



# Don't Do This!

**GLENN YOUNG**  
GLENN YOUNG & ASSOCIATES, LLC

**JOEL OLENER**  
PROCESS SAFETY AND SECURITY  
INTERNATIONAL, LLC

These are some of the worst process safety management (PSM) practices we have seen. Don't make these mistakes.

Over our extensive careers in the chemical process industries (CPI) and the field of process safety management (PSM), we have observed many good — and bad — practices.

For example, in the 1970s, one of us worked at a major commodity chemical manufacturing complex with 10 individual plants onsite. Management's attitude was "run it till it breaks and then patch it," and we averaged three to four explosions, fires, or releases per year.

When the U.S. Occupational Safety and Health Administration (OSHA) published the PSM standard in 1992, an internal company debate raged over whether or not we were already in compliance with the regulation. Management eventually brought in an outside auditor to answer the question. The resulting audit report was so damaging that it was instantly sealed up under attorney-client privilege and was never seen again.

This article summarizes some of the worst PSM practices that we have seen, both as employees at manufacturing companies and as consultants at various clients' facilities.

### Maintenance

A company gave maintenance managers a quarterly bonus based on how far under budget their expenditures were. This gave the managers a financial incentive to *not* provide maintenance. Almost all of the site maintenance managers routinely qualified for their bonuses — with

predictable results. The worn-out equipment consistently leaked, failed, and was otherwise a hazard to operate.

*Paying maintenance managers to not do their jobs is a worst practice. Don't do this!*

A common reason for safety system failure is that nobody is assigned direct responsibility for their inspection and maintenance. In one plant, emergency isolation valves had been installed on pressurized equipment, but the valves were tested only when it was convenient to do so — which was on scheduled turnarounds that were held every two or three years.

A safety control that is not tested is worse than one that does not exist. If employees know that no safeguard exists, they can implement administrative controls to accommodate for the lack of the safeguard. However, if a safeguard is part of the design, operators assume that the safety controls will work on demand. But unless the controls are routinely tested, operators are relying on safeguards that may not function.

*Failure to routinely test safety-critical equipment is a worst practice. Don't do this!*

When control systems are tested, it is critical that the tests be "fully functional," which means that all parts of the system are tested. This includes the sensor(s), the logic, the



This article is based on a paper presented at the 2016 AIChE Spring Meeting and 12th Global Congress on Process Safety, April 2016.



actuated element(s), and the communications between all elements. Some mechanical integrity programs omit some or all of these elements from testing. Testing part of the system, or parts in isolation (e.g., omitting the communications), is insufficient to ensure function on demand.

***Omission of ANY part of a safety-critical control system from routine testing is a worst practice. Don't do this!***

### Operations authority

One day, the lead operator of a plant announced over the radio, in an alarmed voice, "TRIP THE FURNACE!" The board operator immediately complied, but before the trip sequence was complete, the plant manager skidded around the corner, yelling, "Don't trip it! Don't trip it!" As it turned out, during the previous turnaround, the furnace outlet piping was decoked by bead-blasting, which caused significant thinning. The piping was so thin that the 16-in. furnace outlet bend was becoming translucent. Had it failed, the hot and flammable gaseous contents, at 250 psig, would have been released in a massive explosion.

After the furnace was secured and cooled, the plant manager assembled the operations staff and demanded that no process interruption would be made in the future without his personal approval. Some of the operators refused for safety reasons and were threatened with termination. Process operators must have independent authority to use their best professional judgment to apply whatever emergency safety measures are necessary.

***Waiting for management approval before implementing emergency measures is an almost sure way to create disasters and is an absolute worst practice. Don't do this!***

### Operational knowledge

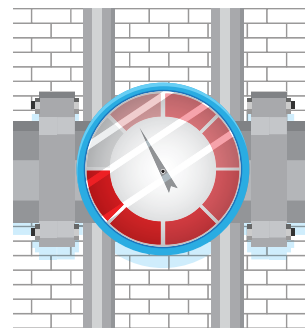
A plant being audited had a cyanogen bromide process with runaway potential. The board operator being interviewed by the auditor did not know the warning signs of a runaway reaction, the rate at which such a reaction would propagate, or the maximum safe operating temperatures or pressures of the reactor. When asked why this was not of concern, the operator explained that the entire process was in a sealed room that was vented to a scrubber. When asked if the sealed room was robust enough to withstand a reactor failure, the reply was "I never thought of that!"

