Lessons Learned Bulletin No. 15

Chemical Accident Prevention & Preparedness

Learning from incidents involving power supply failures

The aim of the bulletin is to provide insights on lessons learned from accident reported in the European Major Accident Reporting System (eMARS) and other accident sources for both industry operators and government regulators. JRC produces at least one CAPP Lessons Learned Bulletin each year. Each issue of the Bulletin focuses on a particular theme.

This 15th issue of the Lessons Learned Bulletin (LLB) focuses on industrial accidents originating from power supply failures. The LLB accompanies the upcoming publication of the JRC's technical report on power supply failure in industrial accidents. For this study, we analyzed 90 reports of chemical incidents in multiple industrial sectors where power failure was part of the sequence of events, either as an initiating event or as a secondary failure. When the cause of the power failure was internal, there may be two sets of lessons learned identified, one pertaining to preventing the power failure itself and another pertaining to preventing the loss of containment after a power loss occurs. The terms "incident" and "accident" are used interchangeably.

Please note:

The accident descriptions and lessons learned are reconstructed from accident reports submitted to the EU's Major Accident Reporting System at

https://emars.jrc.ec.europa.eu

as well as other open sources. EMARS consists of over 1100 reports of chemical accidents contributed by EU Member States and OECD Countries.

The bulletin highlights those lessons learned that the authors consider of most interest for this topic, with the limitation that full details of the accident are often not available and the lessons learned are based on what can be deduced from the description provided. The authors thank the experts who provided advice to improve the descriptions of the cases selected.

Case 1 –Explosion and release of a caustic mixture in an aluminum plant

Sequence of events

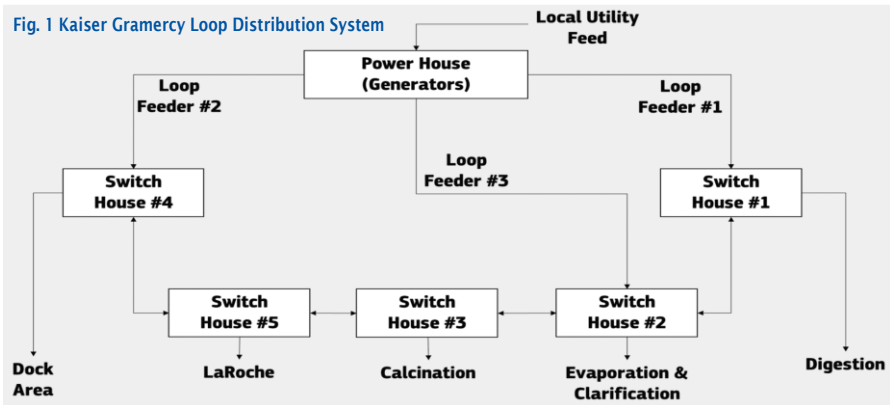
An electric fault in one of the plant's electrical switch houses caused a power failure in a metal processing plant while under normal operation. The single line drawing of the electrical loop distribution system is illustrated in Figure 1. The plant converts bauxite to alumina in a series of steam-heated pressure vessels. The power failure caused all the plant's electrically-powered process machinery to stop, including the pumps that moved slurry and liquor through the digestion process, causing the flow and pressure to back up through the tanks. However, the gas-fired boilers in the power house continued to produce steam, which began to build up in the desilicator and digesters.

The increased pressure in the tanks in the digestion area was not relieved as quickly as expected because the two pressure relief systems in the digestion area were not functioning properly. The pressure transmitter system that protected the digesters did not function because it had been turned off, shortly before the explosion.

Additionally, excessive accumulation of scale in the relief piping and the overflow pipe (that connected the blow-off tank to the relief tank) severely reduced the pipe's flow area, impeding its ability to relieve the increasing pressure in the vessels in the digestion area. Because of these various factors, pressure built up in the desilicator, the four digesters, the nine flash tanks, and the blow-off tank. All pumps stopped, including those circulating process material through the heat exchangers for cooling. Several vessels over-pressured and exploded releasing highly corrosive caustic material, causing injuries to the employees while extensively damaging the plant.

The investigation determined that the explosion occurred as a result of a build-up of excessive pressure within a vessel or vessels in the digestion area of the plant, and the subsequent rupture of the vessel or vessels. Rupture of the vessels exposed the superheated liquid contents to atmospheric pressure resulting in a boiling liquid expanding vapor explosion.

Fig. 1 Kaiser Gramercy Loop Distribution System



Source: United States Department of Labor. Report of investigation: Nonfatal Explosive Vessels Accident. Mine Safety and Health Administration. Arlington, VA, July 5, 1999. .https://ncsp.tamu.edu/reports/MSHA/msha.htm

MAHBulletin
TECHNOLOGY INNOVATION IN SECURITY UNIT
Directorate E - Space, Security and Migration
European Commission Joint Research Centre
21027 Ispra (VA) Italy *https://ec.europa.eu/jrc/*

European Commission

Number 15
JRC 125443

(Continuation from Case 1)

The force of the explosion injured 29 employees, many of them critically. It caused catastrophic destruction to the digestion area and released more than 400,000 pounds of sodium hydroxide into the atmosphere.

The explosion also caused glass breakage and minor structural damage in three towns within a 3-mile radius of the explosion. Several residents also complained of respiratory problems.

Important findings

The accident occurred due to two independent failures that intersected and resulted in disaster. The first failure was a lack of timely inspection and maintenance of the electrical power distribution system. The investigation determined that the electrical fault was probably caused when three transformer leads came into contact with a "bus", a rigid connection point for further distribution of electrical power. These leads had not been tightly secured and apparently had come loose, enabling contact with the connection point.

