

Lessons from the Chernobyl Disaster: The Importance of DFMEA in Nuclear Power Safety

Rose Maire Gebara

Master's Student

Department of Industrial Engineering

Lawrence Technological University

Southfield, Michigan 48075 USA

rgebara@ltu.edu

Daw Alwerfalli

Director of the Master of Engineering Management

Department of Mechanical Robotics and Industrial Engineering

Lawrence Technological University

Southfield, Michigan 48075 USA

dalwerfal@ltu.edu

Abstract

This paper applies a Design Failure Mode and Effects Analysis to the Chernobyl disaster to identify technical, organization and human failures that lead to the 1986 reactor explosion. The RBMK-1000 reactor was built with a dangerous combination of graphite-tipped control rods, a water-cooling system, a positive void coefficient and low enriched uranium. This combination made the perfect environment for meltdown caused by positive SCRAM effect. Procedural violations, inexperienced operating crew, poor communication, and lack of a safety culture compounded with these design flaws created a ticking time bomb. Many of these failure modes were scored to be the maximum severity rating that the DFMEA has, due to the generation environmental damage the health consequences that continue to affect the region. This analysis demonstrates how the absence of risk assessment, mitigation, safety protocols allowed a preventable failure to blow up into a catastrophe that will last generations. These findings demonstrate the important role DFMEA has in modern engineering and its importance in preventing future tragedies.

Keywords

DFMEA, FMEA, Nuclear Power Plant, Risk Assessment, Nuclear Meltdown, Chernobyl, Quality

1. Introduction

Safety tends to be paved in blood. The Titanic, Texas City Refinery explosion, Lac-Mégantic rail disaster, Deepwater Horizon Oil spill, Challenger Explosion and the Chernobyl nuclear disaster all have one thing in common they did not do adequate risk assessments. Risk assessments are not only good to make sure that the product we create does what we create it to do but also to keep the people who use said product and possibly the people and environment around the product safe. In nuclear power plants this is extremely important. As meltdowns of these plants cause a huge amount of damage not only to the plant workers but the surrounding areas and sometimes it is felt on a wide scale. The best example of risk assessment failure in nuclear power plants was in the Chernobyl disaster on April 26, 1986. In fact, it is the only one where the design of the plant itself is mostly to blame however, reports show that the employees were also not qualified nor trained to run the plant safely. Chernobyl is

one of the reasons that some of the public fear these plants and do not want them built. Even though these plants are mostly safe, giving great electric output and are better for the environment. Especially with tools engineers now have at their disposable like DFMEA. The purpose of this article is to stress that when it comes to designing products, mainly nuclear power plants, to do more than adequate risk assessment to make sure that these plants are safe. To demonstrate this importance the DFMEA process is applied to Chernobyl's reactor four to find possible failure modes.

1.1 Objectives

The objectives of this paper are as follows:

1. To apply a Design Failure Mode and Effects Analysis to the Chernobyl reactor 4 meltdown
2. To use DFMEA to evaluate the design flaws of the RBMK-1000 reactor
3. To analyze how human factors and weak safety culture can compound failure modes
4. To demonstrate the importance of use of DFMEA in the nuclear industry
5. To explore how lessons from Chernobyl have affected design in modern nuclear power plants.

2. Literature review

While nuclear power is the safest way to create power when things go wrong, they are cataphoric (World Nuclear Association, 2026). To prevent disasters the International Atomic Energy Agency (IAEA) has come up with many guidelines to design, build and upgrade anything in a nuclear power plant (International Atomic Energy Agency , 2005). These guidelines include FMEA and DFMEA (Figure 1). The IAEA states that DFMEA should be conducted before all designs are released to be built. Countries such as the United States of America follow these guidelines, requiring by law to have documents such as DFMEA documentation to be submitted to before anything can be done. (Hoag, 2014).