Operations staff must be given enough information to safely operate the process. This includes the maximum safe limits for temperature, pressure, flow, or any other critical aspects of the equipment being operated. Management

concern about trade secrets of a proprietary process is an insufficient reason to not educate the operations staff about safe operating limits.

***Keeping operators in the dark about the safety limits of their equipment is a worst practice. Don't do this!***

In several plants, the operations staffs of multiple packaged waste-heat boilers were unaware of the mechanics of boiler steam explosions. When the water levels drop in a boiler, exposing the fired tubes to heat without the thermosiphon cooling provided by circulation



through the boiler, the tubes become red hot and then soften. If boiler feedwater flow is then resumed, the cold water hits the overheated, softened tubes, and a steam (phase-change) explosion occurs. The head of the boiler is typically blown off, and fatalities can occur. The relief valves on the steam drum are insufficient to vent this localized overpressure.

Boilers are just as deadly as highly hazardous chemicals in terms of explosion potential. Although most boiler operators are aware of the hazards of unburned fuel in the boiler firebox, many are not trained on the mechanics of steam explosions. The mechanics of boiler steam explosions must be included in every boiler operator's training.

***Allowing operators to run boilers without an understanding of steam explosions is a worst practice. Don't do this!***

### Operating procedures

In a recent incident ([www.csb.gov/williams-olefins-plant-explosion-and-fire-](http://www.csb.gov/williams-olefins-plant-explosion-and-fire-)), an experienced supervisor was preparing a heat exchanger for service. The exchanger had been isolated from the process by block valves, but apparently flammable process liquids had leaked through the closed valves into the exchanger's cold process side. The supervisor opened the valves on the exchanger's hot process side to warm up the exchanger, but without first opening the cold side to the process. The cold process side liquids expanded in the isolated shell of the exchanger and the leaking manual block valves could not release the cold liquids quickly enough to avoid a pressure rise. Since the cold side of the exchanger had no mechanical overpressure protection, it eventually exceeded the maximum allowable working pressure (MAWP) and failed catastrophically.

The engineering solution that would have prevented this incident is to provide overpressure protection (a pressure safety valve or rupture disc) on the cold side of the exchanger. But the incident could also have been prevented

## Safety

if the operating procedures had specifically instructed first opening the cold side of the exchanger to the process before applying energy (heat) to the exchanger. Engineering safeguards are the most reliable, but ensuring that operators are trained in the safe way to put equipment into service is also mandatory.

***Failure to have operating procedures that document the safe way to put equipment into service is a worst practice. Don't do this!***

Another common problem is that many operating procedures do not capture institutional knowledge. One of the largest demographic shifts in the U.S. workforce ever is taking place now. As the baby boom generation retires, they take with them decades of process knowledge. They are being replaced with younger workers, who, regardless of how technically competent they are, lack the experience and training of the retiring workers.

To avoid losing this valuable experience, companies should assign older workers to review and supplement operating procedures. Adding "caution" and "danger" statements to existing procedures gives new trainees not only information on *how* to safely perform a task but also *why* the task must be performed that way and the hazards created by failure to follow the procedure. This information increases the likelihood that the training will be remembered and followed.

Another best practice is to pay retiring employees a small annual retainer and keep them as consultants. In turnaround situations, for example, having extra experienced employees on staff is a good way to reduce injuries and to ensure smooth and timely restarts. If situations arise that are baffling (e.g., product quality issues, unexpected pressure drops across distillation columns or scrubbers, etc.), these retired, experienced operators can be called to shed light on problems that they have dealt with in the past. Retirees can also assist in updating operating procedures.

Don't let decades of valuable institutional knowledge walk away upon retirement. Find ways to utilize the experience of retirees.

