ISSN: 2754-4982

Journal of Civil Engineering Research & Technology

SCIENTIFIC Research and Community

Research Article

Open Access

The Role of Maintenance in Reducing the Risk of Technological Disasters

Robert G Batson

Department of Civil, Construction, and Environmental Engineering, the University of Alabama, Tuscaloosa, Alabama 35487-0205 USA

ABSTRACT

In this article, we begin with characterization of technological disasters, emphasizing that human errors in one or more phases of the system life-cycle set the stage for disaster. To counter the unexpected, designers include multiple independent safety barriers capable of preventing the occurrence or mitigating the consequences of such unexpected events. The integrity of the barriers depends on adequate levels of maintenance. Maintenance actions sometimes cause technological disasters, but are shown in large part to prevent malfunctions in technology control systems and safety barriers. We argue that well-planned and executed maintenance actions are key in the reduction of risk of technological disasters. In our research, we reviewed well-documented technological disasters in a variety of organizations such as commercial aviation, nuclear power generation, and petroleum and chemical processing. Using a three-factor cause analysis scheme (human error, equipment or process failure, safety barrier failure) we analyzed twelve disasters and found these factors present in each disaster description. In each analysis, we paid particular attention to the role of maintenance managers and technicians in reducing the risk of disaster. However, maintenance was also a direct causal factor in six of the twelve (50%) disasters analyzed. In addition, we identified the phase of the technological system life-cycle when the disaster occurred.

***Corresponding author**

Robert G. Batson, PhD, PE, Department of Civil, Construction, and Environmental Engineering, The University of Alabama, Tuscaloosa, Alabama 35487-0205 USA. E-mail: rbatson@eng.ua.edu

Received: June 11, 2021; **Accepted:** June 17, 2021; **Published:** June 23, 2021

Keywords: Maintenance, Risk, Technological Disaster, Human Error, Technological Life-Cycle Phases, Safety Barriers.

Introduction

A technological disaster is a catastrophic event that is caused by either human error in controlling the technology or a malfunction of a technological system. The human error could have occurred in any phase of the system life-cycle: design, construction/installation, operations, maintenance, or decommissioning/disposal. The term malfunction should be interpreted broadly, to include either failure of hardware or software involved in normal system operation, or failure of so-called safety systems, multiple or independent safety barriers that are capable of preventing or mitigating the consequences of unexpected events during operations or servicing.

Okeh and Haugen observed that "efforts have been made to enhance defenses against major accidents based on lessons learnt from accidents...It is common to deploy multiple and independent safety barriers"[1] -- a practice referred to as 'defense-in-depth' by Reason [2]. Okeh and Haugen continue "The integrity of the barriers cannot be maintained without an adequate level of maintenance. Maintenance is therefore a key activity to reduce the risk of major accidents." They caution that "Maintenance may have a negative effect on barrier performance if the execution is incorrect, insufficient, delayed, or excessive." In fact, there are examples where maintenance of the operating system or safety system has been the "triggering event" in an accident chain. Chiles states "Maintenance is the soft underbelly of the system, an open door to disaster" and cited delayed maintenance, the shutting off of safety devices, or letting them break without replacement [3].

Technological disasters differ from typical industrial accidents in that they:

- Are generally catastrophic, meaning swift and severe effects on many individuals, broad swaths of infrastructure, and multiple aspects of the environment (air, water, animals, plants, etc.)
- Can affect localized or wide-spread areas
- Are frequently unpredictable, though one author Chapman argues differently as explained below [4].
- Can significantly affect infrastructure (not unlike natural disasters)
- Can be triggered by natural events (e.g., earthquakes, hurricanes, floods)
- May chronically grow over a long timeframe but go unnoticed, or may result because of a single major event (most technological disasters are seemingly abrupt)
- When abrupt, take the responders and management by surprise
- Chronic problems are often exposed after such a brief, well-defined event.

