Loss Prevention Bulletin

Improving process safety by sharing experience

Revisiting the Tacoa Power Plant boilover

Issue 290, April 2023

Are all critical safety systems created equal?

Four good practices from PSM audits

Ageing plants – Corrosion is the real enemy (Part 2)

Implementing inherent safety in design

Accidents of the future – Part 10

IChemE Safety Centre

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

TRAINING

LIVE ONLINE | ON-DEMAND | FACE-TO-FACE | IN-COMPANY

Learn with IChemE

IChemE is a market leader in process industry training with an extensive range of courses to help you develop your chemical engineering and process safety knowledge. Courses are delivered both online and face-to-face.

Upcoming courses

LIVE ONLINE

- Advanced Process Safety Considerations for Hydrogen Projects
- Bowtie Analysis and Barrier-Based Risk Management
- Fundamentals of Process Safety
- Hazard Identification Techniques
- HAZOP Leadership and Management
- HAZOP Study for Team Leaders and Team Members
- Layer of Protection Analysis (LOPA)
- Managing Human Factors
- Pressure Systems
- What Engineers Need to Know About Hydrogen Safety

FACE-TO-FACE

- Bowtie Analysis and Barrier-Based Risk Management
- Fundamentals of Process Safety
- HAZOP Study for Team Leaders and Team Members
- HAZOP Leadership and Management
- Layer of Protection Analysis (LOPA)
- Managing Human Factors

LIVE ONLINE

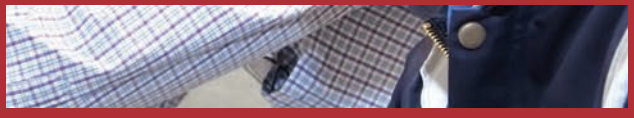
All our courses can be delivered in-company, on-site or online.

Bowtie Analysis and Barrier-Based Risk Management

10 May, Manchester, UK
From 23 May, 10:00 BST, Online

Learn about the bowtie risk assessment methodology and how to apply it effectively to facilitate risk-based decision making.

LPB 290



www.icheme.org/training

Contents

Loss Prevention Bulletin

Articles and case studies from around the world

Issue 290, April 2023

Editor: Tracey Donaldson
Publications Director: Claudia Flavell-While
Subscriptions: Hannah Rourke
Designer: Alex Revell

ISSN 0260-9576/23

Institution of Chemical Engineers
Davis Building, Railway Terrace,
Rugby, Warks, CV21 3HQ, UK

Tel: +44 (0) 1788 578214
Fax: +44 (0) 1788 560833

Email: tdonaldson@icheme.org
or journals@icheme.org
www.icheme.org

0260-9576/23/$17.63 + 0.00

Incident

Case study — Revisiting the Tacoa Power Plant boilover 40 years on

Ewan Stewart, Senior Process Engineer at Wood & Queensland Joint Chemical Engineering Committee Chair

Summary

Venezuela's deadliest industrial disaster occurred on 19 December 1982. An explosion in a fuel oil tank at the Tacoa Power Plant, then operated by Electricidad de Caracas, had already claimed the lives of two operators. However, as the resulting fire continued to burn, emergency personnel, onlookers, and media gathered in the vicinity — all unaware of the ominous heat wave creeping to the bottom of the tank. Suddenly, a heel of undrained water was vaporised, ejecting the tank's contents in a violent eruption which gushed burning oil down the steep hillside. Caracas suffered severe blackouts as the grim news emerged. 40,000 people were evacuated. 500 were injured and more than 150 lost their lives.

Keywords: Fuel oil, tank, fire

Prólogo

I can remember when I first learned of this incident. I had been reading *Incidents that Define Process Safety* when I found the double-page dedicated to the Tacoa tragedy. Shocked at the magnitude of destruction from a single tank, my initial curiosity was stalled by the Spanish-English language barrier. For years the incident remained inaccessible, although I have often wondered exactly what happened that day. Last year, as the 40-year anniversary approached, I decided to give things another go. This time I had the help of unlocked archives, a vastly improved google-translate, and several experts who were able to direct me towards reliable source material.

Avid LPB readers will know that as of January 2021, the *Loss Prevention Bulletin* has been fully accessible for all IChemE members, and a search of the records revealed that the Tacoa tragedy was covered in issue 57 of this publication (https://www.icheme.org/media/5781/lpb_issue057p026.pdf). Few might be aware that the (USA) National Fire Protection Association also has a freely searchable archive. After some sleuthing, I discovered that the NFPA had been invited to the scene to provide advice in the wake of the incident. A three-page account of their findings in *Fire Service Today* appears to be the source for much of the information that is currently available in English. However, this stops short of detailing the failings that led to the incident's escalation.

Frustratingly, I have learned that many aspects of the Tacoa tragedy are to this day, still up for debate. Although official investigations were undertaken on behalf of the Venezuelan government, these were never made public. Fortunately, as the years have passed, information has been leaked via court proceedings, articles in the local broadsheet, *El Nacional*, and first-hand accounts of those that were there and survived. In this write-up, I hope to build on earlier publications, and to fill some gaps of not just what occurred, but how and why.

La Planta Termoeléctrica Tacoa

Officially part of the *Ricardo Zuloaga Generator Complex*, the facility was named Tacoa after the seaside village in which it is situated. The original Tacoa thermo-electric power station was built on reclaimed land next to its sister Arrecifes plant in the 1950s, and this was supplemented with the Tacoa expansion plant in the late 1970s. The overall complex supplied 1700 MW of power to the greater Caracas area.

The site is instantly recognisable for its picturesque surroundings and for the three gigantic red and white chimney stacks of the expansion plant. These soar high above the facility, which is sandwiched between the cerulean blue Caribbean Sea and tropical green hills. When the 1970s expansion was made, the only area to install two heavy fuel oil

Figure 1 – The Ricardo Zuloaga Generator Complex. Tanks 8 and 9 were located at the site of the modern-day demineralised water tank (visible behind the tip of the expansion plant's middle stack)

0260-9576/23/$17.63 + 0.00

tanks (no. 8 and 9) was high on the hillside. This topography would play a role in the tragedy to come.

Ignición de un fuel oil pesado

A key mystery in this incident is the behaviour of the process fluid, number 6 fuel oil. Also known as residual fuel oil or bunker C, this is primarily produced from the bottom cut of a refinery's distillation column. Known for being tar-like and sluggish, number 6 fuel oil cannot be pumped without first heating it. Each of the Tacoa expansion plant's fuel oil storage tanks were equipped with six internal steam coils for this purpose. Late on 18 December, night shift operators recorded abnormally high temperatures in the feed line from the storage tanks to the fuel oil burners. Consequently, staff isolated one steam coil, leaving a single coil in operation. Although this was enough to clear the feed line temperature alarm, conditions within tank no. 8 remained far from normal.

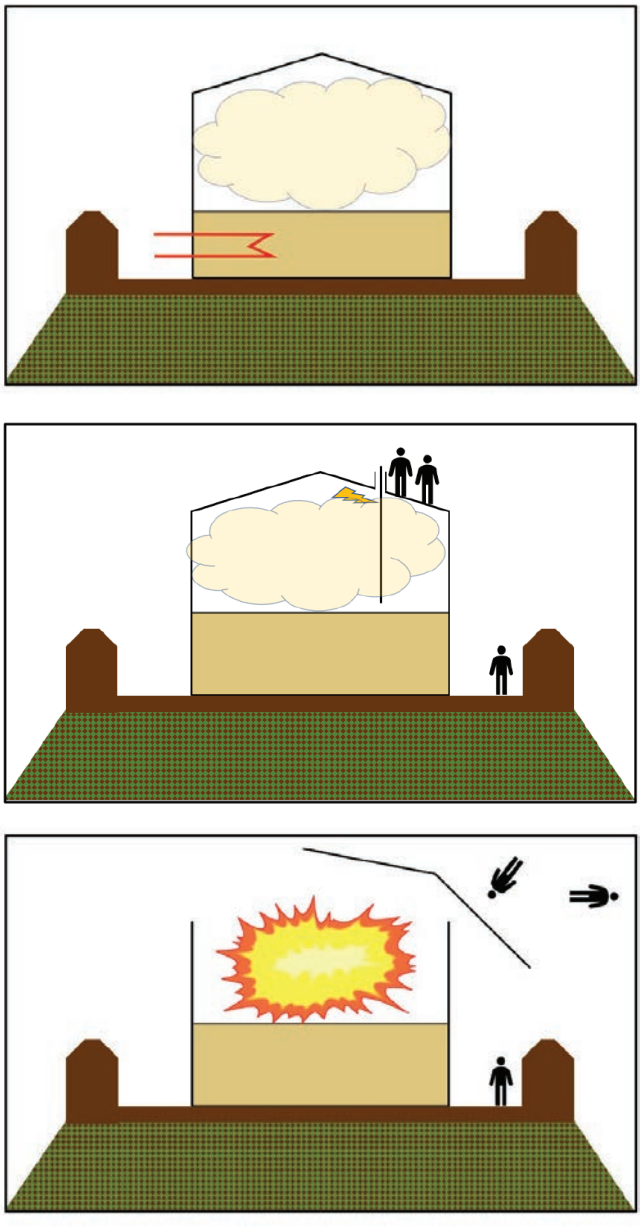


Figure 2 – (Top to bottom)
1. *Fuel oil overheated above its flashpoint.*
2. *Opening of gauging hatch allows air to intersperse with hydrocarbon gas. Ignition source unknown.*
3. *Explosion expels tank roof. Two operators killed.*

One might be curious as to how a heavy fuel oil is able produce a flammable atmosphere. The answer is a combination of blending and inappropriate temperature. Firstly, the specification for number 6 fuel oil allows for lighter ends to be combined with the residual oil to achieve a reduced viscosity, provided that flash point limitations are met. Varying degrees of blending can produce fuel oils with wide-ranging characteristics far removed from the original residual oil. The evidence suggests that the alarms and trips at the Tacoa power plant were configured for a different blend to that which was in the tanks at the time of the incident. Despite the flash point of the fuel oil being 71°C, the high temperature alarms were set at 80°C, with the boiler feed observed as high as 88°C. The lighter components of the blended fuel oil were being boiled-off within the tank.

Shortly before dawn the next morning, a three-man crew drove up the steep and narrow road to check the level on tank no. 8. This was necessary to facilitate offloading from a docked tanker. Whilst one operator remained in the vehicle, the other two climbed the access stairway to the roof of the 55m diameter 17m tall tank. As the men opened the gauging hatch, hot hydrocarbon vapour interspersed with the air creating an explosive mixture. The source of the subsequent ignition is much contested and will likely never be known. The most widely accepted theory is that there was an attempt to illuminate the dip tube for reading either with a match, lighter or a non-intrinsically safe lamp.

What followed was a massive explosion that ripped off the tank's conical roof. The two operators on the roof were launched into the air and killed. The third crew member was narrowly able to escape as severed oil lines fed a growing fire in the tank's containment dike. By the time he reached the safety of the control room, a gigantic black plume loomed over the facility from menacing flames high on the hillside.

Proteccion contra incendios inadecuada

It soon became clear that Electricidad de Caracas had no contingency plans for a fire in their fuel oil storage tanks. The company lacked a fire-brigade, and their staff had no training or instruction. Three water storage tanks located higher on the hillside held a dedicated firewater reserve, and this was supplemented as required by seawater pumps. Despite this, there does not appear to have been any coordination of the electricity company employees to obtain water from these sources.

The emergency response was delayed by more than 20 minutes as the first fire engines navigated tortuous roads to reach the remote site. Worse still, the track leading to the burning tank was dangerously exposed to a sharp drop on one side. It was too steep and narrow for anything other than an off-road vehicle. Firefighting apparatus arrived from across the region over the next few hours, with engines parked in the streets below, unable to access the elevated fire.

Carrying what equipment they could, responders made their way up to the burning tank on foot. It was then that the neglected condition of the fire response systems became apparent. Of three firewater pumps, only two units were

0260-9576/23/$17.63 + 0.00

operational. As a result, there was insufficient pressure for any hydrant or cooling line to reach the inside of tank no. 8. Further, a dedicated 2,000-gallon foam concentrate tank was found to be completely empty. Under any circumstances, extinguishing an open tank fire of this size would be extremely difficult; the lack of water and foam made this task impossible. The order was given to let the tank burn itself out. However, given the intensity of the fire, action was still required to prevent spread to the neighbouring dikes.

Despite the challenging access, the fire department were eventually able to position a small pumper truck on the hill overlooking tank no. 8 and had also managed to procure several barrels of foam concentrate. However, the necessary plant water to combine with the concentrate could not be sourced; the available connection, a coarse thread NPT (National Pipe Thread), was incompatible with the fine thread NH (National Hose) utilised by the fire department. Desperate for any means to access the water, responders decided on a risky improvision. As the fire raged on close behind them, they set to work fabricating a connection with open flame cutting / welding torches.

Whilst the responders scrambled on the hillside, a crowd had started to gather around them. The press had quickly arrived and were broadcasting live on-scene coverage. Locals and holidaymakers were drawn to the spectacle, some congregating on the beach, and others on the streets below the tank's steep dike walls. Many ascended the hill to get as close as possible to the action. The ensuing fiesta atmosphere betrayed the severity of the situation. Something very unsettling was beginning to take place within the tank...

Ingredientes de la ebullición

What happened next was a situation that no-one was prepared for. In fact, it was unprecedented. Both the NFPA and the American Petroleum Institute (API) had long held the position that no. 6 fuel oil, a refined product, was not subject to boilover. This stance was substantiated by loss history and experimental efforts to induce such an occurrence. Despite this, it is evident that a boilover did occur that day.

With the loss of the tank roof in the initial blast, the resulting open-top tank fire satisfied the last of three requirements for a boilover to occur. The other two ingredients; the presence of water, and an oil with wide ranging boiling characteristics, had been present all along.

There are many means through which water can accumulate in fuel oil storage, for example via leakage of a steam coil, or rain ingress through non watertight components. Although there were some attempts to shift blame on the fire department for applying water to the tank, these accusations were later rebuked. The consensus appears to be that small concentrations of water in the fuel oil supply were expected as part of the marine bunkering. Over time, the water would separate into a layer that would be periodically drained; this operation had not been carried out for an extended period prior to the incident. It is unclear why the water was not drained during the fire. Perhaps the necessary valves were engulfed by the dike fire, or maybe the precaution was not deemed necessary as a boilover could not have been anticipated.