***Failure to capture institutional knowledge of retiring employees is a worst practice. Don't do this!***

### Emergency response

Operators at a vinyl chloride monomer (VCM) plant opened a drain valve on a reactor full of liquefied flammable gas ([www.csb.gov/formosa-plastics-vinyl-chloride-explosion](http://www.csb.gov/formosa-plastics-vinyl-chloride-explosion)). As the reactor contents escaped, a vapor cloud

began to form. The operators issued a shelter-in-place order and tried for a full 15 minutes to stop the source of the leak rather than calling for an evacuation. Eventually, the vapor cloud found an ignition source and a massive explosion occurred, with multiple fatalities.

The company had failed to provide clear instructions on when to evacuate. Unless the operations staff has clear evacuation guidelines, it is the nature of operators to keep trying to fix the problem. But there comes a point in incident management where further efforts to fix the problem are likely to be futile and/or create imminent danger for proximate personnel. At that point, the focus must change from equipment protection to protection of life and health. Unless the company has clear guidelines for the specific circumstances requiring evacuation, and unless the operating staff is stringently and routinely trained on those guidelines, lives will continue to be lost.

***Failure to provide operations staff with clear guidelines on when to evacuate is a worst practice. Don't do this!***

A chemical plant's firewater reservoir and header system had been designed when ground was broken for construction at the site. Since that time, the number of production units onsite had more than doubled. No survey of the fire system had been conducted to determine whether the firewater capacity was sufficient for the additions.

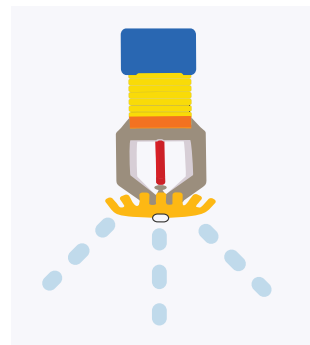
When new processes or debottlenecking of existing processes are contemplated, utility systems must be reanalyzed via a management of change (MOC) procedure.

***Failure to review firewater demands during debottlenecking or new construction is a worst practice. Don't do this!***

Flare header systems are often designed during the initial plant design. Over time, the plant adds streams to the flare header without recalculating the header capabilities. Because there could be a total release of flammable and toxic materials from multiple sources to the flare header system, the site must be designed for multiple simultaneous worst-case flows.

***Assuming that the original flare header design will work as designed is a worst practice. Don't do this.***

Many plants omit the scenarios used in the development of their risk management plan (RMP) from the emergency brigade's drills. Since the RMP worst-case scenario events are the worst events identified for the site and the alternate-case scenarios are the most likely failure events, the emergency brigade must consider all of them in drills. To skip these events not only creates regulatory liability, but it also



leaves the emergency team unprepared for the worst-case scenarios.

***Failure to use ALL RMP scenarios as emergency drill scenarios is a worst practice. Don't do this!***

A plant stored all of its emergency gear (bunker gear, hazmat suits, air monitoring equipment, etc.) in a single building. If a release or fire occurred that blanketed the building in smoke or toxic chemical clouds, all of the emergency gear would be unavailable. Emergency gear should always be stored in multiple, physically separated locations to ensure that at least some of the gear will be available on demand.

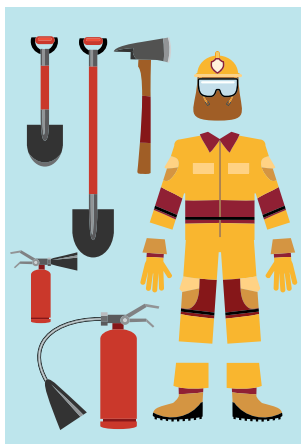
***Storage of all emergency gear in a single location is a worst practice. Don't do this!***

During a PSM inspection of one facility by the U.S. Environmental Protection Agency (EPA), personnel were asked whether they had drilled for the scenarios of an airliner coming down on the plant, a ship detonation in the adjacent shipping channel, and a railcar derailment and boiling liquid expanding vapor explosion (BLEVE) on adjacent tracks. The site's PSM manager responded that since those were beyond the plant's control, they had not been reviewed. The plant was cited for failing to prepare for external events. Since the plant was in the takeoff and landing path of a major international airport, and was adjacent to navigable waterways and rail lines, the events were credible even though the plant had no direct control over them.