The second failure was the extraordinarily poor management of risks in the production process such that it had virtually no resilience in the face of a power loss. According to the investigation report, risk awareness was low among both staff and supervisors and deviation and ad hoc solutions to safety failures were accepted as routine at the plant. In particular:

- It was common for spikes in pressure to occur in the digestion process, resulting in the sudden filling of a flash tank with slurry, even though the relief system valves and piping were only designed to handle steam. During these process upsets, slurry could be ejected through the pressure relief valves into the pressure relief system piping. The slurry would then build up and harden in the valves and piping.
- Testimony also revealed that slurry discharge into the vapor lines was a constant concern of plant management, because the discharge contaminated the condensed steam that was collected by the heat exchangers. To keep relief valves from leaking in such situations, plant personnel routinely isolated the valves by closing the blocking valves around them. This also disabled the valves and had the effect of reducing the protection provided by the pressure relief valve system.
- The investigation stated that plant employees did not even have a superficial understanding of the operation of the digestion system. They had not been trained to recognize hazards, such as non-functioning pressure relief valves, and had no knowledge concerning the maximum operating pressures of each vessel, nor had they been trained to respond to unanticipated power failures.
- Moreover, the plant's supervisors on site at the time of the explosion were unfamiliar with its power distribution system, so that they could not identify the location of the electrical fault and quickly restore power.

Lessons Learned

Preventing electrical faults. Electrical faults usually occur either through the 'hard wiring' of the electrical distribution system or at the individual equipment level. Numerous errors in installation and maintenance can create conditions for an electrical fault. Hard wiring should be checked by a certified electrician and inspected and tested regularly to ensure no faults are developing in the cables and power outlets. Distribution boxes, switches and wiring can suffer wear and tear (aging) becoming inoperable or otherwise suffer a malfunction. The electrical equipment and facilities should be protected from temperature extremes, humidity and damp, and other sources of wear and tear.

Training on power failure scenarios and safe recovery. Plant personnel, both workers and supervisors, should have training on how to respond to a power failure to maximize safe recovery. Supervisors should be able to assess the power failure and take immediate and appropriate action to counter its negative impacts. Workers need to be informed of what can happen when a power failure occurs and their role in restoring the operation to safety.

Protect operations and equipment from unsafe actions. Process operations should not routinely create adverse side effects, e.g., contaminated vapor in the heat exchanger, forcing staff to take unsafe actions to avoid them, such as disabling safety equipment. The operator should conduct workplace examinations to identify conditions and practices that pose hazards and promptly correct them.

In the wake of a power failure, the fitness of operating equipment can often make the difference between an incident with no or minor impacts and a major catastrophe. The unsafe conditions in the digester operations also damaged the integrity of the safety equipment, creating blockages in the relief valves and piping. In particular, maintaining the integrity of safety equipment so that it is always available on demand should always be among the site's top priorities.

Ensure availability of overpressure relief systems. An inherently safe process design has to reflect all process conditions. Power outages can affect a facility's consumption units and the circulation of process mediums (through digesters, flush or intermediate storage tanks) while production units are still operational. Whether gas-fired boilers producing steam, or compressors/pumps connected to a separate power grid (that is not affected), emergency shutdown architecture (logic) has to take into account that any operating equipment upstream of the "black out" area needs to switch off to avoid overpressure. Piping, process circulation equipment and intermediate storage tanks downstream of processes where power was lost need to be able to accommodate any incoming flow originating from that area. At the same time, when production upstream stops, equipment need to be protected from breakdown due to continuous operation without process medium flowing through (e.g., compressors running dry).

***The sequence of events and important findings are adapted from**: United States Department of Labor. Report of investigation: Nonfatal Explosive Vessels Accident. Mine Safety and Health Administration. Arlington, VA. July 5, 1999. https://ncsp.tamu.edu/reports/MSHA/msha.htm*

Case 2 – Release of chlorine in a chemical plant following a failure of the public power supply

Sequence of events

A chemical plant suffered a temporary power loss when the public power supply was momentarily interrupted, and subsequently the emergency power supply also failed. In one of the installations, gas produced by a chemical reaction (a mixture of chlorine, nitrogen, hydrochloric acid and carbon dioxide) was being separated into various streams. Following the loss of power, 120 kg of chlorine gas were released at ground level.

A cloud of chlorine drifted towards a nearby waste-disposal company where 32 employees were working on the construction of a new chemical oven and notified the chemical plant of their distress. The site was evacuated, if somewhat chaotically, and the affected employees were sent to the hospital for medical check-ups.

(Continuation on page 5)

Chemical accident risk management against power supply failures; Prevention & Preparedness

Despite recent investments in smart grid technologies and alternative energy sources, power failures still pose a significant threat to all industries

Access to energy sources is critical for all industries. From chemical manufacturing, to refineries or warehouses, productivity and business continuity rely vastly on the uninterrupted supply of electricity. However, the potential for power failures may also contribute to chemical accident risk on hazardous sites. Unexpected power failures, e.g., triggered by a natural hazard event or equipment failure, can cause a loss of containment of a dangerous substance. When power interruptions and restarts are deliberate, they need to be planned in advance to avoid inadvertently causing release of a dangerous substance.

The Major Accident Hazards Bureau (MAHB) of the European Commission's Joint Research Centre studied reports of 90 chemical incidents from multiple industrial sectors to understand how and why power supply failures cause chemical accidents and identify practices to prevent them and mitigate their effects. The findings were analyzed to provide lessons learned to support risk assessment and risk management decisions on hazardous sites.

