Narora fire accident theoretical report

Compact Reactor Simulator - Exercises in Reactor Kinetics and Dynamics/SH270

Jakub Matl, Quentin Louis Poirier, Atilla Cakir
KTH Royal Institute of Technology
School of Engineering Sciences in Physics, Nuclear Engineering

May 1, 2023

Contents

Jakub Mátl, Quentin Louis Poirier, Atilla Cakir
jmatl@kth.se, poirier@kth.se, atillac@kth.se

Introduction

Safe nuclear power plant operation requires a robust approach to safety management, including multiple layers of defense to prevent accidents and mitigate their consequences. This approach, known as "defense in depth," involves a combination of functional and engineered barriers to prevent the release of radioactive material to the environment. A strong safety culture, which emphasizes a commitment to safety from all levels of the organization, is also essential for safe operation [1]. In the following text, the Narora Fire Accident (March 1993) will be studied and discussed in terms of defense in depth (DID), safety culture and commentary about the possible safety assessments. The computer codes and software quality assurance will also be discussed with a focus on the accident.

Defense in depth

The concept of defense in depth involves deploying multiple levels of equipment and procedures hierarchically to ensure the effectiveness of physical barriers between radioactive materials and the environment, workers, and the public. This approach is implemented in the design and operation of a nuclear power plant to offer graded protection against various transients, incidents, and accidents, which may include equipment failures, human errors, and external events. The objective is to maintain the safety of the plant in normal operation, anticipated operational occurrences, and accidents [2].

General objectives

The general objectives of DiD are as follows [2]:

- to compensate for potential human and component failures,
- to maintain the effectiveness of barriers that prevent damage to the plant, environment and barriers themselves,
- to protect the public and the environment from harm, even if the barriers are not fully effective.

Structure

Defense in depth is typically structured into five levels, each providing additional protection in case the previous level fails. The first level aims to prevent abnormal operation and system failures, followed by the second level which detects and controls these issues. If the second level fails, the third level activates specific safety systems and features to perform safety functions. If the third level fails, the fourth level focuses on accident management to limit the progression of severe accidents and prevent or mitigate external releases of radioactive materials. The fifth and final level aims to mitigate the radiological consequences of significant external releases through off-site emergency response [2]. Figure 1 shows the relationship of the instrumentation & control (IC) systems to DiD structure.

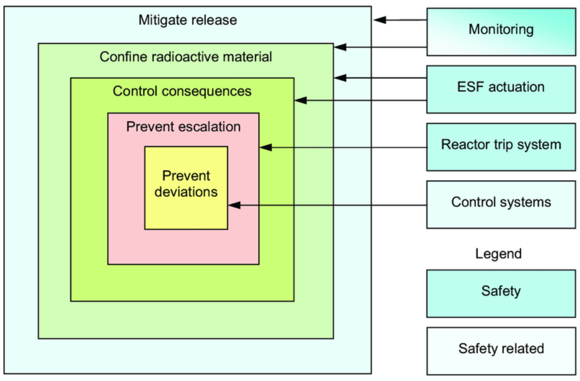


Figure 1: The IC systems in relation to DiD structure [3].

The DID ensures that a single human or equipment failure at one level of defense, and even combinations of failures at more than one level of defense, will not lead to the propagation of failure to subsequent levels. Therefore each level should be independent [1].

Safety culture

Safety culture is an important element in ensuring the effectiveness of defense in depth. The term safety culture was first defined in INSAG-3 as "the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants". In other words, safety culture is an assembly of characteristics and attitudes in an organization that prioritize giving the necessary attention to safety concerns due to their significance [4].

Safety culture played a significant role in the Narora fire accident and will be discussed later on.

Narora fire accident

General knowledge about Narora NPP

Narora Atomic Power Station (NAPS) is a nuclear power plant located in Narora, in Uttar Pradesh, India. This power station held two CANDU type PHWR (Pressurize heavy water reactor) of 220MWe. The two NPPs were officially connected to the grid in 1991 (Narora 1) and 1992 (Narora 1). Both of the reactors use heavy water as a moderator and primary coolant; natural uranium is used as a fuel. For further discussion about the Narora fire accident, the turbine generator and auxiliary systems will be described [5].

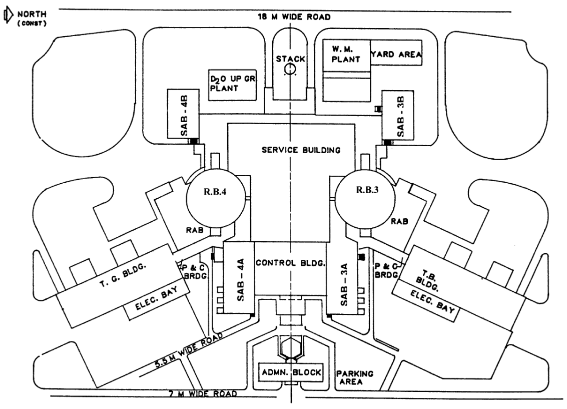


Figure 2: Site layout of a typical indian PHWR [6].

Steam turbines for both reactors have a configuration of one single flow high pressure (HP) turbine and one double flow low pressure (LP) turbine tandem coupled with a 2-pole generator. The generator is provided with a hydrogen-cooled rotor, stator core

& overhang and water-cooled stator conductors. The auxiliary lube oil system is located over the generator [5]. Further discussion about the role of these systems in the fire accident will be carried out in the following text.

Course of the event

On May 31, 1993, after 28 months of operation, two steam turbine blades malfunctioned in NAPS-1 which was at nominal power, causing a major fire accident. The first of two NAPS reactors experienced an accident caused by fatigue, resulting in two LP turbine blades breaking off and cutting through 16 additional blades located in the LP turbine. The change in angular momentum led to significant blade vibrations, causing the cooling pipes carrying hydrogen gas to break, releasing the hydrogen into the turbine. The hydrogen came into contact with the oscillating blades, and when a spark was generated by the blades, it ignited because hydrogen is a highly flammable gas. Additionally, oil from the turbine system leaked and added to the flames, causing the fire to spread throughout the turbine building. As a result of the fire, the cables supplying power to the secondary cooling systems caught fire, leaving these systems inoperable. The accident caused a general blackout in the plant. The smoke reached the main control room via the ventilation, making it unusable. In addition, the fire spread through the cables into the control equipment room (CER) [7, 8].

The accident was classified as level 3 on the INES scale. To address the situation, operators manually activated the reactor's shutdown systems, climbed to the top of the reactor building with battery-operated portable lighting, and opened valves to release liquid boron into the core, slowing down the reaction and preventing recriticality. To ensure heat removal from the primary coolant system, operators also started diesel-driven firewater pumps and used water meant for fire suppression and started pumping the water into the steam generator (SG) in the secondary circuit. The water coming to the SG served as a heat sink and ensured the natural circulation in the primary circuit and sufficient residual heat removal [7].