Chapman argues that technological disasters are predictable in terms of how each system is designed, constructed, operated, and maintained [4]. Of course, if the technology or its application is new, predicable behavior rests on formal risk management, culminating in proper and dependable testing of design concepts, construction processes, and operational and maintenance procedures. Much of the "surprise" of technological disasters

is not due to lack of testing or standard operating/maintenance procedures, instead Chapman argues that it is the complexity and opaqueness of socio-technical systems. Complexity in essence "masks" the hazards and reduces the effectiveness of genuine attempts at risk management. Complexity engenders two risks:

1. Greater chances that a significant weakness will be built into at least on part of the system (e.g., a critical subsystem or the interface between two subsystems)
2. Complex systems are ambiguous to the extent that those who operate and maintain them are only partially aware of how the different parts of the system are interlinked.

Finally, technological disasters are man-made in that they evidence:

1. Overlooked red-flags in design, construction, operations, and maintenance
2. Cutting corners in design, construction, operations, maintenance, and disposal
3. Incorporated innovation (use of new technology) which outpaces preparation in operations and maintenance
4. Modifications (systems evolve over time with unintended consequences for safety)
5. Human errors as described in Reason and Hobbs [5]: Errors of omission--failure to perform a necessary step or action; Errors of commission--taking an action that should have been avoided.

Materials and Methods

Classification of Technological Disasters

Considering industrialization, urbanization, transportation, and energy generation trends among advanced economies in the early 21st century, categories of technological disasters that come to mind include:

Structural Failures--buildings, bridges, dams, mines and tunnels, rail-lines, roads

Industrial Failures--chemical and petroleum process industries, nuclear power plants, processing of hazardous materials (explosives, minerals and metals, biohazards)

Overwhelmed Public Facilities--highways and airports, electrical power grids, water treatment and distribution, sewage and storm drains, garbage landfills, hazardous waste landfills

Long-term environmental degradation--air and groundwater pollution, acid rain, ozone depletion, global warming, sea-level rise, species extinctions.

Specifically, in the US, the Federal Emergency Management Agency (FEMA) recognized seven categories of "technological hazards" FEMA [6]:

- Dam failures
- Fires (residential, commercial, industrial, other properties)
- Hazardous material events (uncontrolled releases from fixed sites or during transport, including pipelines)
- Nuclear accidents (uncontrolled releases of radioactive materials at commercial power plants or other nuclear reactor facilities, or during shipment of materials)
- National security hazards--hazards that come from actions by hostile forces against the land, population, or infrastructure of the nation
- Power failures--interruptions or losses of electrical service for extended periods of time
- Telecommunication failures--failures of data transfer, communications, or processing brought on by failure of equipment or software

Although these categories were specified by FEMA, governments in each industrialized, advanced economy have agencies and regulations to carefully manage all seven of these hazards, excepting nuclear accidents (in those countries where there is no mining, transport, processing, nor utilization of radioactive materials).

Causes of Technological Disasters

Previous attempts to classify causes of high profile technological disasters in the process industries were found in the literature. Shaluf, Ahmadun, and Shariff reviewed accident reports from major hazard installations (MHIs)--industrial organizations dealing with hazardous substances which exceed the threshold quantity [7]. The observed "MHIs are characterized by high complexity and tight-coupled organizations. Although the MHIs are secure installations and cannot fail due to a single error, due to the high complexity and level of interaction among subsystems, designers and operators are unable to predict failures at MHI units...The world has seen many major accidents from the operations of MHIs...This paper reviews the factors that led to the technological disaster and also summarizes the causes of technological disasters in Malaysia." The taxonomy of causes suggested by Shaluf, Fakhru'l-Razi, and Shariff is rational but complex [7]:

1. Human factor
1.1Operator errors (included poor inspection and maintenance)¬--errors of omission of steps or entire task
1.2 Management errors (includes poor planning and budgeting)
2. Technical factor
2.1 Design errors (includes poor design of control and/or safety system)
2.2 Mechanical failures (includes failure of control and/or safety system)
3. Organizational factor
3.1 Policy failures
3.2 Inadequate resource allocations
3.3 Communication failures
3.4 Misperception of the extent and nature of hazards
3.5 Inadequate emergency plans
4. Operational factor
4.1 Operator errors of commission such as wrong button, disconnected safety systems, mix-up of hazardous substances, communication errors
4.2 Maintainer errors of commission such as incorrect maintenance or repair work, unauthorized work including modifications to a control or safety system
5. Warning factor--such as: failure to react to recommendations from inspections; failure to investigate near misses, safety violations, incidents, and accidents; failure to consider and implement safety audit recommendations
6. Triggering event--an event caused by operator or maintainer error, first line management error., or an inadequate safety management system
7. Defense factor--such factors include: inadequate detection and alarm system; insufficient personnel to respond to emergency conditions; lack of emergency response planning including liaison with external support.

After review of investigation reports for four technological disasters in process industry facilities in Malaysia, these authors slightly revised the above taxonomy, as follows:

1. Social errors--errors made by operators and managers of the plants
2. Technical errors--"fundamental precondition errors" are technical errors such as design errors or equipment failures
3. Organizational errors (procedures and documents)--errors in

the link between: the operators and their management; the social and technical sides through policy, regulations, rules, manuals, and plans (training in standard operation procedures, emergency plans, etc.)

4. Operational errors (errors of commission at the human-technical interface)--operator errors, hazardous material storage errors, equipment modification errors, incorrect repair or maintenance of equipment (lack of reference to standard maintenance procedures), and finally maintenance errors of omission.
5. Warnings--failure of plant management to react to internal warnings (mistakes, violations, near misses, accidents, etc.) and external warnings (mistakes and accidents which occur at similar organizations).
6. Triggering event (the one event after which the disaster is unavoidable)--and unsafe act in combination with unsafe conditions trigger the event, which leads to more component failures, and ultimately equipment failures.
7. Defense errors--inadequate detection and alarm facilities, lack of integrity of containment (defense) facilities, lack of adequate emergency response plan.

A more recent article Okoh and Haugen focused on eight maintenance-related majors accidents in the oil and gas and chemical process industries, three of which involved explosions [1]. In particular, the main objective of the paper was "to discuss how maintenance has influenced some major accidents in the oil and gas and chemical process industry." The authors concluded that "the most occurring barrier-based factor is maintenance error, and the most occurring maintenance management factors are deficient planning, deficient execution, and deficient checking." Concerning maintenance errors, according to Reason and Hobbs [5], errors of omission--failure to carry out necessary actions or tasks, usually during installation--are the largest category of maintenance errors. Reason and Hobbs cite both US and Japanese nuclear power plant records showing that in both cultures, roughly 2/3 of errors associated with maintenance-related activities involved the omission of necessary steps, and go on to state that comparable figures are found in aviation maintenance. A well-researched record of many more technological disasters was located, and became the basis for our analyses, as described next.

In the text Inviting Disaster: Lessons Learned from the Edge of Technology, Chiles documents 62 disaster case studies he researched from a range of industries, including transportation (rail, oil tankers, passenger ships, airliners), construction (dams, bridges, buildings), nuclear power generation, natural gas distribution, electrical power distribution, off-shore oil drilling, military operations (airships, submarines, missiles, air defense early warning systems), spacecraft operations (manned, unmanned), and petroleum and chemical processing [3].

Results/Observations: Analysis of Technological Disasters using Three Factors

We chose twelve of the technological disasters as described by Chiles (approximately 20% of the disasters he reviewed) for their diversity and the involvement of maintenance as a causal or mitigating factor. Depending on Chiles' review, we were able to analyze each accident and proceeded to group the causes into three categories:

1. Human errors made during one or more life-cycle phases of the technological system: design, construction, operations, maintenance, and disposal.
2. Failure of a component, equipment or computer program item, process, or entire installation.
3. Failure of one or more "safety barriers" to perform as expected; or, a safety barrier that was omitted from design or construction, or was in a disabled state when called upon--meaning it was deemed unnecessary, turned off due to frequent false alarms, rendered inoperative due to maintenance, etc.