Impacts of power failure-related accidents on hazardous sites

The accident reports indicated that power failures on hazardous sites have resulted in 21 fatalities and over 9500 injuries worldwide since 1981, as well as significant property damage and production loss from resulting fires and explosions. The impacts from one power failure can be devastating. The most catastrophic event in the study occurred in Sakai (Osaka), Japan in 1982, that killed 6 people, injured 9,080 others (of which 8,876 were offsite) and destroyed 1,788 buildings. As another example, a power failure-related accident that occurred in Puertollano, Spain, caused 9 fatalities, 10 injuries and around €54 million in property damage with over 25% of the plant destroyed. It is notable that many incidents had significant offsite impacts, particularly from toxic releases. More than half of the cases (48 cases or 53%) involved a toxic release and of these, evacuation and shelter in place were ordered in 12 cases (13%). As a case in point, a power failure at a refinery in Antwerp, Belgium in 2008 caused the release of hydrogen sulfide. The toxic cloud traveled about 50 kilometers over Belgium and parts of the Netherlands, affecting several hundreds of people and causing 57 persons to seek medical care. Nonetheless, only a small number of cases (8%) had significant impacts on the environment, affecting mostly aquatic life. In one case, effluent from a sugar refinery was released following a power failure in 2012 polluting the Oeuf stream of Pithiviers-le-Vieil in France, causing a massive fish kill.

Power failures characteristics

Our study showed that there are a number of commonalities between power failures and hazardous sites. In particular, power failures:

- Are often unpredictable (i.e., weather conditions or pubic supply failures).
- Can affect multiple units and equipment (common mode failure).
- Can affect most industries with one or more unintended consequences.
- May destabilize units and compromise process safety, sometimes in ways that may not have been foreseen.
- Can have delayed impacts if process consequences are not recognised and controlled.
- Can have worse impacts when poor process safety practices have already weakened operator resilience.
- Can have significant impact on facilities even without loss of containment, such as loss of product from flaring, loss of revenue from plant shutdowns, and damage to equipment and buildings.

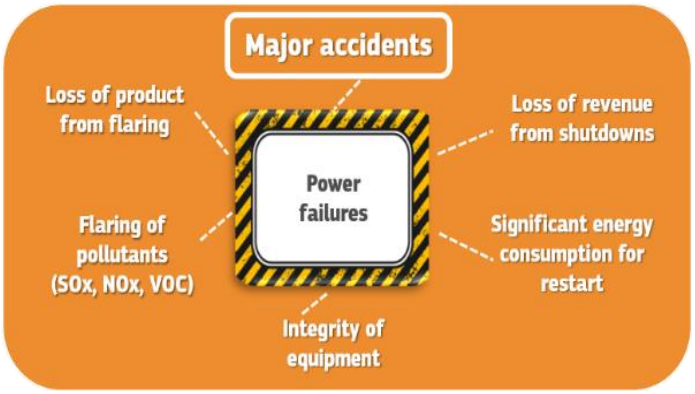


Figure 2. Impact of power failures

Scenarios triggered by a primary failure in the external power supply

Of the accidents studied, 34 incidents (or 38%) were initiated due to a loss of offsite power supply. Power failures or outages can be categorized into two distinct phenomena; blackouts and brownouts. Blackouts refer to a complete loss of power, whereas brownouts occur when facilities experience power disturbances, such as voltage fluctuations (partial outage), that can cause damage to electronics or equipment. Power suppliers may impose brownouts for load reduction in an emergency or in order to avoid a complete blackout. Each electrical apparatus may react in a different way to such voltage fluctuations, and some may be severely affected while others are not affected at all. Across the incidents studied, in 20 cases (22%) the public power supply failed while extreme weather conditions were reported as contributing factors leading to cascading technical failures and consequently power outages in 14 cases (16%). Electrical substations, either internal or external of a facility, as well as the power grid experienced failures following mostly thunderstorms (12 cases) or severe snowfall.

Chemical accidents that follow power failures are a combination of two accident sequences. The first accident sequence is the power failure itself, sometimes also followed by the failure of backup systems. The second accident sequence begins with the loss of containment triggered by the power failure. The facility's response to the power failure will determine to a great extent the outcome of the second accident sequence. A controlled response may entail triggering shutdown procedures or addressing the power failure by switching the facility's suppply to redundant power sources. Safe recovery from a power failure avoids a sequence of events leading to loss of containment and potentially a serious or catastrophic chemical accident.
Typically, power failure is followed by variation of one of the following circumstances:

- With the support of an uninterrupted power supply (UPS), connection to a backup power supply and/or controlled shutdown of the site
- With the support of a UPS system, the site continues functioning but the backup power supply fails, and the site goes into a controlled emergency shutdown
- Without a backup power supply, some processes, or the entire site, may undergo an uncontrolled emergency shutdown.
- Following the planned or unplanned shutdown, the site or specific processes will start up again. This is called recovery.

There are always high risks even in controlled shutdowns and startups. Uncontrolled emergency shutdowns entail even higher risks, but plants can still plan measures that can reduce impacts from these types of events.

Causes of primary power failure

The JRC study also found that the loss of primary power failure was mostly attributed to failures of onsite electrical equipment or electrical components (35 cases or 39%) as shown in Figure 2. Most electrical equipment failures were related to:

- Electrical switching and isolating apparatus, such as circuit switches and circuit breakers that failed to open or close on demand (13 cases).
- Transformers failing (11 cases).
- Short circuits (e.g., due to faulty equipment, loose wire connection), resulting in flow of abnormally high currents through equipment or transmission lines (8 cases).
- Defective cabling (due to improper installation or insufficient maintenance) (5 cases).
- Undervoltage (reduction in the system voltage) or overvoltage (swell in voltage levels), significantly affecting the "power quality" causing disruption of power to and from equipment (3 cases).