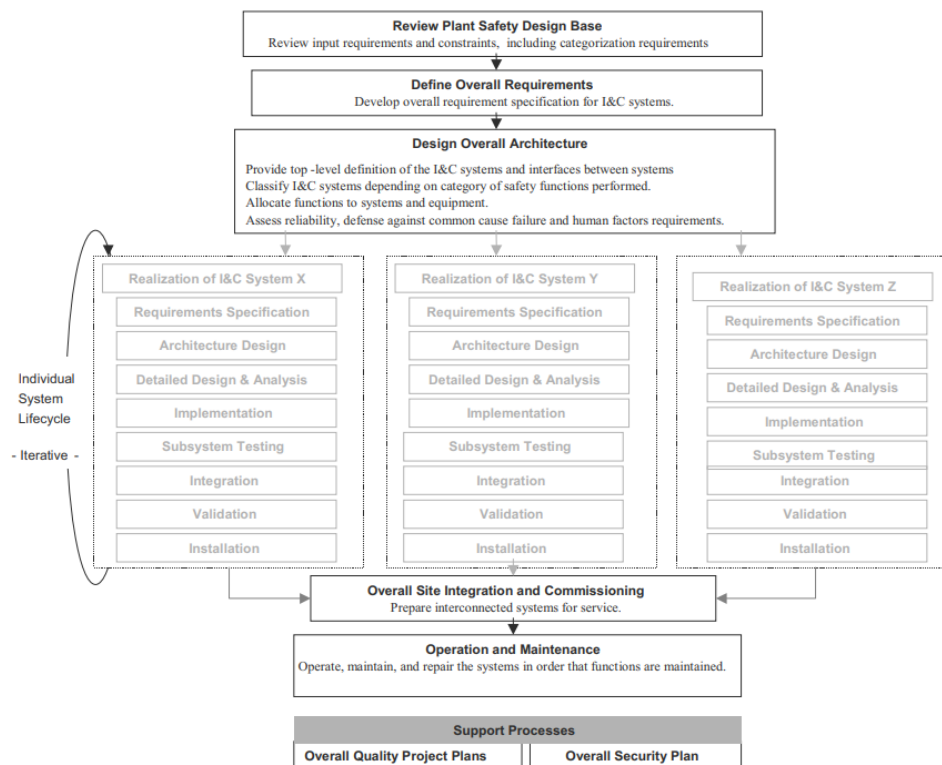


Figure 1. Life Cycle for Overall I&C development (International Atomic Energy Agency , 2005)

Chernobyl reactor meltdown was the result of a combination of bad design and human error. However, out of the three major nuclear power plant disasters Chernobyl was mainly due to bad design and not by human error. The main issue was the reactor design itself. The Soviet designed RBMK 1000 reactors were built to be as cheap as possible with the highest power output, 3200 MW, that was possible (World Nuclear Association, 2026).

The type of reactor 4 is a graphite moderate pressure tube type (Figure 2) (World Nuclear Association, 2026). Unlike nuclear power plants outside of the Soviet Union this type of reactor had no intervening heat exchanger nor containment structures. Another unique design decision was that this type of reactor was cooled by water and moderated by graphite.

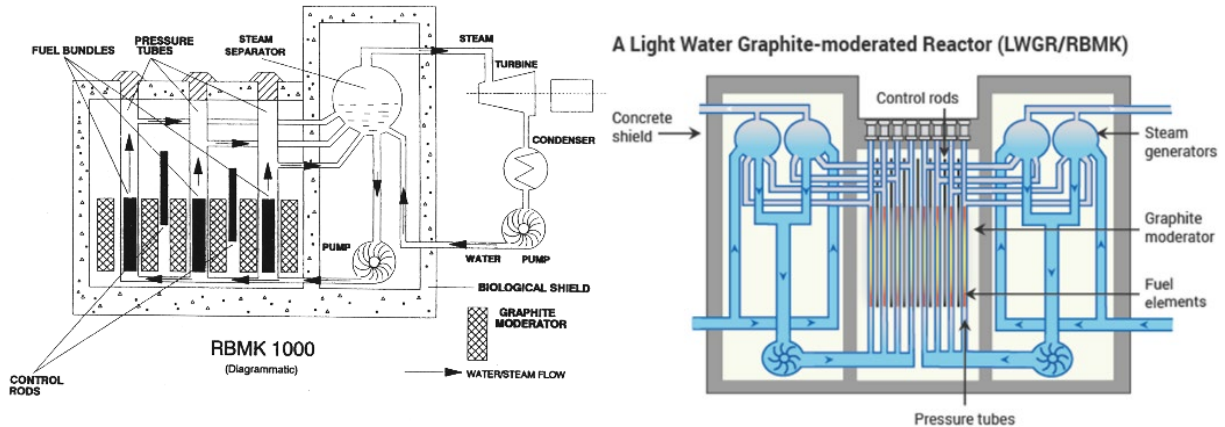


Figure 2. RBMK – 1000 Reactor (World Nuclear Association, 2026) (World Nuclear Association, 2026)

One of the most dangerous features is that this reactor had a positive void coefficient due to being cooled by water and moderated by graphite (World Nuclear Association, 2026). In other types of reactors, the void coefficient is not the dominate component of the overall power coefficient of reactivity. Having a positive void coefficient means that the RBMK reactors use this coefficient as the main component of the overall power coefficient of reactivity. Unknown to the Soviet nuclear power plant employees this feature could under the right conditions can cause a positive SCRAM effect. The positive SCRAM effect is an effect where after the shutdown, also known as SCRAM, signal the control rods enter the core and this increases the reactivity in the core instead of stopping or reducing the reactor activity. The engineers at the power plant did not know about the SCRAM effect.

However, a positive SCRAM effect had already happened in another reactor (Chernov & Sornette, 2016). In November 1975, a reactor near Leningrad had a reactivity excursion after an emergency shutdown. The investigation team concluded that the reactor core needed to be redesigned, noting that the control rods and the speed of the SCRAM needed to be changed to reduce the void coefficient. These design recommendations were not acted upon until after the Chernobyl disaster.

3. Methods

The first step is scoping of DFMEA (Ansys, 2023). This involves defining product requirements and determining the appropriate level of detail for the analysis. At this stage, the team can decide whether to break down into subsystems or be represented using a functional block diagram.

The second step is failure mode and effects definition. This begins with defining the intended functions of the product, followed by identifying the potential failure modes. Then to define the effects of the failure; how it is affecting the product, can a failure from one system affect another, and how severe the failure is. After evaluations are complete, each failure scenario is then to be rated, 1-10, by the team using the severity rating table (Table 1).