The power cables played a vital role in the accident as they were not constructed from fire-resistant materials. It later turned out that if this had been the case, the turbine hall explosion would not have occurred [8]. The event timeline is included in the appendix in Table 1.

Breach of DID

Fail-safe principle

One of the golden rules of nuclear safety is the "Fail-safe principle". It means *Any malfunction should result in safe plant conditions* (KTH nuclear safety course). For the Narora incident, this criterion was not met. A single failure of a turbine's blade came close to degenerating into a severe accident. The worst was avoided by adequate and timely action by the operators. This underlines a major error in the NAPS design and one could call into question the quality and independence of the safety assessment of the NPP, whether in the

- probability safety assessment (PSA),
- deterministic safety assessment (DSA) or
- evaluation of the engineering factors important to safety.

A safe design would have been a design where the failure of some blade would have destroyed neither the turbine, the secondary loop or the whole engine room. For instance, it could have been achieved by having an extra margin on the thickness/ductility/toughness of the steel insulating/sealing hydrogen from the secondary loop or by using an already established and reliable turbine.

Lack of safety culture

Having a strong safety culture is crucial in ensuring the effective implementation of defense-in-depth measures. It fosters a proactive approach to safety, where employees/managers/leaders all emphasise "to make nuclear safety the overriding priority" [9]. However, there is strong evidence that the Indian nuclear industry from the late 20th century has failed to develop an appropriate safety culture. This is a serious matter because as the IAEA points out "establishing a strong safety culture is one of the **fundamental management principles** for an organization dealing with radioactive material" [10]. All the more important other pieces of evidence suggest:

- the Narora fire could have been avoided,
- the utility and the regulator still don't have learned the lessons of the Narora incident.

Failing leadership

An industry can seek safety above all if and only if there is a constant impulse from the executive/top management of a company toward safety. Through two examples, we will illustrate the failure of the Indian nuclear industry to have a sane safety culture.

In 1989, General Electric (GE) discovered a design flaw in the supplier's turbines for the Indian nuclear industry. This company supplied the two turbines for the Narora nuclear units. Thus, both GE and the turbine manufacturer recommended to NPCIL (Nuclear Power Corporation of India) that the blade designs from already-working NPP be replaced to prevent potential accidents. However, NPCIL did not take action on this advice until 6 years after the Narora accident, following the occurrence of the anomaly at Gopalakrishnan's NPP occurred in 1999 [7]. The reasons behind NPCIL's delayed response are unclear, but failing to act on critical safety knowledge and recommendations can have serious consequences [9].

Secondly, more explicitly, through the words of industry executives from that time, we can infer the whole mindset of the top management. Here is a list of public citations from officials coming from the DAE.

- ... *the necessity of a dome on the top of the reactor vessel and the core catchers needs to be challenged ... after all, if the reactor can be designed to be inherently safe or if the probability of failure of the shutdown function can be brought to 1 in* 10^8 *per demand, why invest more funds for a safety features. (Paranjpe 1992, 513)*[7]
- ... *it is 'important' that 'the people (operating the nuclear plant) should be confident about safety' (Subramanian 2000)*, from a former chairman of the Nuclear Power Corporation [7].

What emerges from these citations is a focus on cost competitiveness over safety and a belief that despite incidents such as Three Mile Island and Chernobyl, nuclear power plants were inherently safe.

Taken together, this suggests that safety was not the primary concern of India's nuclear industry leaders in the late 20th century.

Absent or faulty systems

In the following text, the safety systems or systems related to safety that failed or were absent will be discussed.

At the time about three and a half minutes after the blades ruptured, the power cables began to burn, leading to a loss of off-site power (LOOP). The operators had to manually activate the primary shutdown system because of the loss of electricity. This can be considered a major failure of the inherent safety design because the operators had to manually shut down the reactor. The diesel generators automatically started after the LOOP occurred, but tripped because of the loss of control power supply (loss of offsite power). That drove the NPP into its most dangerous state (based on the PSA), a station blackout event (SB). Operators were forced to climb up to the top of the reactor building carrying only portable flashlights and manually opened the valves with soluble boron to avoid reactor recriticallity. Both of these actions were meant to be automatic and can be considered as a significant breach of DiD layer (the primary shutdown system and soluble boron system activation failed). The operators' actions should not be taken for granted. Overall, the inherent safety of the station showed to be inadequate [7, 8].

In comparison, the VVER-100 shutdown rods are being held in the upper position using an electromagnetic field. When AC power is lost, the electo-maget stops working and the shutdown rods fall into the active core and trip the reactor. This way the inherent safety is improved and the reactor is shut down when a blackout occurs.

In addition, the secondary cooling pumps were not working because of the station blackout. To provide sufficient cooling of the reactor, firewater was pumped using diesel generators into the secondary circuit.

Here is an example of the propagation of error through DiD layers: Because of the blade rupture, the hydrogen caused an explosion. The fire was transported via burning oil, so later on, the power cables caught on fire. This led to a station blackout, and therefore, the primary cooling system and secondary coolant pumps were not available. The firewater pumped into the steam generator served as a heat sink to ensure natural circulation through the core and remove the residual heat. Therefore, the firewater system was not available to deal with the fire, and external fire extinguishers had to be called. This delay in extinguishing the fire led to significant damage to the turbine building. All of the above is an example of the propagation of errors caused by non-independent systems design [8, 7].

Another example of how the failure of a single system propagated is the smoke coming from the oil. Because of the poor design of the ventilation, the smoke coming from the oil combustion was transported to the main control room. This made the room unhabitable and operators were forced to leave the main control room [11].

Possible technical solutions

To reduce the probability of the root cause, redesigning of the turbine blades is one of the solutions. Even though General Electric in 1989 recommended design modification to an Indian turbine manufacturer, the NAPS operator NPCIL did not take any action. This is an example of how the safety culture of the Indian authorities affected the defense-in-depth and increased the possibility of the accident happening [7].

The fire-resistant coating of the power cables would reduce the effect of the fire spreading and would avoid station blackouts. Another way to reduce the consequences is to increase the distance between the turbine and the oil tanks. By doing this, the vibrations should be significantly reduced and therefore large oil flow out of the tank could have been avoided [8].

The other design solutions might be [8]:

- installing cables in separate ducts to prevent damage to power cables in case of fire in one duct,
- installing of smoke detectors and water sprinklers,
- using adsorbers like charcoal to purify and catch smoke in case of an accident,
- having an emergency control room fully isolated and independent from the outside (theirs was inoperative due to the blackout),
- putting additional distance between the turbine and the oil tank.