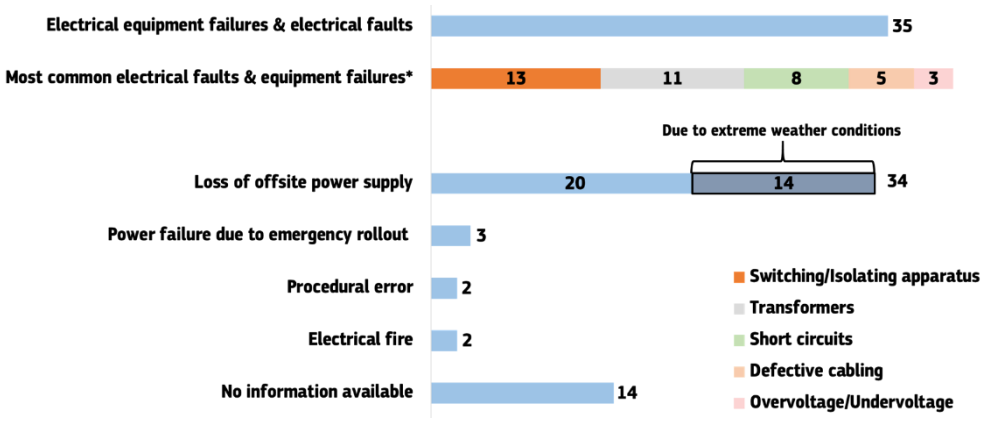


Figure 3. Causes of primary power supply failure (N=90)
(*Some cases have more than one failure)

Failures in the redundant power supply

In 33 cases (37%), redundant systems were in place but failed to operate successfully, leading to unsuccessful recovery from the primary power failure. The majority of failures related to the backup power systems were found in generators. Typical scenarios included:

- Failure of onsite generators (whether steam or fossil fueled) (19 cases).
- Failure in the switching operation between the primary power supply and the available backup systems (7 cases).
- Failure of the UPS systems (4 cases).
- Other common faults, such as short circuiits (4 cases) and overvoltage or undervoltage (2 cases) led to loss of the redundant power supply.

Impact of power failure on facilities

Electricity is used for a number of different purposes in process plants. Power failures will often affect facilities acting as common mode failures disturbing multiple process aspects simultaneously. Reactor cooling and agitation, for example, were both lost in ten cases (11%). In two of these cases, firefighting and alarms were also lost following a power failure. Power failures can, therefore, affect the smooth function of numerous plant operations, including:

- Operation of machinery, heating, cooling, presure safety valves (PSVs) and instrumentation.
- The basic process control system (BPCS), monitoring devices and alarm, and control mechanisms such as valves, pumps or agitators
- Safety critical instruments and emergency equipment

Moreover, digital control circuits may experience disruptions. During an undervoltage scenario, control signals may fall below the threshold at which logic controllers can reliably detect the represented equipment state (valve open or closed, motor pump open/closed or flowing downstream/upstream). Upon recovery the signal may differ from the actual position of the equipment, leading to blockades or flow contradictory to process intent.

Loss of power can result in a cascade of failure in a facility. Such cases have been observed where loss of power rendered boilers inoperable, consequently affecting the steam production.

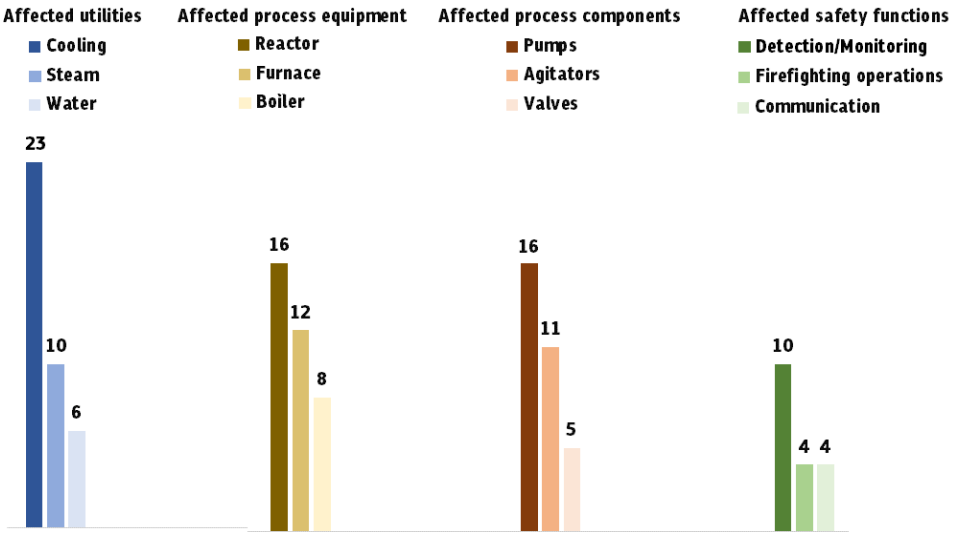


Figure 4. Process utilities, equipment, components and safety functions affected by the power failure (N=90)

Cooling was the utility most affected (23 cases or 26%) among cases in which power loss adversely affected one or more utilities, as shown in Figure 3. Loss of electrical driven pumps will result in loss of cooling since heat exchange depends primarily on continued pump operation, both for the process fluid and for the cooling water. A sudden current fluctuation may trigger the pump's motor overcurrent protection and stop the pump creating blocked routes. Cases where pumps tripped in an open position following a power outage, allowing process material flow unexpectedly have also been noticed. Other cooling equipment affected can include fans of air-cooled heat exchangers and fans on ovens or furnaces intended to avoid the formation of a flammable or explosive atmosphere

Reactors were found to be the most vulnerable equipment, since cooling and/or agitation over reaction mixtures were lost in 16 cases (18%) leading to potential runaway scenarios. In 12 cases (13%) furnaces, necessary for processes such as steam cracking, failed following a power outage whereas boilers, one of the most fundamental systems of a refinery or chemical processing plant responsible for steam production were lost in eight cases (9%). Other equipment affected by power loss included pumps, circulating process substances, firefighting water or cooling mediums (16 cases or 18%) and agitators for reaction mixtures (11 cases or 12%).