Contrary to what was believed at the time, it is apparent that the heavy fuel oil fire in tank 8 had a sufficient range of

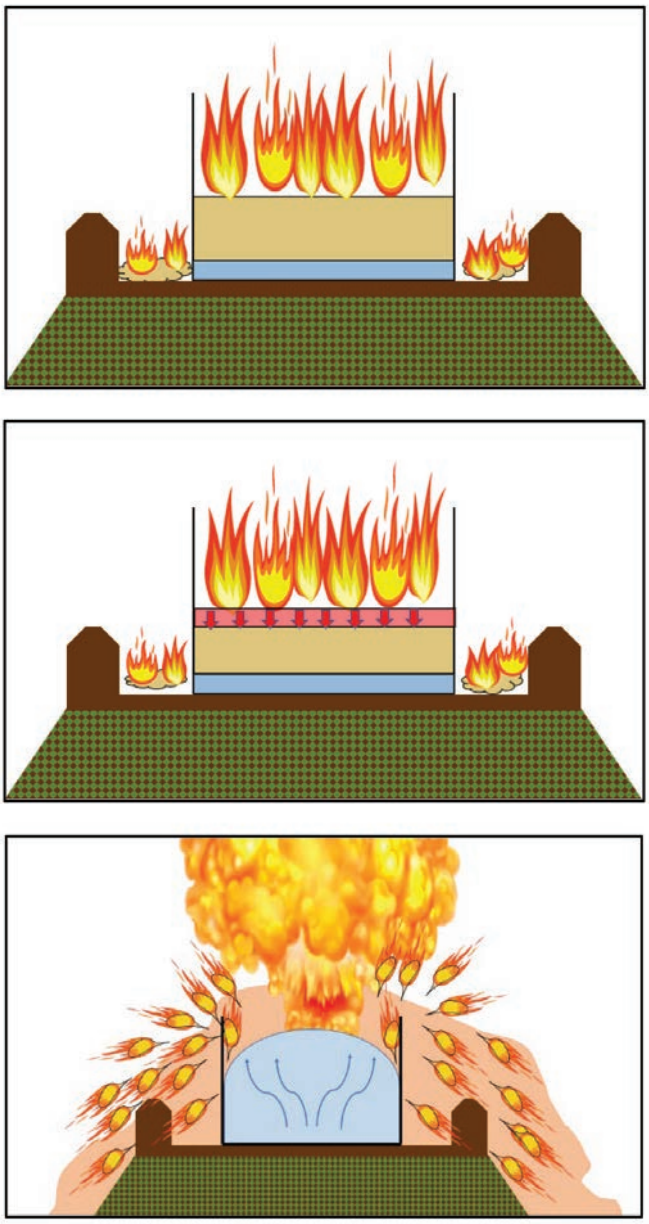


Figure 3 – (Top to bottom)
4. Loss of tank roof results in open-top tank fire.
5. Heat gradient starts to develop within tank as hot residues sink.
6. Heat wave reaches water heel resulting in rapid expansion into steam. A violent boilover occurs expelling the tank contents.

hydrocarbon components, including both light ends and viscous residues, for a *heat wave* to be generated within the tank. In an open tank fire of this nature, it is predominantly the lighter components that are consumed at the surface. The unburned heavier components, heated intensely by the fire, form a layer which is heavier than the surrounding oil. Gradually, this hot dense layer sinks and grows within the tank. At around midday, six hours after the initial outbreak, the heat wave had reached the tank's water heel at a temperature between 150 and 315 degrees Celsius.

Initially, the water would have superheated beyond 100 degrees Celsius due to the hydrostatic head of oil above it.

0260-9576/23/$17.63 + 0.00

And then, suddenly, the water would have flashed into steam, expanding by as much as 2000 times, ejecting the contents of the tank in a vicious eruption.

Volcán hecho por el hombre

Those on the ground observed a gigantic fireball rise out of the tank and into the sky. The intense radiant heat was accompanied by a storm of searing rain. Burning oil spilled over the dike, pouring over settlements and through the streets underneath the steep dike wall. Molten asphalt from the roads mingled with the oil creating a noxious mixture which continued to flow downhill, destroying everything in its path; cars, fire trucks, helicopters. A small beach, some 300m from the tank 8 was consumed in flames as those that could jumped into the sea.

There are many harrowing accounts of the boilover; stories of heroism, trauma, and great personal loss. The exact death toll is unknown; however, estimates are in the region of 150. Of these were 40 uniformed firefighters, dozens of civil defence workers, 17 plant employees, 10 media workers, and scores of civilians. The tragic events at Tacoa accounted for one of the highest single incident losses of firefighters until this unfortunate record was settled by the collapse of the World Trade Centre towers on 11 September 2001.

Whilst secondary to the human cost, the damage to property was enormous at an estimated $50M USD ($150M in 2023 terms). This included the destruction of 60 vehicles and most of the fire apparatus on scene, as well as fire damage to 70 occupied dwellings. Miraculously, the power plants remained relatively unscathed due to their concrete perimeter walls.

The fire in tank 8 was extinguished by the sudden inrush of air during the boilover. However, as the burning oil flowed over into the downhill containment dike, this resulted in a sustained fire around tank 9, another heavy fuel oil tank of

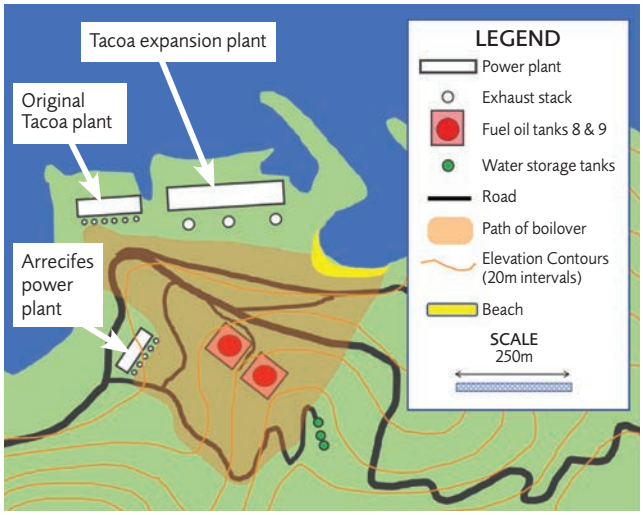


Figure 4 – Map of the Tacoa Power Plant and surrounds recreated by author from google-earth, photos, and videos. Indicative only.

similar size and construction. After several hours of exposure, the roof of tank 9 lifted, but did not fully detach. Much of the extraordinary helicopter footage available online of the Tacoa tragedy shows tank 9 on fire, whilst tank 8 lies blackened and crumpled on the hillside above. As a precaution against another boilover occurring in tank 9, the army evacuated 40,000 people from the area. The second boilover never came and the fire in tank 9 burnt out two to three days later.

Mejoras en seguridad

The events of 19 December 1982 left a permanent scar in the psyche of thousands of Venezuelans. The public demanded

Figure 5 – Image extracted from "Incidents that Define Process Safety" shows the aftermath. Both tank 8 (foreground) and tank 9 (background) appear blackened and crumpled. Notice the steep drop-off of the dike walls and settlements underneath.

0260-9576/23/$17.63 + 0.00

answers, however, these were not forthcoming. The official report of the investigative commission was known to consist of six volumes, however only a superficial 12-page summary was released due to ongoing litigation around the incident.

Electricidad de Caracas made widespread changes to the plant following the tragedy. Aided by the completion of a supply pipeline to the generator complex, the company shifted its dual-fuel turbines to run predominantly on natural gas. Tanks 8 and 9 were removed, and in their place was installed a huge, demineralised water reservoir to feed the boilers. The fire protection systems on all other fuel oil storage tanks were upgraded to include a dedicated ring main and anti-spark systems. As further measures to eliminate potential ignition sources, a hot work permit system was enforced, and smoking was prohibited throughout the plant.

The electricity provider also made improvements to the operation of its fuel oil import and storage facilities. Procedures were introduced to put more scrutiny on incoming marine tankers; each cargo would be tested prior to offloading and if the flash point was found to exceed a minimum limit, the load would be rejected. Similarly, systems were put in place to limit the temperature generated in the storage tanks; at all times this was limited to at least 3 degrees Celsius below the minimum accepted flashpoint. This ensured that flammable vapours could no longer be generated in the tanks.

The company took extensive precautions to prevent the escalation of future incidents. Emergency response plans were written up, regularly reviewed, and updated. Working groups were formed with local fire departments, bringing all parties together for the discussion of safety and training issues. Additionally, a dedicated emergency brigade was established onsite. This was equipped with tankers, rapid intervention trucks, and all other apparatus necessary to guard vigil over the facility.

El capitulo final

So, what has now become of the Tacoa power plant, 40 years on? The vital infrastructure of the *Ricardo Zuloaga Generator Complex* went on to provide reliable electricity to millions of Venezuelans for years after the incident. During this era, the country's generation and power grid was described as *"the envy of Latin America"*.

In 2007, Electricidad de Caracas was nationalised, bringing its assets under the control of state-owned, Corpoelec. As part of this shift, the facilities were renamed as the *Josefa Joaquina Sánchez Bastidas Generator Complex*. In the years that followed, Venezuela has suffered from a prolonged socioeconomic crisis, which persists to this day. With a lack of government funds to maintain public infrastructure, it appears that the generator complex has fallen into disrepair and is no longer operational. In recent years, return of power generation capability to Tacoa has become highly politicised against the backdrop of a national generation deficiency and frequent *mega-blackouts*. However, rumours persist that the plants are being permanently dismantled.

The enduring legacy of the Tacoa tragedy is that the NFPA and API updated their guidance to recognise the potential for boilover in fuel oil storage tanks. This change has influenced the safe design, operation, and emergency response of plants around the world. Whilst this is clearly a positive, it is disappointing that many of the other contributing factors from this incident were never disclosed. By not sharing freely our lessons learned, we do an injustice to those affected. Worse than that, we condemn others to a similar fate. Forty years on, it is surely time for the official investigations to be made public, and for Tacoa's full story to be known.

This article would have been much shorter had it not been for the help of Rixio E Medina. I would like to dedicate it to the memory of his dear friend, boss, and mentor, Ibrahim Alfonzo Ferrer. Ibrahim was the Corporate Manager of Industrial Protection at Lagoven (formerly Exxon in Venezuela) and was one of the many that perished in the Tacoa tragedy. I also extend my gratitude to Miro Popić, Maikel Popić, and Eric Omaña for the reference material they have generously provided.

Editor's note

Ramin Abhari's latest graphic novel depicts the events that took place at the Tacoa Power Plant 40 years ago and can be accessed at **https://www.icheme.org/knowledge/loss-prevention-bulletin/free-downloads/cartoons/lpb-cartoons/**

0260-9576/23/$17.63 + 0.00

Safety practice

Are all critical safety systems created equal?

David Black, Baker Engineering and Risk Consultants, Inc., USA

Summary

Industrial facilities generally embrace good practices related to maintaining comprehensive Process Safety Information (PSI) and making sure that Management of Change policies include proper documentation updates. However, those practices are not necessarily applied uniformly to fire protection and emergency response assets and systems. This can lead to significant problems when attempting to use fire and emergency assets or when conducting inspections, testing, maintenance, or repairs (ITMR) of these assets. This article will discuss the importance of maintaining engineering documentation for fire protection systems and other emergency response assets by applying the same discipline and attention given to other PSI to ensure those critical safety systems are available when needed and function as intended.

Keywords: Fire protection, emergency response

Introduction

Global safety practices have evolved over the past 30 years to include a strong awareness of the importance of maintaining proper documentation. The best practices ensure that unit design data, such as Process Flow Diagrams (PFDs), Piping and Instrumentation Diagrams (P&IDs), operating procedures, etc., are rigorously maintained and updated throughout the lifespan of a facility, and that changes to critical documents are managed carefully through good Management of Change policies. Where there is regulatory oversight of process safety, the maintenance of Process Safety Information (PSI) documentation is a pillar of that regulatory structure.

The level of attention paid to a facility's PSI may vary, but most operating companies incorporate at least the following basic tenants for their PSI:

- Documentation is kept in an accessible location known to all stakeholders;
- Documentation is strictly controlled to allow access to the information as needed, but ensures that no changes can be made without proper review and approval;
- PSI document changes and updates are included in the tasking associated with Management of Change (MOC) policies and an MOC task cannot be considered closed-out until the PSI documentation is fully updated to reflect the physical or procedural changes in the operation.

Background

Our company is engaged with helping operating companies in the oil, gas, chemical, petrochemical, and related industries be at optimum readiness to respond to emergencies. Various approaches are used, but the effort often includes activities such as protection system design reviews, fire hazard analyses, protective system inspections and testing, and policy/procedure development.

When clients are asked if they consider fire protection systems to be *safety-critical assets*, the answer is almost without fail, "Yes, of course." The question typically asked next: "Do you maintain and document those systems with the same rigour as process safety critical systems?" often receives very different answers.

If the answer is anything less than an enthusiastic "Yes!" then there is likely an opportunity to make improvements in the management and documentation of fire protection and emergency response systems.

Fire Protection Systems – typical documentation findings

All too often we identify major discrepancies in documentation related to a facility's fire protection and emergency response systems. Typical discrepancies often include:

- inaccurate, incomplete, or outdated firewater plot plans;
- missing engineering documentation on firewater delivery systems such as water spray, deluge, gaseous suppression, etc.;
- multiple versions of critical documents, with significant conflicting information between versions;
- inspection, test, and maintenance records that lack needed information or that are outdated.

Firewater plot plans

One of the most encountered discrepancies listed above is outdated or inaccurate firewater plot plans.

Typically, a basic firewater plot plan should show, *at a minimum*, a precise, accurate, and to-scale layout of the firewater piping below ground; the precise locations of isolation valves, hydrants/manifolds, and system risers; and the locations of fire pump installations.

In most cases, we have found that client firewater plot plans meet the basic needs as described above, but often omit other important details.

Better quality plot plans include additional details such as notations indicating the diameters and compositions of underground firewater piping, water spray and deluge system designed flow rates and pressures, fire pump designed flow rates

0260-9576/23/$17.63 + 0.00

Figure 1– Firewater flooding at site

and pressures, firewater source details, types of isolation valves (post-indicating, butterfly, etc.), and so on.

Most often missing from the documents are adequate details regarding multiple isolation or control valves in close proximity to each other. This is especially problematic if the valves are not properly labelled in the field, or if field labelling does not *match* the labelling on the plot. This can lead to delays in isolating lines for critical repairs, as well as mistakes in closing a critical line during an emergency event.

In many cases, plot plans do not reflect all significant changes that have been made to the site's firewater system after it was originally installed. Piping additions, upgrades, or changes made to these systems are often not captured on the plot plan. In some cases, a single plot plan paper copy may have been updated (red-lined) to reflect changes, but other copies maintained in the files or distributed throughout the facility do not show those changes.