***Failure to consider and drill for credible external events is a widespread worst practice. Don't do this!***

Most older plants lack a master shutdown switch. There are many credible situations that might require immediate evacuation of a facility, such as a tornado, earthquake, failure of levees, and toxic releases from adjacent facilities. In such circumstances, the immediate evacuation of personnel will preclude any orderly shutdown of the equipment. A master shutdown switch should be available that:

- closes all chemical and energy feeds to the process
- closes all chemical and energy feeds from the process
- closes all energy



sources in the process (electricity, steam, etc.)

- isolates as many parts of the process as possible.

Such a shutdown will certainly cause rupture discs and safety relief valves to lift, adding to the hazards, but will prevent catastrophic vessel failures, runaway reactions, and domino effects that would be orders of magnitude worse.

***Not having a master shutdown switch is a definite worst practice. Don't do this!***

## Operator fatigue

At a plant's pre-op cleaning and startup, it was typical for the operations staff to work 16 hours per day, seven days a week. During a four-month startup, it was not unusual for operators to go home, sleep, and dream about

operating the plant — and wake up more tired than when they went to bed. Numerous errors occurred during the startup process, most attributable to fatigue.

In another instance, an operator had been on a trip that required him to be awake for almost a full 24 hours. Upon returning home, he was called by the plant to immediately report for overtime duty. He refused on safety grounds, and was subsequently threatened with dismissal if any such refusal happened again.

Fatigue has been proven, again and again, to cause significant operational errors. A company fatigue rule that is understood and enforced is essential to preventing operator errors. Operators who have legitimate reasons for being unfit for duty must be similarly accommodated. A tired operations staff is an accident waiting to happen.

***Failure to have a worker fatigue policy that is rigorously enforced is a worst practice. Don't do this!***

## Quality control

A refinery had been buying pump seals from a particular authorized vendor for decades. Without notification, the seal manufacturer moved its production facility to another country. The seal brand did not change and the seal part number did not change, but poorer seal tolerances caused the failure rate to go from less than 5% to nearly 50%, and several fires resulted. The refinery's quality control program for warehouse spares was limited to checking the vendor and part number of arriving parts. This is inadequate.

The process owner and the vendor should enter into a written legal agreement that requires all changes related to parts — manufacturer, manufacturing location, materials of construction, tolerances, etc. — to be communicated to the



# Safety

process owner *in writing* prior to any change. However, this alone is still insufficient. In order to become an authorized vendor, the supplier must also have such agreements with all manufacturers of the parts it purchases. The vendor-manufacturer agreements should be periodically audited and corrections made as needed. Verifying the quality control of warehouse spares by putting them into the PSM-covered process to see if they fail is not acceptable.

***Failure to have an audited, manufacturer-to-warehouse-shelf quality-control program for spare parts is a worst practice. Don't do this!***

## Disabling safeguards

The entire operating area of a large refinery is electrically classified as Class 1, Division 2. This classification is intended to prevent electrical gear from creating an ignition source in a hazardous atmosphere. In the center of the electrically classified area of the refinery are several large fired furnaces and crackers. As supplied by the vendor, the fired equipment was fitted with an automatic steam purge that actuated on loss of flame or on manual trip of the burners. However, this safety feature had been disabled — the operating staff had manually closed the steam valves to the furnaces, ostensibly to prevent spurious activation and to improve the onstream factor of the equipment.

What the operators did not realize was that the steam purge served several critical safety functions. In the event of a vapor cloud in the operating area, the furnace burners and the red-hot refractory can serve as ignition sources. The steam purge is intended to reduce this risk by instantly quenching the burner flames and simultaneously cooling the refractory. In addition, if the vapor cloud itself puts out the burners (because the mixture is too rich to burn), the steam purge creates enough flow through the furnace to reduce the likelihood of a back-flash ignition.

When informed of the purposes of the automatic steam purge, the operators still refused to recommend reinstating it. When asked what would happen if a flammable vapor cloud formed, the operators stated that they would enter the cloud and manually unblock the steam purge valve. In fact, one such vapor cloud had already occurred, and the operator was able to run into the flammable vapor cloud and open the steam purge before ignition.