Failing of learning lesson from past experience

The lack of drawing lessons from past failures is evident in the history of incidents in India's nuclear plants. Prior to the Narora accident in 1993, there had been at least three fires at the Rajasthan reactors, repeated turbine blade failures in Indian reactors, and frequent oil leaks in turbine generator systems. Furthermore, similar factors that led to the Narora accident had previously occurred in other countries. For instance, in 1989, a reactor in Spain experienced turbine vibrations resulting in oil leaks and hydrogen coolant escape, leading to a violent fire that spread and disabled emergency systems. These incidents highlight a failure within the DAE (Department of Atomic Energy) to learn both from failures in India but also abroad and take necessary safety measures. This demonstrates a serious lack of safety culture in the Indian nuclear industry in the late 20th century.

Structural problem

All these issues covered a more structural problem concerning the Indian nuclear regulatory authorities (AERB). In many countries after an accident such as the one in Narora, the regulator would have launched a full inquiry and would have forced the utility to install fire resistance wires and change all turbines. That wasn't the case in India. In fact, compared to the standard of other nuclear countries, the AERB is not a purely independent body from the political/India administration. Thus political pressure or political doxa could bias/alter the regulator's works that should remain technical and purely objective. Still in 2012, a report from the "Comptroller and Auditor General" (CAG) highlights "the legal status of AERB continued to be that of an authority subordinate to the central government, with powers delegated to it by the latter" [12]. Overall, it is crucial for regulatory bodies to remain independent and objective to ensure the safety of the public nuclear industry.

All the points raised above demonstrate a glaring lack of safety culture in the Indian nuclear industry in the early 1990s. This failure to implement the safety culture probably contributed, as discussed earlier, to making the Narora incident possible.

Mitigating factor of the event

We note two key elements that have enabled a return to a stable and secure state for the NPP. Firstly a succession of right actions on time of operators. This clearly demonstrates their high qualification and training level. This also proves the robustness of the Emergency Operating Procedures of the plan (EOP). Secondly the inherent design of the reactor which includes

- the possibility of removing the decay heat passively by thermosyphon from steam generators,
- sufficient safety margins on the design for thermosyphon cooling. [13]

All together, this has avoided the Narora to deteriorate into a severe accident with core damage or worst. It also shows that even when the safety culture failed at the top, it did not contaminate the whole industry.

Safety assessment

The Narora incident has brought to light a significant shortcoming in both the design and management of the Narora nuclear power plant, as discussed earlier. This failure is attributed to the inadequacy of the "Safety Assessment, particularly in the deterministic and probabilistic analyses. These analyses failed to identify critical sequences that could result in high-risk events, such as the one that occurred in Narora. In the next section, we will explore the various concepts and techniques utilized for safety assessment and suggest possible analyses that could have detected the fundamental design flaws of the Narora NPP.

Introduction

The process of ensuring safety has developed over the past few decades into three different approaches to design against accidents: rule-based, deterministic, and probabilistic methods. The last two will be discussed in more detail in the following text [14].

Early safety assessments in the USA used deterministic analysis with conservative assumptions and calculations to measure the effectiveness of safety barriers and systems. Design basis accidents (DBAs)[1] were created to test the plant's ability to handle prescribed accident scenarios. The safety of a nuclear reactor was therefore defined as an ability to withstand a set of given accident scenarios. However, the exclusion of multiple failures was shown to be unjustified after the Three Mile Island accident. As a result, probabilistic methods were introduced are now they are being used worldwide to identify and evaluate accident scenarios involving multiple failures, and are increasingly used in other countries to enhance nuclear safety [14].

The purpose of the safety assessment for the plant is to (a) pinpoint potential pathways for exposure in both normal and abnormal situations; (b) evaluate the effectiveness and extent of the protection and safety provisions, and (c) establish the expected magnitudes of potential exposure [2].

It includes analyzing every aspect of the plant that is important for protection and safety. This covers the location, design, and operation of the plant. To guarantee that the design satisfies the relevant safety standards, a systematic method called safety assessment is used throughout the plant's lifecycle, starting from the site evaluation and reactor design, through the operation of the reactor to decommissioning of the facility and remediation of the site. The formal safety analysis is just one aspect of safety evaluation [16].

Deterministic safety analysis

Introduction

Regardless of the likelihood of such events and accident scenarios, deterministic safety analysis (DSA) demands the designer offer protection or mitigation for them. It evaluates the effectiveness and performance of safety systems created to achieve the DID objectives using (usually) conservative analysis methodologies [14]. The DSA is used to demonstrate the capability of prevention of the DBAs (such LOOP), and anticipated operational occurrences (AOOs). The DSA should also prove the ability to mitigate beyond design basis accidents (BDBAs such as SBO). To decide whether the safety systems ensured adequate safety, the acceptance criteria (AC) are used. Deterministic safety analysis' fundamental strategy entails defining the bounding values of crucial plant variables and demonstrating through analysis that the requirements are satisfied for typical initial events. Some of the acceptance criteria are presented in the following text, namely the LOCA-related [14, 15].

The AC is divided into two levels [17]:

- Global/high-level criteria related to doses to the public or prevention of consequential pressure boundary failure. Often defined in law or by the regulatory body.
- Detailed criteria defined by designer or analyst. Sufficient, but not necessary to meet the global ones.

The acceptance criteria also might be categorised into three groups [17]:

- Safety criteria (SC) - the criteria related directly to safety, considering the radiological impact or the integrity of the barriers that prevent the release of the radioactive material,
- Design criteria (DC) - the criteria and limits for the design of individual barriers, components or systems used as a precondition for meeting the safety criteria,
- Operational criteria (OC) - the criteria that the operator must comply with for both routine operations and anticipated operational situations, established preconditions that must be followed to meet the DC and SC.

Single failure criteria

The term "single failure" refers to an event that causes a component to lose its ability to carry out its safety functions. In cases where multiple failures arise from the same event, they are considered as a single failure. In fluid and electrical systems, single-failure assumptions are employed if a single failure

[1] According to Pershagen, "Design basis accidents are a special category of events which are not expected to occur at all during the reactor lifetime but which are postulated as a basis for the design of the safety systems" [15].

of an active component (assuming proper functioning of passive components) or a single failure of a passive structure, system, or component (assuming proper functioning of active components) does not lead to the loss of the system's safety function. The SFC must be used in safety analysis in order to support the high reliability of safety functions that are crucial to the safety and to help ensure that the intended safety function can still be carried out in the case of a single failure [14].

Accident type

Safety-related events are usually divided into three types. The first type is related to LOCA accidents and the second to transients. These types of events are usually used for LWR analysis. The third type concerns external events [15]. In this classical classification, the Narora accident is classified as a loss of power transient and more specifically SBO.

