Nuclear Accident of NPP Jaslovské Bohunice A1 and Safety Theory Overview

Authors: **Ondřej Lachout, Nicolas Becquet**

E-mail: **lachoond@cvut.cz, nicolas92.becquet@gmail.com**

Institution: **KTH Royal Institute of Technology**

Subject: **SH2705 VT23 Compact Reactor Simulator**

Date: **06/04/2023**

Introduction

This report deals with a description of two accidents, which happened on a formal Czechoslovak NPP Jaslovské Bohunice A1 and a theory overview on safety of NPP with the relation to the mentioned accidents.

1 Overview on safety theory of NPPs

In recent years the development of new technologies has dramatically increased. We are continuously building and improving technologies concerning both efficiency and safety. Safety has an important role in all technology aspects.

All man-made machines undergo accidents or failure, no matter their level of technical advancement. NPPs aren't an exception to this rule, and when designing an NPP, engineers shouldn't think that accidents cannot occur because their probability is very low. NPPs are extremely complex systems and we cannot fully predict their behaviour, during accidents but also during normal operation. Transients can occur at any time in any part of NPP.

From what is written above comes the necessity of dealing with safety in nuclear industry.

1.1 Safety objectives

When talking about safety, we first have to define what safety means. Safety can be understood differently be individuals. Majority of people are more afraid of flying by plane than going by car, but statistically (see Table 1) flying by plane is more than 100x safer per km-distance, rather than going by car.

Table 1: Death of people in the USA between the years 2000-2009 [13]

Means of transportation	**Number of deaths (people/BIL km)**
Motorcycle	132.1
Car	4.52
Ferry	1.97
Train	0.26
Public transport	0.15
Coach	0.07
Plane	0.04

When calculating risk one shouldn't consider subjective understanding a risk. For this propose risk is rigorously defined as:

$$RISK = \sum_i PROBABILITY_i \cdot CONSEQUENCES_i \tag{1}$$

This definition of risk shows how it depends from two independent variables, the probability of an event and the consequences of the occurring of that event. Thus, two very different events can represent the same risk, because an event with a high probability of occurring but low consequences can represent the same risk as an event with a low probability of occurring but dramatic consequences.

In nuclear industry, all types of events and accidents should be considered. When we talk about accidents in an NPP, people often think about the most severe accidents. Of course, those accidents must be considered because even if they have a low occurrence probability, their consequences are so serious that they represent a high risk. However, all the events that have less serious consequences but represent the same risk because they have a higher probability of occurring should be considered with the same importance and the same efforts should be made to decrease the risk.

The main goal of nuclear safety is to prevent all kinds of accidents from happening, i.e. lowering their probability, but this probability can never reach zero, and that is the reason why nuclear safety has to also consider the possible consequences of those events. In the next chapters, the approaches for lowering the risk will be explained.

1.2 Operational and accident conditions

Maintaining safe operation of a nuclear reactor is essential. During operation, nuclear reactor undergoes various states. Those states can be, according to IAEA-SSG-2 [9] described as follows:

- Normal operation,
- Abnormal operational conditions,
- Emergency conditions.

Normal operational conditions

Normal operational conditions are anticipated conditions in which the reactor is designed to operate. These conditions include the reactor's power level, temperature, pressure, coolant flow rate, and other relevant parameters. All those parameters are carefully monitored and in case of their deviation needed steps have to performed to keep the reactor safe.

The normal operational conditions are determined based on the reactor's design, as well as its intended use, and take into account various safety considerations to prevent accidents and ensure the protection of personnel and the environment.

Abnormal conditions

Abnormal operational conditions of a nuclear reactor refer to conditions that deviate from the normal operating conditions, which could lead to safety risks.

There are many safety systems, that have to immediately work to maintain the reactor, people and environment safe.

The IAEA recommends that nuclear power plant operators conduct comprehensive safety assessments to identify potential accident scenarios and develop strategies to prevent or mitigate their consequences. These assessments should take into account both internal and external hazards and consider a range of factors, including plant design, equipment performance, and operator training and qualifications.

Emergency conditions

Emergency reactor conditions refer to any situation where the normal operation of a nuclear reactor is disrupted, and the safety of the reactor and its surrounding environment may be compromised.

This can include a wide range of events, such as equipment failures, human errors, natural disasters, or malicious etc. In emergency reactor conditions, the reactor operators must take immediate action to control the situation and prevent any release of radioactive materials into the environment.

