Process safety practice

# It's OK, we have a back-up

Roger Stokes, BakerRisk, UK

## Summary

Electrical power, steam, compressed air, nitrogen, hydraulic systems, other energy sources and key utilities such as cooling water are essential for the safe and reliable operation of many facilities. The provision of reliable back-up systems is necessary in the event that one of these supplies is lost. However, events have occurred where the loss of multiple systems, potentially originating from the failure of a single service or common cause failures, have resulted in consequences that were not considered by either the original or subsequent risk assessments.

Back-up systems are not always available, and operations/maintenance teams are often reluctant to fully test them in case they result in loss of supply or consequences that they were intending to prevent in the first place.

Hazard Identification and Risk Analysis (HIRA) should identify the requirement for back-up systems but might not consider events when these systems fail. Complacency regarding the reliability of back-up systems could lead to the "unsinkable Titanic approach", whereby site management and operational staff mistakenly believe the back-ups are sufficiently robust.

This paper provides some examples where back-up systems have failed and offers advice on design, operation, and maintenance to reduce the risk of failure. It discusses procedures, human factors, and emergency exercises that should be considered in the event of a total failure of back-up systems.

Keywords: Back-up systems, design and testing

## Background

The inspiration to develop this paper came from the Baltimore Bridge collapse that occurred on 26 March 2024, after the container ship *MV Dali* struck the southern pier supporting the central spans of the Francis Scott Key Bridge. A sudden loss of power generation on the vessel led to a cascade of events, including the effective loss of steerage and an impact resulting in not only the bridge collapse but also six fatalities. At the time of writing, the NTSB in the USA had not issued their final report. Further details are provided in case study 1. Considering how similar events have occurred in the process and power industries, lessons can be drawn from the Baltimore event.

Back in the 1980s, in ICI, there were detailed emergency procedures and a checklist-type booklet that was usually attached to the mimic panel in the control room. This booklet typically included instructions for events such as power failure, instrument air failure, cooling water failure, fire, bomb threats, etc., but did not always include multiple failures of services.

Today, the safe operation of our processes is even more dependent on reliable energy supplies and are usually provided with emergency back-ups for critical services. These can range from the immediate (albeit short-term) availability of a battery-based Uninterruptible Power Supply (UPS) to the engine driven generators that may take a minute or more to become operational, but can provide power for a longer period. Despite these measures, we continue to suffer from events where the back-ups fail, which can result in a cascade failure of multiple services. Unless there is a contingency plan for such eventualities, this leaves the operating teams having to innovate on short notice to safely control or shut down the process. This may result in sub-optimal solutions that could worsen the situation, especially where they do not have the tools, training, or experience to handle the situation.

This paper is intended to encourage facility management not only to consider the suitability and reliability of their back-up systems, but also provide procedures and training/exercises/process design improvements to help operations personnel optimise their performance in case the back-up systems do not work properly.

## Understanding the risks of energy failure in the process industries

The circumstances and scenarios associated with energy failure on supplies to equipment and control systems should be identified by methodologies such as HAZOP, LOPA, and FMEA. However, these may not always study the consequences of multiple failures, and it may be appropriate to consider such events separately. A dedicated study that involves examining scenarios where primary and back-up systems may fail due to a common cause or a domino failure of multiple services should be considered.

Potential consequences in the process industries could involve equipment damage, loss of containment, injury, fire, and environmental damage. These issues could arise for a number of reasons, including loss of process control of reaction (chemical/nuclear), loss of cooling or heating, thermal shock due to rapid cooling of fired equipment, loss of vent scrubbing/incineration, blockage by solids, or other abnormal situations during shutdown or even restarting after an unplanned outage.

## Identification of essential services

In many cases, sustaining all operations may be impractical




0260-9576/25/$17.63 + 0.00

due to the extensive energy requirements. Thus, the first step should involve the identification of services that are crucial for safe operation, essentially a "safe hold" or emergency shutdown of the facility. Essential services might, for example, include critical instrumentation and electrical drives such as instrument air compressors, emergency scrubbers (vent fans and circulation pumps), steam boilers (feed water pumps and exhaust fans), cooling water pumps, refrigeration systems, DCS control systems, emergency lighting, firewater pumps, and critical remote isolation valves (ROVs). Equipment associated with chemical reactions (especially exothermic reactors) may require emergency power for cooling systems, agitators, and runaway prevention systems. Other critical services could include nitrogen, firewater, and hydraulic systems.