Each LWR is given an ECCS in order to lessen the effects of a LOCA. When a LOCA occurs, an automatic control system detects it and activates and coordinates the operation of the various ECCS components as necessary. The purpose of the ECCS is to cool and control the cladding's temperature increase by the supply of water (through spray and/or flooding systems), preventing major core damage and the release of radionuclides from the fuel rods. According to CFR and Appendix K of CFR (USNRC a; USNRC a), the US regulations (and comparable standards exist in IAEA guidelines) demand that the ECCS of light water reactors satisfies the following acceptance criteria [14, 16]:

- Peak cladding temperature up to 2 200 °F
- At any position and time, the loss of thickness of the cladding by oxidation must be below 17% of the original cladding thickness.
- Hydrogen generation from hot cladding-steam less than 1 % the amount of hydrogen produced in case of full cladding oxidation for the whole core.
- The core geometry remains coolable at any time.
- Long-term cooling must be planned and achieved.

In a contrast to LOCAs, transient events are those that cause a reactor trip while maintaining the reactor-coolant boundary. A number of Deterministic and Probabilistic Safety Analysis (DSA) factors, including equipment failure or a human mistake, could result in a transient. Situations where the reactor power increases, the coolant flow decreases, or the coolant pressure increases are the three main areas of concern for transients. Each of these three scenarios has the potential to cause a core melt or a breach of the reactor coolant system (RCS).

DSA can be conservative or best-estimate.

- The conservative approach demands using pessimistic or worst-case assumptions and models, to ensure safety with a sufficient safety margin. The regulatory bodies require mostly conservative DSAs. One of the drawbacks of the conservative DSA is the fact, that too conservative and inadequately pessimistic models can lead to unrealistic results [17].
- The best-estimate (BE) or realistic DSA uses models and assumptions that are realistic (while upholding some level of conservatism), and uncertainty analysis is included. For the BE DSA, it is typical, that the codes used must be carefully validated against experimental measurement and the user must be experienced. The most important part of the realistic analysis is the uncertainty of the results [17].

Conservative safety analyses are relatively easy to perform and were really popular back in the day. Still, analysts should be aware of the uncertainties and possible deviations in their calulations. On the other hand, the best estimate analysis plus uncertainties (BEPU) should lead to the most realistic results. The input should also contain uncertainties and the availability of the systems in the analysis should be based on PSA. This makes the BEPU DSA time-demanding and more challenging [17].

In the appendix, Table 2 the different types of DSA are listed. In this case, the BE analysis can also give uncertainties depending on the input.

Probabilistic safety analysis

Introduction

In the 1970s, the probabilistic methodology was first applied to nuclear safety through risk analyses in various countries including the USA, UK, and Germany. These analyses aimed to calculate individual and population risks from nuclear power plant operations and compare them to other natural and industrial risks. Prior to this, statistical methods were mainly used for reliability analyses in industries such as aircraft manufacturing. PSA was invented to evaluate the safety of nuclear power plants by quantifying the likelihood and consequences of potential accidents and to identify areas for improvement in plant design and operation. Traditional safety analysis methods were limited in their ability to account for uncertainties and complex interactions, but PSA allowed for a more comprehensive and realistic evaluation of safety[18, 19].

In practice, the goals of PSA are to [19]:

- identify and define the various combinations of events that could potentially result in a severe accident,
- identify weaknesses of a design,
- estimate the probability of occurrence for each combination,
- evaluate the resulting consequences.

The sequence of events that led to the Narora fire was not taken into consideration. More importantly, beyond the low probability of such a scenario occurring in a reliable turbine, the failure to account for the risk of losing the seal of hydrogen cooling is concerning. It is well known in many industries, that firstly hydrogen is a highly flammable element, but also a light core subject to leakage. Thus, it is rather incomprehensible that the designers have placed an oil tank (also highly flammable) above a turbine containing hydrogen when places were available elsewhere in the turbine building [7].

Structure

The PSA is structured into individual stages depending on the scope of the analysis.

The first stage, also called "PSA level 1", focuses on the estimation of the core damage frequency (CDF). The analysis includes [18]:

- identification of accident sequences leading to core damage,

- analysis of the performance and reliability of the safety systems,
- quantification of accident-sequence probabilities.

The second stage, "PSA level 2", consists of [18]:

- core meltdown and radioactive substances release study,
- study of the core melt and the released radionuclides in the containment,
- containment response to severe accident conditions analysis,
- release of radioactive substances study.

The "PSA level 3" is a risk analysis with a wider scope of interest. The analysis deals with the issue of [19]:

- dispersion of radionuclides in the surrounding environment
- the effects on the health and environment.

Event and fault tree

PRA level 1 involves a methodical analysis of the reliability of important systems and components that may contribute to event sequences leading to core damage. To carry out this task, the event tree or fault tree methodology is generally used [18].

To create an event tree, it is necessary to describe the basic safety functions that prevent the core from overheating and damage:

- nuclear chain reaction interruption,
- sufficient supply of coolant,
- decay heat removal.

The event tree is a set of possible sequences, where the specific safety function can either be a success or a failure with a given probability. Each event tree begins with initiating event, which is the "starting point" of the analysis. The principle of the event is going from cause to event, therefore the consequences of each initial event with specific probability can be calculated. Each possible sequence of the following events is discussed in the terms of the basic safety functions and if they are fulfilled. Using this approach, the CDF can be established [18].

The fault tree has an opposite approach, where the causes are deducted from the consequences. Therefore, the failure of the safety function is the initial event. Three levels of fault trees can be distinguished depending on the scope of the study:

- function fault tree,
- system fault tree,
- component fault tree

When looking at the function fault tree of the power supply on Narora's PSA what is paradoxical is that the risk of fire was considered. They even considered the risk of CCF like highlights in this sentence: *In case physical diversity and fire barriers are provided, the effects of CCFs emanating from the external environment e.g. fire, change in room ambient, temperature etc. would be reduced.* [20]. Now the question is whether they have considered or not in the PSA the failure probability of the power supply (mainly SBO) due to a CCF such as an on-site fire. As mentioned before, fault trees were not provided, therefore it is impossible to conclude. Although the details of the calculations were not provided, they still provided the probability of failure of in-site power (class IV&III) due to all common causes of failure [20]. Figure 5 in the appendix highlights that 1/3 of the failure probability is driven by CCF. Moreover, the overall function failure probability is also pretty "high" (compared to the standard in the industry) for such a crucial system: 3×10^{-3} failure per year. Similarly, proportions are also available for the loss of off-site power. Thus designers may have considered that adding fire-resistance wires was not cost-pertinent because the failure rate will not change much: maximum reduction of 1/3. However, it is important to keep in mind that probabilities got as results from PSA contained huge uncertainties. Thus the use of this tool in the design should preferably be based on the precautionary principle.