Delivery system documentation

A plant's fire sprinkler systems, water spray systems, or deluge systems are usually designed to address specific needs of the equipment or area being protected. Systems are expected to deliver a minimum density of firewater over a covered area based on the specifications used for the design. For example, vessels containing Liquefied Petroleum Gases (LPGs) are often protected with an automatic water spray system designed to deliver[1] 0.25 gpm/sq. ft (10.2 lpm/m^2). The required total flow rates and operating pressures for these systems are dependent on the sizes of the piping and nozzles used, the length of piping throughout the application area, and other factors. The pressure and flow requirements are often displayed on the system's riser in the form of a placard or adhesive label. These details are also provided on engineering drawings and specifications that are usually delivered to the client when those systems are commissioned.

In the case of design drawings and specification packages, experience has shown that these packages are often misplaced, discarded, or simply "disappear" sometime after the system is installed. Attempts to locate system design data may take hours or days, if they are found at all.

To help ensure that the most important data is readily available, most professional fire protection installers will provide a rigid metal placard with the design details stamped into it, then affix the placard to the riser with a wire or other robust fastener. In some jurisdictions, providing such labelling is required by applicable building or fire codes. This helps ensure that important data remain on display at the point where testing and inspection parties are likely to need it most.

Other methods to post the design data on the riser usually involve an adhesive label applied to the riser pipe, with pressure and flow requirement data handwritten on the label in permanent ink. These forms of display are not as sturdy as metal placards, but as long as the riser and sticker are kept clean, dry, and out of exposure to direct sunlight, the data can remain available and readable for many years.

Unfortunately, hydraulic data placards can become detached over time. Wires or other fasteners used to secure them to the risers can corrode or break, allowing the placards to detach and fall to the floor in a riser room, potentially getting lost or thrown away.

Adhesive labels can wear out, or the adhesive can degrade to the point where the labels detach, and they then often get discarded as trash. Even if labels remain attached to the riser, the ink can fade due to environmental exposure, smudge from moisture or condensation (if a non-permanent marker or ink was used), or otherwise become unreadable over time.

[1] *API-2030, "Application of Fixed Water Spray Systems for Fire Protection in the Petroleum and Petrochemical Industries", 4th edition, American Petroleum Institute, Sept. 2014*

0260-9576/23/$17.63 + 0.00

Ultimately the system design data needs to remain available in its original forms, thus the original engineering data package for each system should be kept on file and updated as needed.

Fire pump and water source documentation

The heart of any water-based fire protection system is the fire pump or pumps used to supply the necessary pressure and flow to the delivery points. These pumps are among the most critical protective equipment in a facility, and their design documentation, piping diagrams, ITMR records, etc., are critical to keeping them operating as intended.

Fire pumps are designed and built to ensure that they perform in adverse conditions. The pumps and their prime movers (most commonly either an electric motor or diesel engine) are designed to specifications based on the requirements of the firewater application systems they support. Fire pumps must be able to deliver the maximum expected firewater demand flow and pressure to ensure a fire can be controlled with minimal escalation and damage. Failure of a fire pump or pumps during an emergency can mean the difference between success or failure of the response effort.

Firewater demands can change anytime a new unit or storage facility is built. Fire pump design details should be reviewed any time a site undergoes a significant change to ensure that the pump(s) and related components can handle changes to the firewater demand.

Fire pump operational and performance testing also rely on the availability of accurate and up-to-date documentation. Performance testing relies on knowing a fire pump's design ratings for flow and pressure, since that is used as the benchmark to determine if a pump is performing as intended. The records of previous tests are very important to establish trends over time and to note any changes to the system that may explain or help diagnose problems if they arise during testing.

In many cases, test records are maintained, but noted discrepancies recorded on those documents do not result in a work order or other action to remedy the noted discrepancy.

Figure 2 – Firewater flow measurement

Other types of system documentation

While there are many other types of systems and categories of documentation that are important to maintain, the above examples are amongst the most critical in a facility. The discrepancies discussed above are amongst the most common types encountered during fire protection studies at operating facilities.

Other types of systems that rely on important design, ITMR, and related documentation include gaseous suppression systems, mobile apparatus (fire trucks, trailers, etc.), fixed and semi-fixed foam delivery systems, fire and gas detection, and alarm systems, just to name a few.

Vendors and contractors that provide and/or install these systems are usually required to provide a full engineering package along with all operating and maintenance documents, procedures, and cautionary / advisory documents related to that system. Responsible parties in an operating facility should not only understand the documentation needed to care for all the different protective systems employed in their facility, but also ensure that documentation remains available and is properly maintained.

Why documentation matters

Fire protection systems documentation plays an important role in emergency response, system ITMR activities, training, and when planning site changes or expansions.

Emergency response

Identifying and addressing gaps in documentation for fire protection systems may not seem like critical priorities – that is, until you realise that you need that information urgently. Emergency response situations always require urgent access to the right information.

During a fire there is rarely time to track down needed documents such as emergency response plans, fire pre-plans, firewater plot plans, etc. In the case of emergency response plans and fire pre-plans, those documents help ensure that critical tactical information is in the hands of responders and incident commanders during the firefight, and it must be available and accessible without delay.

In the case of firewater plot plans, the urgency may not be as evident, but consider the case where a facility experiences a significant explosion followed by a fire. Even a relatively minor explosion can do significant damage to above-ground firewater piping in the vicinity of the blast. Ruptured firewater piping is like a cut in a major artery – the firewater can "bleed out" from a ruptured segment and deprive intact portions of the system of flow and pressure where it is needed to combat the fire. To limit that impact, responders must quickly isolate ruptured segments of the system and divert flows to surviving hydrants, firewater monitors, and fixed systems.

Emergency responders must rely on accurate and detailed firewater plot plans to find and operate the valves that will "stop the bleeding" in the ruptured segments of the firewater network. Without that documentation, isolation will be delayed while they attempt to locate and identify the needed valves. In a rapidly developing fire situation, this delay can turn an otherwise manageable situation into a catastrophe.

Even during a less urgent situation, prompt isolations may be

0260-9576/23/$17.63 + 0.00

necessary when there are unexpected leaks or breaches in a firewater system. In some cases, isolations may be preventive – sections need to be isolated before damage can occur. For instance, during a sudden freezing weather event, segments subject to freeze damage may need to be isolated and drained to prevent freeze-related ruptures, and to keep other areas operational. Finding and operating isolation valves in this case may not be as time-critical as in a fire emergency, but without access to a detailed and updated firewater plot plan, staff could spend unnecessary hours trying to locate, identify, and operate the proper valves.

ITMR activities

Inspection activities require appropriate documentation to locate equipment quickly and accurately when needed observations or measurements must be taken. Isolation valves need weekly or monthly inspection and exercising. Sprinkler or deluge risers need to be checked for valve alignments, proper pressure readings, etc.

Documentation becomes more critical during system tests. Plot plans and other forms of documentation help testing parties better understand the kinds of results they should expect from their tests and to aid in the diagnosis of unexpected test results.

Maintenance and repair activities also rely on proper documentation to help plan repairs, stage activities, and ensure that the maintenance/repair activities don't cause unnecessary impairments to other areas of the facility.

How to maintain proper documentation and manage changes

The following first steps will help establish the needed practices to keep fire protection and emergency response systems, and their attendant documentation, available and updated.

- **Include fire protection, detection, and emergency response assets in your company PSI policy**
  Recognise that non-process safety systems and connected process safety systems have equal importance. Expressly adding or including fire protection and similar systems to your corporate or site policies governing PSI documentation will help ensure that your systems and documentation are maintained with equal rigour and discipline.
- **Include fire protection, detection, and emergency response assets in your company MOC policy**
  Ensure change management applies to protection systems, just as it does for process equipment. This must include managing changes to documentation, just as is done for P&IDs and operating procedures.
- **Conduct periodic audits of protection systems' documentation**
  Even well-intended facilities can let their attention to protection systems lapse. The duties and responsibilities of staff cover so many details that not everything can always be an area of focus and diligence. Structuring periodic, focused audits of the policies and practices that govern fire protection and emergency response assets will help identify areas for increased attention and improve the execution and outcome of policies.

Conclusions

Maintaining good documentation and managing change properly is just as important for fire protection and emergency response assets as it is for process equipment and related safety systems. Unfortunately, fixed fire protection systems are too often the "forgotten" assets in a site's emergency response toolkit. They are easy to take for granted.

Instead of allowing fire protection systems to languish, competing with process safety systems for budget and attention, sites should align the two types of safety systems, managing them with identical sound policies and resources. This includes maintaining the appropriate documentation.

To do otherwise leaves a site relying on the "tribal knowledge" of emergency response departments to know where to find things, how they behave, what they're meant to do, and how to take care of them.

Tribal knowledge is always a useful thing but relying on it to keep your site ready for an emergency is an unnecessary risk.

0260-9576/23/$17.63 + 0.00

Safety practice

Four conduct of operations best practices — lessons learned from PSM audits

Adam M Musthafa, Indonesia

Summary

Conduct of operations is the performance of operational and management tasks in a deliberate and structured manner[1]. The aim is to have predictable and consistent personnel actions, capable and stable processes, and reliable equipment and plant operations[2]. During process safety audits, we discussed with the frontline workers and observed workplace conditions and process equipment to understand how the organisation formalises the communication process, control equipment status and process parameters and how operations activities are carried out. This paper discusses four positive conduct of operations observations from process safety audits in various major hazard facilities.

Keywords: Conduct of operations, shift handover, surveillance, logging

Complete and high-quality shift/crew handover

Shift/crew handover unfortunately is one of the processes that is prone to become a tick-the-box activity. Over time, shift changes can become incomplete, informal, or completely skipped[3]. Some audits have found that the shift handover form is signed without discussion between the party leaving the workplace and the one who will take over the responsibility. In a major hazard facility, even a small mistake and miscommunication can lead to major consequences. That is why safety critical communication like shift/crew handover should not only include the exchange of information through a standardised format, but also feedback and confirmation that the receiver fully understood the information being communicated. Figure 1 shows the overall flow of information within a shift operation with the handover meeting being the first critical meeting.

In an oil gas plant, there was a high potential near miss of having high level at a flare knockout drum. The high-level alarm and trip function at the knockout drum was bypassed at the time awaiting spare parts to repair the sensor. The night shift had a habit of draining the compressor scrubber manually (remote opening of the actuated valve from the control room) to the knockout drum to avoid the sour liquid taking its normal route to the production separator. This was done to reduce the consumption of the H_2S scavenger and avoid out-of-specification export as the condensed liquid from the compressor scrubber contained a significant amount of H_2S. By routing this to the knock-out drum, the H_2S was flashed first at the drum before being pumped back to the production separator which in turn reduced H_2S content in the crude oil export.

This practice was not communicated to the day shift. One day, the night shift operator kept the drain valve to the knockout drum open at the end of the shift. Liquid from the compressor scrubber slowly but continuously flowed to the knockout drum until it was almost full. Fortunately, the operator noticed it on time before the liquid overflowed to the flare stack. He started both knockout drum pumps to normalise the level and stop the flow from the scrubber.

While this near miss involved some design issues, we will focus on the handover process in this paper. Upon investigation, one of the root causes was found to be that the handover did not include this specific event of manual draining. Blaming the worker for not having the required conversation adds no value to the management system. It is vital to dig deeper to understand why handovers are sometimes ineffective.

During audits, workers were asked why some of these handover processes are not conducted properly. Usually, the frontline worker says that they are not given enough time to do so. Personnel leaving their station to go off-duty will be always eager to leave, so there is time pressure not only at a personal level but also from peers, and especially so if the site worker utilises a common transport means like buses or transport vessels (offshore). Their concern is that if they spent too much time discussing for handover, they will cause their colleagues to have to wait for them at the transport.

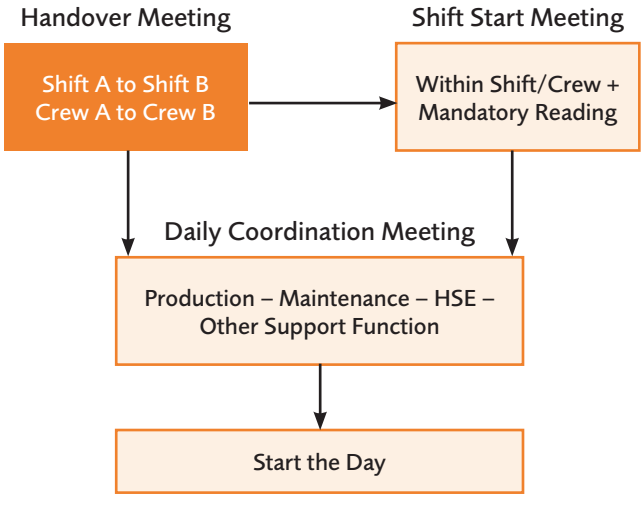


Figure 1 – Critical flow of information in operations

0260-9576/23/$17.63 + 0.00

Handover checklist	Shift logs and structure round sheets
Guide the discussion to be *structured and avoid missing topics:* Any safety or asset integrity issues (incidents, near misses, and any unwanted events) • Special activities conducted during the shift/crew operations • Ongoing, suspended, and terminated work permits (including lockout & tag out and change of locked valve position) • High-risk works precautions and specific instructions • Bypasses of safety systems • Discussion on the shift log and structured round sheets (see next column)	Facilitate discussion with *actual data and time of occurrence on:* • Process parameters and identified anomalies (including critical alarms) • Specific equipment issues • Structured round data collection missed/ not completed • Specific events/ activities

Table 1 – Checklist and shift logs and structure round sheets function in handover discussion

Crew handover is more critical as the incoming personnel may not be able to contact the outgoing crew if they leave the platform using a helicopter or transportation vessel. In one of the upstream oil and gas plants, the time for handover is formally set for a minimum of forty-five minutes. The superintendent would formally declare that it is time for handover when the incoming crew arrive, and everyone will start the discussion together. Personnel will leave and go to the transport together once all personnel have completed their handover properly.

Checklists, structured round sheets, and shift logs are used to guide the discussion (see Table 1). The handover checklist will guide the discussion to be structured and avoid missing information, while the shift logs and structured round sheets will provide additional information related to the time of occurrence of specific events, activities or parameter reading. For operators, this handover not only includes the parameters and activities conducted during the shift but also the anomalies they faced and what action had and had not been taken. The handover form will also be submitted to the supervisors not only to verify that the process had been completed but also to allow the supervisor to give additional feedback and or information in case something is missing.

In cases where outgoing or incoming personnel are not able to conduct the handover in person, the personnel shall inform the outgoing production supervisor. The handover form should still be used, and later the supervisor will hand over the information to the relevant personnel accordingly using the same form. When there is complex work or a situation that requires the personnel to be at the site together to discuss, they will inform the supervisor or superintendent to provide more time for them to go and discuss at the specific location.