1.3 Defense in depth

Defense in depth (DID) is a concept that is a central part of the philosophy of nuclear safety. The NRC defines it as creating multiple independent and redundant layers of protection and response to failures, accidents, or fires in power plants. Its main purpose is to protect people and the environment outside of the plant from harm and ionizing radiations as much as possible. Defence in depth is achieved by five-stage protection principle:

- Prevention of abnormal conditions,
- Control of abnormal conditions and fault detection,
- Control of DBA,
- Control of BDBA and SA,
- Mitigation of radiological consequences.

Those principles are significantly important when talking about safety.

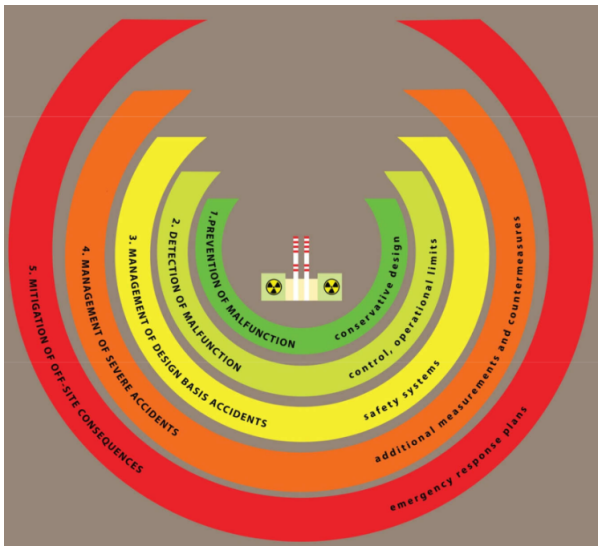

Figure 1: Graphical visualization of DID [2]

Prevention of abnormal conditions

The first feature that allows a good prevention of incidents in a power plant is the design of the plant itself. The design and manufacture must be of high quality and there should be large design margins when it is possible, so that the reactor can operate outside of normal operating conditions without failing, because it is impossible to guarantee that the reactor will not reach abnormal conditions. Frequent inspections and maintenance operations must keep those margins high. Moreover, the critical systems should be as redundant as possible.

On the other hand we can never prevent all kinds of events, for this purpose protection in needed!

Abnormal conditions control and fault detection

Abnormal conditions control in a nuclear reactor are conditions which are maintained by normal reactor systems. For example fuel burn-up in PWR is controlled by boron concentration in coolant or by CR insertion.

There has to be a periodical control of proper system operation and their non-destructive testing.

DBA control

In case of DBA we should be able to control the event and maintain its safe resolution using safety system so the event doesn't cause BDBA. In doing so concepts of redundancy, diversity and physical separation are applied. Those concepts are explained in simple terms as:

- Redundancy means having more systems of one kind in case of one systems failing (prevents single system failure)
- Diversity means having more systems of different kind (prevents common cause failure)
- Physical separation means having system on physically separated places (prevents damage in one certain part of NPP)[1]

Control of BDBA and SA

BDBA accidents have not been anticipated while designing the power plant. It was not known that this type of accident could happen or its probability was judged to be too low to be taken into account, so no system has been incorporated in the plant to deal with it. In this case, the radioactive materials have to be localized and kept inside the plant.

When it comes to dealing with severe accidents, the release of radioactive materials in the environment must be avoided at all costs, and the main barrier is the concrete containment building, reinforced with steel. Other systems like the core catcher help keeping the radioactive materials inside the plant.

Mitigation of radiological consequences

This last echelon can be considered as dealing with worse-case. When there are significant releases outside of the plant, radiological consequences must be mitigated. Mitigation relies mainly on off-site emergency procedures.

Radial protection plans and emergency protection for the public are required. Among those we classify iodine prophylaxis, emergency planning zones, control of agriculture and other.

1.4 Acceptance criteria

What is and what is not acceptable will depend on the possible risk (see equation 1)

Acceptance criteria should ensure a sufficient level of DID. When building a new NPP there are always 3 key players, who must cooperate and communicate with each other for the lifetime of a NPP. Those key players are:

- Government,
- Regulatory body,
- Operating organization.