Table 1. Severity Rating (Ansys, 2023)

Effect	Criteria: Severity of Effect	Ranking
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	10
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	9
Very High	Vehicle/item inoperable (loss of primary function).	8
High	Vehicle/Item operable but at a reduced level of performance. Customer very dissatisfied.	7
Moderate	Vehicle/Item operable but Comfort/Convenience item(s) inoperable. Customer dissatisfied.	6
Low	Vehicle/Item operable but Comfort/Convenience item(s) operable at a reduced level of performance. Customer somewhat dissatisfied.	5
Very Low	Fit and finish/Squeak and rattle item does not conform. Defect noticed by most customers (greater than 75%).	4
Minor	Fit and finish/Squeak and rattle item does not conform. Defect noticed by 50% of customers.	3
Very Minor	Fit and finish/Squeak and rattle item does not conform. Defect noticed by discriminating customers (less than 25%).	2
None	No discernible effect.	1

The third step of DFMEA is risk assessment, this consists of obtaining a risk priority number (RPN) and developing risk matrices to identify which failure modes are the most critical to correct (Hartwell J. , 2022). The first step for finding the RPN of a failure mode is to evaluate three criteria: severity, occurrence, and detection. Each index is scored out of a scale from 1-10 scale.

- For Severity, a score of 1 reflects the failure has a minimal impact on the product, while a 10 indicates a catastrophic failure.
- For Occurrence, a score of 1 means a low likelihood of failure occurring, while 10 means it has a high probability of failing.
- For Detection, a score of 1 means a high chance of detecting potential failure, while a 10 means the failure is exceedingly difficult to detect.

To calculate the RPN, the scores for severity, occurrence and detection are multiplied together (Figure 3). The resulting RPN is then used to rank the failure modes from lowest to highest risk. The team uses this ranking to determine what failure scenarios require prioritize corrections and what failure modes are considered an acceptable risk.

Functions	Requirement	Failure Mode	Effects	Severity	Class	Causes	Control Methods				RPN
							Prevention Control	Occurrence	Detection Control	Detection	
Automatically paint the door of the car	Fully cover the required area of the door with required color	Foreign body in painting layer of the door	Bad appearance	5	6	Contamination of the room	Check room cleanliness every day	6	Appearance check after painting 100%	4	120
		Door surface is not covered	Bad appearance of the door; Car surface is not protected.	Door is not set correctly in the painting machine		Door setting working instruction	8	Appearance check after painting 100%	4	192	
				Painting machine with trav		Painting		Appearance	4	192	
	Paint thickness meet the required specification	Paint layer is too thin	Color is not good Durability of painting layer is shorter than specification		8	Spraying parameter is incorrect	Painting parameter setting instruction	8	Check the thickness of the first piece sample	6	384

$RPN = \text{Severity} \times \text{Occurrence} \times \text{Detection}$
 $= 5 \times 6 \times 4 = 120$

$$RPN = \text{Severity} \times \text{Occurrence} \times \text{Detection}$$

$$= 5 \times 6 \times 4 = 120$$

Figure 3. RPN (Hartwell J. , 2022)

A risk matrix is a tool used to help with the prioritization of corrective actions for failure modes (Figure 4) (Hartwell J. , 2022). These matrices combine two or three evaluation criteria to evaluate what failure mode needs corrective action. The metrics evaluated in a risk matrices can be any combination of RPN, severity, occurrence, or detection. A risk matrix compares the different criteria and colors in the resulting conclusion in the matrix: acceptable (green), consideration (yellow) and needs corrective action (red).



Figures 4. Risk Matrixes (Hartwell J. , 2022)

The last step, step four, is risk mitigation and prevention (Ansys, n.d.). Using the severity rating, the RPN and the results of the risk matrixes, the DFMEA team recommends a plan of action to the appropriate groups to address the identified risks. These preventive actions can include but are not limited to making a user's manual, changing in product design, recommending training for users, and a maintenance guide. All this information is recorded in a DFMEA document. This document not only documents the corrective changes that need to be implemented but also a formal record of the DFMEA process.

Literature search was done using the TechCat+ engine at Laurence Technological University library, Copilot, google and Chat GPT. Search phrases included: Chernobyl disaster, Fukushima nuclear power plant, nuclear power plant DFMEA, DFMEA, DFMEA vs FMEA, Chernobyl timeline, Positive SCRAM effect, RBMK reactors, RBMK reactor flaws, DFMEA software, Chernobyl New safe confinement, Chernobyl Russia strike, radiation sickness, affects from Chernobyl on Europe, Environmental effects from Chernobyl, DFMEA failures, disasters that had bad DFMEA

4. Applying DFMEA to Chernobyl

The DFMEA methodology was applied to the RBMK-1000 reactor 4 in Chernobyl to identify the failure modes that contributed to the disaster. Due to the nature of DFMEA, this analysis will be focused on the design phase. The inherent weakness of the reactor and how this weakness allowed this explosion to happen will be analyzed. While human error played a significant role, this approach focuses on the design flows in the system that would result in operators making mistakes that escalated the danger.

First, let's look at the scope of this reactor. Due to this being a postmortem of the accident, the scope will include the major design faults that led to the accident.