Deliberate stupidity in the face of life-threatening hazard is an artifact of institutional inertia. Since the operators had always done it that way, their resistance to change was high. Even after a letter was sent to management, to our knowl-



edge, the steam purges are still manually blocked.

***Deliberate disabling of safeguards is a worst practice. Don't do this!***

## Equipment siting

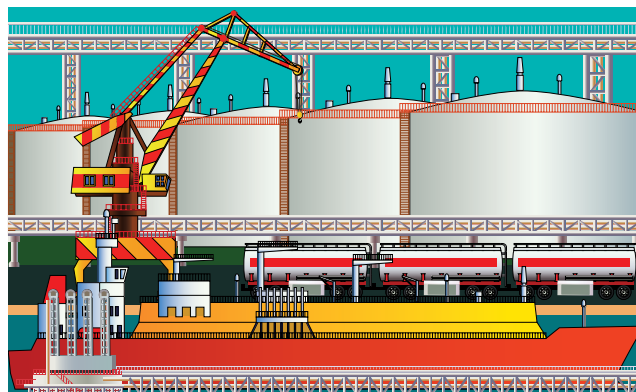
It seems that the larger the company, the more likely that management will be resistant to change. Some executives seem to feel that any safety practice worth having would have been previously discovered and subsequently implemented, and that there is no need to utilize outside resources for auditing or to suggest previously unknown safety improvements. This insular mindset is a major reason why the process safety programs of many large refining companies are typically about 10 years behind those of chemical companies. The pipeline industry is typically 15 to 20 years behind the chemical manufacturing industry.

Consider the layout at the refinery mentioned in the snuffing steam example. Two 150,000-gal atmospheric tanks holding light naphtha are sited in the middle of the operating unit. The naphtha is kept in liquid phase through refrigeration. The tanks have level controls and high-high level trips, but emergency discharge is to atmosphere through tip-up manways atop the tanks. If the tanks ever overflow, a cold, dense cloud of naphtha vapor would form in the center of the operating area. The fired equipment is in close proximity. The resulting vapor cloud explosion would likely destroy the refinery and adjacent plants in a domino-effect sequence.

During the process hazard analysis (PHA) of the refinery, an engineer stated that since no such catastrophe had occurred in almost 40 years of operation, that scenario was not credible. Another letter to management was required ...

***Refusal to address obvious equipment-siting hazards is a worst practice. Don't do this!***

The same refinery also had a major barge and ship-loading terminal on an adjacent river. The nearest shut-off valves for the large loading headers were over a half-mile from the terminal, and the valves (which were designed to close very slowly to prevent line hammer) were not all remotely actuated. If a ship were to strike the loading dock,



multiple headers containing flammable products would rupture, and operators would need to close manual valves or trip pumps to prevent additional flows to the fire. The loading dock fire would be uncontrolled since the firewater headers would rupture at the same time.

The PHA team was encouraged to recommend putting emergency isolation valves on product headers closer to the loading dock. The same engineer refused, saying that such a collision with the dock was not credible, since it had not yet happened. (No more letters — I no longer do work for that refinery.)

***Refusal to locate safeguards proximate to the hazards they are intended to control is a worst practice. Don't do this!***

### Deficient pre-startup checklists

Fireproofing had been installed on the skirts of a distillation column because a horizontal flange on the column's bottom (inside the skirt) had the potential to cause a fire hazard. (Having such a flange inside a support skirt is a bad design, although many legacy vessels and distillation columns have similar flanges.) The fireproofing was removed for a skirt inspection during a turnaround and was not replaced. On startup, the flange inside the skirt leaked, causing a pressurized jet fire that began cutting the column skirt. The entire column leaned by 10–15 deg. before the column was depressured and the fire extinguished. Had the company been less fortunate, the column would have collapsed, with domino effects.

The pre-startup checklist did not require inspection and verification of fireproofing prior to charging the process with flammable chemicals. All safety systems should be inspected and verified prior to startup. The pre-startup safety review (PSSR) checklist should have caught this deficiency.