The requirements for essential services will be specific to individual processes and should be identified by the risk assessments described above in the design stage to include the required start-up time (or immediate availability via a UPS) and duration of operation required. These aspects also require consideration when changes are made that should be implemented via an MOC process.

## Diversity of energy supplies

Diversity of energy generation for some of these essential services may help to reduce the consequence of a single failure, such as loss of main power (for example, diesel-driven instrument air compressors, cooling water, and fire-water pumps are often provided to provide a back-up that is independent of the main power supply). However, unless these operate continuously, they may require a stand-alone starting system (or manual starting) to be fully independent from the main power systems. They are often linked to a UPS to allow them to start. Where extremely high reliability is required, such as the nuclear industry, the diesel engine generators are often started with compressed air that is permanently held in a pressurised receiver.

Diversity of the site power supply itself (for example independent, 100% redundant supplies from different sub-stations) may provide a more reliable supply. However, these may be subjected to common cause failure, such as storms, floods or earthquakes (case study 4). Site power supplies have been lost despite the apparent diversity of power supplies, due to regional power failure (case study 2). Back-up supplies of nitrogen are not always available (case study 3).

## Standards and guidelines for emergency power

Standards and guidelines for emergency electrical power supplies include:

- NFPA 110: Standard for Emergency Power and Standby Power Systems (EPSS), 2025
- NFPA 111: Standard on Stored Electrical Energy Emergency and Standby Power Systems (SEPSS), 2025
- IEEE Std 446: Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Operations, 1995
- IAEA standard SSR-21 Rev 1: Nuclear Design of Electrical Power Systems for Nuclear Power Plants - IAEA Safety Standards Series No. SSG-34

It is notable that the required reliability is not discussed in either standard; these requirements would be unique to each application.

## Design and testing of emergency back-up systems

Where the consequences of the failure of back-up systems are severe, a holistic approach should be considered when designing them and must include electrical and process specialists, process safety engineers, technicians, and emergency response planners. This should help ensure that the back-up systems are available at the required capacity and duration as determined by the risk assessment.

For electrical systems, the use of artificial loads (usually via load banks) provides a more reliable test than a simple engine and voltage test. However, unless the system is designed to provide an actual load to the facility during testing, load tests may not provide a 100% guarantee of operation when it is called upon.

Ideally, the systems should be designed to allow for complete end-to-end testing, without risk of interrupting the supply to the production facility. This may be a challenge for older systems where facility management would only consider testing during a turnaround. Where the frequency of turnarounds reduces, so does the test frequency of the back-up systems. In such cases, it may be appropriate to review the design of the testing regime such that some (or all of it) can be conducted with the facility operational.

## Planning for multiple failures of energy supplies

Various scenarios involving multiple failures of energy supplies should be considered as part of the risk assessments described above. Techniques such as "what-if" PHA studies could be used to identify such eventualities and, where possible, additional safeguards might be considered. However, this may not always be practical, and there may still be scenarios where operators and technicians must step in to deal with situations manually. Although it may be an extreme example, during the Fukushima Daiichi nuclear meltdowns in 2011 (case study 4), operators were able to view individual instruments by connecting pairs of 12-volt car batteries. Would provision of portable 24V power packs be a sensible approach in the event of instrumentation power failure?

Some other examples include:

- connection of a firewater supply to an emergency scrubber
- hiring in, or relocating portable equipment, such as diesel power generators, pumps, and hydraulic packs.

## Human factors

Human factors and training for coping with unplanned events form a key part of the emergency planning process, and all stakeholders should be involved to practice such situations, perhaps as desktop studies. Some individuals might be better




0260-9576/25/$17.63 + 0.00

at handling abnormal events than others. Crew Resource Management (CRM) was originally developed in the aviation industry and has been adapted into other industries as "Team Resource Management" or Non-Technical Skills. This area has been defined as "the cognitive, social and personal resource skills that complement technical skills, and contribute to the safe and efficient task performance."[1] Some of these issues can be identified by conducting emergency exercises, and training/refresher training should be ongoing exercises. Further details are provided in the CCPS Book on *Management of Abnormal Situations*.[2]