- Producing reliable and enough electrical power to the region it is designed for
- Nuclear fission must be able to stable and controlled
- Operation at any power level should be safe or have a clear procedure to make it safe
- If an explosion occurs preventing the release of radioactive material outside of the plant
- Have a protocol if radioactive material is released into the environment

Given the dangerous nature of potential hazards associated with radioactive materials, a high level of detail is required. Therefore, the reactor should be divided into the following subsystems:

- Reactor core and fuel channels
- Graphite rods (moderation system)
- Water cooling system
- Control rod
- SCRAM mechanisms
- Reactivity coefficient measurement
- Containment and safety systems
- Fire protocol

To understand the failures of the design and the crew, it is necessary to understand the sequence of events that led to the explosions. This reveals how the weakness in the design and the inexperienced crew created a chain of failure leading to the meltdown of reactor 4.

On April 25, 1986, engineers start to prepare for a safety test by lowering the power and disabling the emergency core cooling system (World Nuclear Association, 2026). When the shift changed at 11:10 pm a less experienced crew took over the preparation. This crew never received the proper instructions for the safety test. In the early morning of April 26, the power plummeted to an extremely low level causing the reactor to become unstable. The inexperienced crew defied the safety guidelines and removed most of the control rods to raise power and stabilized the reactor. To make this more complicated to get the operating reactivity margin it took the instruments 10-15 minutes for the computer to collect all the data and to calculate the ORM (International Nuclear Safety Advisory Group, 1992). Once the reactor stabilized the safety test began, however the power was still too low required for the test, but the supervisor told the crew to proceed. The instrumentation could not give correct measurements under the low power conditions. Giving the crew a false sense of controllability at the low power. To start the test, they need to start turbine coasting by closing the turbine feed valves, which performed as expected. Then the operator pressed the emergency button, AZ-5, causing the control rods to begin to enter the core of the reactor. This caused the reactivity in the bottom of the core to increase, which caused the power to rise. The turbine valves were then opened causing an increased flow of water to the core leading to more power created. This caused the fuel elements to rupture, leading to more steam causing more power to be generated. The increased reactivity and the increased amount of water caused a large amount of water to convert to steam. Steam started to rapidly accumulate in the reactor causing a sharp rise in pressure. The pressure became too much causing the first explosion. The second explosion is thought to be caused by zirconium-steam reactions producing high amounts of hydrogen. This pressure was too much for the upper biological shield to handle causing the second explosion and moving the 1,000-2,000-ton upper biological shield (Figure 5). This explosion sent radioactive fuel, radioactive graphite rods, and building material all over the area. About 1200 tons for hot radioactive graphite was ejected from the core leading to many fires in the surrounding area.

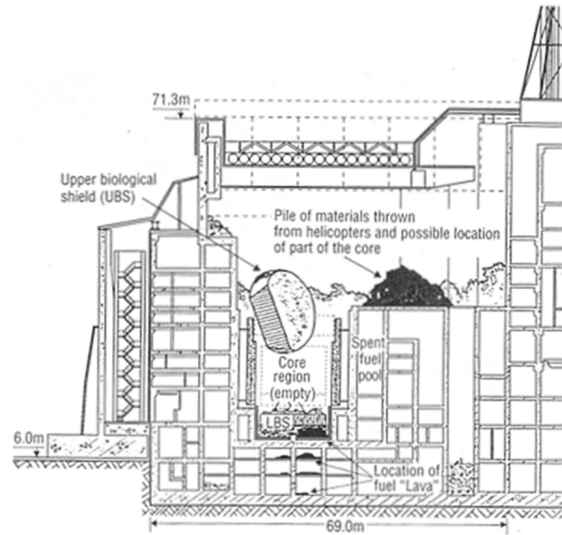


Figure 5. Damage of Reactor 4 (World Nuclear Association, 2026)

There was no proper protocol, plan nor training to deal with this disaster (World Nuclear Association, 2026). In the same way of not altering the engineers of the danger of the positive SCRAM effect firefighters were not told about the dangers that they would face in putting out the fires. Even if they were told they had no training in how to handle this nor did they have the proper safety equipment to deal with radiation.

These subsystems will make identifying failure modes, the cause and effect of these modes manageable within the DFMEA process.

The second step is to create a severity rating. Due to the potential damage that a meltdown can cause the severity rating table was altered to fit that potential harm (Table 2).

Table 2. Chernobyl Severity Rating

Effect	Criteria: Severity of Effect	Ranking
Catastrophic	Nuclear meltdown, radioactive material breaches the biological shield and contaminates the surrounding areas. Damage is done to the core, fuel channels, rods, etc. Core is exposed to the atmosphere	10
Extremely High	Nuclear meltdown, radioactive material breaches the biological shield, only the building is contaminated. Damage is done to the core, fuel channels, rods, etc., Core is not exposed.	9
Very High	Nuclear meltdown, radioactive material is contained in the core and core is not exposed. Damage is done to the core, fuel channels, rods, etc.,	8
High	Nuclear meltdown, radioactive material is contained, no damage is done, core is not exposed.	7
High Moderate	Significant amount of damage is done to the facility or significant breakdown of systems. Nuclear reactors can be turned off or are not affected.	6
Moderate	Breakdown of systems or damage to equipment, nuclear reactors can be turned off or are not affected.	5
Low Moderate	Minor equipment damage, possible temporary loss of function, no impact to safety.	4
Low	Noticeable effect to system, no damage nor impact to safety, easy to correct	3

Very Low	Minor effect to function, no effect on equipment nor safety	2
None	No effect	1

The third step is to evaluate the risks by rating the severity (S), probability (P) and the ability to detect (D) failure, then calculating the RPN (Table 3). Due to the complexity of the RBMK-1000 reactor, the items or subsystems are simplified to only what caused the disaster.