***A thorough PSSR checklist that has been reviewed and independently verified is essential for startups. Failure to have one is a worst practice. Don't do this!***

Another time, at the same plant, the PSSR was “pencil whipped” by operations staff eager to satisfy management's desire for a rapid restart of the plant. The plant restarted without incident, but the liquid product contained fine entrained solids, and there was a high differential pressure across a furnace outlet quench vessel. The plant was shut down for troubleshooting, and when the quench vessel was opened, a full set of scaffolding that had been left inside the vessel was discovered. The scaffolding boards had disintegrated (creating the cellulose particles in the product), but

the metal scaffolding structure gleamed like chrome.

PSSR checklists must not only be complete and comprehensive, but also should be independently verified. Most PSM incidents occur during startup and shutdown, and adherence to a good PSSR procedure can eliminate many of them.

***Failure to double-check PSSR items, including clearing lockouts and blinds, is a worst practice. Don't do this!***

### Process hazard analysis

The worst problem with PHAs involves node development, particularly the use of nodes that are unworkably large. One PHA divided an entire ammonia plant into just four nodes. Using nodes this large can have several bad consequences. The PHA team takes many weeks to review a single node; they get bored and can become sloppy. They also can get lost in the details of such huge nodes, and obvious hazards slip through the cracks without notice. Small nodes can always be combined, but large nodes are hard to split.

***PHA nodes that are too large are a worst practice. Don't do this!***

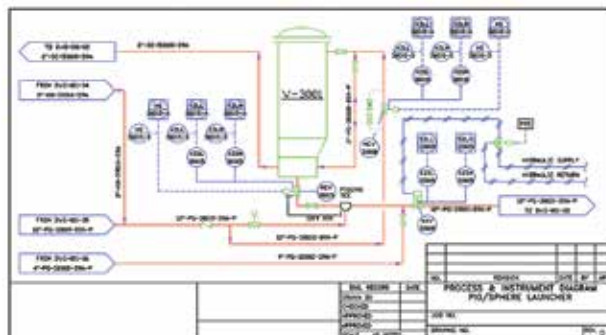
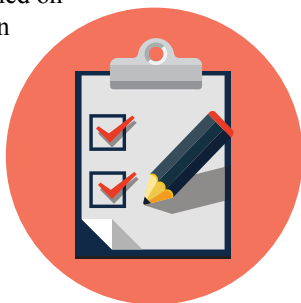
The second worst problem we've seen with PHAs is the over-reliance on revalidations to save money. The PSM standard requires facilities to update their PHAs every five years. Updating can involve either completely redoing the PHA or validating that the previous PHA is still accurate. Since revalidations can take less time and cost less than full redos, some plant managements continue revalidating the original study.

The study that is the basis for the revalidation limits the effectiveness of a revalidation. It is not realistic to think that the PHA techniques of five, 10, 15, or even 20 years ago are sufficient to find and address the hazards that you are looking for now.

A policy of performing every-other PHA from scratch has multiple benefits. The nodes will be drawn differently, and this alone makes it likely that the PHA team will catch previously unrecognized hazards. When PHAs are revalidated multiple times, their utility fails miserably.

***Failure to make every-other PHA a complete redo is a worst practice. Don't do this!***

The third worst issue with PHAs is the granting of



# Safety

excessive authority to management review teams to decline or modify PHA recommendations. Management should be given guidelines that limit their authority to reject or modify PHA recommendations, for instance, only if:

- the PHA team overlooked a credible safeguard
- the recommendation is not technically feasible — which does not mean too expensive
- layer of protection analysis (LOPA) or event-tree analysis has shown that the risk with existing safeguards is acceptable
- an equivalent option will provide equivalent safety
- the recommendation has no safety, health, or environmental consequences (*i.e.*, it is operational only).

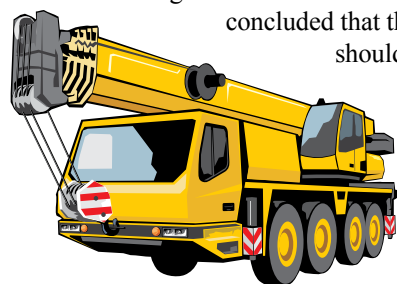
And, any time management rejects or modifies a PHA team recommendation, they need to document in writing why the rejection or modification provides an equivalent level of safety to what the team recommended.

