

Chapter 1

OVERVIEW

© M. Ragheb
1/17/2026

1.1 INTRODUCTION

We consider the evolution of Safety Analysis as an aspect of the stewardship of the public's health and safety. A safety engineer in a given discipline has a significant professional and ethical responsibility to uphold the public's safety at large.

Historically, kings and monarchs had the responsibility to protect their subjects' health and safety. Their responsibility primarily emphasized disease control. The Monarch's responsibility for the public's safety was replaced by the responsibility of the professional organizations and the state agencies in the industrial age. In the nuclear age with the consideration of higher energy density sources, the responsibility lies with the states and an array of international organizations.

1.2 PRE-INDUSTRIAL PERIOD

In the pre-industrial age the rules upholding public safety were based on religious considerations. In 400 BC there was building and sanitary engineering codes in the Indus Valley. Even earlier in 2,000 BC in the Middle Kingdom of Egypt and at the Incas period, excavations reveal the existence of bathrooms and sewage facilities in their cities.

At the time of the ancient Greeks, principles of hygiene and the relationship between environmental factors and the prevalence of disease were understood. They were expressed in the Hippocratic collection on epidemiology: "Air, Waters and Places."

At the time of the Romans the relationship between swamps and malaria (In Latin: mal: bad, aria: air) was established leading to an effort to drain swamps, even though mosquitoes were not directly implicated as vectors for the malaria parasite. The Romans brought fresh water to their cities around the Mediterranean using water aqueducts. They built public baths with hot water, sewage systems and used dust respirators. In 532 AD, the Emperor Justinian I of Byzantine set quarantine posts at the borders of the Eastern Roman Empire, and required certificates of health for admission to its capital Constantinople, as an effort to combat the plague pandemic.

Public health was upheld by state religion. In Judaism and Christianity the Old Testament's books of Leviticus and Numbers, dietary laws, rules of hygiene, precautions against contagious diseases, and prohibitions against consanguine marriages are enunciated. These are similar to their counterpart contemporary rules related to food preservation, epidemic control and hereditary diseases.

The Islamic faith emphasized cleanliness in the ablution ritual before its five daily prayers, and established rules against eating dead animals and eating food containing blood, a known nutrient-rich growth medium for disease vectors.

In Britain, the common-law concept of public nuisance emphasized the protection against polluting public water supplies. In 1309 ordinances regulating cesspools and

sewers were established. Similarly, in France, Germany and Italy, the tanners were prohibited from washing animal skins in rivers or the water supply.

In Florence, Italy, meat slaughtered on Friday was forbidden to be sold on Monday in butchers' shops. Refrigeration did not exist then, and meat was preserved through salting, smoking and the use of spices.

In the nineteenth century, migration to the large cities from the countryside was associated with the spread of communicable diseases. Smallpox epidemics occurred in London during the period 1723-1796, with a periodicity of five years, claiming 3,000 lives each time. Infant mortality became rampant: in the 1740's when 75 percent of London's infants died before the age of five years. Typhus and scarlet fever prevailed.

Victorian England saw a marked improvement in nutrition and working conditions. In the Public Health Act of 1848, local Boards of Health enforced sanitation requirements.

1.3 INDUSTRIAL AGE

The industrial age saw the birth of energy sources, particularly the steam engine. For higher efficiency according to Carnot and Watt theories, engineers sought ever and ever higher steam temperatures and pressures.

The original boilers and steam generators were simple pressure vessels prone to catastrophic failures that were associated with significant loss of life. In current steam generators safer boiler designs, such as tube-fired boilers, inspections have reduced the incidence of catastrophic failures to a rare event with a failure likelihood of:

$$L = \frac{1}{100,000} = 10^{-5} \left[\frac{\text{failure}}{\text{vessel.year}} \right] \quad (1)$$

This likelihood is statistical in nature and should be understood accordingly. If there are 1,000 vessels, then the likelihood is understood to have a failure frequency of once every 100 years:

$$L = \frac{1}{1,000 \times 100} = 10^{-5} \left[\frac{\text{failure}}{\text{vessel.year}} \right]$$

If there were 10,000 vessels, then the failure frequency would be once in 10 years:

$$L = \frac{1}{10,000 \times 10} = 10^{-5} \left[\frac{\text{failure}}{\text{vessel.year}} \right]$$

In general, the failure likelihood L is expressed as:

$$L = \frac{f}{N} \left[\frac{\text{failure}}{\text{vessel.year}} \right] \quad (2)$$

It should be noticed that L in Eqn. 2 is strictly a likelihood, or a per unit frequency, and not a probability, since mathematically, probability has strictly no units.

In England in 1866 there were 74 boiler explosions per year claiming 77 deaths. By 1900, the number was reduced to 17 boiler explosions per year leading to 8 deaths. By this time, boiler inspections were established in England by the Manchester Steam User Association. In the USA the American Society of Mechanical Engineers (ASME) issued the ASME Pressure Vessel Codes.

After the Steam Engine came the internal combustion engine introducing speeds never experienced before in transportation by rail, road and air. This required the imposition of regulations, inspections and design standards.