See Table 1 for the detailed results of this "three factor analysis" which harkens back to textbook explanations of causes of accidents being unsafe acts (human errors), unsafe conditions (unsafe equipment or environment--equivalent to hazards), or both; two contributions we have made are 1) identification of the life-cycle phases where the human errors occurred--there may be more than one--and 2) explicit consideration of the role of safety systems under either human or automatic control, and the importance of maintenance of such safety systems.

Table 1: Three-factor Analysis of Twelve Technological Disasters from Chiles [3]

Disaster and Date	Human Error	Equipment or Process Failure	Safety Barrier Failure
Sultana US Steamboat Boiler Explosion April 27, 1865	Instead of replacing two iron plates on the boiler wall, an iron "patch" was used to cover a crack, but the iron was thinner than the wall. The safety relief valve on the boiler should have been reset to 100 psi, but remained at 145 psi setting for undamaged boiler, a crucial omission. Sultana had 2300 union soldiers aboard, about 8 times the legal capacity. Many of the overload stood or sat on the upper decks, making the boat top-heavy. Both of the side-by-side boilers had water levels too low.	All three boilers exploded, probably due to tilting of the overloaded boat in turns, which drained water from the high-side boiler.	The pressure inside the boilers was permitted to grow 45 psi above the 100 psi called for by the thickness of the patch. Safety barrier could not do its job due to incorrect setting.
USS Maine Battleship Explosion Feb. 15, 1898	The design of the below-decks compartments house bituminous coal in a bunker separated by a bulkhead from a magazine containing gunpowder, not realizing the explosive hazard if the coal ignited.	The coal suffered spontaneous combustion and the heat transfer through the steel bulkhead ignited the gunpowder.	Bulkhead did not keep the gunpowder from exploding and did not contain the explosion, so most of the crew died from the concussion, fire, or ship sinking.

New London Texas schoolhouse gas explosion Mar. 18, 1937	School district dropped its contract with local utility for natural gas (treated with a malodorant as a warning for leaks), and began using cheaper untreated residue gas from local oil fields.	The heating system had a faulty connection and leaked gas for several hours, creating an explosive gas-air mixture in the basement which ignited when an electrical switch in an industrial arts class was closed.	The safety barrier for leaking gas (rotten egg smell) was omitted in gas supply in order to save money on utility bill.
Thresher (US nuclear powered submarine cannot surface) April 10, 1963	Used brazed connections in sea-water piping; Design attempted to provide fast and foolproof deballasting; Provided no way for crew to override nuclear reactor shutdown; batteries on board are the only backup power.	Silver-brazed joint in seawater piping broke and sprayed salt-water on electronic controls, causing automatic shutdown of nuclear reactor.	Crew attempted an "emergency blow" of pressurized air into the ballast tanks, but rapid ice formation in particulate strainers in air system blocked the airflow; batteries on board could not power the sub to the surface.
Apollo 13 (US spacecraft) April 13, 1970	Liquid oxygen tank is designed with a thermostat rated for less voltage than the rest of electrical system; Liquid oxygen tank had been damaged in factory assembly, shaking internal plumbing loose--not reported, nor repaired.	During testing on launch pad, the liquid oxygen tank would not empty normally (due to earlier damage); Technicians used built-in tank heater to vaporize liquid; Thermostat short-circuited and allowed tank interior to overheat and burn off Teflon wire insulation.	Wire insulation to prevent sparks in oxygen-rich environment is no longer effective; On way to the Moon, tank heater causes spark, and combustion bursts the tank; Crew improvised way to use Lunar Lander oxygen and survived--a near miss.
Three Mile Island Unit 2 (US nuclear power plant) Mar. 28, 1979	Designers provided no instrument to tell the operators how much water was in the reactor coolant pipes; Two workers opened part of steam-making loop for maintenance regarding a non-critical problem, but permitted a few ounces of water to seep backward into compressed air lines, reaching control line to valves controlling all filters in steam-making loop; Operators misinterpret signals (think reactor coolant level is dangerously high); Operators cut back on emergency cooling system, letting water out at 160 gallons per minute.	The pilot-operated relief valve (PORV) on pressurizer opens, but does not close on automatic command; Coolant begins draining out of reactor through pressurizer to a drain tank; Operators believe the instruments which tell them the PORV is closed, when it is not.	Main alarm Klaxon was sounding and approximately 100 alarm lights were flashing, making it difficult to concentrate and understand what had happened. An off-duty manager arrived and correctly diagnosed the failure. The stainless steel reactor vessel held the partially melted reactor fuel and kept it from escaping. Estimated total cost was $4B.
Kansas City Hyatt Regency Hotel, Skywalk Collapse, July 17, 1981	Original design to suspend the fourth-level and second-level skywalks, each using four rods attached to ceiling, is deemed too difficult to construct; Constructor modifies the design to where second-level skywalk is suspended from fourth-level skywalk, using four shorter rods but same connectors as original. Structural PE approves the proposed revision without doing necessary computations, which would have shown loads on the linking connectors had doubled. Hotel policy permitted as many people as would fit in the space to occupy each of the walkways during a large party, also permitting the main floor to be fully occupied.	Connectors for rods hanging second-level skywalk from fourth-level failed, sending both skywalks and all occupants crashing down on dance floor occupants below.	Connectors were not resized for double the load, plus a factor of safety. Stiffeners on the walkway structure where the connectors were installed were not used. No other means of support for the second floor walkway was provided. 114 deaths.