Uncertainity

The PSAs usually exclude external events, like earthquakes, floods or tsunamis, therefore the uncertainty of these events is not defined. When taking corrective actions to prevent failures in nuclear plant components, it may be difficult to assess their impact on reliability accurately. Some relevant issues, such as accident progression phenomena, human behaviour, and low-level radiation health effects, are challenging to model with reasonable accuracy, resulting in a level of uncertainty in the results of PSA. Expert opinions are sometimes used to estimate such uncertainties, which can propagate through the analysis stages, producing probability distributions of calculated results [19].

The predictions for the likelihood of nuclear reactor core damage have varying levels of uncertainty, depending on the type of analysis used. In Level 1 analyses, using well-known reactor designs, the uncertainty range is about ten times the predicted value, with a 90% confidence interval. However, as the complexity of the analysis increases in Level 2, uncertainties become much more significant, with the potential for the uncertainty range to extend over several orders of magnitude. Including atmospheric dispersion and low-dose-response relationships in Level 3 analyses adds more uncertainty. Therefore, it is essential to understand these limitations when using PSA [19, 18].

Human factor

One of the difficulties associated with PSAs is human behaviour. In addition, the influence of the human factor might be significant in some situations, therefore it is desired to design the reactor with the minimum human intervention needed. One of the major problems in the PSA is modelling the failure rate of the operators under normal and stressful situations. In stressful situations, human behaviours can be completely irrational and modelling them is complex and requires the use of social sciences. Those human errors may be caused by vagueness of procedures, improper instrumentation or just error of operator interpretation and deduction. To include these effects in the PSAs is difficult considering the numerous actions of the operator. Significant progress has been made in studying the human response, but stress will always play a crucial role in actual situations [19]. That's why considering operators' actions as granted as did NPCIL after the Narora accident is no more than dangerous gambling [7].

Common cause failures

When discussing PSA, it's important to differentiate between two types of failures: independent and dependent. Independent failures occur randomly, while dependent failures are correlated. If fault tree analysis only considers independent failures, the estimated failure probabilities may be unrepresentatively low. Different types of dependencies exist, such as the failure of a support system causing several other systems to be unavailable or identical components failing due to a common cause. Two groups of dependent failures are commonly considered: functional dependence and common cause failure (CCF). System failure with functional dependence may include auxiliary power systems, ventilation, or control signals. In this case, a direct functional relationship between the systems is defined. The failure of one system will cause the failure or unavailability of the other. In contrast, CCF involves two or more systems without direct functional relationships. Common cause failure may result from external events or propagation failure. In the case of the Narora fire accident, typical CCF can be observed. The failure of the LP turbine blades propagated through the hydrogen explosion, oil leakage and burning, power cables burning to station blackout, and unavailability of the primary shutdown system, primary cooling system, and other systems [18].

Considering highly redundant systems, the CCF might play an essential role in the overall failure rate. Most of the models use existing information about single failure events to formulate the probabilities of multiple failures. However, the causal dependence between the observations and multiple failure modes is mostly not clear, especially in highly redundant systems [19].

In numerous NPPs, one of the worst events possible is a station blackout (SBO) which means losing both off and on-site electrical power. A station blackout involves losing all active components/functions such as the circulation pump (loss of flow). One of the main reasons why the Narora fire came within just a hair's breadth away from disaster was because of the station blackout due to the widespread damage to the power grid by the fire. Thus fire was a common cause of failure having impacted all active devices. According to Narora's PSA (more detailed later), SBO accounts for 75% of the core damage frequency and is therefore definitely the worst-case scenario possible [20].

Computer codes

To ensure the safety of nuclear systems, various safety requirements and regulations have been set. Meeting these safety requirements relies heavily on computer codes, which provide accurate predictions of a system's behaviour and identify potential safety hazards. As such, they are subject to rigorous validation and verification processes to ensure their accuracy and reliability. The main use of computer codes is found in the DSA, dealing with reactor thermo-hydraulics, dynamics, thermo-mechanical and structural behaviour or radiological impact. As previously mentioned, different DSA types require the use of various codes (e.g., conservative, BE, or realistic codes). Conservative codes are often proprietary, owned by the operator or other private company. In this case, the code is focused on a specific nuclear power plant and often is not available for third-person use [17].

When selecting the computer code, it is necessary to check the following conditions to justify the right performance of the analysis. The validity of the physical models employed to describe the processes is substantiated. The simplifications made in these models are justified, as are the correlations utilized to represent physical phenomena, with their respective limits of applicability being identified. It is crucial to recognize the range of conditions within which the model or calculational method is intended to apply and to avoid extending its application beyond this range. The numerical methods incorporated into the code are precise and robust. A methodical approach has been taken in the design, coding, testing, and documentation of the code. Furthermore, an evaluation has been performed to ensure that the source code is consistent with its description in the system code documentation [17].

System codes

System scale analysis focuses on the entire nuclear power plant design and usually the model represents key components of the reactor configurations like steam generators (LWR), pressurizers (LWR), reactor pressure vessels, pumps and safety systems connected to the core cooling circuit. System scale codes are able to predict the overall response to operational events. The simulations provide information on relevant system parameters such as pressures, coolant, control volumes, and temperatures of materials in the modelled structures over time. The thermohydraulic system codes are usually based on solving five or six conservation equations, usually using implicit or semi-implicit schemes. Through these codes, one can simulate the operation and behaviour of the reactor, including accident sequences, to assess the safety level of the nuclear power plant [21].

The nuclear engineering industry uses a variety of state-of-the-art thermohydraulic system codes to simulate the behaviour of fluids, such as water, in nuclear power plants. Some of the most widely used codes include RELAP5, TRACE, APROS, POLKA-T, CATHARE, ATHLET, and RETRAN. These codes employ a control volume approach with big nodalization and state-of-the-art thermohydraulic (TH) models, including multi-fluid models [22].

There are some limitations to the system codes. One of the main issues of TH system codes is the free nodalization of the control volumes. Since there is no right way to nodalize large systems, significantly different results may be obtained. Another difficulty is the amount of available input parameters, resulting in various possibilities and a variety of different results. One of the frequently discussed topics might also be the initial and boundary condition and time step size specification. When performing DSA, it is crucial for the user to have sufficient experience in working with given code [22].

Overall, thermohydraulic system codes play a critical role in the safety analysis of nuclear power plants. The advancement of these codes has allowed for more accurate and detailed simulations of the behaviour of the system, including the effects of thermal-hydraulic factors on reactor dynamics.