It must be noticed that these regulations were imposed *after* the hazards had been exhibited through many unfortunate deaths and injuries.

1.4 THE NUCLEAR ERA

Nuclear fission introduced an energy source with an energy density far exceeding any other form known to humanity whether from natural sources such as wind, solar or hydroelectricity or chemical sources such as the steam engine and the internal combustion engine.

Nuclear Power Safety has attempted, rather successfully, to anticipate the risks *before* their occurrence and prevent them through:

1. Design,
2. Control,
3. Regulation.

The development of nuclear devices during World War II generated experience in the production of enriched uranium and of plutonium in research reactors. These were followed by the introduction of power reactors initially for naval propulsion, then for land-based electrical power generation.

This higher energy density source necessitated the formation of Reactor Safeguards Committee in the USA in 1947, followed by the Atomic Energy Act of 1948. The Advisory Committee on Reactor Safeguards (ACRS) merged the Reactor Safeguards Committee and the Industrial Committee on Reactor Location Problems in 1951.

Industrial nuclear power became feasible with the first nuclear electrical power plant operating at Shippingport, Pennsylvania in the USA in 1957. This followed the Atomic Energy Act of 1954.

The financial liability of nuclear utilities and insurance companies was limited by the government covering the liability in the same way it covers it for other disasters such as floods, hurricanes or severe storms by the Price-Anderson Act of 1957.

Safety Analysis studies introduced new methodologies for the design and operation of this new energy system. These methods were shared by other engineering fields such as structural engineering and aerospace, generating the nascent engineering discipline of Safety Engineering, with its own professional society, and a professional degree offered at some universities.

Two of these landmark studies are the WASH-740 and the WASH-1400 safety reports.

1.5 FIRST REPORT ON NUCLEAR POWER PLANTS ACCIDENTS: WASH-740

This report issued in 1957 was undertaken by the Brookhaven National Laboratory (BNL) at Upton, on Long Island, New York, USA. In this report, the probabilities of accidents were thought to be small. However due to unrealistic assumptions, such as the total release as well as full ingestion of the fission products by the population around a plant in the case of a reactor accident, the predicted consequences were deemed unrealistic.

This report introduced the Maximum Credible Accident Method giving rise to:

1. A probabilistic approach to the siting of nuclear power plants introduced by Farmer in 1967 and by Otway and Erdman in 1970.
2. The methodology of Accident Analysis introduced by Garrick in 1967, Salvatori in 1970, Brunot in 1970, Otway in 1970, Crosetti in 1971, and other prominent researchers.
3. The technique of “Fault Tree Analysis” followed by “Consequence Analysis” of the postulated accidents by Mulvihill in 1966.

1.6 REACTOR SAFETY STUDY (RSS), RASMUSSEN REPORT: WASH-1400

This study was conducted at the Massachusetts Institute of Technology (MIT) under the leadership of Norman Rasmussen. A draft report was released in August 1974, followed by a revised version in October 1975. A review report designated as the “Lewis Report” from the University of California at Santa Barbara as NUREG/CR-0400 followed.

The report was initiated in response to a letter from USA Senator Pastore to James Schlesinger, Atomic Energy Commission (AEC) Chairperson, and requested risk information for the Price-Anderson Act renewal.

The report considered more realistic modeling of accidents events than the highly conservative previous WASH-740 report.

The technique of “Event Tree Analysis” was introduced to link the system’s “Fault Trees” to the accident initiators and the core damage states. The techniques of “Fault Tree Analysis” and “Event Tree Analysis” have become standard techniques for the probabilistic safety analysis of engineering systems.

This was adopted as a pattern for performing Probabilistic Risk Assessment (PRA) and provided a basis for comparison of different risk estimates.

The report compiled a useful failure data base for a plant’s components. It found that human error could be a major contributor to reactor accidents. It clarified the impact of test and maintenance, and pointed out to the possibility of common-mode interactions.

The report identified transients and Small Loss of Coolant Accidents (SLOCAs) as the major risk contributors to reactor accidents rather than the Large break LOCAs. It also established that the risk of existing nuclear power plant designs is small compared to other natural and man-made societal risks.

The findings and methodologies of the report were later vindicated and proved suitable for Safety Analysis by the Three-Mile-Island, Chernobyl and Fukushima accidents.

1.7 GOALS OF SAFETY ANALYSIS

Accidents and disasters do occur with consequences that include human deaths and injuries, economical loss or environmental degradation. They could occur in man-made structures, and could be caused by natural events.