Ocean Ranger (US Offshore Floating Drill Rig) Feb. 15, 1982	Designers placed a small observation window in the ballast control room situated in one "leg" of the semisubmersible drilling rig, but failed to appropriate structure and window material to withstand strikes by high waves to which window would be subjected; Crew was not trained that if the rig was tilted, ballast pumps did opposite of what was expected.	Storm wave broke out the window; sea water splashed onto electrical gear and valves to empty/fill the ballast in all four legs of the rig began operating randomly; Rig tilted and attempts by operators to use ballast pumps to level the rig only increased the tilt, sending ocean water into openings in upper decks.	Two of three lifeboats were destroyed in the evacuation, and entire crew (84) perished.
Union Carbide Bhopal Disaster Dec. 3, 1984	Factory producing highly toxic methyl isocyanate (MIC) for herbicides had poor maintenance of plant and safety systems; Had staff reductions of 50% during previous five years: Corporate safety audit in May 1982 found "slipshod maintenance procedures," supposedly corrected; A "shantytown" was erected on land right up to the plant fence; Of four "safety systems": 1) Vent gas scrubber tower, 2) Refrigeration system to keep MIC at low temperatures, to avoid over pressurization and venting of toxic gas, 3)Continuous torch to burn away escaping MIC vapor, 4)Water spray (for firefighting only); three (1-3 above) were shut down, fourth was ineffective.	Refrigerant was drained for other uses in the plant, due to shortages; Two MIC storage tanks were having trouble maintaining nitrogen gas pressure, an inert gas used to pump liquid MIC out of the tank and to protect from chemical contamination; Scrubber tower was leaking alkaline water through pipes from MIC tanks, reacting MIC vapors to form "gunk trimmer" on pipe walls; During planned maintenance to remove the trimmer using pressurized water, metal barriers (blinds) to prevent wash water from flowing backward into MIC tanks were not installed; 100 gallons of wash water entered one of the tanks, and started a heat-producing chemical reaction.	Flare was out of service; Refrigeration system had no refrigerant; Scrubber tower was down for maintenance; Water spray could not reach top of tower where MIC vapor was escaping into open air; Casualties: 7000 dead; 40,000 permanently disabled; 400,000 injured.
Piper Alpha UK Off-Shore Drilling Rig, July 6, 1988	Off-shore platform processed large volumes of natural gas from other nearby rigs via pipes; Daytime maintenance crew was repairing gas-condensate pump but did not finish before shift change, and a safety valve was left disconnected; Crew verbally warned a supervisor on next shift that backup pump should not be turned on, though no lock-out tag-out procedure was used; There was no automatic shutoff incoming gas from other rigs, in case of fire; Automatic firefighting system on the rig had be set from automatic to manual, and never activated ; Owners had ignored recommendations from a recent safety audit to remedy fire hazards from natural gas risers; Workers and managers had gotten sloppy about following the "permit-to-work" system which was supposed to prevent use of equipment under repair.	Main condensate pump failed, and evening shift tried to start the backup pump, leading to an explosion at the partially repaired pump.	Safety valve has been disconnected; "Permit to work" paperwork was either not delivered to evening shift, or not communicated to workforce by management; Explosion knocked down firewalls protecting rest of rig; Fire spread, first to gas processing equipment, then to risers carrying gas from other rigs at 2000 psi, and finally to crew living quarters; Platform firefighting system never activated automatically, nor manually; Took one hour before all incoming gas was stopped; 167 died and $1.1B platform was destroyed.