Mitigation and emergency response equipment lost functionality in a number of cases. Safety functions, such as gas detectors, as well as monitoring systems (e.g., level sensors) were affected by power failure in 10 cases (11%). In four cases firefighting operations, water hydrants or sprinklers, were deemed inoperable following the power failure, while in four more communication internally or externally to the facility was lost.

(Continuation from case 2)

Important findings

- Since the chlorine gas treatment unit failed, the gas should have been directed through a vacuum created by two fans to a scrubbing system to destroy the chlorine. However, without a source of energy the fans were stopped. At the same time, the security system required the valve opening up to the flare to close.
- The emission went unnoticed and no gas alarm was sounded because the chlorine, being heavier than air, passed under the chlorine detection system (located at a height of 3 m), and in any case, may have been inoperable also due to lack of electricity.
- Unfortunately, it took the operator nearly 8 minutes to inform the authorities of the release because the telephone network was also overloaded due to the general power failure.

Lessons Learned

Failure of the backup system. The plant was equipped with emergency power supply but it failed to function on demand. Most plants use an uninterruptable power supply (UPS) that protects the plant from input power interruptions. The power provided by the UPS is of short duration, only giving enough time for the plant to shut down safely, or for the backup generator to start up. The UPS backs up the digital control system (DCS) to keep control of plant operations until systems can be safely shut down or until the auxiliary generator kicks on. The UPS is critical to safety and diagnostic tests should be conducted according to recommended frequencies of the manufacturer and the battery should be replaced once it exceeds its life expectancy.

Failures of backup systems can be caused by corrosion, internal shorts, sulphation, dry-out, and seal failure that depending on the type of failure, may be caused by improper design (e.g., wrong voltage), improper storage conditions (e.g., high temperature, extended period without use), over usage, improper usage or the lack of maintenance, periodic inspectiond and testing.

Addressing the availability and reliability of backup systems, operators should:

1. Make sure that the backup systems do not fail under the same conditions that cause the primary power to fail (e.g., during a flood).
2. Try to find a solution (if possible) that allow the plant to safely shut down even when primary and backup systems have both failed.
3. If this is not possible, assess what would happen in case both systems are down.
4. Inspect, maintain, and test all backup systems regularly to ensure that they are ready to function on demand.

Risk assessment. The release of chlorine gas and the failure to detect the gas suggest that the risk assessment may have overlooked particular factors. It may not have considered that the backup power supply could fail. The risk assessment should also ensure the adequacy of detection systems and whether the fail-safe positions of control valves are programmed appropriately.

Communication networks. It is easily foreseeable that the public power supply would cause congestion of communication networks, as businesses and residents will seek to know what happened, or solve problems it may cause. Local authorities should work with the various stakeholders, e.g., network providers, hazardous operators, and emergency responders, to establish emergency protocols for communicating during crises, such as prioritizing certain interactions and clients, arranging for additional capacity, etc.

***Source**: eMARS No. 259, 15 November 1991, ARIA No. 14438*
https://www.aria.developpement-durable.gouv.fr

Case 3 – Ammonia release from a refrigeration plant

Sequence of events

Following a power outage, a refrigeration plant released 14.5 tons of anhydrous ammonia as a result of a series of procedural errors. At the time of the incident, the plant was in the process of loading two international ships with frozen poultry when the facility's refrigeration system experienced a hydraulic shock event that lead to a catastrophic piping system failure. The ammonia cloud released from the roof mounted pipe and traveled 0.25 miles across the river adjacent to the plant.

Three employees went to the roof and succeeded in closing the valves about 4 hours after the initial release. All other employees evacuated the facility to a location upwind from the ammonia release. Ammonia released within the blast freezer due to the failed evaporator coil contaminated 8 million pounds of poultry and packaging material. Ammonia concentrations were recorded as high as 7,275 parts per million (ppm) in the contaminated blast freezer later that day.

The majority of the ammonia was released through a compromised portion of the system's 12-inch suction pipe located on the roof. Ammonia was also detected within the facility as a result of a second leak from a rupture in the evaporator head of the blast freezer.

One of the plant employees sustained injuries after briefly losing consciousness from ammonia inhalation. Moreover, downwind from the release were crew members of ships docked at the plant's jetty as well as 800 contractors working to clean up an oil spill. Nine ship crew members and 143 of the offsite contractors downwind reported exposure. Of the exposed victims, 32 required hospitalization, and 4 were placed in intensive care.

Important findings

- Damaging hydraulic shock events are typically induced by condensation. They frequently occur in low-temperature ammonia systems. Condensation-induced shock events often involve the transition from high temperature and pressure to low temperature and pressure, during and after the defrosting of evaporators with hot gaseous refrigerant. The investigation concluded that ammonia released during the event was likely a result of condensation-induced shock, vapor-propelled liquid, or a combination of both, that ruptured the evaporator piping manifold and suction header.