Table 3. RPN

Item/subsystem	Function	Requirement	Failure Mode	Effects	S	Causes	P	Prevention control	D	Detection control	RPN
Reactor Core and Fuel Systems	Produce Power	Sustained and controlled Fission	Not Sustained nor Controlled Fission	Core becomes Instable	9	Low enriched fuel, low power	7	Use 3%-5% enriched fuel	7	Limited measuring instruments	441
Moderation System	slow down neutrons, sustain continuous fission	Moderate Fission	Positive Void Coeff	Uncontrolled power increase and steam created	10	Graphite Rods combined with water cooling system	8	Redesigning the control rods to not give rise to water columns	9	Limited measuring instruments, unknown to crew	720
Water Cooling Systems	Cool Reactor Down	Cool reactor without affecting the reactivity	Steam created, Fuel damage, failure to cool	Pressure creates an explosion, overheated core, increased reactivity	10	Graphite Rods combined with water cooling system	6	Redesigning the control rods to not give rise to water columns	8	Flow monitoring, limited control over each channel	480
Control Rod	Control rate for Fission	Keep fission rate in a stable and controlled state	Rods do not lower or delayed/slow lowering	Reactivity cannot be stabilized	10	Reactivity of the controls, extracted state designed too high	6	Shorter insertion length	8	Regulated via feedback from detectors	480
SCRAM Mech	Emergency stop	Put control rods in place	Rods do not lower or delayed/slow lowering	Reactivity cannot be stabilized	10	Reactivity of the controls, extracted state designed too high	8	Shorter insertion length of rods, mechanism slow to react	9	Regulated via feedback from detectors	720
Reactivity Coef. Measurement	Measure Coef.	Tell operator the reactivity of the fission	Not measuring correctly or at all, undertrained operator	Reactivity is unknown, proper corrective actions cannot be taken, inexperience leads to operator actions increase reactivity	10	Bad, damaged unmaintained equipment, inexperienced crew	5	Check sensors, have multiple, proper training	7	Limited real time sensors	350
Containment and Safety Systems	Radiation shield	Keep radioactive material and radiation particles inside core	Shield Fails, crack or full destruction	Radioactive materials or partials are in the environment and core is exposed	10	Damage due to pressure from steam, earthquake, tsunami, military attack	2	Possible second shield, not allowing pressure build up	10	Radiation Alarms, workers looking at core	200
Fire Protocol	Fire response	Containing fire safely and knowledge of potential harm of radioactive materials	Firemen exposed to radioactive materials, radioactive contamination to second site	Firemen die or get sick from radiation positioning, other areas infected to radiation leading to more people being exposed	10	No communication	10	Tell firemen what they are dealing with, training prior to instant.	10	None	1000

For the RPN matrix threshold of high risk is $RPN > 500$, medium risk is 200-500, and the low risk is < 200 . From the minimal data an RPN matrix can be made but not fully.

Severity	10										
	9										
	8										
	7										
	6										
	5										
	4										
	3										
	2										
	1										
		1	2	3	4	5	6	7	8	9	10
RPNx10											

Figure 6. RPN Matrix

As seen in the RPN matrix, all these issues are either medium risk or high risk (Figure 6). If a DFMEA was done on the RBMK-1000 reactor these potential failures might have been spotted.

The final step of DFMEA is risk mitigation and prevention. Unfortunately, these preventatives and mitigating actions became clear after the Chernobyl disaster. Based on the DFMEA conducted in this study, the recommended actions would be; improved training for reactor operator and chief engineer, a thought out plan for accidents, accurate real-time measurements, use of 3-5% enriched uranium, faster SCRAM rod insertion time, an emergency systems that don't need to be shut down for testing the reactor, system redundancies, fail safe systems, a containment structure, a stronger safety culture, and replacement of the graphite-tipped control rods.

This analysis using DFMEA makes it very clear that failures were not random or bad luck. They were identifiable and correctable during the design process of the reactor if someone sat down and thought of what could go wrong. In addition, the failure to make sure that crew had the necessary knowledge and training the disaster could have been reduced. However, just due to the design there would have been a major meltdown with the RBMK-1000 reactor. It is only a question of where and when. There are many lessons that can be gained by understanding what happened at reactor 4 that day, not just in nuclear power industry.

5. Lessons Learned

5.1 Engineering Lessons

There are many lessons that can be learned from an engineering viewpoint, safety is paved in blood. One of the major lessons is that risk analysis during the design phase is super important. Going though and trying to find how this can fail can bring up issues that were not obvious before. Also, when finding an issue after the product is produced, doing the time to redesign to remove or lessen the severity, probability, and increase detection of the failure mode.

Another lesson is the need for fails safe systems. The emergency stop failed and there was nothing the crew could do but watch. With how dangerous a meltdown is there should be something that can be done to manually stop or have the reactor start to shut its self-down when it becomes unstable. This also can be done with redundancy. To have another way to decrease the reactivity would have stopped the meltdown. If there was another set of rods able to descend the meltdown could have been avoided.

Accurate instrumentation that shows data in real time would have shown the engineers better data to react in a more appropriate matter. 10-15 minutes is an extremely long time to get data about the reactivity that should be achieved in real time or with a very small delay, less than a second. In addition, the instrumentation was not accurate at the low power at the beginning of the test. Leaving the crew with a false sense of control and completely blind when the situation becomes out of control.