British Airways BAC 1-11 airliner June 10, 1990	Maintenance manager on "graveyard" shift decided to replace left front windscreen with deadline 3.5 hour away; 84 of 90 bolts were 7D, an error from previous maintenance; The job involved 1) review of instruction manual, which stated use 8D bolts, 2)unscrew 90 bolts from rim of windscreen, 3) remove old glass and fairing strips, 4)install new windscreen and bolt it in place; Manager decided to replace all 90 bolts, rather than only those whose bolt heads had been damaged from removal process; The storeroom supervisor told him he should be using 8D bolts (ignored) and there were not enough 7D in stock to complete job; Manager drove to a "parts depot" and searched for a carton of 7D, but in poor lighting he mismatched the bolt he brought along and with drew 84 8Cs from inventory(1/14 inch narrower than 7Ds); He returned and hurriedly installed the 84 8Cs without checking torque of resistance; only six original bolts that were re-used were holding the windscreen in place.	Windscreen with all 90 bolts (84 undersized) flew out under cabin pressure at 17,000 feet; Captain was partially sucked out of the opening, though he was still alive when aircraft made an emergency landing at South Hampton, 18 minutes after blowout.	Captain and co-pilot had unbuckled their chest straps but left their lap belts fastened; Co-pilot could fly and land the airplane with the pilot in duress and cockpit depressurized; Two cabin crew were instrumental in holding the captain's legs during the crisis; Maintenance manager made several errors and did not follow instruction manual, and had no one to check his selection of replacement bolts nor his installation work. Captain sustained moderate injuries, but survived.
ValuJet DC-9 airliner crash, May 1, 1996	Aircraft was designed with no fire or smoke detector, nor extinguishing system, in cargo hold; Such a fire safety system was not required in FAA regulations; Aircraft carried supplementary oxygen for passengers if cabin decompresses while flying above 14,000 feet, delivered through a tube connected to a lanyard-activated canister that burned sodium chlorate to produce oxygen flow for up to 20 minutes; While burning, the outside of each canister reaches 500°F; Pure oxygen and temperatures this high were deemed acceptable by FAA; Canisters had a set life, and had to be periodically replaced using a "routine work card" which said nothing about disposal of expired canisters, though it said install a plastic safety cap immediately over the igniter to prevent accidental ignition if the lanyard was pulled or some other action caused the hammer to fall.	Maintenance contractor SabreTech was to remove outdated chemical-type oxygen canisters from two airliners, but failed to install the small plastic caps that prevented accidental ignition; Canisters collected together in boxes in a DC-9 cargo hold for transport started to ignite due to loading process or vibrations during flight, setting off a fire detected only after aircraft was in flight from Miami to Atlanta; a tire in the same cargo hold exploded and the fire burned through lining in the cargo compartment and reached key electrical wiring, so signals from cockpit to engines were lost: Pilots lost control of aircraft, crashing into the Everglades, killing all 110 on board.	Removed canisters were not "set off" by the contractors, though this would have prevented the accident; Having no supply of safety caps, contractor failed to install these in removed canisters; Canisters were collected together in five cardboard boxes, with bubble wrap padding, and moved from SabreTech "parts rack" to ValueJet holding area; Stock clerk decided to ship them back to ValueJet main depot at Atlanta, with no HAZMAT warning labels; instead, the shipping labels said "empty" canisters were in the boxes.