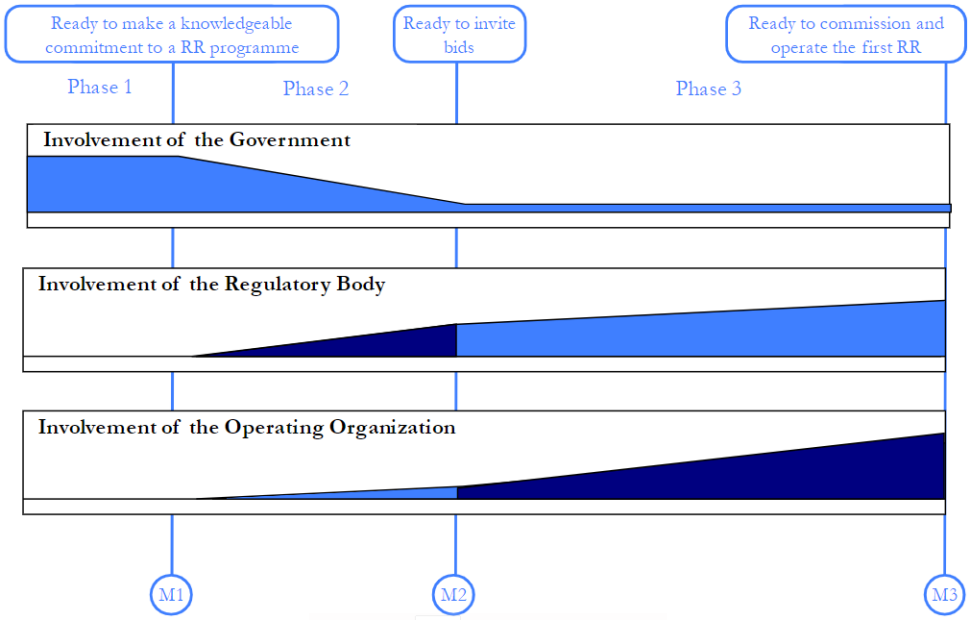

Figure 2: Involvement of those 3 key players during the lifetime NNP [7]

Involvement of those 3 key players during the lifetime NNP is presented in Figure 2

There are and there will always be things, systems and events which we don't fully understand and that could play a serious role in possible accident. The goal for people dealing with safety is trying to understand the possible and unpredictable scenarios.

When checking the fulfilment of all desired parameters set by regulatory body, there is always a gap between design capacity and safety margin. Via calculation and other testing it has to be assured that those limits are never surpassed. (see Figure 3)

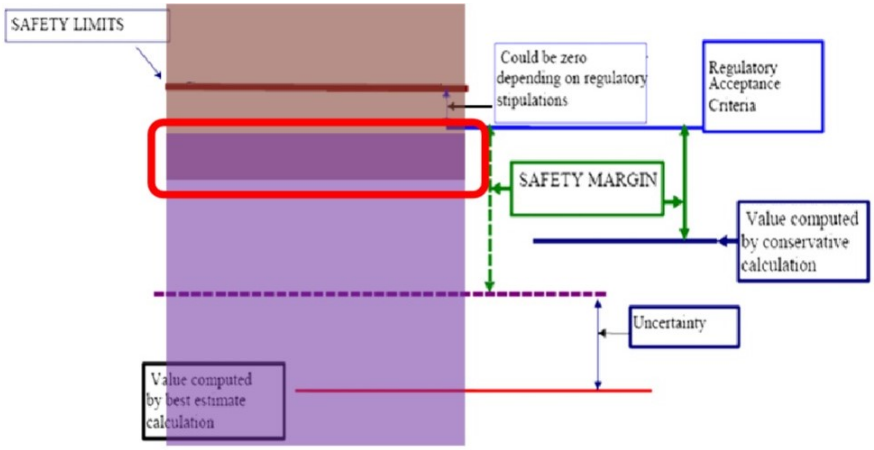

Figure 3: Safety margin and safety limits visualization [12]

Even if we can decrease the risk accidents represent, we cannot make it reach 0 and one of the purposes of nuclear safety is to define the limit between which level of safety is acceptable and which level is not.

The acceptance criteria and the single-failure criteria are examples of the main criteria which drive the actions of engineers when they build and operate an NPP. They aim to ensure that a sufficient level of Defense in Depth is maintained even in the case of an incident. This level of Defense in Depth is reached by ensuring a sufficient level of redundancy and independence.