Figure 2. Ruptured 12-inch diameter end cap of low-temperature suction line piping on the roof of the facility.
Source: United States Occupational Safety and Health Administration (OSHA), as cited in United States Chemical Safety and Hazard Investigation Board, Safety Bulletin, Key Lessons for Preventing Hydraulic Shock in Industrial Refrigeration Systems, Anhydrous Ammonia Release at Millard Refrigerated Services, Inc., January 2015

- On the afternoon before the incident, the facility and its refrigeration system experienced a loss of power that lasted more than 7 hours. While attempting to troubleshoot equipment issues after the system regained power, the refrigeration system operator manually cleared an alarm in the system.
- This resulted in an interruption of a defrost cycle that was in progress for a blast freezer evaporator.
- Because the operator manually intervened to clear the alarm and thus reset the control system, the control system did not recognize that the blast freezer evaporator unit contained high-

pressure hot gas when it allowed the suction stop valve to open during the system restart. Rather, the control system signaled the suction stop valve and liquid feed valves to simultaneously open in order to return the evaporator to cooling mode operation. This manual bypass of the programmed defrost sequence allowed the low-temperature liquid and hot gas to mix in the same pipe, causing the hot gas void to collapse as it rapidly condensed to a liquid. This created pressure shocks that ruptured the evaporator piping manifold and low-temperature suction piping on the roof.

- The employees attempted to isolate the source of the release while equipment upstream was still operating in order to avoid shutting down refrigeration for the entire facility. Thus, the release quantity was significantly greater than it would have been had they simply shut the system down. According to company procedure, the e-stop button should have been activated earlier by the plant engineer, but the engineer made a decision to locate and isolate the release instead.
- When the employees on the roof attempted to isolate the source of the leak, all other equipment connected to the low-temperature suction header was still in operation. Other blast cell evaporators kept operating and ammonia was stil being fed to the ruptured suction line. This caused an intermittent expulsion of ammonia as pressure from the evaporators increased upstream of the failure. If the employees had instead decided to use the emergency stop button located in the control room, they would have shut down the compressors and pumps, and de-energized valves. In this way, they could have stopped the circulation of ammonia into the other evaporators and decreased the quantity of ammonia that flowed out to the failed suction line.

Lessons Learned

Power loss may not be the direct cause of this incident, but the event underlines the significance of procedures and training when attempting to recover from power outages, especially when operators and personnel interact with process control and alarms. It also illustrates the importance of testing emergency preparedness and response using a power outage scenario. Moreover, this incident underlines the delayed consequences of a power failure if it is not addressed properly.

The investigation of this incident produced a number of important lessons learned that are specific to an unplanned interruption of an ammonia refrigeration system. Other types of facilities will have different procedures but the logic is the same. Appropriate barriers should be in place to ensure that an unplanned interruption does not result in an unplanned release of a dangerous substance.

Ensure that different substance flows can remain isolated and contained after an unplanned shutdown. Defrost control systems with interlocks should have been programmed to ensure the low-temperature liquid feed and hot gas remained isolated during the initiation and termination of the hotgas defrost cycle in the event of a power outage, cycle interruption, or other abnormal situation. Moreover, the defrost control sequence should have been programmed to automatically depressurize or bleed the coils in defrost upon restart after an outage or interruption, prior to opening the suction stop valve to set the evaporator into cooling mode. If feasible, automated processes should always be designed to prevent ruptures and releases caused by their abuse or by procedural errors.

Automate safe procedures for shut down and start up as much as possible. After an unintended interruption, refrigeration system operators could have avoided the need for manual intervention to the defrost cycle sequence by inserting a sequence of automatic programmes activated upon restart that automatically identified and bled coils of evaporators in defrost prior to the power outage.

Given it was a programmable hot gas defrost system, pump-out times should have been made long enough to ensure removal of a sufficient amount of residual liquid refrigerant in the evaporator coils prior to introducing hot gas, especially after low-load periods or power outages. Moreover, manual interruption of the evaporators in defrost and equipment control systems by unauthorized personnel should not have been allowed. A procedural error in the control system meant that there was no restricted access to control system modifications and manual override was possible. Had password-protected controls been in place, they could have been used to restrict access to only authorized personnel trained to modify the refrigeration system sequence and pump-out times.

Test and train on emergency shutdown scenarios. When it became clear that the ammonia release coud not be promptly isolated, the emergency shut-down should have been activated to de-energize pumps, compressors and valves instead of the attempt to isolate leaking equipment while the refrigeration system was still running. Shutting down the equipment would have stopped the circulation of ammonia and limited the release of additional ammonia from components running upstream of failed equipment and piping.

The accident information is adapted from: *United States Chemical Safety and Hazard Investigation Board, Safety Bulletin, Key Lessons for Preventing Hydraulic Shock in Industrial Refrigeration Systems, Anhydrous Ammonia Release at Millard Refrigerated Services, Inc., Jan. 2015. https://www.csb.gov/millard-refrigerated-services-ammonia-release/*

Case 4 – Fire in an electrical service room in a chemical plant and release of toxic gas

Sequence of events

An electrical fault on a cooling water pump caused a short circuit affecting the hydrazine hydrate unit of a Seveso chemical plant. Due to the fault, a fire broke out in the power supply switchboard C3, damaging the electrical infrastructure housed in the substation. Connection to the backup power supply could not be established while emergency power supply (UPS) was lost shortly after, resulting in complete loss of power as well as loss of the Distributed Control system (DCS). Since cooling was lost, the exothermic reaction in the hydrazine unit created overpressure. In consequence, a mixture of ammonia and steam was released to the atmosphere through a valve and the bursting disc of the unit's vent treatment tower.