Discussion and Conclusions

We defined and provided characteristics of technological disasters, emphasizing that human errors in one or more phases of the system life cycle set the stage for disaster. Maintenance actions in large part prevent malfunctions in technology control systems and safety barriers. Despite concerted efforts by maintenance managers and technicians, technological systems do fail. In essence, the complexity and opaqueness of socio-technical systems "mask" the hazards (unsafe conditions) that arise unexpectedly during operations or servicing. To counter the unexpected, designers include multiple independent safety barriers capable of preventing the occurrence or mitigating the consequences of such unexpected events. The integrity of the barriers depends on adequate levels of maintenance. Maintenance is therefore a key activity to reduce the risk of major accidents.

We reviewed classification schemes for technological disaster types as proposed by FEMA, and two detailed taxonomies of causes of technological disasters in the oil, gas, and chemical process industries. The second taxonomy concentrated on maintenance-related disasters, concluding that the most occurring barrier-based factor is maintenance error, and the most occurring maintenance management factors are deficient planning, deficient execution, and deficient checking.

In our research, we analyzed twelve technological disasters as documented in Chiles from a variety of organizations, comprised of [3]:

Explosions	3
Commercial aviation	2
Nuclear power generation	2
Oil and gas exploration	2
Chemical processing	1
Space exploration	1
Structural failure	1

Using a three-factor cause analysis scheme (human error, equipment of process failure, safety barrier failure) we analyzed twelve disasters and found these factors present in each disaster description. In each analysis, we paid particular attention to the role of maintenance managers and technicians in reducing the risk of disaster (probability it would occur, consequences if it did occur). Maintenance was a direct causal factor in six of the twelve (50%) disasters analyzed, as identified below along with identification of the phase of technological system life cycle where the disaster occurred:

Sultana Boiler Explosion	Operations after Inadequate Corrective Maintenance
Three-mile Island Unit 2	Operations with Hazard Introduced by Maintenance
Union Carbide Bhopal Disaster	Corrective Maintenance
Piper Alpha Off-Shore Oil Rig	Operations after Uncompleted Corrective Maintenance
British Airways BAC 1-11 Airliner	Operations with Hazard Introduced by Maintenance
ValuJet DC-9	Operations after Inadequate Disposal of hazardous materials generated from Time-based Maintenance

Maintenance is often characterized as one approach to reliability assurance, but based on the involvement of maintenance activities in largely preventing technological disasters, maintenance also plays a huge role in safety assurance. This mindset needs to be adopted from top management all the way down to those who plan, perform, or support maintenance activities.

References

1. Okoh P, Haugen, S (2013) The influence of maintenance on some selected major accidents", Chemical Engineering Transactions 13: 493-498.
2. Reason J (1997) Managing the Risks of Organizational Accidents, 252pp, Ashgate, Hampshire, UK.
3. Chiles JR (2001) Inviting Disaster: Lessons from the Edge of Technology, 338pp, HarperCollins, New York.
4. Chapman J (2005) "Predicting technological disasters: mission impossible? ", Disaster Prevention and Management 14: 343-352.
5. Reason J, Hobbs A (2003) Managing Maintenance Error: A Practical Guide, 183 pp, CRC Press, Boca Raton, FL.
6. FEMA (1993) "Technological Hazards", Part II of Principal Threats Facing Communities and Local Emergency Management Coordinators, accessed June 6, 2019, https://nehrpsearch.nist.gov/static/files/FEMA/PB94147212.pdf, pp248-291.
7. Shaluf, I. M., Fakhru'l-Razi, A., Shariff, R. (2003) "Technological disaster factors," Journal of Loss Prevention in the Process Industries, 16: 513-521.