## Case study 1 — *MV Dali*, Baltimore Bridge collapse[3]

### *Description*

The *MV Dali* is a 289-metre-long container ship (see Figure 1), propelled by a single 41,480 kW low-speed diesel engine driving the propeller at between 27 rpm (dead slow) and 80 rpm (full). The engine is started by compressed air and since there is no gearbox, it has to be stopped and started in the reverse direction to allow the vessel to go astern. High voltage (HV) electrical power is provided at 6.6kV to the HV bus by up to four diesel generators (DG), with two operating (DG3 and DG4) at the time of the incident and DG2 on automatic standby (see Figure 2). The voltage is stepped down to low voltage (LV) bus 440V by two (100% redundant) transformers. The engine oil lubricating pump and bow thruster is driven by a HV motor, and the engine water cooling pump and hydraulic steering gear pumps are powered by the LV system. An automatically starting emergency generator is provided on the LV system.

The vessel is fitted with alarms and automated shutdown trips, including a main engine trip to prevent damage to the engine if either the lubricating oil or the cooling water pumps stop.

The Francis Scott Key Bridge in Baltimore was opened in 1977 and comprises a 2.8-km-long steel and concrete construction supported by multiple piers, with the central shipping navigation channel between pier numbers 17 and 18. The piers were surrounded by a "crushable concrete box and timber fendering system."

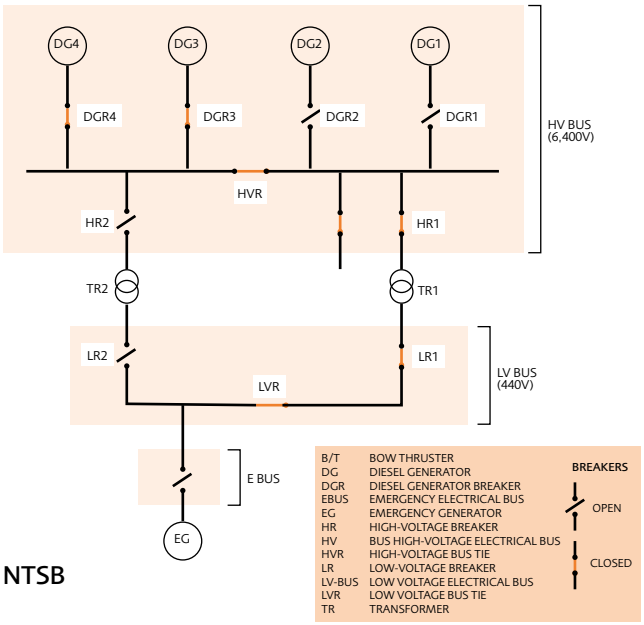


*Figure 2 – Simplified single line electrical drawing*[4]

## Incident

The *Dali* was carrying 4,680 containers (56,675 tonnes), including some hazardous cargos and displaced 112,383 tonnes at the time of departure from Baltimore harbour at 0036 hrs on 26 March 2024, assisted by two tugboats with two pilots on board.

The tugboats let go at about 0107 hrs, and about two minutes later, the main engine speed was moved to slow ahead (approximately 35 rpm). By 0125 hrs, the *Dali* was headed southeast and was about three ship lengths northwest of the Francis Scott Key Bridge, running at about nine knots, when the HV and LV circuit breakers (HR1 and LR1) on either side of the transformer TR1 both unexpectedly opened (see Figure 2). Since TR2 was isolated at the time (by HR2 and LR2), this resulted in the loss of the LV system, the automatic shutdown of the main engine due to loss of power to the cooling pumps, and the loss of steerage due to loss of power to the hydraulic steering pumps.