The next lesson is to validate the physics of the void coefficient. Knowing if a positive void coefficient is dangerous via calculations, finding if it is unstable or how it reacts with the systems around it. Another thing they could have done is exploring what others are doing and not doing. If everyone is not using a positive void coefficient there might be a good reason.

The last engineering less is the important of containment structures if the material you are working with is dangerous. Containment structures could be the only thing that stops contamination of dangerous material in the environment. The more dangerous the material the more serious the containment structures should be. In addition, it is speculated that the second explosion was due to the core being exposed to the atmosphere. If there was a stronger and possibly a second containment structure the radiation could have been somewhat contained. Also, it could have kept fires from starting if the structures were made from nonflammable material.

5.2 Organizational Lessons

Since about 80% of all nuclear incidents are due to human behavior there is a strong emphasis on a strong safety culture (World Nuclear Association, 2026). The safety culture of nuclear power plants is an all-hands-on deck approach. Workers undergo extensive training and retraining to make sure accidents don't happen. There is also a high emphasis on high security, especially when it comes to possible terrorist attacks. There are also detailed accident management procedures for nuclear meltdowns, damage caused by natural disasters and safe sudden shutdown procedures for seismic events.

There is a strong international effort so that disasters like Chernobyl don't happen again. The IAEA created an international safety agreement to maintain fundamental safety principles and a high level of safety (International Atomic Energy Agency, n.d.). This group meets regularly to develop and promote new and high-level safety protocols.

The safety culture in the Chernobyl plant was abysmal. There were many glaring issues that did contribute to the disaster. One of these issues was that the Chief Engineer had the ability to deviate from test procedures (International Nuclear Safety Advisory Group, 1992). In fact, the Chief dismissed normal regulations for disabling the emergency core cooling system during the test that caused the explosion. The operators had a poor understanding of the importance of the amount of control rods in the core had to do with the operating reactivity margin. There was also a general lack of understanding of where responsibilities lie. The operating crew had a great lack of operating experience combined with a plant wide problem with communication.

Chernobyl lack of accident management was evident with the emergency response. Emergency responders were not trained nor equipped to handle the disaster. Over 100 firefighters responded to the fire they ended up receiving the highest amount of radiation (World Nuclear Association, 2026). This resulted in many getting acute radiation sickness which ranged from mild to severe. While most survived, many were left with cataracts, scarring and ulceration and in the worse cases severely immunocompromised (Atomic, 2000).

5.3 Modern Nuclear Safety and DFMEA

The safety of nuclear power plants is important to the environment, workers, and the surrounding community. Keeping plants from melting down, workers from getting exposed, or radiation leakage is important to the safety of everything in and surrounding the plant. From redundant systems, comprehensive monitoring, training, and regular testing modern nuclear safety is defense-in-depth approach (World Nuclear Association, 2026). Worldwide agencies like the IAEA and World Nuclear Association create protocols and work to make nuclear power safer. From improved training, implementing better instrumentation and containment, to safety standards nuclear power plants are much safer. The industry now has safety culture down to a science: prevention, monitoring and action. The U.S Department of Energy has regularly done major risk assessments and continues to develop technology to make nuclear power plants safer (Vedros, Christain, Otani, Cheng, & Gonzales, 2024).

Following the Chernobyl accident, safety improvements were implemented to all RBMK reactors (World Nuclear Association, 2026). The major improvements were retrofitting the control rods, a faster SCRAM rod insertion time, and fast-acting emergency protection. Even with all these improvements many of these reactors were never built, shut down, or are scheduled to shut down (Table 4).

Table 4. List of RBMK Reactors

Location	Unit	First Power	Unit net capacity (Mwe)	Status
Lithuania				
Ignalina	1	1983	1185(originally 1300)	Closed 12/2004
	2	1987	1185(originally 1300)	Closed 12/2009
Russia				
Kursk	1	1976	925	Closed 12/2021
	2	1979	925	Closed 01/2024
	3	1984	925	Operating until 2029
	4	1986	925	Operating until 2031
	5	-		Construction cancelled
Leningrad	1	1973	925	Closed 12/2018
	2	1975	925	Closed 11/2020
	3	1979	925	Operating until 2030
	4	1981	925	Operating until 2026
Smolensk	1	1983	925	Operating until 2028
	2	1985	925	Operating until 2030
	3	1990	925	Operating until 2050
Ukraine				
Chernobyl	1	1977	925	Closed 1996
	2	1978	925	Closed 1991
	3	1981	925	Closed 2000
	4	1983	925	Reactor destroyed April 1986
	5	-	925	Construction cancelled
	6	-	925	Construction cancelled

The famous sarcophagus that contained the reactor was never made to be permanent and over time has become less effective (Institution of Civil Engineers, 2016). A new protective structure called the New Safe Confinement was designed and built to replace the sarcophagus. Given Ukraine's membership in the IAEA, they used those guidelines, which includes DFMEA, to design the structure (International Atomic Energy Agency, 2025). Using DFMEA, the engineers were able to construct the confinement that to last 100 years before needing to be replaced. To ensure that it would last that long they also designed it to withstand severe weather.