Reactor dynamic codes

PARCS, SIMULATE3K, POLKA7, and DYN3D are reactor dynamic codes to simulate the behaviour of nuclear power plants during transients and accidents, while also considering criticality concerns. These codes require a detailed presentation of the core neutron kinetics, which is a key factor in predicting the behaviour of the reactor during transient. In the past, these codes did not include detailed thermal-hydraulics for the reactor circuit due to computer capacity limitations. However, the lack of detailed thermal hydraulics is not limiting if there is a well-mixed single-phase flow in the primary circuit. The need for more complicated thermal-hydraulic progressions, combined with criticality concerns, has led to the development of advanced thermal-hydraulic modelling [23].

As we have seen previously, one of the main characteristics of the Indian PHWR is the passive cooling of the decay heat. Therefore, the demonstration of such an important characteristic requires at least the use of already verified thermal-hydraulic codes or dynamic reactor codes. We can now ask ourselves the question of which type of code used to demonstrate passive cooling among the conservative codes, BE, BEPU etc. From the vendor's/utility's point of view, using a totally conservative approach is practical. Indeed, it ensures to have a sufficient margin in case the worst happens. In fact, as pointed out earlier, it was due to good design and high margin that passive cooling of the primary did not fail after during the Narora event. In fact, this example shows how important it is in the design to use reliable codes (verified) and validate models in order to demonstrate the effectiveness of safety functions.

Severe accident codes

Severe accident computer codes such as MELCOR, SCDAP/RELAP5, MAAP, and ASTEC are utilized in nuclear engineering to simulate and analyze the progression of severe accidents in nuclear power plants. These codes employ complex models and algorithms to calculate the behaviour of nuclear systems during accidents, including core damage, fission product release, and containment response. They can also predict potential consequences of severe accidents and aid in the development of safety measures to mitigate their effects [24].

SBO is a BDBA and therefore is not studied properly during the design. However, nothing hampers research organisations to study reactors' behaviour in those extreme cases and unlikely events ($f \leq 10^{-5}/y$). In fact, performing case studies (use of deterministic codes) is very valuable in the nuclear industry. Whether it is an operation transient or a severe accident, the physics involved are so different, and the systems are so complex and coupled to each other that it is necessary to use case studies to determine the general dynamics of the NPP. From these kinds of studies, a better understanding of the behaviour of the reactors can be derived. Those kinds of knowledge in the case of SBO for Narora's type reactor could have been very valuable for the operators.In addition,the general dynamics of different NPPs were examined and it was determined that there is a radiation dose between the limits determined by the "Atomic Energy Regulatory Board" (AERB) at different distances. [25].

Internal code assesment

Both verification and validation refer to a process of code reliability improved and reduction of incorrect application risk. Usually, the internal code assessment is done by the developer of the code.

Code verification pertains to examining the source code in relation to its documentation description. This process involves practices related to software quality assurance (SQA) and efforts to detect and correct errors in models and numerical algorithms utilized for solving partial differential equations [22].

Code validation involves evaluating the precision of predicted values by comparison against relevant experimental data. Essentially, code validation focuses on quantitatively assessing the accuracy of the code by comparing it with high-quality validation experiments. These experiments are thoroughly documented and characterized, including careful estimates of experimental measurement uncertainty. Through the validation process, the code's results are consistent and demonstrate that the entire system can produce meaningful outcomes. In other words, the code functions and produces the intended results [22]. The process of internal code assessment is described in Fig. 3.

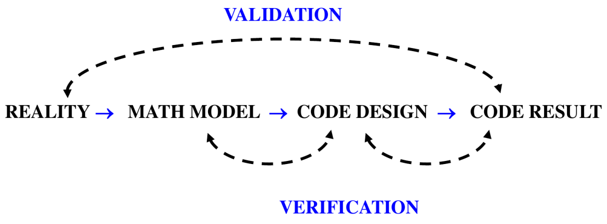


Figure 3: Process of internal code assessment - validation and verification [26].

Independent code assesment

Independent code assessment is a process when an independent third party quantifies the code accuracy using the experiments performed in an integral test facility (ITF) and the code calculations. The external code assessment usually involves the qualification of the user and the nodalization and covers the topic of qualitative and quantitative accuracy [22].

The internal and external code assessment is described in Fig. 4.

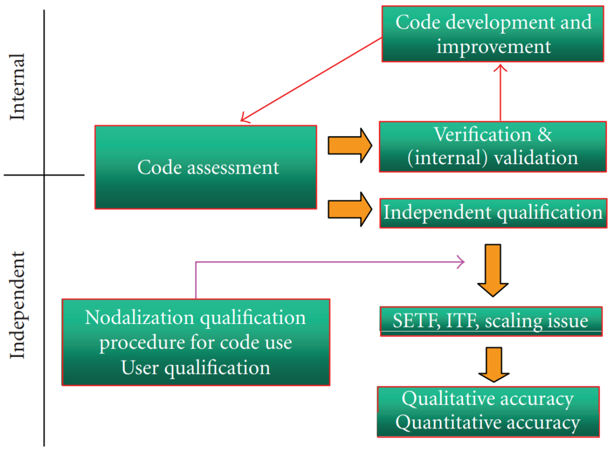

Internal
Independent
Code development and improvement
Code assessment
Verification & (internal) validation
Independent qualification
Nodalization qualification procedure for code use User qualification
SETF, ITF, scaling issue
Qualitative accuracy Quantitative accuracy

Figure 4: The internal and external code assessment [22].

In terms of Narora accident

Several computer codes could have been done to identify the insufficiency of the safety systems that failed during the Narora fire accident:

- System code: The system code with logical modules can be used to model the behaviour of complex systems, including power plants. By simulating the impact of the station blackout and subsequent failures of safety systems, the model in system code can help identify potential vulnerabilities in the system and ways to improve its reliability, like the unavailability of the emergency cooling system, the primary shutdown system or the boron injection system. Still, the station blackout is not part of the DBA, therefore it was not included in the safety analysis.

- Fault Tree Analysis (FTA) software: As mentioned earlier, FTA is a useful tool for analyzing complex system failures. In the case of the Narora incident, FTA software could be used to model the single failure that lead to the station blackout and subsequent failures of safety systems.

- Emergency response planning software and severe accident codes: Following the Narora incident, emergency response planning software could be used to simulate the impact of similar incidents and help develop more effective emergency response plans for nuclear power plants. Speaking about the severe accident codes, the awareness of the potential consequences of the radiological impact could lead to a greater emphasis on safety.

References

[1] International Nuclear Safety Advisory Group. *Basic Safety Principles for Nuclear Power Plants: 75-INSAG-3 Rev. 1.* Vol. 1082. International Atomic Energy Agency, 1999.

[2] International Nuclear Safety Advisory Group. *Defence in Depth in Nuclear Safety: INSAG-10: a Report.* International Atomic Energy Agency, 1996.