A handover is a form of safety-critical communication. The organisation should consciously provide adequate time for this process to be completed properly.

Disciplined operational surveillance and logging

In addition to monitoring the information available in the control room, operators should physically inspect their equipment on regular tours or rounds[1]. Operations surveillance or structured rounds is a means of early identification of any abnormalities, deviation from the normal operating condition, and potential equipment degradation. Operator round sheets typically document the status/condition of field equipment every few hours[2]. During the surveillance or structured round, the operator usually also conducts field data collection (especially those not nodes at control room/ DCS), performs basic equipment care, and conducts a visual inspection of the equipment for any signs of degradation.

The commonly identified weakness is not having a structured and formal expectation, procedure, and form to conduct the surveillance and logging. Some operations let each unit develop their own format of logging form with different levels and scopes of surveillance. Other operations do not specify the frequency of surveillance or structured round, and in this situation, it is generally found that the practice degrades over time. In the worst scenario, the operator just writes the same parameter with the morning reading without reading the gauge/ indicator again at the site.

In one upstream oil and gas site, the structured round is fully defined with the recommended route, checklist of equipment to be visually inspected, what to inspect, the frequency

System/ Equipment	Action	Frequency	Acceptance criteria	Response to deviation	Observation
Gas generator (GM-101)	Record gas exhaust temperature	3 / shift	Normal operating range is 700-850°C	Report to the supervisor Initiate investigation Inform the instrument technician to confirm instrument accuracy	

Table 2 – Example of structured round checklist

0260-9576/23/$17.63 + 0.00

at which each piece of equipment needs to be inspected, acceptance criteria for the visual inspection/checks, and response required in case deviations are identified (see Table 2).

By having the acceptance criteria and action to be taken written, the operator gets "why" the structured round is required and important. When people understand the "why", they take the task more seriously. The acceptance criteria given also shifted some level of decision-making and analysis to the frontline level, increasing their engagement level and helping the organisation to identify signs of weaknesses early.

The implementation of the structured round is also measured and verified periodically. The number of deviations to planned round frequency and the number of deviations identified during the round are measured as leading indicators. The indicators are reviewed by management periodically and intervention is given whenever there are signs of weakening implementation discipline. Not only have the surveillance and logging become consistent, but they also become a reliable system.

Clear roles and responsibilities

Workers should clearly understand their authority, responsibility, and required interfaces with other work groups[2]. Everyone must understand clearly and acknowledge their responsibility. All equipment and system/business processes should be "owned" by a competent person who is responsible for monitoring and verifying the equipment or system's health, managing any changes and modifications, and maintaining the equipment's integrity and system effectiveness. The ownership should be as specific as possible. This should not be a group of people, for example, "process engineers", or the ownership will degrade.

In one of the audits in a utility plant that has multiple systems, three panel operators were working together. Upon being asked who has the final responsibility to attend to any of the boilers, gas turbines, nitrogen generators, waste treatment, and firewater system, the operators responded that all three shared the same responsibility. No one was assigned to particularly take responsibility for any specific unit.

For a major hazard facility, such arrangement should be avoided. Even when the work can be shared in day-to-day operations, each operator should be given a specific unit that has their "ownership". When the ownership is distributed and everyone needs to look after everything, it is quite common for people to depend on each other and assume it is "someone else's" responsibility[2]. This resulted in "nobody" assuming any responsibility in case any anomaly needed to be attended to.

In another organisation, the responsibility to maintain and coordinate process hazard analysis (PHA) was given to process engineers (three of them available with one manager). While the manager was accountable, they did not have the time to be the administrator of the system, and ultimately there was no systematic implementation as nobody was specifically maintaining the system. Each engineer waited for the manager to instruct them to do a specific task on maintaining the PHA system. During the audit, no approved PHA facilitator list had been developed. No refresher training for the PHA system was conducted. There was no risk communication conducted once the PHA for a particular plant was conducted to relevant personnel. Only tracking of HAZOP action items was conducted as part of PHA system administration.

In an organisation with clear roles and responsibilities, each equipment group was assigned an equipment owner. The list of owners was posted and everyone in the organisation knew to whom they should discuss if they had concerns, questions, or needed to modify something. The same thing was implemented for systems or business processes. These owners and delegates not only had personal ownership and accountability of the system but also become the subject matter expert on each equipment and/or system. Overlapping responsibilities are identified and eliminated. A simple tabulated list approved by senior management can be very effective to set and communicate this accountability (Table 3).

Proactive process safety observation program

Unsafe condition and unsafe act reporting where personnel conduct a walk or observe a task being conducted and identify positive and doubtful/ unsafe items has been a best practice in industry for more than 30 years. However, one aspect that most organisations are still struggling with is how to implement a similar program in process safety.

There is no doubt that process safety and asset integrity would benefit from the same observation program. However, the challenge here is not that people do not care about their equipment, but that they do not know what to report. Some personnel may struggle to identify what constitutes an equipment integrity issue. Others who are trained and experienced may have seen the same condition for years

Equipment group	Integrity owner Name (position)	Manager Name (position)
...	...	...
...	...	...
...	...	...

Process safety management system elements	System coordinator Name (position)	System coordinator Name (position)
...	...	...
...	...	...
...	...	...

Table 3 – Example of equipment integrity owner and PSM element coordinator/owner list

0260-9576/23/$17.63 + 0.00

that they no longer have the sensitivity to such issues. Some may even be reluctant to see or admit to degrading critical equipment as an issue (status quo bias).

In one of the audits, one chemical plant published a booklet to help people identify asset integrity issues during site visits and safety walks. This booklet not only helped newer workers to identify issues with asset integrity at an earlier stage but also refreshed more experienced workers on what good equipment working conditions should look like. Some of the examples shown in the booklet included:

- proper drain and vent or piping with end cap/blind
- picture comparison between acceptable vs non-acceptable corrosion levels on the valve, piping, and other equipment
- drain valve with splash guard for hazardous service
- picture comparison between cracked fireproofing or damaged insulation vs fireproofing and insulation in good condition
- picture comparison between proper bolting vs long and/or short bolting on joints and other relevant equipment
- picture comparison between properly supported instrument/equipment vs long non-supported instrument/equipment
- picture of how junction boxes and the electrical enclosure should look like (complete bolting, proper sealing, etc.)
- lifting gear with proper colour coding
- correct position of valves (inlet and outlet block valves of PSV should be locked open)
- fire extinguisher pressure is acceptable based on the green-coloured area or other visual cues on the pressure gauge.

Leaders should encourage the reporting of bad news[3]. By having more people engaged in observing and raising process safety and asset integrity issues, anomalies and equipment degradation can be identified earlier. In this organisation, observations that were process safety-related were monitored to understand personnel awareness and the imperative of process safety.

Conclusions

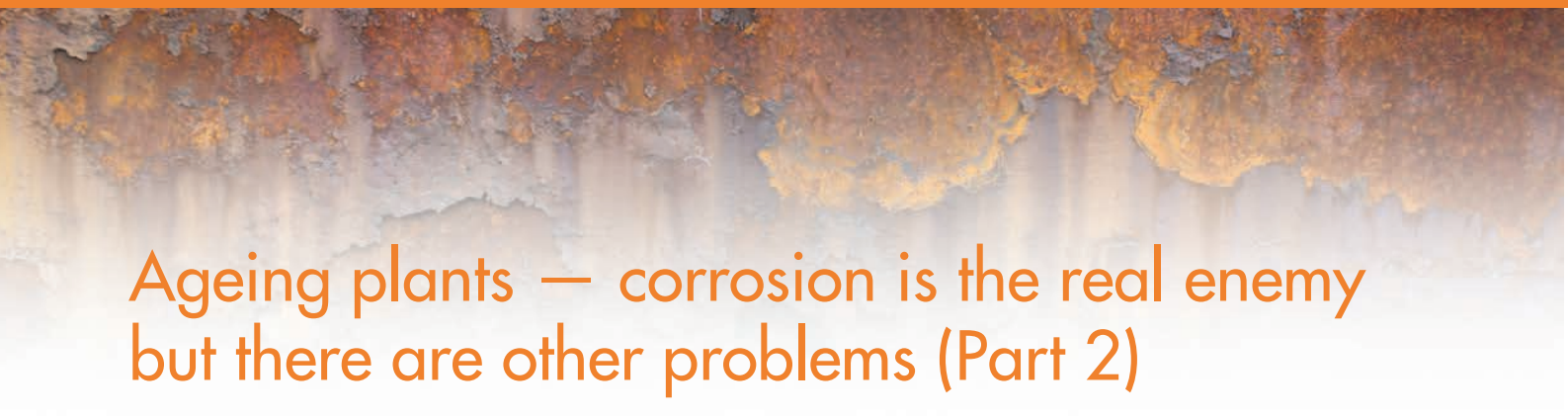
Conduct of operations is about how to make daily operations and operations management tasks structured and systematic. This paper discussed some best practices from various major hazard facilities. Firstly, the organisation should invest time and resources (to develop proper tools) to enable complete and high-quality shift/crew handover to happen. Secondly, disciplined operational surveillance and logging requires properly designed sheets with adequate information such as acceptance criteria and action in response to any deviation. Thirdly, clear roles and responsibilities should be established in safety-critical activities, including maintaining barrier integrity. Finally, to allow the organisation to implement a proactive process safety observation program, the collective competency of the organisation should be enhanced by providing the right tools and information to allow them to contribute to the program.

Reference

1. *Center for Chemical Process Safety. (2007). Guideline for Risk Based Process Safety. Hoboken, New Jersey: John Wiley & Sons, Inc.*
2. *Center for Chemical Process Safety. (2011). Conduct of Operations and Operational Discipline. Hoboken, New Jersey: John Wiley & Sons, Inc.*
3. *Center for Chemical Process Safety. (2018). Essential Practices for Creating, Strengthening, and Sustaining Process Safety Culture. Hoboken, New Jersey: John Wiley & Sons, Inc.*
4. *Center for Chemical Process Safety. (2007). Risk Based Process Safety. Hoboken, New Jersey: John Wiley & Sons, Inc.*

0260-9576/23/$17.63 + 0.00

Safety practice



Ageing plants — corrosion is the real enemy but there are other problems (Part 2)

Robert Canaway, Suregrove Limited, UK

Summary

Much has been written about the ageing of plants and concerns have been raised about the useful lifespan of industrial plants. This has arisen because most companies have had to prolong the deployment of their facilities beyond their intended life due to:

- worldwide growth increasing demand for products
- prohibitive costs for new replacement plants
- state employment requirements
- sales (often complete plants) to buyers

The main concerns are corrosion, erosion, wear and tear and obsoleteness.

Corrosion is the real enemy costing owners millions per annum in every country. It is one of the most potentially damaging losses to any commercial, private, or industrial property. An estimated one-sixth of all new worldwide steel production is used to replace corroded metal — corrosion problems are increasing in frequency and severity, not decreasing. The reasons for this are declining material quality (cheaper, less sustainable products are demanded for plants under design/construction) and inadequate corrosion control engineering combined.

Keywords: Corrosion, ageing plant

Critical aspects which can lead to failures and remedial measures (continued from Part 1)

Firewater systems

Systems in older sites may have been designed with poor deluge coverage (e.g., sphere or bullet wettage). There are guidelines in NFPA for the water rates in litres/m^2/min and the items to be deluged. Firewater systems often leak though corrosion as the headers are buried underground. Modern sites tend to use non-metallic firemains but these are of low strength. One aspect which should be evaluated is subsidence and collapse of ground through instability particularly from an earthquake event. For example, the firemain at Izmit refinery was shattered into 4000 pieces (17 August 1999 – 7.6 magnitude).

Passive fireproofing

This decays with time due to moisture ingress (particularly where freezing conditions occur during winter). The ice formed expands and lifts the passive fireproofing away from the structure – the trapped water causes structural corrosion. There is some progress in using different materials such as mastics in place of the concrete, but the compound has to be non-flammable, must not melt under severe ambient conditions or heat generation, and be cost effective.

Obsoleteness

This has accelerated with advances in electronic systems. A good DCS system will often last less than ten years even when upgrades are applied.

Some in-line instrumentation cannot be rectified unless the plant is shut down (with extended periods between turnarounds this has become a concern).

It is interesting to note that some older systems still in use today have, in fact, a higher reliability than some of their modern counterparts as they were 'built to last'.

Poor material selection

Cheap materials used for corrosive services (e.g., sour water strippers processing water containing acetic acid are often constructed from carbon steel). Where the acid condenses will eventually lead to vessel failure.

Poor quality steels with high impurities represent an opportunity for corrosion to progress. Change of process conditions which cause accelerated deterioration (more severe temperature, pressure, acidity, alkalinity). High sulphur, acidic or salty feedstocks require material upgrades to avoid rapid deterioration.

The use of material selection process/utility diagrams or corrosion identification PFDs/UFDs is highly recommended. In most mature plants the corrosion areas are known by the operator/owner.

Figure 1 a is a typical flowsheet marked up to indicate expected high corrosion areas.

0260-9576/23/$17.63 + 0.00

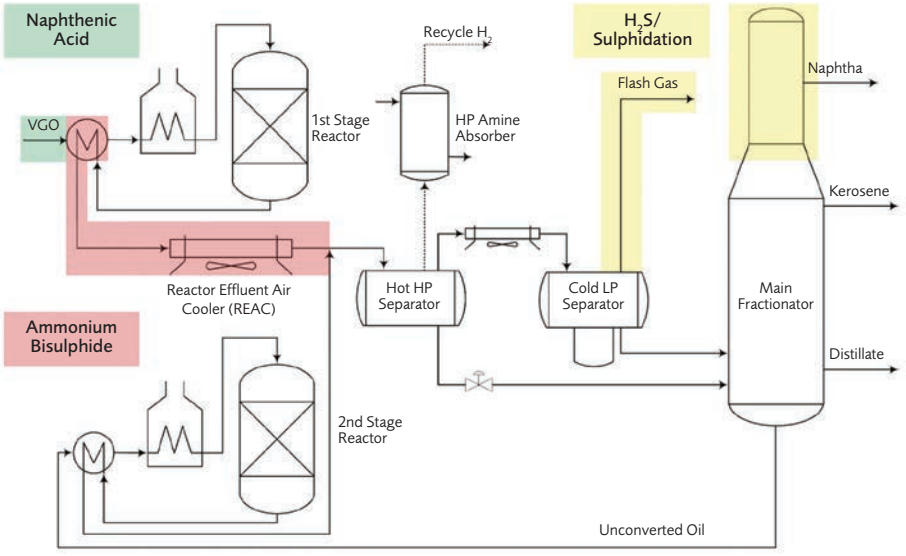


Figure 1 – High corrosion areas identified on PFDs

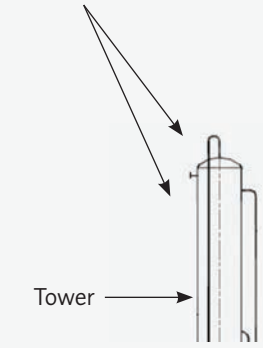


Figure 2 – Tower top

Difficult plant areas

Difficult plant areas e.g., vertical pipework for overhead lines which can corrode but cannot be easily inspected due to the elevation and compactness against the vessel top section.