[1]The importance of physical separation was recognized after the last nuclear accident (Fukushima 2011). If there was a SG somewhere the tsunami wave couldn't have reached the consequences wouldn't be as serious

That sufficient level is defined by the requirements it has to meet :

- There should be a sufficient number of systems dedicated to each protective function so that no single failure results in the loss of that protective function.
- Removal of service, for example during maintenance, of any component or channel shouldn't result in loss of the minimal degree of redundancy. For example, if only two systems are dedicated to a protective function and one of them is undergoing maintenance, if a single failure occurs in the other one, the protective function is no longer assured, and this should be avoided.
- All protection systems should be designed so that they allow periodic testing, even while the reactor is in operation. It should be possible to test channels independently to determine failures and losses of redundancy that may have occurred.

Another important aspect of the acceptance criteria is that pressure in primary and secondary systems should not exceed design limits. More generally, for all components in the power plant, the load should not exceed the capacity. There must be what is called a design margin between the load in normal operation and the load a component is capable of handling. However, load and capacity are random variables characterized by a mean value but also a standard deviation. Thus, there is a certain probability that load would exceed capacity, and it is important to know the size of the overlapping to have an idea of the reliability of each component.

When working on neutronics of thermohydraulics calculations one has to always consider uncertainties within this calculation.

1.5 Safety assessment

Safety assessment is a critical process in nuclear engineering that involves evaluating the potential hazards and risks associated with nuclear power plants. The main goal is to identify potential hazards, ensure that adequate measures are in place to prevent accidents and minimize their consequences, and identify the measures that need to be taken to comply with safety requirements. It is carried out during the entire lifetime of the plant as it can be necessary for several different procedures such as (between many others):

- Licensing of a new plant/renewing of the licence of an operating plant for extension of its lifetime
- Upgrading or modernization of the plant
- determining and updating operational limits and conditions
- Periodic safety reviews

The overview of safety assessment process is visualized in Figure 4.

Safety assessment can be performed by the designer, licensee or regulatory body.

IAEA document [8] recognizes approach to safety assessment. This approach have several requirements. In the text below, the most important ones are summarized and briefly described:

- **Scope of the safety assessment** shall be carried out for all applications of technology that give rise to radiation risks, further determination of scope and level of detail the safety assessment should meet.
- **Responsibility for the safety assessment** shall rest with the responsible legal person, that is, the person or organization responsible for the facility or activity.

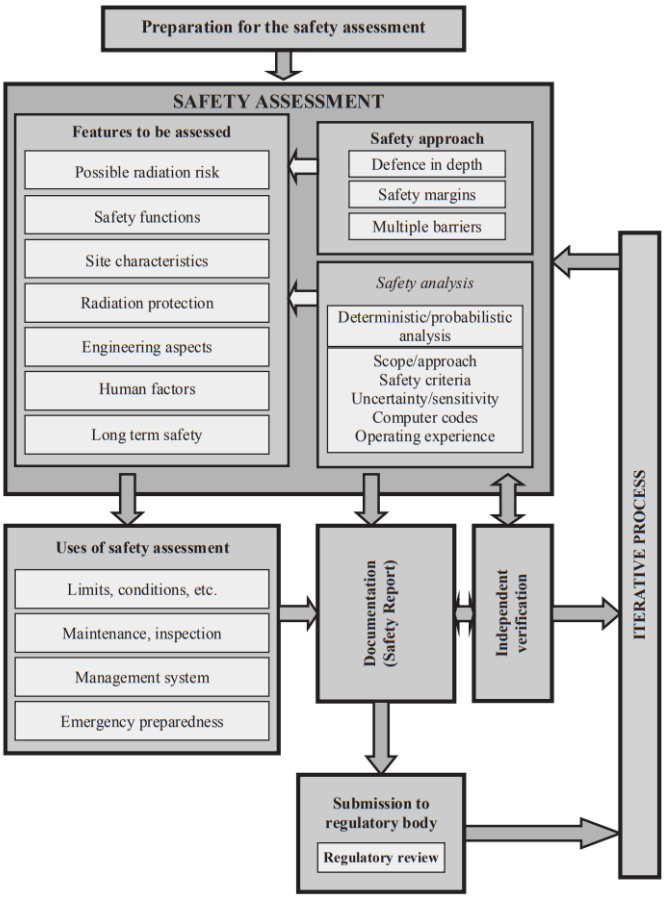

Figure 4: Overview of the safety assessment process [8]