[3] F. Altkind et al. *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants.* Jan. 2011.

[4] JN Sorensen. "Safety culture: a survey of the state-of-the-art". In: *Reliability Engineering & System Safety* 76.2 (2002), pp. 189–204.

[5] *Status report 74 - Indian 220 MWe PHWR (IPHWR-220).* Tech. rep. Vienna, 2011.

[6] S.S. Bajaj and A.R. Gore. "The Indian PHWR". In: *Nuclear Engineering and Design* 236.7 (2006). DOI: https://doi.org/10.1016/j.nucengdes.2005.09.028. URL: https://www.sciencedirect.com/science/article/pii/S0029549306000707.

[7] M.V. Ramana and Ashwin Kumar. "'One in infinity': failing to learn from accidents and implications for nuclear safety in India". In: *Journal of Risk Research* 17.1 (2014), pp. 23–42. DOI: 10.1080/13669877.2013.822920. URL: https://doi.org/10.1080/13669877.2013.822920.

[8] G DivyaDeepak. "Accident Analysis of Narora Fire Accident". In: *power* 3 (2012), 24sec.

[9] L Joseph Callan et al. *Principles for a strong nuclear safety culture.* 2004.

[10] IAEA Safety Culture. "A Report by the International Nuclear Safety Advisory Group". In: *IAEA Safety Series* (1991).

[11] Ik Hyeon Jang and Yong Hun Jung. "A Review of Representative Fire Incidents in Nuclear Power Plants". In: (2022). URL: https://www.kns.org/files/pre_paper/47/22S-407-%EC%9E%A5%EC%9D%B5%ED%98%84.pdf.

[12] Atomic Energy Regulatory Board. "AERB". In: *Regulation* 2.3 (2012).

[13] Pratibha Mahawar et al. "International Journal of Science and Research (IJSR)". In: ().

[14] Dan Gabriel Cacuci. *Handbook of Nuclear Engineering: Vol. 1: Nuclear Engineering Fundamentals; Vol. 2: Reactor Design; Vol. 3: Reactor Analysis; Vol. 4: Reactors of Generations III and IV; Vol. 5: Fuel Cycles, Decommissioning, Waste Disposal and Safeguards.* Vol. 1. Springer Science & Business Media, 2010.

[15] BENGT PERSHAGEN. "9 - Deterministic Safety Analysis". In: *Light Water Reactor Safety.* Ed. by BENGT PERSHAGEN. Oxford: Pergamon, 1989, pp. 170–208. ISBN: 978-0-08-035915-1. DOI: https://doi.org/10.1016/B978-0-08-035915-1.50014-X. URL: https://www.sciencedirect.com/science/article/pii/B978008035915150014X.

[16] Sean Roshan. *FSH2705 Simulation Course - Safety Assessment and Safety Analysis (pressentation).* 2023.

[17] *Deterministic Safety Analysis for Nuclear Power Plants.* Specific Safety Guides SSG-2 (Rev.1). Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2019. ISBN: 978-92-0-102119-9. URL: https://www.iaea.org/publications/12335/deterministic-safety-analysis-for-nuclear-power-plants.

[18] BENGT PERSHAGEN. "10 - Probabilistic Safety Analysis". In: *Light Water Reactor Safety.* Ed. by BENGT PERSHAGEN. Oxford: Pergamon, 1989, pp. 209–256. ISBN: 978-0-08-035915-1. DOI: https://doi.org/10.1016/B978-0-08-035915-1.50015-1. URL: https://www.sciencedirect.com/science/article/pii/B9780080359151500151.

[19] *Probabilistic Safety Assessment.* INSAG Series 6. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 1992. ISBN: 92-0-102492-4. URL: https://www.iaea.org/publications/3789/probabilistic-safety-assessment.

[20] AK Babar et al. *Probabilistic Safety Assessment of Narora Atomic Power Project.* Tech. rep. Bhabha Atomic Research Centre, 1989.

[21] Eleonora Skrzypek and Maciej Skrzypek. "Computer codes in the safety analysis for nuclear power plants. Computational capabilities of thermal-hydraulic tools, using the example of the RELAP5 code". In: *Journal of Power Technologies* 94.5 (2015), pp. 41–50.

[22] A. Petruzzi and Francesco D'Auria. "Thermal-hydraulic system codes in nuclear reactor safety and qualification procedures". In: *Sci. Technol. Nucl. Install. ID 460795* (Jan. 2008).

[23] Ulrich Rohde et al. "The reactor dynamics code DYN3D – models, validation and applications". In: *Progress in Nuclear Energy* 89 (2016), pp. 170–190. ISSN: 0149-1970. DOI: https://doi.org/10.1016/j.pnucene.2016.02.013. URL: https://www.sciencedirect.com/science/article/pii/S014919701630035X.

[24] J.P. Van Dorsselaere et al. "Chapter 8 - Integral Codes for Severe Accident Analyses". In: *Nuclear Safety in Light Water Reactors.* Ed. by Bal Raj Sehgal. Boston: Academic Press, 2012, pp. 625–656. ISBN: 978-0-12-388446-6. DOI: https://doi.org/10.1016/B978-0-12-388446-6.00008-3. URL: https://www.sciencedirect.com/science/article/pii/B9780123884466000083.

[25] "Atoms with Mission". In: A Golden Jubilee Commemorative Volume (2007). URL: https://dae.gov.in/writereaddata/publ/saga/vol2/pdf2/Chapter20-2007.pdf.

[26] Sean Roshan. *FSH2705 Simulation Course - Computer codes, validation & verification (pressentation).* 2023.

Appendix

Table 1: Timeline of events [8]

Time line	**Event**	**Cause**	**Reason**
0 ms	rupture of turbine blades	root cause[1]	accumulated stress/mechanical fatigue
38 sec	rupture of hydrogen seals	contributing cause[2]	vibrations in the generator unit
40 sec	rupture of lube oil lines	contributing cause	vibrations in the generator unit
1 m 20 sec	fire spread through the generator bus duct in the TB and CER	direct cause[3]	lubricating oil as a medium of transport
3 m 24 sec	power cables burning	root cause	lack of fire-resistant insulation

