safety is actually one of the main things that make them profitable. A company that isn't running safely isn't going to be sustainable in the long run."

Russ Elveston, PE, a consulting safety engineer and 30-year OSHA veteran, agrees that PSM requires a fair amount of capital to implement, but is still a good investment. "Process safety is a quality program that can improve bottom lines, but no one believes it until they see the numbers over time," says Elveston.

Still, adopting practical process safety often means overcoming a huge amount of psychological baggage and denial. "Some users don't want to seek or think about that edge," says Summers.

One well-known effort that seeks to enlighten and update traditional process safety attitudes is Shell Exploration & Production's Hearts and Minds program (www.energyinst.org.uk/heartsandminds). Established in 2002, the program was developed by Shell and the U.K.-based Energy Institute

and helps companies involve all of their staff members in better managing health, safety and environmental issues. Its organizational presentations include "Understanding Your Culture," "Seeing Yourself as Others See You," "Bringing Your RA Matrix to Life," "Improving Supervision," "Managing Rule Breaking" and others.

Enlightening Litigators, Too

Besides changing the old attitudes of their colleagues, engineers willing to discuss and document process safety efforts openly must also convert their firms' attorneys. "We're still seeing some hesitancy on the part of the legal community about putting an official stamp of approval on a risk matrix because they're worried about the exposure of a potential plaintiff using that information," says Campbell. "It's taking awhile, but even the lawyers are becoming convinced that it's a more defensible position if you can show you have a consistently applied RA combined with a risk matrix that puts you in the same ballpark as the rest of your industry."

Better Safety Tools

While audits, assessments, standards compliance specifications, training and consistent implementation all contribute to better process safety, there also are many improved and safety-certified tools that can support users safety efforts. Besides safety-certifying individual devices, organizers also are developing certifications for larger systems based on operator tasks and equipment and system life cycles. Also, TÜV Rhineland's (www.us.TUV.com) Functional Safety Program is training hundreds of functional safety experts who can advise their colleagues and other users on safety issue and requirements.

"In past years, the effort was to get safety PLCs certified, and most users have these now. The next step was to develop tools that make it easier for equipment to apply safety standards, so safety lifecycle devices were developed that have more intelligence in their boxes," says Fialkowski. "They include self-documenting tools with paper trails based on today's configuration that document what was done, when, and who did it. This enables checks and balances of prior inspections that can aid compliance and safety. We're also seeing more configuration out in the field, and these documenting tools can help show what bypasses were made, what was done in a system's bowels and show resulting feedback. This brings remote adjustments up to the management level and helps further minimize human error."

Fialkowski also says adds that online proof testing is emerging now that allows users to test devices more often. Similar to partial-stroke valve testing, online proof testing allows users in the control room to order via a fieldbus a transmitter to bypass and test a transmitter, and not have to worry as much about tripping their plant.

Similarly, Yokogawa Corp. of America (us.yokogawa.com) reports that its Pro-Safe RS software examines data coming into its DCS from I/O points via its Vnet/IP network and actively watches for "excursions out of tolerance" to help users monitor their systems and improve overall safety.

Staying Aware

While eternal vigilance is well-known as the price of freedom, it's also the coin for other crucial items, including long-term process safety.

Campbell explains that another reason some users ironically resist new process safety techniques is because they've been successful with older methods. "It's hard to quantify, but sometimes people rationalize dragging their feet on process safety because they haven't blown up a heater in 30 years," he says. "A given facility may have had few or no major incidents in many years, and so they come to believe that an accident can't happen to them. These users must be reminded that compliance with OSHA's PSM rules is not optional. In these cases, process safety is more psychological than technological, and so it can help to merge an application or facility's safety rules with its reliability requirements."

Likewise, Summers reports that after performance-based processes based on RAs emerged in the 1990s, they evolved into quality-based processes that became even more highly analytical. "The problem is that numbers can become a crutch if too much faith is placed in them," she explains. "Sometimes excessive belief in mathematics can cause users to hide behind requirements that are too broad and don't provide the functional safety originally needed to prevent an accident. People can forget the actual uncertainty in their data and the limits of what they're considering in their analyses, and this can cause an artificial sense of security that their safety system must be as good they believe it is. However, when we're talking about uncertainty, the odds can play against us because what we're routinely worried about, such as productivity and uptime, can negatively affect safety." ■

Jim Montague is Control's executive editor.