During the incident, approximately 280 kg of ammonia were released, a large portion of which was brought to the ground by spraying set up by the plant's firefighters. The plant was shut down for a week with operating losses of thousands of euros, while the cost to rebuild the electrical substation was €430,000.

Important findings

- Power was supplied to the substation (DCS and the cooling pump circuit) through a transformer. A circuit breaker, placed upline from the electrical fault, could have isolated the fault, blocking it from shifting from the pump to the transformer, but it was stuck. Thus, the transformer caused a homopolar fault (short circuit). The circuit breaker upline from the transformer opened and the whole substation lost power.
- The fire spread to all components of the substation through the electrical cables. The electrical generator started, but the switchover could not take place as the connecting cabling was damaged by the fire.
- Smoke and heat from the fire migrated to a room in the proximity of the substation that housed the uninterruptable power supply (UPS) system. Once the temperature reached 40°C, the UPS switched to standby mode, disconnecting the power of the DCS.
- The electrical generators, designed to provide backup power supply, started, however, the power switchover could not take place as the electrical cables had been damaged by the fire.

Lessons Learned

Eliminate electrical faults and their propagation. Load shedding practices, minimization of cable lengths and techniques such as IR thermography can reduce the risk of heating faults and consequent short circuits in electrical cabinets. Independent fault detection systems incorporated on transformers, such as the Buchholz relay, can also assist in isolating the distribution grid from an electrical fault. Electrical faults can propagate from subsystems and cause unit or plant-wide power disruptions if isolation apparatus, such as circuit breakers don't trip on demand or fail to open (FTO).

Such failure can happen due to a damaged trip mechanism, incorrect trip timing, or incorrect breaker calibration, based on the fault current. A solid maintenance plan for electrical installations, including Inspection and testing of circuit breakers, can expose the potential for such failures and enhance the reliability and availability of these systems.

Power supply independence and critical equipment partitioning. The Distributed Control System must remain operational at least during the first 30 minutes following a power failure to ensure that the related unit has been sufficiently secured. Monitoring and control devices connected to that system are critical to unit's transition to safe state, thus a second independent electrical network should be available to take over and supply the DCS. Emergency power sources, such as the UPS, should be physically separated from electrical substations and independent from other electrical supply networks. Design of redundancy should also take into account and provide protection against common cause of failure, for example, a fire that can cause the breakdown of the primary and the UPS or the backup power supply. In this case, the fire was a common cause of failure for both the power switch and the UPS.

Critical utilities, including cooling, heating, steam, water, air, nitrogen or ventilation are prone to failure if electrical supply is lost. In that sense, utilities, such as cooling of reactors performing exothermic reactions, should be ensured by applying redundancy techniques optimizing components' reliability.

Switchover among redundant power sources. Power supply switchover between independent sources (whether redundant lines, backup or emergency sources) can fail due to equipment breakdowns, electrical fires, propagation of electrical faults but also failures in the switchover design logic. Examples of such failures are cases where the switchover logic was not designed to operate while both primary and backup power supply are online, resulting in a plant-wide power outage. In order to make sure that switchover between different sources is available and functions properly, the risk assessment should evaluate all potential power disturbance scenarios, as well as establish a solid inspection and testing plan of electrical installations.

Source: ARIA N° 28416, https://www.aria.developpement-durable.gouv.fr

Case 5 - Fire and flaring at the steam cracker unit of a petrochemical site

Sequence of events

A general loss of electric power, followed by a loss of backup power affected the establishment resulting in loss of steam supply to the steam cracker unit. Black smoke from the flares of the steam cracker unit was observed during the night, while after midnight flames were seen coming from a flue. Two distinct events were taking place: a loss of steam supply throughout the platform and a fire in a furnace of the steam cracker unit. Flaring was finally reduced by restarting the production installations and starting up the secondary boilers.

The operator launched its internal emergency plan, cut the supply hydrocarbons to the steam cracker furnace, lowering the intensity of the fire, which was controlled the following morning. By restarting the boilers, it was possible to reduce flaring, but black smoke was still visible until the following day. A total of 1,440t of hydrocarbons were flared over a period of two days.

Important findings

- The loss of electric power was caused by defects in junction boxes between two sections of thick buried cables.
- A loss of the main and then emergency power supply resulted in the loss of steam supply to the platform and, more particularly, to the steam cracking unit and consequently to the flaring system. The operator's steam-load shedding strategy was to first cut off the steam supply to the flare stacks (necessary to improve combustion) and then cut off steam supply to production units.
- The fire in the furnace of the steam cracker unit started when the tubes where the hydrocarbons circulated broke and fell to the bottom of the furnace. It would seem that the hydrocarbons then caught fire. The loss of steam shut down the furnace suddenly, which in turn led to thermal shock and damage to the tubes.

Lessons Learned

Ensure safe depressurization. During a power failure, units may need to be depressurized. This is normally happening via the combustion of process mediums through flaring. However, a power failure in many cases has affected the steam supply rendering the steam-to-vent gas ratio imbalanced. Consequently, the desired mixing of waste gases and steam is not achieved, leading to incomplete combustion of toxic gases with adverse effects on human life and the environment. It is important to avoid overpressure and consequent rupture of vessels or piping by depressurizing units via flaring. However, it is also crucial to maintain an uninterrupted steam supply for that reason. This can be achieved by establishing redundant power sources which are regularly inspected and maintained ensuring the uninterrupted steam supply. Production has to shut down before the steam supply is lost. Flush storage for potential waste or production substances in excess needs to be available to facilitiate unit depressurization.