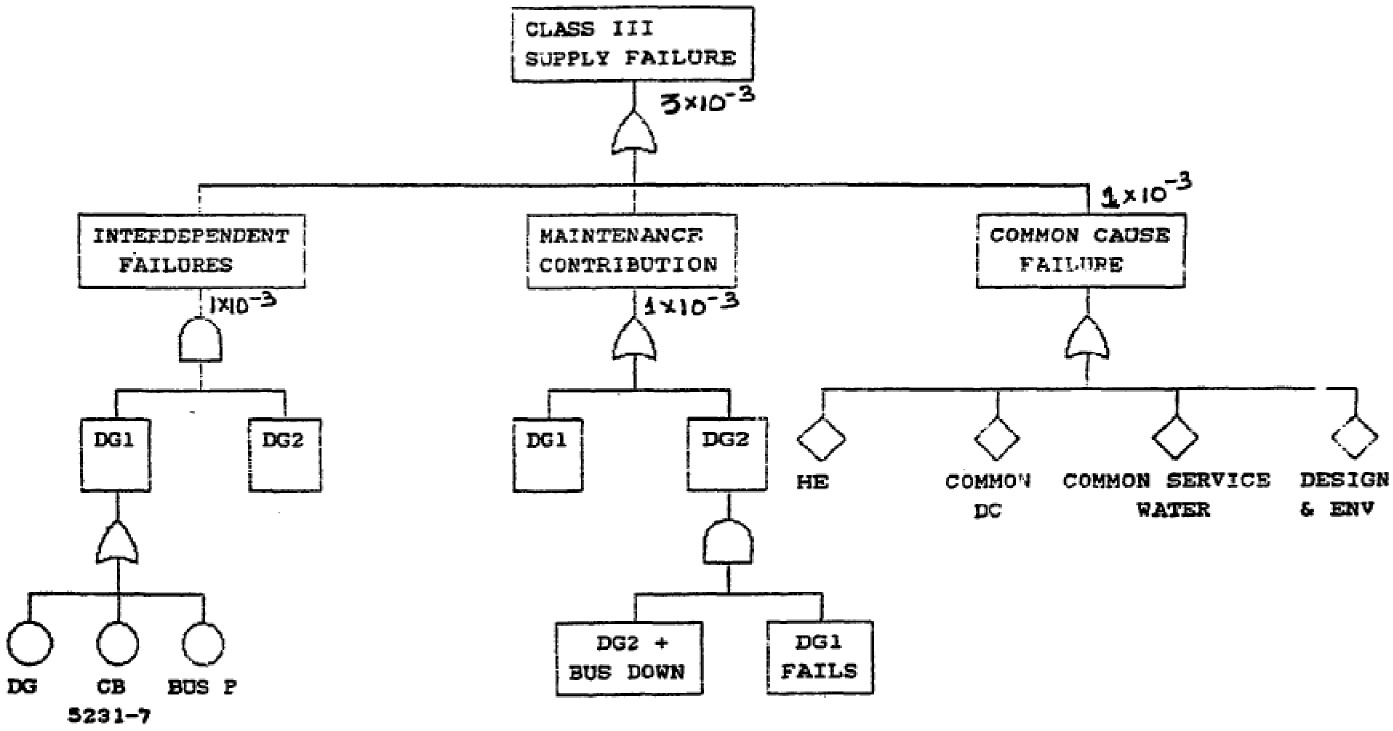
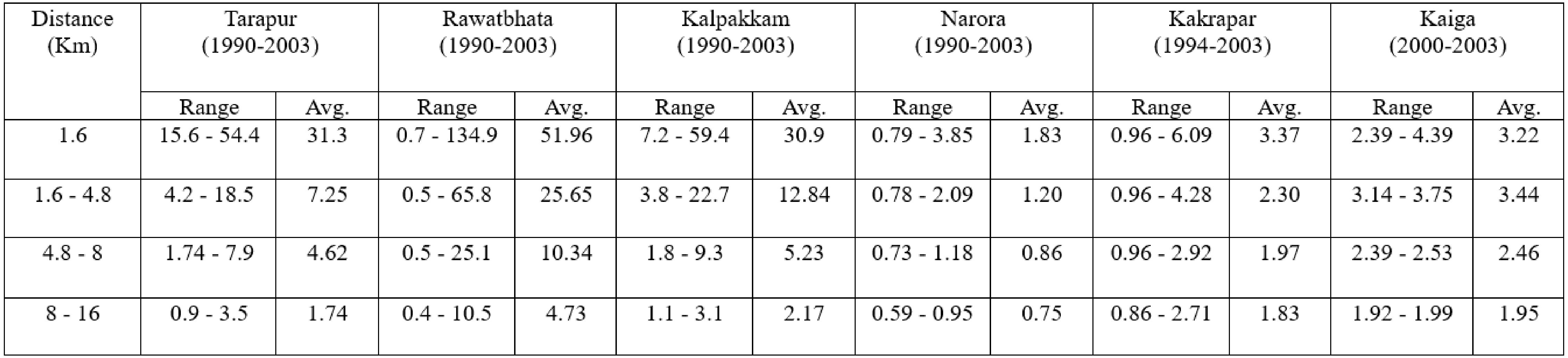


Figure 5: Extract of the PSA of Narora power plan concerning the emergency in-site power supply [20].

Table 2: Types of DSA [16].

Applied codes	Input & BIC[2]	Assumptions on systems availability	Approach
Conservative codes	Conservative	Conservative	Deterministic
BE codes	Conservative	Conservative	Deterministic
BE codes + Uncertainty	Realistic + Uncertainty	Conservative	Deterministic
BE codes + Uncdertainity	Realistic + Uncertainity	PSA-based	Deterministic + probabilistic

[1] Root cause is defined as a cause which if prevented the event would not happen [8].
[2] Contributing cause is defined as the cause which increased the probability of the event happening [8].
[3] Direct cause is a set of immediate precursors that caused the event [8].



Distance (Km)	Tarapur (1990-2003)		Rawatbhata (1990-2003)		Kalpakkam (1990-2003)		Narora (1990-2003)		Kakrapar (1994-2003)		Kaiga (2000-2003)	
	Range	Avg.	Range	Avg.	Range	Avg.	Range	Avg.	Range	Avg.	Range	Avg.
1.6	15.6 - 54.4	31.3	0.7 - 134.9	51.96	7.2 - 59.4	30.9	0.79 - 3.85	1.83	0.96 - 6.09	3.37	2.39 - 4.39	3.22
1.6 - 4.8	4.2 - 18.5	7.25	0.5 - 65.8	25.65	3.8 - 22.7	12.84	0.78 - 2.09	1.20	0.96 - 4.28	2.30	3.14 - 3.75	3.44
4.8 - 8	1.74 - 7.9	4.62	0.5 - 25.1	10.34	1.8 - 9.3	5.23	0.73 - 1.18	0.86	0.96 - 2.92	1.97	2.39 - 2.53	2.46
8 - 16	0.9 - 3.5	1.74	0.4 - 10.5	4.73	1.1 - 3.1	2.17	0.59 - 0.95	0.75	0.86 - 2.71	1.83	1.92 - 1.99	1.95

Figure 6: Environmental Radiation Dose (µSv/y); (AERB Dose limit 1000 µSv/y) [25].