In one incident, a high-pressure boiler was blown-down to a lower-pressure vent tank. The PHA team recommended a relief valve or rupture disc to protect the vent tank. For economic reasons, management decided to instead car-seal open the vent valves from the vent tank to atmosphere. The unit's piping and instrumentation diagram (P&ID) was inaccurate — a block valve in the vent tank's line to atmosphere used by operations during startup to minimize the noise of steam venting was not shown on the P&ID and did not get car-sealed open. On the next startup, the operators did throttle the vent, the vent tank did overpressure, and the top dome of the vent vessel was blown off into a pipe rack, where it put a large dent in an anhydrous ammonia pipe. Had the ammonia pipe ruptured, multiple fatalities would have been virtually certain. If the PHA team's recommendation had been implemented, this incident would not have occurred.

***Failure to force management into documenting their reasons for rejection or modification of PHA recommendations is a worst practice. Don't do this!***

## Incident recognition and reporting

At one plant, a review of all incidents over the last five years identified seven instances of mobile cranes striking overhead pipe racks. This trend had not been previously recognized — each individual incident report



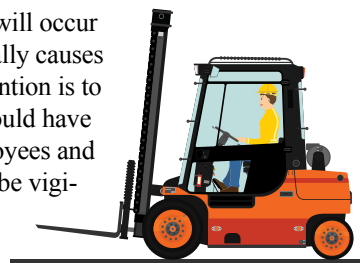
concluded that the crane operators should be retrained to not strike the overhead racks. When a near-miss occurs this frequently, it should be identified and addressed by engineering

controls. If it is not feasible to raise the piping over the roadways, then at least a bump-guard should be installed to prevent cranes from striking the piping.

***Failure to analyze all incidents for trends on a periodic basis is a worst practice. Don't do this!***

Employees and contractors often do not recognize PSM near-misses. A contractor driving a forklift approached an intersection with pipe racks on the far side. When he tried to stop for the stop sign, the brakes failed. He shut down the engine, drifted to a stop, and radioed for a tow back to the maintenance shop. There was no collision; there was no injury; there was no damage. The driver did not think of this as a near-miss until he was asked, "What could have happened if the forklift had plowed into the pipe rack?" To prevent the possibility of future collisions, the intersection was fitted with a vehicle barrier.

This type of incident will occur multiple times until it finally causes a disaster. The only prevention is to continually ask, "What could have happened?" Unless employees and contractors are trained to be vigilant and thoughtful about any out-of-the-ordinary event, many PSM near-miss incidents will be overlooked.



***Failure to define PSM near-misses and to train employees for awareness is a worst practice. Don't do this!***

Another common worst practice is to not identify PSM near-misses in incident reports. Virtually every plant has recorded incidents with PSM potential that were not designated in the reports as being PSM near-misses. This lack of PSM awareness is not only a regulatory liability, but it is also an impediment to preventing catastrophes. Near-misses are opportunities to identify and fix potentially disastrous hazards. Unless the near-misses are identified as having PSM potential, however, they will not receive the attention they deserve.

***Failure to correctly categorize PSM near-misses is a worst practice. Don't do this!***

## Personnel access

A large complex has multiple plants, some of which are covered by the PSM standards and others that are not. Personnel control was done at the front gate of the complex, where everyone entering and leaving the site signed in and out. No records were kept of who was in what unit of the site, for what purpose, or for what duration. When the inadequacy of this for personnel accounting was explained, the safety representative strongly disagreed.

The purpose of personnel accounting is to enable the owner to promptly verify that everyone escaped in the event

of a fire, explosion, or release. Without such verification, the emergency brigade must assume that some people are still in the area, which puts responders at risk as they search for those who might be missing.

***Not knowing who is in the PSM-covered area at all times is a definite worst practice. Don't do this!***

## Work permits

It is common for welders, assistants, and fire-watch personnel to leave an area for a variety of reasons, including tool procurement, bathroom breaks, and lunches. Many hot-work procedures do not require the welding crews to verbally confirm the validity of their hot-work permits prior to resuming work. This is a bad practice because conditions in the operating area can change in an instant. A valid hot-work permit may be temporarily suspended if a leak occurs, an atmospheric blowdown begins, or for other reasons. Unless the maintenance crew knows that conditions are safe, they should never resume hot work after a hiatus. Verbal communication with the permit issuer is the only way to confirm that the hot-work permit is still valid.