A dead leg register for a site might contain 15000 items which should be eliminated.

Pipelines

Pipelines are particularly vulnerable when they are subject to:

- inadequate cathodic protection (none fitted or failure to operate)
- a change of soil conditions along the route
- stray electrical currents close-by
- biological effects
- water crossings, beach approaches
- stressing
- blockage from hydrates, wax
- low points allow water accumulation on the bottom segment
- gas lines may be subject to 'slug-flow' which occurs after cooling of the gas and formation of liquid.

Also, in mature sites there may be buried lines and accidents have occurred when excavating 'live lines'.

Repairs using clamps and wrapping which vary enormously. A simple G-clamp used to squeeze the pipe to prevent leaks, sealing compound and wraps are used in low pressure services. Welded sleeves can be used where the repair can take the maximum allowable working pressure, but these are expensive (a 48-inch line 100 bar pressure rated welded sleeve might cost USD 500000).

All piggable pipelines should be checked by an intelligent device every five years. The device travels along the route to find wall thinning and once this is ascertained to be a risk to the design pressure the pipeline should be re-rated and/or repaired. Pipelines are often constructed using 23 m lengths so a section can be removed and replaced.

Some operators use patch welded repairs which is not recommended for pressurised services – even for water services. Patch welds will corrode at the welded edge and are not completely reliable.

Control rooms and substations

Upgrading existing facilities requires a thorough study to ascertain the following:

- The true blast resistance of the building in bar which may vary from 0-0.7. Explosion prediction models can then be used to generate pressure contours (allowing for an accidental gas release, cloud drift and delayed ignition). If the predicted overpressure is larger than the building design parameters, then the building will not withstand the explosion forces. Re-constructing the building may be impractical (cost prohibitive) so the options will be relocation to a less hazardous area or construction of an annex which will be able to survive a blast situation. If DCS is replacing an old control system, the space required is often considerably less and this may be a suitable option (control room personnel safety and systems protection).
- Control rooms, substations and plant buildings with poorly sealed non-gas-tight doors and cable transits expose ignition sources and create hazardous enclosures. These deficiencies are often found on ageing plants and should be corrected. Positive pressurisation inside each building will prevent toxic and/or flammable gas ingress.
- Poorly designed HVAC systems encourage gas ingress and do not remove heat generation from electrical devices causing them to overheat. Often the design did not cater for heat dissipation and the high ambient temperatures experienced at various locations in the world. Buildings should have clean air intakes facing away from the process and also dampers activated by in-line gas detectors. If the building is under closed air condition, then the heat rise should be calculated to find out whether the equipment can still function properly.

0260-9576/23/$17.63 + 0.00

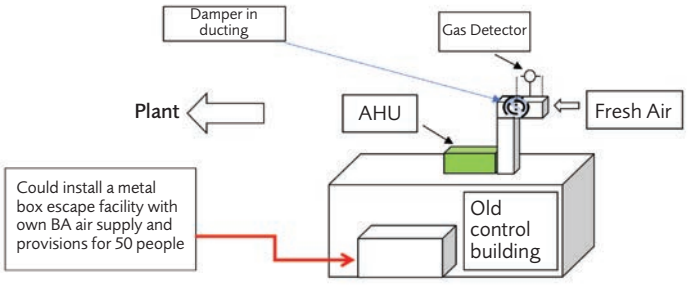


Figure 3 – Control building requirements

- Use of polyurethane sealers for cable entries is to be avoided – this type of sealant is flammable and porous (with age).

Boilers/furnaces[7]

Boiler/furnace condition deterioration begins with loss of firebox integrity, and this can cause hazardous situations as air ingress results in the formation of explosive gas mixtures (start-up) and obviously tube condition – pin-hole leaks, stress corrosion at hairpin bends, cracking of tube walls caused by over-firing. There is a useful life standard; 20,000-60,000 hours before replacement is typical.

Cross connected flue gas ducting is often found which can lead to operational problems for the stack and furnace and also increased lining corrosion.

Operators should make sure that there is enough dilution steam capacity to lower temperatures and prevent damage.

Sometimes older plants are found with primitive burner management systems which have poor interlocking of safety devices. All fuel lines should have double isolation (not using the control valve as one blocking valve).

Heat exchangers

Shell and tube exchangers can be subject to fouling, and this creates an environment for plugged tubes, corrosion and/or erosion.

Condition of stab reboilers (flanged mounted on column) is also a concern as the tubes often develop unnoticed failures and the design cost saving is not warranted.

Plate exchangers are often noted to develop leaks with ageing. They offer a neat space saving solution in some services but are not as robust as shell & tube designs.

Air coolers have poor mechanical strength and may not be robust enough for any significant changes in temperature or pressure (when revamping the plant).

Flare/vent/blowdown

Older plants often do not have any spare capacity in their relief systems so connecting more or increased relief loads requires expansion of the collection system. There is some benefit in using balanced pressure safety devices to cater for higher back pressures.

These systems are also subject to slow corrosion caused by sulphur/chloride deposits condensing in the pipework. Often material selection needs to be upgraded in plants with acid gases. Turning to Incoloy for flare headers is extremely expensive.

Block valves (locked open) often corrode (liquid accumulates at the valve), and they need to be repositioned (or rotated) to eliminate pockets (refer to API codes).

Relief devices including pressure relief, bursting discs can also fail due to worn out parts or fouling, it is useful to run a pre-pop test on all valves and produce a schedule of failure numbers. This should be lower than 1% but if it is up to 10%, increased frequency of testing is required (i.e., shorter time intervals between inspections). Testing should always be carried out on the 'as found condition' not after cleaning up.

Some older sites have process areas, spheres or bullets which are not connected to a flare relief system. It is a safer option to connect to a flare system for relief cases and environmentally better. There is often no or limited duplicity in older sites. The reason for this is that turnarounds were more frequent, and these were then serviced every two years. In modern units some plants run in excess of three years between turnarounds. It is not recommended to allow any PSV to remain in place over 36 months between tests.

Relief caseloads should be re-examined to ensure the relief valves are of sufficient capacity versus the latest codes.

Blowdown (depressurisation systems) are usually designed to API 521 where the pressure should be reduced to 50% operating in 15 minutes or 7 barg. The blowdown loads are split into fire zones (segments) so that a phased plant shutdown will not overload the flare system.

Drains/Sewers[9]

Problems occur with sludge or blocked gullies. In one case in South America the owner decided to excavate their sewers after 60 years' operations – there was over 600 tonnes of hydrocarbon sludge/soil in the sewer.

Rainwater drainage on mature sites should be checked when pooling occurs as this indicates the laterals are blocked with silt. If the plant does not drain the water will create a humid atmosphere and enhance external corrosion of the plant and damage to the passive fireproofing.

Besides foliage growing in drainage gullies other debris can accumulate such as gloves, plastic, solid product and so on. A flow test (using firewater) will determine blockage points.

Offshore facilities/jetties

Marine facilities require special attention – due to the high risk of corrosion from chlorides and water interfaces. Uninterrupted painting coats are required, neoprene sleeving for jacket legs extending 3 metres above the sea level and below can be used.

Marine growth (barnacles) which form a thick layer will increase the drag around the structure. Unfortunately, due to river and ocean pollution many facilities can suffer blockages including the firewater pump caissons. Seawater/river water for cooling must be equipped with filtering systems which are capable of removing trash.

Water systems[11]

Any metallic system which handles, processes or stores water in any form will corrode. The main concern is that these areas are usually left until there are flooding issues because water is not deemed a hazardous substance. By the time rectification is

0260-9576/23/$17.63 + 0.00

applied the system can often be beyond repair.

Many operators are deploying polyethylene or polypropylene piping:

Mechanism	Failure cause	Repair action
Internal corrosion – resulting in deep pitting	Acidic or alkaline conditions, free water promotes corrosion, oxygen ingress, light rust congregating in dead legs, low points	Low pressure systems can be replaced with PE or PP
External corrosion – bare surface pitting	Weathering (rain, snow), humidity or water spray causes wet conditions, change of soil line conditions for buried lines	Low pressure systems can be replaced with PE or PP

The advantage of substitution to polymer material is the elimination of corrosion (non-acid services, moderate temperatures and pressures) but these materials do not have high strength and can be damaged by vehicles being used on-site (cranes and maintenance vehicles).

Leak detection on pipelines

Basic material balance devices cannot pick up small leaks due to accuracy limitations. Significant leakage is detected by pressure loss or gas detection. There are guidelines for re-pressure testing. Attempts to counteract loss of pressure by increasing flow is the wrong selection (reference Ufa LPG leak 4 June 1989 where trains ignited an LPG leak in a valley).

Fire/gas detectors

These should be regularly tested and replaced as the detector often becomes poisoned by atmospheric pollution. Many older sites have 'common fault' fire and gas alarms which indicate a malfunction but do not identify the precise location (detector number). It is interesting to note that newer designs often have twice as many detectors in the field than older designs.

Atmospheric storage tank floor plates corrosion

Atmospheric tanks corrode at slow rates – usually from water being present over the floor plates and this causes pitting (see case study 2). This is accelerated by floor plates being in contact with the underlying soil and moisture (absence of insulating barrier). API recommends that an internal inspection should be carried out on a ten-year cycle unless inspection data dictates otherwise.

Roof corrosion occurs on unpainted surfaces and underside where condensation deposits chemicals such as sulphur. Tank shells are more resilient but there can be corrosion at the circumferential weld between the shell and floor plates.

Scanning of the floor and annular welds should reveal anomalies but even this is not 100% reliable. Leaks for products are often detected by site personnel (smell or observation).

Refrigerated tanks often are double wall with insulation between. The insulation deteriorates with time and needs to be replaced or supplemented. This can often be seen by ice formation on the outside wall in areas where the insulation is underperforming. Double or triple walled tanks should not be de-commissioned unless they have exceeded their approved lifespan or problems have been detected. Warming up and re-cooling stresses the tank welds and may contribute to failures. Normally these tanks are in clean/dry service so the inner tank should not corrode.

Cup tanks (which have an outer bund for spillage retention) should always have annulus drains for removal of rainwater.

Inspection of tanks is a difficult task requiring careful scanning of all areas. The use of polymer-based coatings for the bottom 2-3m is often helpful in controlling water-based corrosion.

Pressurised storage

Spheres and bullets are more resilient to corrosion. This is because they are usually handling water-free clean products and the product vapour pressure maintains an oxygen free environment. The main concern is when these items are insulated, and the storage temperature is lower than ambient. Water condenses under the insulation resulting in pit corrosion.

Particular attention needs to be paid to the condition of the shell welds (completeness and any corroded areas), the leg joints (where they are attached to the shell) – a deflector plate can be installed. Inspection should check for corrosion under the fireproofing coating to avoid collapse (some spheres develop longitudinal cracks in the legs due to corrosion caused by trapped water). Elimination of flanged connections and small fittings below the liquid level should be considered.

Mounded bullets (buried in soil) are often deployed to avoid the risk of Boiling Liquid Expanding Vapour Explosion (BLEVE); however, inspection is difficult to find corroded areas.

BLEVE (Boiling Liquid Expanding Vapour Explosion) risk can be eliminated by drainage away from underneath the sphere or bullet shadow and routing spillage to an open impounding pit.

Steel structures[8, 9, 10]

All steel structures will eventually corrode normally at high stress points, welds, bolted connections and at ground interfaces. These should have been adequately painted during construction and also regularly repaired. When revamping a mature site, the weight loading may increase, and additional supports are required.

Most warehouses are built using a structural frame and it is the roof which is likely to suffer weathering and/or corrosion. Many occupied buildings are built of reinforced concrete and have a long lifespan.

Caverns/underground facilities

Caverns and undersea voids are suitable for storage of hydrocarbons, waste gases. However, they have a finite lifespan before leakage occurs.

0260-9576/23/$17.63 + 0.00

Dust accumulation

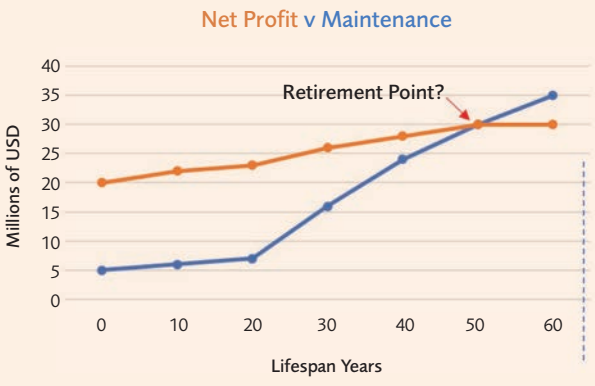
Many processes generate dust and in confined locations this may become airborne and be ignited to cause severe explosions (see case study 4). Dust accumulation particularly in confined areas such as buildings is always a risk and a health hazard.

Concluding remarks

This paper illustrates some of the key aspects in assessing the condition and corrective measures for ageing plants. Areas which require particular attention are:

- Condition of the facilities in particular the remaining thickness of all pipework, vessels, towers, drums, internals, and the expected lifespan. Inspection data is essential to assess the plant status.
- Any record of thermal cycling — too many startups / shutdowns – a new ethylene cracker which experiences 20 SUs or SDs in its first year will have aged ten years.
- Exposure to abnormal process conditions (severe pressure or temperature and/or change of composition or flow rate of processed fluids). This may alter the erosion/corrosion rates significantly.
- Weathering – particularly on coastal plants (jetties and structures which enter the sea; or are exposed to saliferous environments and high ambient temperatures).
- Submerged structures (such as support jackets which corrode or can collect marine growth causing drag effects).
- Flooded jacket steel structures members in offshore platforms which are subject to aggressive sea conditions and topsides exposed to increased sea wave height.

Figure 6 – Retirement point



Once the maintenance costs including any ongoing repairs approaches the net profit it is usually time to retire the plant. Any reduction in profit (for example a declining oil reservoir with higher water production) may lower the net profit) but unfortunately maintenance costs do not go down with age.

Some plants may be energy inefficient indicating a revamp is required to recover more of the waste heat or more modern equipment which uses less energy.

The key decision will be whether to continue operation or to retire the facility.

Retirement is usually based on:

- declining demand for the products from the plant
- the costs to continue and the net profit

Decommissioning can be expensive (removal of offshore structures) and demolishing and removal of existing plant is often demanded by authorities.