*Figure 1 – MV Dali*[4]

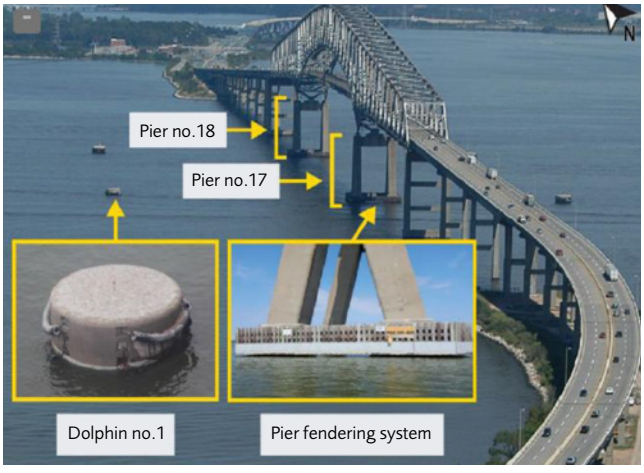


*Figure 3 – Francis Scott Key Bridge*[4]



0260-9576/25/$17.63 + 0.00

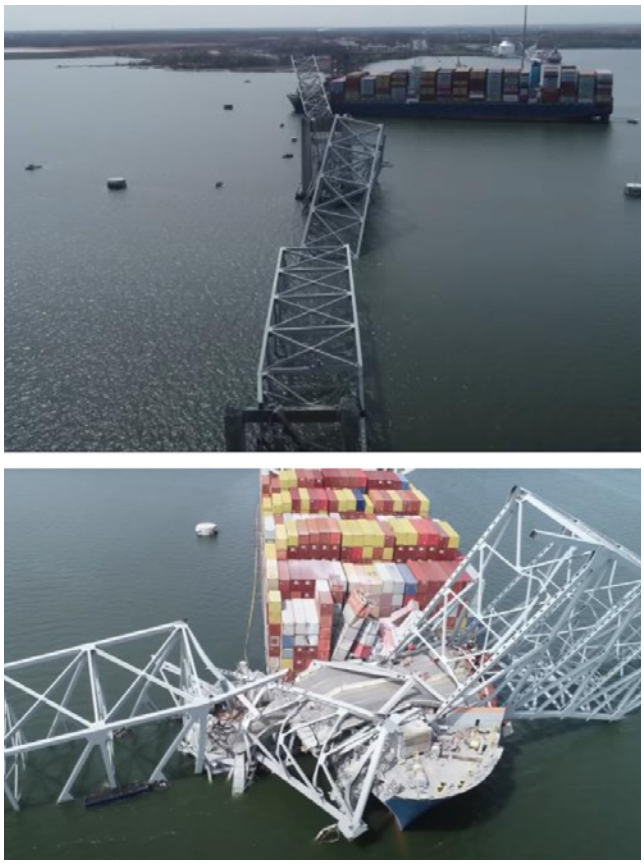

*Figure 4 – Photographs of the* Dali *and Francis Scott Key Bridge after the incident*

Although timing details were not available from the preliminary report, the emergency generator (EG) started, providing LV power to critical systems. This should have restored power for the emergency lighting, emergency steering pump, and engine cooling, but by this time, the main engine had tripped and would have required restarting. The crew manually closed HR1 and LR1, but shortly afterwards, the HV switchgear DGR4 and DGR3 tripped out, causing a second blackout to the HV system. Although the standby main generator DG2 had started automatically, providing power to the HV and LV bus via switchgear DGR2, there was no time to restart the main engine.

Approximately two minutes after the first power trip, at 0127:01, the pilot ordered an anchor dropped, but this did not prove effective. At 0127:23, the pilot ordered rudder hard to port, but at 0129.10, just four minutes after the first electrical trip, the *Dali* struck pier number 17 at about 6.5 knots causing six spans to collapse into the water and across the bow. This led to six fatalities and major damage to the *Dali* and its cargo containers (See Figure 4).

## Cause

There were many aspects of causation and incident mitigation that are outside the scope of this paper. The official NTSB report has yet to be finalised, so there may be further items to consider once this has been completed. An update from the NTSB on 24 June 2024, stated that they were examining an electrical terminal block and associated wiring for HR1's

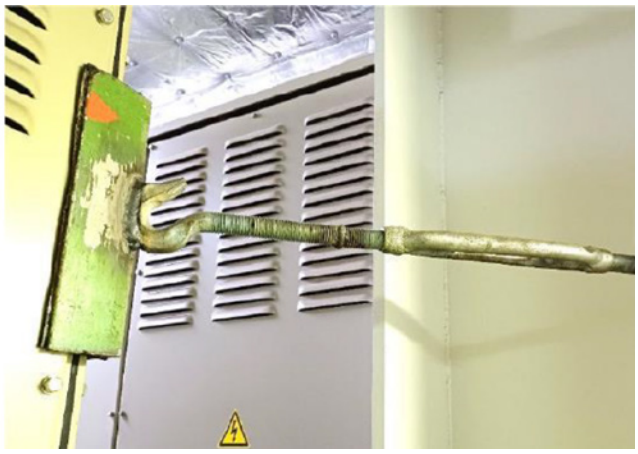

*Figure 5 – Photograph of anti-vibration measures*

"undervoltage release."[5] Another report[6] was issued by the NTSB on 11 September 2024 following a series of technical tests. This showed that there was a loose cable connection that could trigger an undervoltage release trip of HR1. This would result in a 440V blackout.