However, the New Safe Confinement's risk assessment failed to evaluate the risk of an attack. On February 17, 2025, the Russians used a drone strike to damage the protective shelter (World Nuclear News, 2025). Leading to the containment to have a sizeable hole that is leaving the reactor open to the air and the area becoming unsafe. This illustrates that all failure modes should be evaluated no matter how unlikely.

5.4 Long-Term Impacts

Understanding the long-term impacts of the Chernobyl disaster can put severity into perspective. As seen in Figure 7, the radiation contamination was spread over a huge portion of Ukraine immediately after the explosion and the contaminated in 2020 (Harvard Ukrainian Research Institute, 2023). This spread of contamination led to many areas having to be evacuated. In total approximately 336,000 people were relocated. 784,320 hectares of agriculture land and 694,200 hectares of timber forest were now deemed unusable (World Health Organization, 2005). Creating the Chernobyl Exclusion Zone. All of this demonstrates why a 10 was assigned in the DFMEA severity rating table.

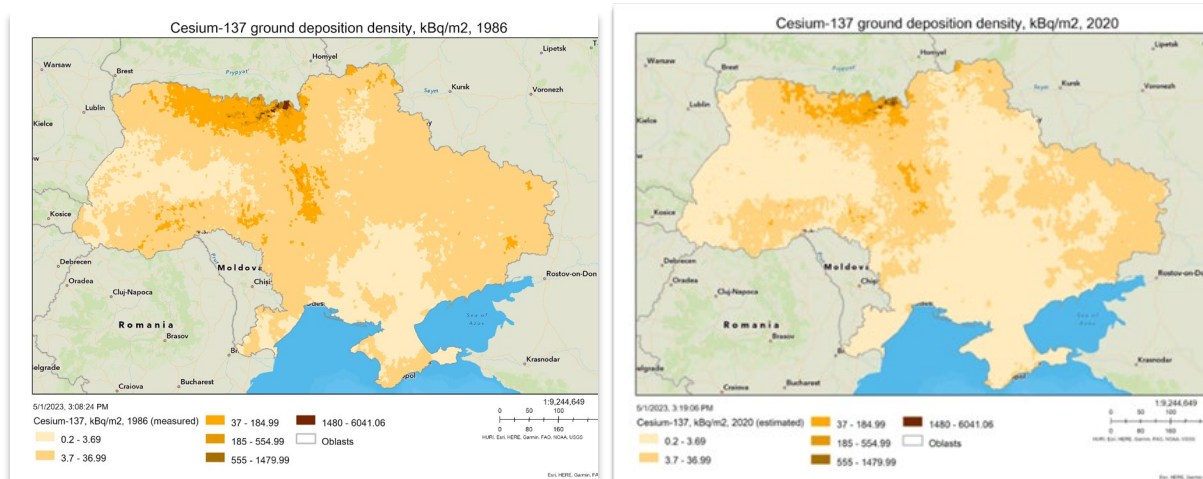


Figure 7. Radiation of Ukraine after the explosion 1986 and 2020 (Harvard Ukrainian Research Institute, 2023)

The reason that the radiation will be around for a very long time is the half-life of the radioactive particles are quite long (Yaroslav, 2021). However, that doesn't mean that elements get safer as they decay as plutonium-241 decays into americium-241 which produces a more dangerous type of radiation.

As stated before, radiation can be quite dangerous. High doses of radiations can cause radiation sick which can lead to a quick death and in lower doses it can cause cancer down the line (National Cancer Institute, 2022). It is estimated that 4000 people died due to radiation exposure from the disaster (World Health Organization, 2005). However, being by the reactor or radioactive material is not the only way to get exposed to radiation. There are many ways to get secondhand radiation exposure such as ingesting contained water and food and particles from air and soil. (World Nuclear Association, 2026).

One of the unexpected consequences was due to the lack of education of the public about radiation. The general fear of radiation leads to increased alcoholism and abortions. (World Nuclear Association, 2026). This demonstrates that to prevent the public's fear from hurting themselves the government and nuclear power plants should educate the public about nuclear power and radiation.

6. Conclusion

This paper demonstrates that conducting a DFMEA on the Chernobyl disaster was the result of a culmination of dangerous design, organization failures and human errors. The RBMK-1000 reactor was designed cheaply to put out as much power as possible with complete disregard for safety. The combination of graphite moderation system, water-cooling system, and low enriched uranium created an extremely dangerous environment. When positive SCRAM effect was discovered and was raised the government ignored the risk of not incurring the cost of fixing them. These issues were compounded by an inexperienced crew, procedural violations, poor instrumentation and a nonexistent safety culture. The ability to detect, control or mitigate was hindered by bad instrumentation and operators' abilities. Together, these failure modes left the RBMK-1000 reactor as a time bomb that happened to go off in Chernobyl.

The consequences of these failures justify the assigning DFMEA highest severity ratings to multiple failure modes. The explosion released radioactive material all over the surrounding areas and carried by the wind all over Europe. Leaving some areas still contaminated with dangerous levels of radiation decades later. Some so dangerous it created the Exclusion Zone. The Exclusion Zone will exist for thousands of years to come as radioactive particles decay. The deaths of first responders, whom at first were not told they were responding to a radioactive event, highlights the human cost of systemic negligence and secrecy. The health effects of this disaster have resulting in thousands of people getting cancer, many leading to death, was one of the worst public health crises. The deaths, long-term health and environmental damage show the generational impact that commands the severity rating of 10.