Key identifiers

- Change of feedstock and its impact on the existing plant, e.g., switching from a sweet crude feed to one which has high sulphur or contains naphthenic acids.
- Change of processing conditions – higher pressure, temperature, concentration, e.g., increasing the partial pressure of hydrogen bearing streams, solids such as sand entering the plant.
- Inadequate inspection data. Some sites have little or no data on the condition of lines, pipelines and the equipment; vessel nozzles may be in poor condition. Three sets of thickness measurements are needed to be able to trend the corrosion rate.
- Poor testing regimes for valves, infrequently operated systems.
- Inadequate 'mothballing' activities to protect unused plant from corrosion and deterioration.
- Poor storage of delicate spare parts, e.g., failure to store rotors for compressors in accordance with manufacturers' instructions.
- Incorrect gaskets, blind plates which do not meet the pressure rating of the line.
- Mismatch of materials particularly bolted connections. Note: the wrong bolt sizes are often found, short bolting and high stress levels caused by incorrect torquing procedures.
- Operation of systems, items way beyond their intended working life, e.g., bolted aluminium reboilers where connections have deteriorated due to the softness of the material should have been replaced every 15 years but are found to have been in place for 30 years plus.
- Obsoleteness – non-availability of plant components – leads to failure to replace instruments which are defective (or using inferior replacements).

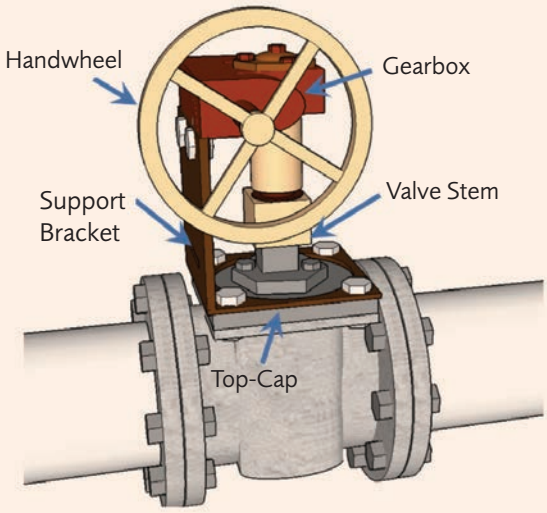
Case studies

About 70% of losses occurring in industry can be traced back to corrosion and most of these are concerning pipework failures releasing flammable materials which ignite and cause serious fires/explosion. Corrosion can be prevented but this requires investment in comprehensive inspection and corrective maintenance. There are other problems such as retention of obsolete designs which should have been replaced, and inadequate control /monitoring systems or allowing dust accumulation.

0260-9576/23/$17.63 + 0.00

Case Study No.1

On 22 November 2016, an isobutane release and fire seriously injured four workers in the sulphuric acid alkylation unit at a refinery in Baton Rouge, Louisiana. During removal of an inoperable gearbox on a plug valve, the operator performing this activity removed critical bolts securing the pressure-retaining component of the valve known as the top-cap (see illustration). When the operator then attempted to open the plug valve with a pipe wrench, the valve came apart and released isobutane into the unit, forming a flammable vapour cloud. The isobutane reached an ignition source within 30 seconds of the release, causing a fire and severely burning four workers.

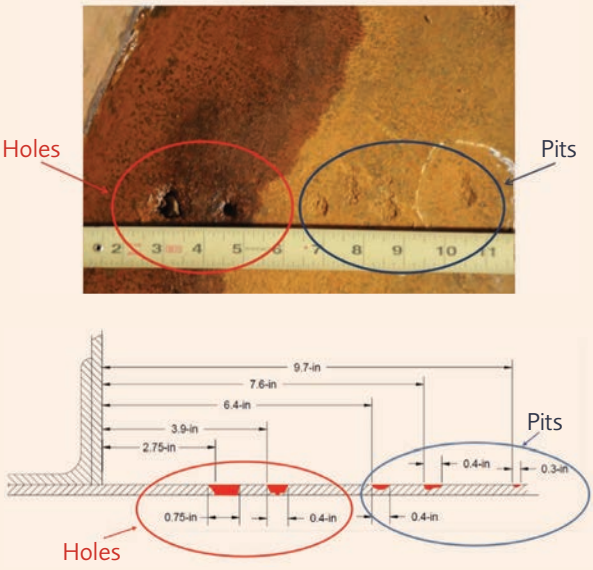


This type of valve should have been replaced or clear working instructions should have been given to the maintenance crew.

Warning signs are useful to indicate direct connections to the internal process for this type of configuration, but the best risk reduction measure is replacement.

Case Study No.2

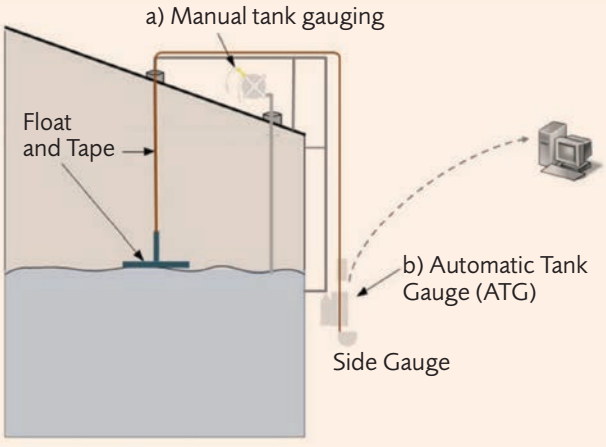
A chemical storage terminal tank leaked in Charleston, West Virginia on 05 November 2017 and contaminated the local water supply leaving thousands of residents without clean drinking water. The 20-foot-diameter tanks were most likely constructed in the late 1930s. The cylindrical shell and cone roof were of an obsolete, single lap-riveted construction. The tanks contained a 0.25 inch lap-welded bottom that inspectors estimated to be a replacement for the original lap-riveted bottom. The bottom interior of tank 396 was found to have deep, isolated pits or crevices near the shell (side) of the tank in addition to two holes on the tank floor, approximately 0.75 inches and 0.4 inches in diameter, which were the source of the leak.



The tank inspection was inadequate for ageing tanks and the advanced pit corrosion was not identified. This eventually made two holes in the bottom plate allowing a toxic chemical to be released into the environment.

Case Study No.3

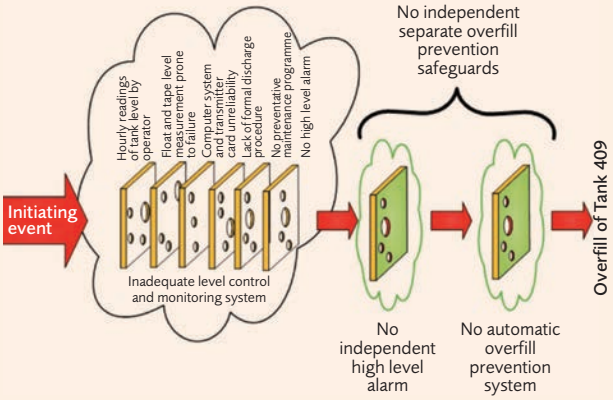
On 23 October 2009, a large explosion occurred at the CAPECO facility in Bayamón, Puerto Rico, during offloading of gasoline from a ship. A 5-million gallon aboveground storage tank overflowed into a secondary containment dike. The gasoline spray formed an aerosol, resulting in a large vapour cloud that ignited after reaching an ignition source in the wastewater treatment area of the facility. The blast and fire from multiple secondary explosions resulted in significant damage to 17 of the 48 petroleum storage tanks and other equipment onsite and in neighborhoods and businesses offsite. The fires burned for almost 60 hours. Petroleum products leaked into the soil, nearby wetlands and navigable waterways in the surrounding area.



0260-9576/23/$17.63 + 0.00

Multiple physical causes contributed to Tank 409 overfill:

- Malfunctioning of the tank side gauge or the float and tape apparatus during filling operations led to recording of inaccurate tank levels.
- Normal variations in the gasoline flow rate and pressure from the ship without the facility's ability to identify and incorporate the flow rate change in real time into tank fill time calculations may have contributed to the overfill.
- Potential failure of the tank's internal floating roof due to turbulence and other factors may have contributed to the overfill.



Case Study No.4

On 12 September 2010 in Cumberland, West Virginia an explosion in the production building was caused by combustible titanium and zirconium dusts that were processed at the facility. The explosion originated in a blender containing milled zirconium particulates and was ignited by frictional heating or spark ignition of the zirconium arising from defective blender equipment. The hydrogen gas produced by the reaction of molten titanium or zirconium metal and water, possibly from wash-down or the water deluge system, may have also contributed to the explosion. A dust collection system was not installed (refer the practices recommended in NFPA 484 for controlling combustible metal dust hazards).

Press Blade Damage

Most solid organic materials (and many metals and some nonmetallic inorganic materials) will burn or explode if finely divided and dispersed in sufficient concentrations. Even seemingly small quantities of accumulated dust can cause catastrophic damage.

Suspended dust burns rapidly, and confinement enables pressure build-up.

Purchasing aged facilities

Before acquiring assets from an owner, due diligence should be undertaken. In particular, examination of all inspection records and the plant availability data, review of the maintenance budget over the past five years, the loss record including near miss register and actual losses both in terms of physical damage and business interruption.

References

1. *Plant Ageing, Management of equipment containing hazardous fluids or pressure, HSE Research Report RR509, HSE Books, 2006*
2. *Plant Ageing Study – Phase 1 Report, ESR/D0010909/003/Issue 2, A Report prepared for the Health and Safety Executive, 27th February 2009*
3. *Energy Institute Document "Guidance for Corrosion Management in Oil and Gas Production and Processing"*
4. *NACE Corrosion Engineer's Reference Book, 3rd Edition*
5. *API 571, Damage Mechanisms Affecting Fixed Equipment in the Refining Industry*
6. *HSE Research Report 076, "Machinery and Rotating Equipment Integrity Inspection Guidance Notes"*
7. *API Recommended Practice 573, "Inspection of Fired Boilers and Heaters"*
8. *Concrete Repair According to the New European Standard EN 1504, Prof Dr Ing M Raupach, RWTH Aachen,*
9. *EN 1504, "Products and systems for the protection and repair of concrete structures"*
10. *BS EN 12696:2000, "Cathodic Protection of Steel in Concrete"*
11. *ISO 14692-4:2000, "Petroleum and natural gas industries -- Glass-reinforced plastics (GRP) piping - Part 4: Fabrication, installation and operation"*
12. *BS EN 61508:2002 Functional safety of electrical/electronic/programmable electronic safety-related systems*
13. *IEC 61511 Functional safety – Safety instrumented systems in the UK process industries*
14. *E/C&I Plant Ageing: A Technical Guide for Specialists managing Ageing E/C&I Plant*
15. *AEA Technology, Developments in electrification systems – Life expectancy of electrical equipment, AEATR-EE-2005-030, June 2005*
16. *HSE CRR 428(2002), Principles for proof testing of safety instrumented systems in the chemical industry*
17. *EEMUA 191:2007 Alarm systems - a guide to design, management and procurement*

0260-9576/23/$17.63 + 0.00

Safety practice

Proven techniques for effective implementation of inherent safety in design

Rajender Dahiya, AIG PC Global Services, Inc., USA

Summary

Inherently safer design (ISD) is a concept that intersects science and art, challenging the status quo to eliminate or reduce risk. Some companies within the process industry have successfully used ISD as an effective risk management tool to help them achieve world class performance.

This paper explains the important role leadership plays in implementing ISD concepts and provides insight into how incremental success can help establish a culture that embraces ISD. Scenarios where project teams experienced a challenge in surfacing new solutions through ISD reviews were identified as the author conducted risk assessments with project managers at complex high-hazard processing plants. The author observed that for some organisations the ISD review, once completed, checked the box and provided an inherently safer design regardless of whether new ideas were brought forward. In others, a robust set of best practices started to emerge, many emphasising ways that project teams can overcome the status quo, essential for safer operations.

The paper concludes with a list of "dos and don'ts" to consider as guideposts for implementing ISD into major projects and operating facilities within high hazard industries.

Keywords: inherent safety, safer design, hazard elimination

Introduction

In 1977, Trevor Kletz suggested that the most effective approach to process risk management was to focus on the elimination of hazards where feasible, rather than relying on safety systems and procedures to manage risk — loss avoidance as opposed to loss prevention, i.e. the loss cannot happen if the hazard is removed from the source[1].

This philosophy, now thought of as Inherent Safety in Design, is an iterative process that can reduce the potential for harm by eliminating or reducing hazards through four principles — elimination/minimisation, substitution, moderation, and simplification. While it is best applied early in a project's design phase, the concept can drive risk improvement throughout the lifetime of a facility. Case studies have proven that the benefits can be far reaching. They range from saving on the costs of maintaining the add-on safety features and safety protocols needed for a layered approach to protecting lives from an incident that never happened.

Yet today, ISD remains a hidden gem in the process industries. While it is not always possible to eliminate hazards, ISD should be the first approach to risk management rather than accepting the process hazards and immediately focusing on hazard management by controls. There are various narratives and theories being put forward as to why there has been low adoption. Misperception from value conflicts, engineering biases and implementation missteps have surfaced as leading contributors.

This paper focuses on how to bring down confusion, and successfully implement ISD.

Context

Hazard identification and risk assessment (HIRA) studies are the key activities in any design process and start at an early stage of the project. Hierarchy of process risk management strategies also called hierarchy of design solutions or hierarchy of controls are applied while performing these studies. Figure 1 shows a typical hierarchy of process risk management flowchart.

As shown in Figure 1, an inherently safer solution strategy takes priority over the use of passive, active and procedural controls (also called safeguards, barriers, or protection layers). However, HIRA studies such as Hazard Identification (HAZID), Process Hazard Analysis (PHA), Layers of Protection Analysis (LOPA), Quantitative Risk Assessment (QRA) are standard requirements in any project. HIRA studies are ingrained into today's engineering design package. They are proven, generally well communicated, well understood, and supported using experienced facilitators. Robust and ever evolving tools and techniques perpetuate the use of these familiar studies.

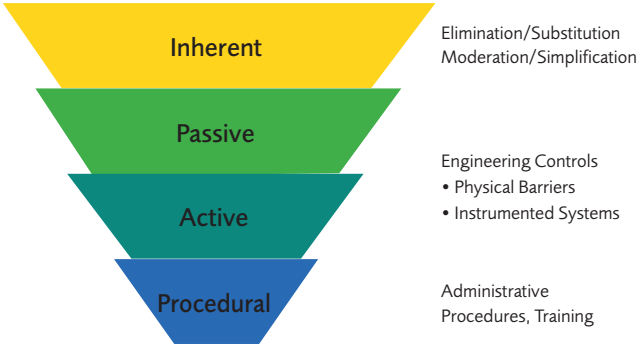


Figure 1 – Hierarchy of Process Risk Management Strategies

0260-9576/23/$17.63 + 0.00

Implementing an inherently safer solution strategy successfully takes courage, tenacity, and a different set of tools that can help an organisation overcome the status quo of focusing solely on engineering and procedural controls as priority strategies. It takes an acknowledgement and understanding of the intent of ISD.