Another potential casual factor is detailed in a civil claim filed by the US government on 18 September 2024[7] that refers to a known problem of excessive vibration on the vessel. It would appear that a relatively crude measure was taken to try to reduce the effect of these vibrations on No.1 transformer. This involved a steel cargo chain turnbuckle that was found welded to a steel beam and wedged onto the frame of the electrical cabinet. (See Figure 5.)

The US government civil claim describes further issues including:

- The transformers did not automatically change over when the first one tripped. This should have been the case if the selector switch was correctly positioned.
- The fuel supply for the generators used a different pump from that used at sea. This was because the vessel was in an emission control zone and therefore had to be supplied with low sulphur diesel. The pump that was in use was a flushing pump that was not set up to restart automatically after a blackout and it tripped out after the first power failure. A pneumatic pump came on in response to the outage but was never intended to supply the full demand requirements of the generators. The second power failure was a result of insufficient fuel being fed to the generators that tripped out automatically when they started to slow down.

Several other issues included:

- Although the power to the bow thruster had likely been restored by the time of the event, it would not have been effective due to the forward speed of the vessel.
- Even if power was available for steerage, the rudder would have been less effective since the propeller had stopped, and there was little water flow over the rudder beyond the forward speed of the vessel.
- Operating the system with the No.2 transformer isolated and the auto-changeover apparently not functioning, provides no redundancy for the LV system (i.e., loss of


0260-9576/25/$17.63 + 0.00

No.1 transformer would lead to an immediate LV outage).

- The bridge piers adjacent to the main shipping channel were fitted with a 100 ft x 84 ft crushable concrete and timber fendering system. It is likely that this was designed when vessels were smaller and was clearly inadequate to protect the bridge in the circumstances of the event.
- Further details are bound to emerge from the ongoing investigation. However, from a process safety viewpoint, key issues would seem to relate to there being a single point of failure (SPOF), whereby a brief interruption of the power supply results in the engine stopping *and* loss of steerage.

## Discussion

Had this occurred out at sea, it is likely that the ship's crew would have had time to deal with the matter before a major incident occurred. In this event, the crew only had four minutes to act to prevent the collision and most likely did all that could be done in the circumstances. There is no reference to the existence of an uninterruptible power supply (UPS) in the preliminary NTSB report. The emergency generator (LV only) should have started within 45 seconds[8] although the actual start-up time is yet to be confirmed. However, this would only have made power available to the emergency steering pump (which operates at a lower speed) and the engine cooling water pumps. Since the engine lube oil pump required the HV system to be operational, the main engine could not be started without the HV system functioning correctly. This is a large, low-speed marine diesel that would take several minutes to restart, even if all required systems were available.

It is understood that the design of the electrical and mechanical systems in the *Dali* is not out of step with other vessels. Thus, this issue may not be unique to this incident, and it is therefore important to recognise the vulnerability of such vessels to a SPOF leading to loss of steerage. This becomes a more significant factor when the vessel is manoeuvring close to a weak potential target, such as an unprotected bridge support.

Although this paper is written with the benefit of hindsight, a risk assessment that challenged the back-up system and its potential weaknesses could have identified the possibilities for such an incident if the vessel is in a critical location. A simple change to operations, such as continuing to use the tugboats until the Francis Scott Key Bridge had been passed, might have prevented this event from occurring. The apparent inadequacy of the fendering system is potentially a result of creeping change, as the vessels became larger and heavier.

## Learning for the process industries

It is essential to fully understand the potential consequences of a loss of energy to equipment and other services, SPOFs, and the effectiveness of back-up systems to mitigate such an event. This could be determined by an appropriate risk assessment such as a Failure Mode and Effects Analysis (FMEA) or a "What-if" HAZOP, perhaps associated with a desktop exercise or computer simulation.