***Failure to require communication with the hot-work permit issuer prior to resuming hot work is a worst practice. Don't do this!***

Another common problem is that the boundaries of the PSM-covered process are not clearly marked. Trucks or golf carts can easily drive into areas where they should not be without a hot-work permit, such as electrically classified areas. At best, a removable chain boundary should be erected around the entire PSM-covered process. At a minimum, lines should be painted on the concrete pad to delineate the perimeter of the PSM process. In both cases, signs should clearly state that vehicle entry without a permit issued by the control room is prohibited.



Operators also sometimes violate the permit rules for PSM process areas. It is not unusual for operators to drive through classified areas in electric golf carts without bothering to obtain the proper entry permits. If contractors and maintenance personnel notice the operators

flagrantly violating the permit requirements (and they do notice!), those contract and maintenance personnel will be less likely to bother with vehicle permits either.

***Failure to prevent unpermitted vehicles in electrically classified areas is a worst practice. Don't do this!***

A consultant was performing his first PHA at a refinery. During a walk-through of the plant, he noticed a leak from a cryogenic propane line and a large visible cloud forming. He

asked if there were any alarms indicating that there was a leak and was directed to the supervisor's office, where there was a combustible-gas analyzer panel. None of the instruments showed any levels of combustible gases above the background readings!



The supervisor was notified that he had a potential catastrophic situation. The supervisor and the consultant went out to inspect the leak. After only a minute or two, the consultant began to get light-headed and made his way to fresher air. But before anyone could say "Stop!" the supervisor, while still standing in the middle of the vapor cloud, pulled out his cellphone and called maintenance to stop the leak. The cellphone was likely not explosionproof, but luckily no ignition occurred.

***Cellphones, cigarette lighters, and torch-strikers in operating areas (without permits) are definitely worst practices. Don't do this!***

## Closing thoughts

The incidents described here are a small fraction of the errors that we have seen that could cause fires, explosions, or releases. When opportunities arise to share such incidents with other safety professionals, do so. By learning from others' mistakes, we have the opportunity to avoid learning through bitter experience.

CEP

**GLENN YOUNG** is an independent safety consultant with 15 years of operating experience, nine years of corporate safety experience, and 16 years of consulting experience. His practice, Glenn Young & Associates, LLC (5261 Highland Rd. No. 193, Baton Rouge, LA 70808; Phone: (225) 772-1588; Email: g.young@gmail.com), specializes in process safety management (PSM) auditing, process hazard analysis, layer of protection analysis, and safety instrumented systems, and has clients that include major chemical manufacturers, refineries, pipelines, and pharmaceutical companies. He is the author of *Background Math for Safety Certification Exams* and *Applied Mathematics for Safety Engineers*, and is currently working on a new book, *The Art of the PHA — Process Hazard Analysis for the 21st Century*. He holds a BS from Louisiana State Univ., is a member of AIChE and the American Society of Safety Engineers (ASSE), and is a Certified Safety Professional and a Certified Process Safety Auditor.

**JOEL OLENER** has more than 22 years of experience in process safety management (PSM) program development, implementation, and auditing. Before founding Process Safety and Security International, LLC (13723 Aspen Cove Dr., Suite 110, Houston, TX 77077; Phone: (832) 515-4342; Email: info@pssillc.com), he worked in the chemical process and pharmaceutical industries, in process and project engineering, and engineering, maintenance, and plant management for Eastman Kodak Co., Sterling Drug Co., and Occidental Chemical Corp. He received BS (1964) and MS (1966) degrees in chemical engineering from the Polytechnic Institute of Brooklyn. He is a member of AIChE and its Safety and Health Div. as well as of the Institute of Internal Auditors' Environmental, Health, and Safety Advisory Committee. He received his certification as a Certified Process Safety Auditor (CPSA) from the Board of Environmental, Health, and Safety Auditor Certifications (BEAC), and currently serves on the BEAC Board of Directors.