Rolling out ISD baseline

For this discussion, it is assumed that companies implementing ISD have a solid foundation for project safety in place and that projects are managed using the stage-gate process. For each stage, an independent gatekeeper or subject matter expert (SME) is assigned to support the implementation. Experienced project teams, robust in-house engineering and design standards and specifications, and leading engineering, procurement, and construction (EPC) companies play a role in the success and safety of projects. It is also assumed that traditional design reviews and HIRA studies are performed efficiently, and that management wants to take advantage of the possibilities that a formal ISD review can offer.

Ensuring roll-out success, pitfalls

The intent of an ISD review is to only focus on inherently safer design opportunities. When ISD review is a new concept for the user, it is an activity that is done in addition to the traditional design process and requires extra efforts beyond checking a box.

Management's failure to fully understand the significance of the change required by the project teams and some of the pitfalls of implementation can be the root cause of ISD implementation mishaps.

In one case study, an ISD review was added to the stage-gate requirements, the team believed that everything was going well, and that the ISD review was well executed per the plan.

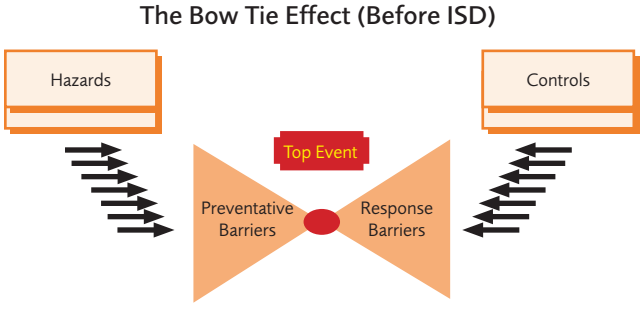


Figure 2 – Hazards Managed by Controls only

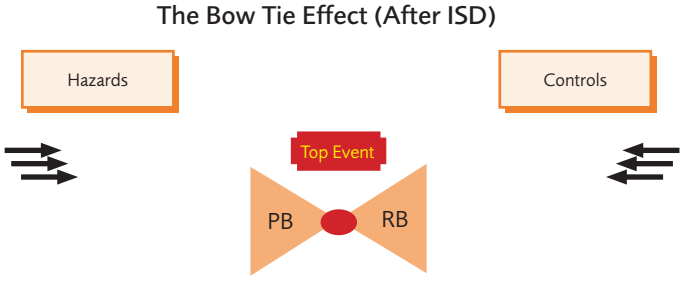


Figure 3 – Hazards Managed by ISD & Controls

Project teams were given an ISD philosophy that had to be met for a project to progress past each gate. There were detailed procedures covering all four ISD principles – elimination/minimisation, substitution, moderation, and simplification that were to be applied from concept through construction and installation stages, and some of the teams were even trained face-to-face.

Yet the outcome of the first ISD review showed no real change in the levels of risk and engineering controls being recommended as solutions. The review was not meeting the intent of the process. For this to be occurring at such an early design stage of the project pointed to insufficient training as a potential contributing factor to a low level ISD concept understanding.

An effective ISD review can be demonstrated using the bowtie. The bowtie is a simple graphical demonstration of hazard management. The more hazards, the bigger is the bowtie with multiple safeguards as shown in Figure 2. The intent of the ISD review is to reduce the size of the bowtie, and the only way to minimise the size of the bowtie is to eliminate the hazards at the source. Figure 3 illustrates where several hazards were eliminated or minimised and the remaining residual hazards were managed by controls. A resulting smaller bow tie is only possible when the ISD review is well understood and implemented.

Role of an ISD champion in the design phase

In this situation where the bow tie size remained unchanged, an ISD champion was brought in to help. An ISD champion can be instrumental in the successful adoption of ISD. The ISD champion's role is to be a subject matter expert, establish a baseline of understanding, and identify potential reasons why ISD was not being used as intended.

To establish the baseline, the ISD champion may look for pitfalls such as:

- Delivery: Is the philosophy and procedures delivered effectively with emphasis needed to ensure adoption of a new concept?
- Ownership: Is there that one "owner" who would be accountable for the outcomes of the ISD review?
- Communication: Are expectations communicated with the clarity and specificity needed to ensure the ISD review was completed to the point where risk elimination and risk reduction ideas were brought forward?
- Training: Is training being delivered by someone experienced in ISD and the organisation's processes?
- Training materials: Do they go beyond the basics? Is there any unintended bias towards old ways by emphasising on controls?
- Mythology: How are the ISD reviews being conducted? Are they conducted like a traditional HAZOP study in which the design is accepted "as is" and then controls are identified to help reduce the likelihood of an incident?
- Morale: Are there instances where people on the team are resisting the ISD review altogether? Was there discussion prior to implementation about the trade-offs and benefits versus the potential for added time to the project timeline?
- Excellence: How is the ISD review positioned within the

0260-9576/23/$17.63 + 0.00

stage-gate requirements? Is there more than a check-the-box line item in the gate checklist?

- Approvals: Is there any indication that ISD reviews are being approved with traditional control applications without demonstrating inherently safer design ideas or new techniques and solutions to eliminate/minimise the hazards presented?

Any one of these pitfalls can cause an ISD review to go off course.

What was wrong and why?

There are four categories of pitfalls that can contribute to an ISD review falling short. The case study above was used to dig deeper into the root causes challenging the successful implementation of ISD. It is essential to understand the pitfalls before best practices can be identified.

- Management program shortcomings
  - inconsistent standards and procedures
  - not fully vetted and communicated expectations
  - unavailable technical support
- Ownership and accountability gaps
  - no ISD program owner
  - no requirement that reviewers and gatekeepers avoid just "checking the box"
  - no method to ensure checking the box does not happen
  - no guidelines and examples that define what an acceptable report should look like
  - no quality check and continuous improvement cycle
- Training and competency
  - ensure ISD understanding across all levels of the project management, especially if ISD is new for everyone on the team
  - the benefits need to be prominent and illustrate relevancy to their immediate situation
- Culture, mindset, and communication

  With any change, there is conflict and a tendency to stay with the status quo. Special emphasis was required to influence project management and train engineers to "sell" this novel idea.
  - An ISD culture had not evolved — project managers were stuck with old techniques and old ways of thinking because they had no evidence that ISD offered enough benefit to overcome their requirements to keep the projects running smoothly on time and within budget.
  - Since everyone on the project team was experienced in traditional hazard identification and risk assessment methods, they naturally were using controls instead of challenging the norm through the ISD review. This line of thinking caused the process to derail.
  - One of the key gaps in communication took place during the hand-off of the design standards and processes to the project managers. With no communication that the ISD review was a pre-requisite to other reviews to determine engineering controls, the project teams fit the review into the regular design standards that had been used for years.

Senior leadership was informed that ISD was implemented and that designs were expected to be inherently safer.

Strategies, methods and techniques to address the gaps

The following new strategies, methods and techniques were adjusted to address the gaps and implement the process effectively.

The objective was to use an ISD to identify new ways to eliminate or reduce risk, leading to a safer process.

- Strategies
  - show how the current implementation was not meeting the intent of ISD
  - set clear expectations and communicate them
  - influence the project management teams on how ISD makes sense
  - provide effective training for facilitators and engineers
  - demonstrate by relevant examples that ISD does work and can work in this situation with the same people and resources by transforming the organisation's mindset and implementation methods.
- Methods and techniques

  To meet the objectives of the ISD process, the following methods and techniques were applied to educate the project management and instil the message of value, now and for the lifecycle of the facility. Seven steps were used to facilitate the necessary change.

  1. *Rejecting reports*
     - rejecting the ISD report, results in a failed stage gate
     - delivering an acceptable ISD report becomes the priority for a project manager to pass the stage gate
     - conducting an independent ISD review
  2. *Set expectations and objectives*

     Expectations need to be clear and succinct. Incorporate the expectations in the design package, stage-gate process and kick off meeting agenda.

The objective of ISD is to understand the hazards and eliminate / minimise hazards at the source instead of controlling them by complex and expensive safeguards. Once applied, the facilities are expected to be safer, simpler, and cheaper which are easier to design, build, operate, and maintain for their lifecycle

  3. *Influence management to embrace the change*

     Specific presentations and detailed training for management including project directors, project managers, and gatekeepers need to be developed and delivered. This training should use real-life, examples and benefits that would resonate with their corporate agendas.
  4. *Train end users to understand and be effective*

     In-house and EPC engineers and designers should also be trained using new detailed training materials that are consistent across the standards and procedures and again, use project specific relevant examples. In this case study, several hundred engineers and designers went through this training.
  5. *Best use of resources*
     - high risk sections of the process should be the focus

0260-9576/23/$17.63 + 0.00

to get maximum benefit from investing minimum time and resources
- a small team of 4-6 engineers should be used compared to 15-20 engineers in a typical HIRA study
- each review should take a maximum of one day

6. *No compromise on quality*
The review and the reports were of high quality. No normalisation of deviation accepted. No check-the-box type of reports existed.

7. *Proved success*
The ISD champion facilitated the first review following the change in approach to ISD implementation. There were incredible, positive, and unanticipated outcomes.

- **Implementation method 1 – combined review**

After the training, project teams liked the concept but still were not seeing the value for conducting independent reviews. They insisted on adding the ISD reviews to the traditional design review process e.g., plant layout review, Piping & Instrumentation Diagram (P&ID) review, PHA, etc.

It was agreed to conduct equipment simplification review with regular P&ID review. This was a controlled setting where the project manager could experience failure early in the process.

The combined review did not work for two primary reasons:
- P&ID review is a matured established process in a specific mindset. That did not allow the review engineers to think outside the box when they were questioned using the ISD checklist.
- ISD questions were completely different to those of a traditional review process. The questions turned into a burden that annoyed the review team and interrupted their usual P&ID review method.

The review was scheduled for two weeks. However, after two days, review team decided that the ISD questions interfered with the P&ID review and brought no value.

This failure helped to strengthen the case for independent reviews.

- **Implementation method 2 – independent review**

This review was done at the end of the detailed design which had already completed the final Hazard and Operability Study (HAZOP). Engineers then wondered what could realistically be changed at this stage. The design and risk management were already taken care of, and the project was ready for construction.

The focus of this review was leak minimisation and process simplification. Checklist and guidewords were used to inspire the team to challenge their own design. The independent review involved:
- a team of engineers from owner and EPC
- a session kicked off with a one-hour training refresher on process simplification
- focus on high hazard processes based on flammable inventory, temperature, and pressure
- the use of plot plans and about 20 P&IDs selected in advance which were already HAZOPed
- session facilitation using the ISD checklist and guidewords
- no controls were discussed in this review
- review was completed in seven hours.

Overwhelming outcomes from a one-day review were recognised by the team. It was not expected in a seven-hour session after a detailed HAZOP that the results would include elimination of more than 70 leak points including piping, valves/flanges, sight glasses, instrumentations, etc.

The project manager was influenced with the outcomes and shared the real-life example with other project teams and thereafter independent ISD reviews were successfully performed with great results.

Inherent safety in operating phase

The best time to apply ISD is in the early stages of a project. However, there are still opportunities in the operating phase of the facility, although, typically with less impact. Taking advantage of the latest reliable technology, errors and mistakes can be reduced by making the operating practices safer, simpler and user friendlier.

The most common improvement opportunities to apply Inherently Safer Techniques (IST) in an operating facility are:

Modification of hardware/software – management of change (MOC)

Take advantage of the latest technology which is more robust and reliable during any modification or change.

- First round of hazard management should focus on ISD without discussing the controls at all. Then depending on the complexity and risks associated with the change, HIRA may be performed.
- Add ISD application to the hazard checklist in the MOC program as a trigger, for example, "Is ISD option evaluated before adding controls to manage the risk?"

Operating and maintenance procedures

A standard format that follows regulations and industry standards and fit for purpose simpler procedures are most effective and can minimise the chances of errors and mistakes.

- Current procedures should be made easily available and accessible either in electronic or physical form.
- Standard operating procedures (SOPs) and emergency operating procedures (EOPs) should be documented separately. Emergency procedures should not be buried deep and mixed with standard procedures.
- A shortcut on the desktop with a logical folder and path should take the user to the latest procedure in the shortest time.
- Emergency procedures should be in simple steps with a checkbox for each step. A hard copy backup of the emergency procedures is highly recommended for easy access during emergency.

Data collection and use

On one hand, digital technology has made life easier, and at the same time complexity is added due to the availability of infinite information and data.

- Identify and define what data is useful and collect only that data. Avoid the cases where tons of information and data

0260-9576/23/$17.63 + 0.00

is piled up, but only minimal useful information is available buried in the larger pile.
- Diligently design or buy the data collection and analysis tools which are fit for purpose and user friendly.

Training and competency

Computer based training is quite common and frequently used. However, in many cases it is not consistent with the procedures. Refresher training is commonly just a repeat of the same training.

- A needs-based training is more effective than repeating the same training as refresher training cycle.
- Appropriate and fit for purpose training techniques deliver better outcomes.

Software and tools

There are excellent and ever evolving software and tools in the market. These tools are used and misused in many ways. There are many cases where an expensive software is bought and implemented, but employees keep using their private spreadsheet and word documents. Those are not user friendly and do not deliver the end results. These software/tools include but are not limited to incident investigation, action tracking, and management of change.

- Before developing or buying any tool(s), define the requirements and expectations then use this as the purchasing guide — i.e., no advanced features which are not required.
- More complex and sophisticated tools are not necessarily better. A simple spreadsheet sometimes can be much better than a million-dollar software package.

Summary

Impactful training and only one day of dedicated effort with a message from one influential manager changed the mindset of an entire project management team. Educating the project management teams and demonstrating results can be the key to success for effective implementation.

Key learning

- An effective training program, with demonstration of benefits, changed the mindset of engineers who were stuck with their established "comfortable" practices. The engineers started thinking "outside-the-box" and taking advantage of new technologies.
- Each step of the process is important for effective implementation. A disconnect in any step can adversely affect the overall purpose of the process. There were multiple disconnects in this case that were resolved.
- The project resources were used to perform all activities including training and conducting the ISD reviews, but the outcome was worthless diluting the whole ISD purpose when it was not well understood, and benefits were not tangible.
- In addition to the independent reviews, ISD principles were applied in regular design reviews as an extension of the formal review. As mindsets changed and engineers started thinking differently, a new tendency was generated to challenge the status quo at each step.