The consequences may be even more serious during transient operations such as start-up or shutdown. Therefore, any emergency systems should be thoroughly tested on a scheduled basis. Emergency procedures must consider actions or mitigations required in the event of a total failure of the back-ups when additional barriers — such as extra engine-driven generators, air compressors, portable electric, or hydraulic packs — may be provided.

## Case study 2 — site supply lost

A large facility was provided with power from twin "independent" feeders. Essential energy services were specified that included the requirement for a reliable supply of steam to safely shut down the process and prevent damage to furnace tubing due to thermal shock. Key features included:

- Three diesel powered emergency generators (100%).
- Three steam boilers, one of which (boiler 1) used its own steam to power the turbine for the combustion air fan and the boiler feedwater pumps, and thus was designated as a high-integrity boiler. The DCS control systems for each boiler was fitted with its own UPS.
- Steam turbine-driven instrument air compressors with back-up from a let-down valve from a nitrogen system.

In the event, both external power supplies failed due to a regional electrical failure. In the utilities area, one of the three emergency generators was under maintenance. The second generator failed to start, and the third generator started but failed to synchronise with the site supplies and tripped out electrically. Thus, no main power was available for the utilities and boilers 2 and 3 tripped out due to loss of feed water pump and combustion air fan. Boiler 1 continued to operate for a short period, with its utilities DCS powered by the UPS. However, the DCS (which was very old and due to be replaced) was inundated with alarms as a result of the power failure, became overloaded, and failed, resulting in boiler 1 tripping out.

Thus, no steam was available for the plant or to drive the instrument air compressor or boiler feedwater pumps. The emergency back-up supply for the instrument air system from the nitrogen system failed to operate since the pneumatic control valve had wrongly been designated as air fail closed. The six furnaces were tripped out manually due to the loss of boiler feed water for the waste heat recovery boilers. Since there was no steam available, several of the furnace tubes cracked due to thermal shock. The downstream plant became pressurised since pressure control valves were designed to close on air failure. There was then a backflow of hydrocarbons from the downstream plant, which leaked out of the furnace tubes resulting in a major, uncontrolled fire within the six furnaces. Electrically-operated remote isolation valves that would have prevented backflow could not be operated due to loss of power. Whilst these valves were fitted with manual handwheels, they each required several hundred rotations, and there was insufficient time to manually close all six valves with the resources that were available.

Three furnaces were severely damaged by the uncontrolled fire and had to be rebuilt.

Key aspects were:

- There was too much reliance on the external power



0260-9576/25/$17.63 + 0.00

supplies being independent, but they were both subject to common cause failure.

- There was inadequate design/testing of generator synchronisation system.
- There was inadequate maintenance and testing of generators; the scope of the test was to mechanically start the generators and verify voltage is generated. No simulated load testing of generators was conducted, and the tests did not include electrical synchronisation.
- The failure mode of the control valve on back-up to instrument air supply was incorrect.
- There was a failure to consider total loss of services in the design/emergency planning/human factors, including inability to manually close outlet valves from each furnace in time.

An overall lesson is that there was no consideration of the possibility of a cascade failure of the back-up systems. One measure that may have reduced the damage significantly would have been a portable device to rapidly close the outlet valves on the furnaces. Alternatively, a procedure could have been developed (and practised) where those critical valves are closed manually by appointed personnel in the event of power and back-up outage.

## Case study 3 — nitrogen back-up failure

A facility that handled hydrocarbons comprised parallel, identical catalytic units that operated cyclically through a reaction and regeneration (with air) sequence. Solenoid valves that separated the units were fitted with a double seal with nitrogen purge between the seals. This was to ensure safe operation when, during part of the cycle, there were hot hydrocarbons on one side of the valve and air on the other. The valves were not always 100% leak-tight, and the nitrogen purge provided an additional layer of protection. The nitrogen supply came from a membrane type generator that was somewhat unreliable so had been backed up with a bank of nitrogen bottles, whilst awaiting its refurbishment.