Inspection and maintenance of electrical subcomponents. A junction box is typically a box with a removable cover that is used when connecting multiple sets of wires together. Wires are attached together by twisting the ends of the wire together and then using an appropriately sized wire nut or glance to secure them from disconnecting. These may need to be explosion or fire proof, metal or plastic. Similarly to any electrical component, regular inspection is required to ensure that wiring is tight and that protection from humidity, weather extremes or damp is in place.

Mechanical integrity. The steam cracking furnace is normally supplied by a feedstock (hydrocarbons) and steam, while the temperature of the furnace may vary from 500°C to 1100°C. The steam adds a huge value to the cracking process as it lowers the pressure of the whole operation and the partial pressure of hydrocarbons during the reaction of cracking. Common furnace shutdown sequence mandates a cool down to a temperature of 200°C at a gradient of 50°C per hour (a period of circa 13 hours) which should be controlled by supplementary firing. In case this sequence is not followed, and an abrupt furnace shutdown occurs, the risk of thermal shock in any component (e.g. tubes, flanges, refractories) is high. It is important to avoid such thermal shocks, by ensuring that any process equipment will transit to a safe state in a stable and incremental rate in terms of temperature. The same applies in cases of mechanical or hydraulic shocks; it is important to maintain stable and non-violent pressure and flow rates either while starting up or when transitioning to a safe state.

Source: eMARS N° 1172, 22 July 2018

Motto of the year

"Accidents are not due to lack of knowledge, but failure to use the knowledge we have."
T. Kletz (2009)

MAHBulletin

Contact

For more information on related to this bulletin on lessons learned from major industrial accidents, or if your organization is not already receiving the MAHB Bulletin, and would like to request to be placed on the distribution list, please contact

MINERVA-Info@ec.europa.eu

Technology Innovation in Security Unit
European Commission
Joint Research Centre
Directorate E - Space,
Security and Migration
Via E. Fermi, 2749
21027 Ispra (VA) Italy

https://minerva.jrc.ec.europa.eu

Please include your name and email address of your organization's focal point for the bulletin.

All MAHB publications can be found in the publications section of the Minerva Portal.

European Commission

Preparing for a power outage [1,2]:

- Have power failure scenarios been identified and evaluated in the hazard assessment?
- Does a solid Inspection and test plan form an integral part of preventive maintenance of the electrical infrastructure?
- Does the facility have an updated Business Continuity & Disaster Recovery plan (BCDR), involving all critical systems components? Is there any conflict between emergency response operations and the continuity of power supply?
- Is the BCDR plan properly communicated among all relevant personnel including top management and external contractors? Does the plan address actions during both short-duration and long-duration outages?
- Are the installations capable of relieving pressure in light of a process upset or while transiting to a safe state in a power failure scenario?
- Have all changes in electrical infrastructure and processes been managed in line with the Management of Change policy?
- Is process equipment regularly tested for vulnerabilities that could cause power disturbances and voltage fluctiations? Are critical components sufficiently protected against overvoltage and undervoltage?
- Are all safety critical functions (involving interconnected valves and pumps) available and operational in case of a power failure?
- Do pressure relief controls have the required capacity during a power failure? Is there enough storage for flushing?
- Are there specific standard operating procedures to manage power outages?
- Are there roles and responsibilities documented and assigned to personnel regarding the time before, during and after a power outage?
- Are there appropriate communication protocols in place?
- Does personnel training ensure awareness of power failure scenarios and procedures to follow for safe recovery?
- Has a power assessment been conducted to determine backup requirements and availability of critical utilities? Is it reviewed periodically?
- In the case of power failure, are there established emergency protocols for communication, internally and externally towards the emergency services and the public authorities (i.e public leadership)? Are these regularly tested?
- Are emergency shutdown response and recovery plans periodically tested?
- Has a priority list been established for power restoration? Have equipment/utilities/units that need to start first been identified?
- Are primary and redundant power sources independent? Is the transition/switchover periodically tested?
- Have any common mode failures originating from the loss of power been identified? Have potential failures that could affect emergency response been identified and addressed?

An emergency and preparedness plan could include the following, non limiting actions, in the event of power failure[1,2]:

- Conduct a thorough pre-startup assessment. Verify that no processes have been affected by the power outage and all units have been stabilized before startup.
- Verify the proper positioning of valves and operability of interconnected pumps according to process intent. A pump facilitating flow towards a closed valve will create overpressure.
- Assess the functionality of communication equipment and critical utilities, such as nitrogen supply, cooling water, steam and flaring, as identified from the process hazard analysis.
- Verify that any redundant system designed to provide power to the critical utilities along with any emergency response equipment (e.g., firefighting systems, alarms) is operating as intended.
- Verify that any monitoring or detection devices are operational and provide all the necessary information such as temperature or pressure. Some devices may require reset windup, such as feedback sensors or controllers, to operate properly following a power failure.
- Verify that downstream storage is available in case process mediums need to be "dumped" or removed from circulation to avoid overpressure or stalling (decomposition or polymerization). Also verify that the route towards storage is clear. Pump and valve positions should not block process circulation towards vats and containment areas.
- Apply load shedding strategies to prioritize startup of critical utilities and equipment while minimizing power demand on startup. Ensure that any automatic startup equipment should remain manually shut down to facilitate the load shedding.
- Notify any upstream or downstream users that may be affected by the shutdown of operations.

[1] *Incident Action Checklist – Power Outages, United States Environmental Protection Agency*
[2] *Chemical Accidents from Electric Power Outages, United States Environmental Protection Agency*