Primary steps to implement ISD

- Write philosophy, a standard and detailed procedure exclusively for ISD review and not to mix with other risk management processes.
- Write key performance indicators and set goals.
- Ensure an owner with authority is in place and supported by upper management.
- Communicate expectations and check for understanding.
- Use a competent facilitator to lead the reviews.
- Review each step of the ISD program for effective implementation.
- Focus on the high-risk processes to demonstrate the largest benefits in the shortest amount of time.
- Conduct independent review first and then incorporate in the HIRA processes.

Conclusion

Eliminating or minimising the hazard at the source by applying inherently safer design is the first element of hierarchy of process risk management. Whenever there are opportunities for a new project or modifications to existing facilities, ISD must be the top priority before jumping to potentially expensive and complex safeguards that will require maintenance for their lifetime and have probability of failure on demand. The benefits can be surprising and long lasting.

The ISD process will only deliver the greatest impact if the intent and concept is well understood, and it is implemented with management commitment and employee involvement. Improving the company culture and elevating the morale of the employees are the cornerstones for success when using ISD. Well written robust management programs, a well-trained workforce and a strong corporate culture are important for best results.

While there are more opportunities to benefit from ISD in situations where engineering controls are used to reduce risk, it should be noted that it is not always practicable to eliminate or minimise all hazards to an accepted level using ISD. Residual risks are then managed by passive, active, procedural, or a combination of these controls.

References

1. *Inherently Safer Design: The Fundamentals by Dennis C. Hendershot, Center for Chemical Process Safety. https://www.aiche.org/cep January 2012.*
2. *Inherently Safer Chemical Process: A Life Cycle Approach. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2nd Edition, December 2008.*
3. *Center for Chemical Process Safety, "Inherently Safer Chemical Processes: A Life Cycle Approach," CCPS, AIChE, New York, 1996*
4. *Hendershot, Dennis C., "Process Minimization: Making Plants Safer," Chemical Engineering Progress, pp.35-40 (January 2000).*
5. *Achieving World Class Performance in Oil and Gas Industry Using Inherently Safer Design www.cetjournal.it https://www.aidic.it/cet/19/77/129.pdf*

0260-9576/23/$17.63 + 0.00

Accidents of the future – part 10

A selection of predictions from our readers

We invite readers to send their views on which accidents they expect to see over the next few years, why these keep happening, and what have we failed to learn.

Please visit https://www.icheme.org/knowledge/loss-prevention-bulletin/submit-material/ if you would like to share your ideas.

A mis-used fulcrum and lever system will result in a serious accident because one end of the lever 'slips' and causes a heavy force to strike an operator

Tony Fishwick

When has a similar accident happened before?
In the late 1970s – see below, and possibly many times since, though fortunately with less serious consequences. The operator in this case suffered a serious, potentially fatal, accident.

Why does it keep happening?
Insufficient care taken in moving or dislodging heavy weight.

What have we failed to learn?
Use of ad hoc, improvised methods of lifting or dislodging heavy weights is potentially hazardous – for example, ad hoc fulcrums and levers.

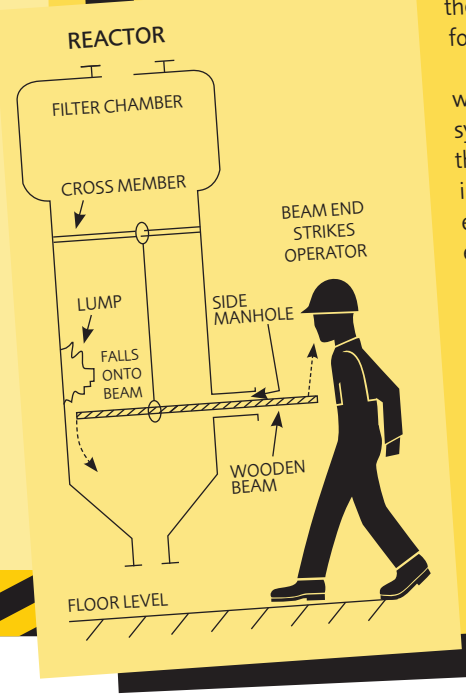
What steps could we take to prevent repetition?
Use proper lifting gear – externally applied force; forklift trucks; hooks and eyes; proper slings, etc.

Moment of madness

Every young physics student knows the principle of moments and its dependence on mass at each end of the lever and distance of that mass from the fulcrum (point of balance). Thus, moment about a point equals "mass" X "distance of the mass from that point."

A batch fluidised bed reactor was being cleaned out between reactions. A large lump of solidified product had stuck to the inside wall of the reactor – not an uncommon occurrence, it has to be said – see diagram. The method that had been used for many years was to suspend a wooden beam from one of the inner cross members of the reactor and swing it back and forth through the open manhole to strike the inside wall of the reactor until the lump eventually broke up into smaller pieces and fell to the bottom of the reactor. The lower edge of the manhole acted as a fulcrum.

The operator stood at rest for a few moments and placed the beam on the lower edge of the manhole. Whilst he did this, a huge weight of the lump – possibly as much as 50 kg – dislodged itself, fell onto the wooden beam inside the reactor, knocking that end of the beam down with very considerable force. The protruding end of the beam shot upwards and struck the operator in the face. It fractured his jaw and eyesocket and dislodged several of his teeth. He was very fortunate not to have been not killed and he did, eventually, make a full recovery.



The investigation into the accident banned the existing method of removing lumps from the inside wall of the reactors, where they could not properly be seen or accessed easily via the manhole. Instead, a system of suspending a lead weight outside the reactor was implemented. The weight was positioned so that it would strike the reactor wall on the outside exactly where the lump was adhered to the wall on the inside. It worked every bit as well as the suspended beam and was very much safer. There are numerous examples of the use of fulcrums and levers in industry, commerce and our everyday lives. A few examples are:

- Levering a full drum of powder or liquid out of a stack using an iron bar and a low brick wall as the fulcrum
- Levering up a full, or partially full pallet in order to get an empty pallet from underneath
- Levering up a full filing cabinet so as to move it on a sack truck
- Levering up the back end of a truck to change one of its wheels

Any of these could result in an accident similar to the one described herein because there may be no way of knowing, or estimating, the weight that would be released if the end of the lever underneath the item to be moved was accidentally, and suddenly, freed. The only safe way in such cases is to lift the item to be moved by such means as hooks and eyes (if they are present), forklift trucks, slings etc

0260-9576/23/$17.63 + 0.00

A trip will fail to operate which will result in a major accident hazard

Roger Casey, Consultant

When has a similar accident happened before?

- Wrong valve causes low level trip malfunction, LPB093 (https://www.icheme.org/media/6099/lpb_issue093p023.pdf)
- Hydrocracker accident, LPB089 (https://www.icheme.org/media/6049/lpb_issue089p013.pdf)
- Storage tank overfilling and double failure, LPB 247 (https://www.icheme.org/media/2112/lpb247_pg02.pdf)
- Buncefield: Why did it happen? (www.hse.gov.uk/comah/buncefield/buncefield-report.pdf)

Why does it keep happening?

Too often, people assume trips and interlocks will work. All trips do is reduce the likelihood of the event occurring, they do not eliminate it. A trip can fail for many reasons:

- Failure of the components of the trip. The sensor e.g. a temperature probe or a gas detector, the logic solver (e.g. microprocessor or hardwired unit) or the final element e.g. an actuated valve.
- Inadequate or incomplete testing of the trip.
- The trip being overridden or not re-instated properly after testing or repair.
- The setpoint has been changed.

What have we failed to learn?

All safety devices such as trips, relief devices, etc. have a failure probability associated with them. For example, in risk analysis a trip based on a basic process control system is often taken as having a probability of failure on demand (PFOD) of 0.1. A SIL2 loop has a PFOD of between 0.01 to 0.001 which depending on the consequences may be insufficient and additional controls may still be required.

What steps could we take to prevent repetition?

Hazard studies, risk assessments, etc. have to assume any protective interlock can fail and look for layers of safety in any major hazard scenario, compromising of additional different interlocks, relief devices or other engineered controls.

Adherence to international standards such as EN 61511. SIL assessment calculations must be performed by competent personnel.

See also Design and Maintenance of Instrument Trip Systems, LPB044 (https://www.icheme.org/media/5683/lpb_issue044p001.pdf)


Safety protocol

Hidden dangers

Phillip Carlos

IChemE

Correction

Loss Prevention Bulletin 288, December 2022

Figure 1 on page 20 of the print version of Issue 288, December 2022 had an incorrect heading. The correct version of the figure is opposite.

Table 2 on page 21 of the print version of Issue 288, December 2022 omitted the following reference:

2022(286),7	Propane release	Employers, contractors, environment

Awareness \ Knowledge	Known	Unknown
Known	Introduce control measures Publicise Monitor compliance/ effectiveness	Conduct research on hazards and risks
Unknown	Obligations to seek known information Conduct safety studies eg HAZOPs Constant attention to safety performance Follow up eg near misses, health complaints	Sense of vulnerability Creativity Proactive

0260-9576/23/$17.63 + 0.00

Information for authors and readers

Panel members

Loss Prevention Bulletin

Helping us to help others

- The *Loss Prevention Bulletin* (*LPB*) aims to improve safety through the sharing of information. In this respect, it shares many of the same objectives as the Responsible Care programme particularly in its openness to communication on safety issues
- To achieve our aims, we rely on contributions providing details of safety incidents. This information can be published without naming an affiliated author, and details of the plant and location can be anonymised if wished, since we believe it is important that lessons can be learned and shared without embarrassment or recrimination.
- Articles published in LPB are essentially practical relating to all aspects of safety and loss prevention. We particularly encourage case studies that describe incidents and the lessons that can be drawn from them.
- Articles are usually up to 2500 words in length. However we are also interested in accepting accident reports to be written up into articles by members of the Editorial Panel. Drawing and photographs are welcome. Drawings should be clear, but are usually re-drawn before printing. Any material provided can be returned if requested.
  For further information, see https://www.icheme.org/knowledge/loss-prevention-bulletin/submit-material/
- Correspondence on issues raised by LPB articles is particularly welcome, and should be addressed to the editor at:

  Loss Prevention Bulletin
  Institution of Chemical Engineers
  165 - 189 Railway Terrace
  Rugby, Warwickshire
  CV21 3HQ, UK
  Tel: +44 (0)1788 578214
  Fax: +44 (0)1788 560833
  Email: tdonaldson@icheme.org

2023 Subscription rates

Complete online collection
£564 + VAT

Print and complete online collection
£630 + VAT (UK)

Print and complete online collection
£654 + VAT (ROW)

The complete collection online provides access to over 40 years of articles, back to 1975. Multi-user site licences are also available. For further details, contact sales@icheme.org

Coming up in future issues of *lpb*

We are especially interested in publishing case studies of incidents related to:

- Organisation structure & process safety
- Emergency planning & response
- Ageing plant
- Lessons from other industries
- Management of Change
- Hazardous waste
- Hidden hazards
- Transfer of hazardous materials
- Electrostatic hazards
- Energy

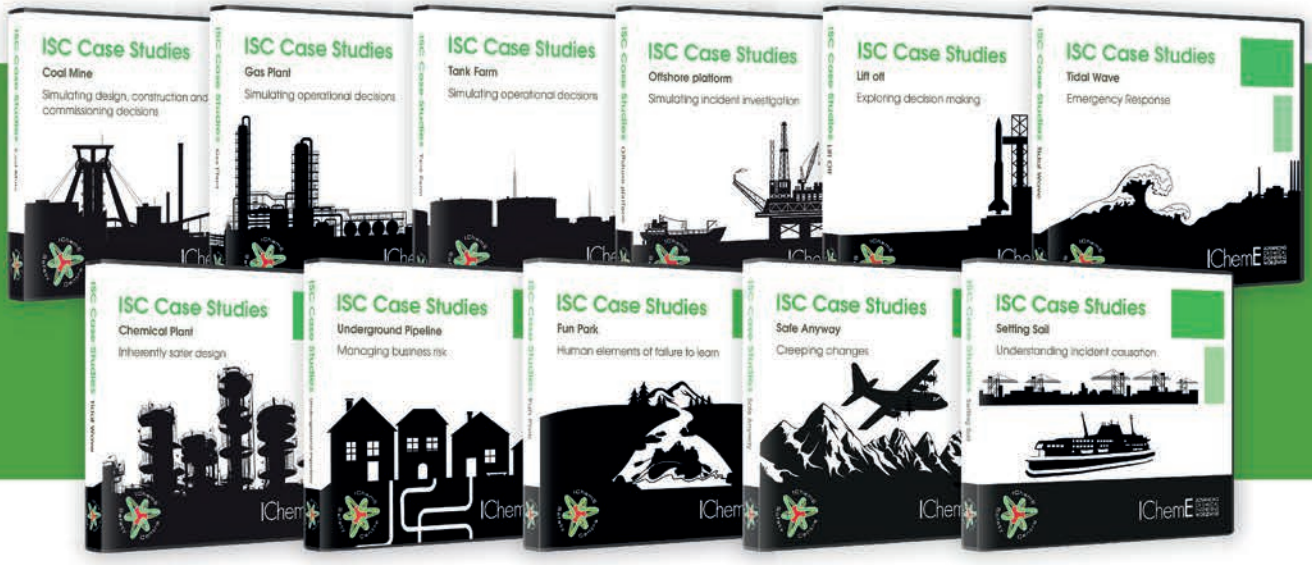
If you can help on these or any other topic, or you would like to discuss your ideas further, please contact the editor Tracey Donaldson on the number above.

0260-9576/22/$17.63 + 0.00

IChemE

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

IChemE Safety Centre



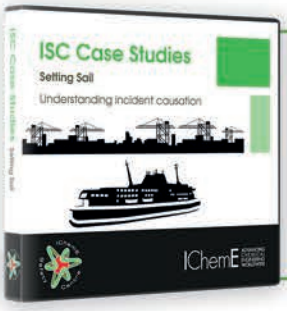
ISC Case Studies

Interactive safety training resources

Our ***Case Studies*** provide a rare opportunity to experience a series of process safety incidents as they unfold, in a real-time setting, without any prior knowledge of the outcome.

Throughout the training session, users will make crucial safety decisions and discover how each decision influences the incident.

This interactive approach helps to illustrate the complex causes behind the incident and enhance participants' understanding and application of process safety procedures.



NEW *Setting Sail* is the latest addition to the case study series. It explores the aftermath of an incident, determining who or what caused it to occur. It looks at the application of controls, as well as identifying issues with requiring people to prove something is unsafe.

www.icheme.org/isc-case-studies

LPB290