An incident occurred where there was a fire inside the process equipment due to the solenoid isolation valves passing. The investigation found that the nitrogen pressure was too low because the generator was operating at low rates due to a fault and the back-up nitrogen bottles were empty. The low-pressure nitrogen alarm operated regularly during the cyclical valve operations and had become a nuisance alarm. Its setting was reduced without using an MOC, and there were no formal checks that the nitrogen bottles were still full.

Key lessons included recognising the failure to maintain critical services (nitrogen generator) and the necessity to use an effective MOC procedure for temporary operations.

Note: Hired-in plant is occasionally used when equipment is undergoing maintenance. For example, diesel-powered air compressors are brought in when site compressors are under maintenance to maintain instrument air pressure. These can become permanent fixtures ("creeping change") and can be beneficial as they provide diversity in the energy source. However, it is important to ensure there are sufficient safeguards, including management of fuel tank level and fitting of alarms to indicate when they trip out.

*Figure 6 – Water inundation at Fukushima Daiichi[9]*

## Case study 4 – Fukushima Daiichi

The Japanese earthquake of 11 March 2011, occurred at 1446 hrs. Its initial impact on the Fukushima Daiichi power station caused a loss of external power supplies, and the three operating nuclear reactors tripped due to the seismic activity. The emergency diesel generators powered up and ran until shortly after 1541 hrs when the tsunami struck the facility and inundated the generator rooms, which were located at/below ground level. Despite heroic efforts from the operating team, the loss of power from the emergency generators led to loss of both control systems and reactor cooling, a subsequent meltdown, and hydrogen explosions that followed over the next three days.

Learning that was specific to back-up supplies included a failure to consider the common cause failure of power supplies following an earthquake and tsunami, despite previous evidence that the sea wall was not high enough to handle such an event.

*Figure 7 – Hydrogen explosion at Fukushima Daichi[10]*


0260-9576/25/$17.63 + 0.00

## Conclusion

Multiple, reliable energy sources are required on hazardous processes to safely control plant and equipment. Failure of one or more of these energy sources can lead to major incidents. This is often mitigated against by the provision of back-up supplies for critical services. However, the design and testing of these back-ups must be carefully considered to ensure they are sufficiently reliable. Emergency procedures should also consider the potential failure of the back-up supplies and include procedures, training, and exercises to minimise the hazardous consequences of such events. It is healthy to maintain a "sense of chronic unease" when it comes to emergency back-up systems.

## References


1. *Flin et al., 2003. "Development of the NOTECHS (Non-Technical Skills) system for assessing pilots' CRM skills," Human Factors and Aerospace Safety, vol. 3, no. 2, pp. 95-117.*
2. *Center for Chemical Process Safety (CCPS), 2023. Guidelines for Managing Abnormal Situations, AIChE, CCPS, New York.*
3. *National Transportation Safety Board (NTSB). "Marine Investigation Preliminary Report - Contact of Containership Dali with the Francis Scott Key Bridge and Subsequent Bridge Collapse," 14 May 2024, ntsb.gov/investigations/Documents/DCA24MM031_PreliminaryReport%203.pdf.*
4. *Dali Container Ship. IMO 9697248, MMSI 563004200, www.vesselfinder.com.*
5. *National Transportation Safety Board (NTSB). "Investigation Update," 24 June. 2024, https://www.ntsb.gov/investigations/Pages/DCA24MM031.aspx.*
6. *NTSB Engineering Group (DCA24MM031) Dali Shipboard Machinery Examination and Record of Electrical Testing, April 1–29, 2024, available at https://data.ntsb.gov/Docket/?NTSBNumber=DCA24MM031*
7. *United States' Claim And Answer To Petitioners Grace Ocean Private Limited And Synergy Marine Pte Ltd's Petition For Exoneration From Or Limitation Of Liability, available from https://www.justice.gov/opa/media/1369026/dl*
8. *Safety if Life at Sea (SOLAS), Chapter 11-1, Part D, regulation 43, 3.1.3. "Emergency source of electrical power in cargo ships," www.imorules.com.*
9. *Tokyo Electric Power Co (TEPCO), 2011. Photographs from Daiichi during tsunami.*
10. *NPR News. Screenshot from Japanese broadcaster NHK of hydrogen explosion in No.3 reactor building, www.npr.org/2011/03/14/134501905/crisis-at-nuclear-plant-adds-to-japans-woes.*







0260-9576/25/$17.63 + 0.00