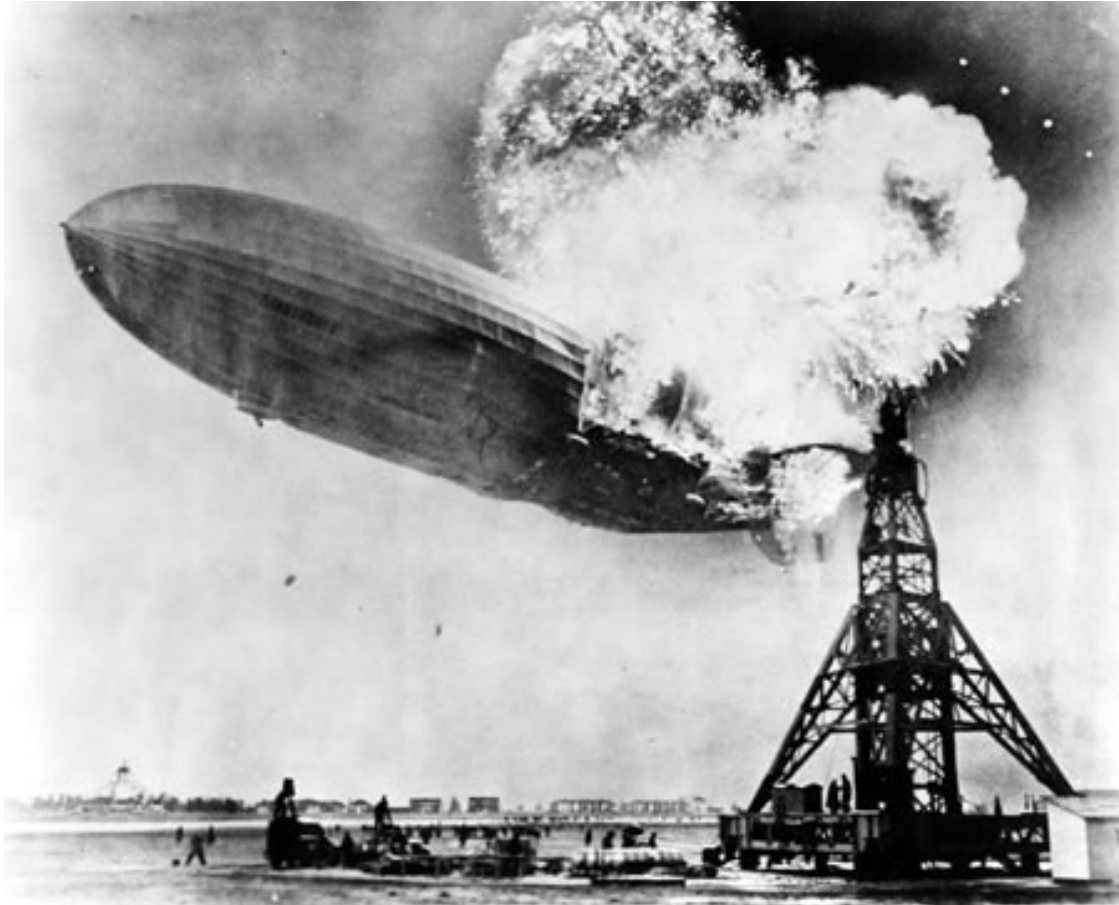


Figure 1. The use of hydrogen instead of helium, led to the Hindenburg accident and the end of the dirigibles transportation era.

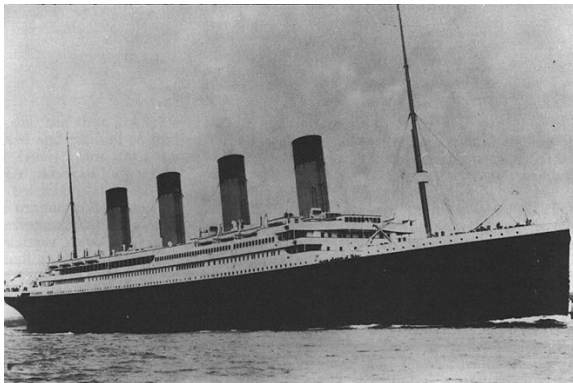




Figure 2. The use of mild steel that becomes brittle at cold temperatures contributed to the sinking of the “unsinkable” Titanic in 1912 on its maiden trip to New York and the end of the large transatlantic vessels travel with bacteria feeding on the wreck in 2019.

In the case of natural disasters, predicting them ahead of time and providing vulnerable human structures, such as dams, levies or shelters or planning management measures such as early warnings and evacuations, can mitigate their consequences.

In the case of man-made structures, they are supposed to be conceived at the design stage so as to anticipate the worst case scenarios and equip them with the appropriate “Engineered Safety Features” or ESFs, so that they occurrence is prevented in the first place. If they ever happen, then those ESFs would function to minimize any loss of life or property.



Figure 3. Three Mile Island reactor accident in the USA, caused by human error in maintenance procedures and equipment failure.



Figure 4. Chernobyl Reactor accident in the Ukraine, caused by human error in operation.

EXERCISES

1. For a rare failure event in chemical reaction vessels with a design failure likelihood of 10^{-4} failures / (vessel.year), calculate the frequency of occurrence for:
 - a. 100 vessels in service,
 - b. 1,000 vessels in service.
2. For a Loss of Coolant Accident (LOCA) likelihood of 10^{-5} occurrences / (reactor.year), calculate the frequency of occurrence for:
 - a. 97 reactors in service in the USA,
 - b. 446 reactors globally.