Almost forty years later, Chernobyl remains the poster child of nuclear engineering failures. Like many other lessons in engineering history, tragedy had to happen first. The global nuclear industry response was to develop many safety standards, regulation, security details, and emergency response protocols. Modern reactors have negative reactivity coefficients, redundancies in shutdown systems, transparencies in reporting, and a safety culture that is the core of plants operations. The safety cultures of today's plants focus on rigorous and repeated proper training, clear communication and conservative decision-making. These principles and lessons from Chernobyl are now fundamental to nuclear power industry worldwide.

Today Chernobyl stands as reminder that overlooking risks can have consequences that can extend far beyond a disaster but for generations. It can be seen in the destroyed landscapes, communities, and generations. This tragedy reinforces responsibility of engineers, regardless of industry, to safety at the center of the design process. It also reinforces the management, operators, engineers and other workers to make sure that the established safety protocols are never compromised. Today's nuclear power plants are safer than ever before, in fact they are the safest type of power plant. The global incorporation of DFMEA has made all this possible. The ability to identify potential failures modes beforehand, the scope of the consequences and how to mitigate them has done wonders for the nuclear power industry. Using DFMEA can stop the next lesson being paved in blood.

References

- Ansys. *What is DFMEA?* Retrieved from <https://www.ansys.com/blog/what-is-dfmea>, 2023.
- Ansys. *What is DFMEA? Design Failure Mode and Effect Analysis (DFMEA)*. Retrieved from <https://www.ansys.com/blog/what-is-dfmea>, 2023.
- Atomic, U. N. *Sources and Effects of Ionizing Radiation*. United Nations, New York, 2000.
- Chernov, D., & Sornette, D. Examples of Risk Information Concealment Practice. In *Man-made Catastrophes and Risk Information Concealment*. Springer, Cham, 2016.
- Hartwell, J. *Complete Guide to the Design FMEA*. Retrieved from <https://www.iqasystem.com/news/dfmea-complete-guide/>, 2022.
- Hartwell, J. *FMEA RPN – Risk Priority Number: How to Calculate and Evaluate?* Retrieved from <https://www.iqasystem.com/news/risk-priority-number/>, 2022.
- International Atomic Energy Agency. *Assessment and Management of Ageing of Major Nuclear Power Plant Components Important to Safety: BWR Pressure Vessels (IAEA-TECDOC-1470)*. IAEA, Vienna, 2005.
- International Atomic Energy Agency. *Convention on Nuclear Safety*. Retrieved from <https://www.iaea.org/topics/nuclear-safety-conventions/convention-nuclear-safety>, n.d.
- International Nuclear Safety Advisory Group. *INSAG-7: The Chernobyl Accident – Updating of INSAG-1*. IAEA, Vienna, 1992.
- LLumin. *Design Failure Mode and Effect Analysis (DFMEA)*. Retrieved from <https://llumin.com/blog/design-failure-mode-effect-analysis/>, 2023.
- Vedros, K. G., Christain, R., Otani, C., Cheng, W. C., & Gonzales, R. *Hazards and Probabilistic Risk Assessments of Advanced Reactors Coupled with Industrial Facilities*. U.S. Department of Energy, Idaho National Laboratory, 2024.
- World Nuclear Association. *RBMK Reactors – Appendix to Nuclear Power Reactors*. Retrieved from <https://world-nuclear.org/information-library/appendices/rbmk-reactors>, 2026.
- World Nuclear Association. *Safety and Security: Chernobyl Accident 1986*. Retrieved from <https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident>, 2026.
- World Nuclear Association. *Safety of Nuclear Power Reactors*. Retrieved from <https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors>, 2026.

Biographies

Rose Marie Gebara received a BS in psychology at Wayne State University in 2016, a BE in mechanical engineering at Lawrence Technological University in 2021 and is working on a ME in industrial engineering at Lawrence Technological University. As an undergraduate at Lawrence Tech, she was the design and build lead for the tail for the school's SAE Aero team. She and the team went on to earn 5th place in the 2021 SAE Aero competition. Also, as an undergrad she was the president of the AIAA. She worked as a test engineer at Stellantis from 2022 to 2024. In this she tested the engine and transmission of future Stellantis and competitor vehicles, benchmarked them and then presented her findings.

Daw Alwerfalli received a BS in mechanical engineering at the University of Tripoli in 1972, A MS in textile engineering at Georgia Tech in 1978, a ME in manufacturing with honors at University of Detroit Mercy in 1981, and a PHD in Manufacturing with honors at University of Detroit Mercy in 1989. He has worked at GNOFI as a senior Manufacturing engineer in Tripoli, Libya from 1972 to 1978. He was an assistant professor in manufacturing engineering masters/doctorate degree programs at University of Tripoli from 1978 to 1979. He was a research fellow at the University of Detroit Mercy in the Manufacturing engineering masters/doctorate degree program from 1979 to 1979 to 1986. He was then a consultant in manufacturing engineering training and education at AWA from 1986 to 1990. He has done industry collaborations with Chrysler Corporations at various Chrysler plants, conducting and leading 9 research projects from 1995-2008. From 1990 to present he is a professor in the mechanical engineering department/director of Master of Engineering Management degree program, college of engineering at Lawrence Technological University. He has many publications and is currently working on many research projects. He has one US patent.