- **Assessment of safety functions and site characteristics** point out, that all safety functions associated with a facility or activity shall be specified and assessed. Site characteristics relating to the safety of the facility or activity shall be carried out.
- **Assessment of the provisions for radiation protection** summarize what shall be determined in the safety assessment for a facility or activity whether adequate measures are in place to protect people and the environment from harmful effects of ionizing radiation.
- **Assessment of human factors** shall be addressed in the safety assessment, and it shall be determined whether the procedures and safety measures that are provided for all normal operational activities, in particular those that are necessary for implementation of the operational limits and conditions, and those that are required for responding to anticipated operational occurrences and to accident conditions, ensure an adequate level of safety.
- **Assessment of safety over the lifetime of a facility or activity** shall cover all the stages in the lifetime of a facility or activity in which there are possible radiation risks.
- **Assessment of defence in depth** shall be determined in depth whether adequate provisions have been made at each of the levels of defence in depth.
- **Uncertainty and sensitivity analysis** shall be performed and taken into account in the results of the safety analysis and the conclusions drawn from it both for deterministic and probabilistic approaches.
- **Independent verification** shall be carried out by an independent organization before it is used by the operating organization or submitted to the regulatory body.
- **Maintenance of the safety assessment** shall be periodically reviewed and updated.

1.6 Safety analysis

Safety analysis is included in the safety assessment, aims to ensure that all the safety requirements are met by the proposed or current design, for a broad range of operating conditions and various initiating events. Thus, it consists in the study of how the reactor will behave under abnormal conditions and if the safety requirements will be met under those conditions. As we said it earlier, it is part of safety assessment and it is particularly important during the early steps like conception of the design or during the licensing process.

Safety analysis shall provide both deterministic and probabilistic approaches to confirm correct behaviour of systems and technologies important to safety.

The goal of safety analysis is to identify hidden failures or weaknesses in safety functions. Main events that safety analysis should consider could be divided into few categories:

- **Reactivity insertion accident** (RIA) may cause instant increase in reactor power and in worse case scenario resulting in criticality on prompt neutrons.
  - Sudden CR withdrawal,
  - Uncontrolled decrease in burnable absorbers concentration,
  - Wrong core loading,
  - Pressure changes.
- **Loss of coolant accident** (LOCA) is an accident with partial or total loss of coolant in a primary circuit.
  - LB LOCA (a full guillotine cut in the main coolant piping),
  - SB LOCA (a small to medium burst in the main coolant piping),
  - Pipe burst in steam generator.
- **Loss of heat sink accident** is an accident resulting in a decrease in heat dissipation from reactor (concerns both primary and secondary circuit).
  - Main pump failure,
  - Flow instabilities in coolant,
  - Lost of secondary water flow in steam generator.
- **Other accident** includes events, which might occur during maintenance. Those events can also lead to large radioactivity release.
  - Accident regarding manipulation with fresh or burned/spend fuel,
  - Accident regarding radioactive waste handling.
- **External events** harming NNP safety.
  - Natural events (earthquake, tsunami wave, wind, ...)
  - Events caused by people (airplane crash, sabotages, military attack, ...)

To perform safety analysis, means to check that all the requirements are met and that a sufficient level of defense in depth has been reached, deterministic and probabilistic methods should be applied.

Deterministic methods consist in using calculational models to study the consequences of an event on the plant's behavior.

Probabilistic methods consist in the study of the reliability of the plant components and safety systems. It evaluates the likelihood of accident scenarios and identifies sequences of events that could lead to serious consequences. Unlike deterministic methods, they include elements of randomness.

1.7 Deterministic safety analysis

In safety analysis, deterministic methods rely on models to predict the behavior of a power plant with a particular set of initial conditions. One of the characteristics of a deterministic safety analysis is that it does not include elements of randomness: the same initial set of conditions have to give the same results.

As it has been said in the section about safety analysis, deterministic safety analysis is particularly important during the conception of reactor design and for the licensing. It is mainly used when it comes to proving that the design of the accident is robust enough to prevent a Design Basis Accident (DBA) to escalate into a Beyond Design Basis Accident (BDBA) or further to Severe Accident (SA). Meaning it must prove that safety systems have been designed so that in case of a DBA, the reactor can be safely shutdown, the residual heat is removed and radioactive releases are below the acceptable limits.

DSA is also used to study normal operation: it ensures that normal operation is safe and is used to establish the conditions and limitations for safe normal operation.

However, the scope of DSA has limitations. DSA is used in case of:

- Simplifying assumptions and bounding situations,
- Design basis events,
- Single failures,
- Unique error of the operator.

Figure 5 shows the principle of the deterministic approach and its result.

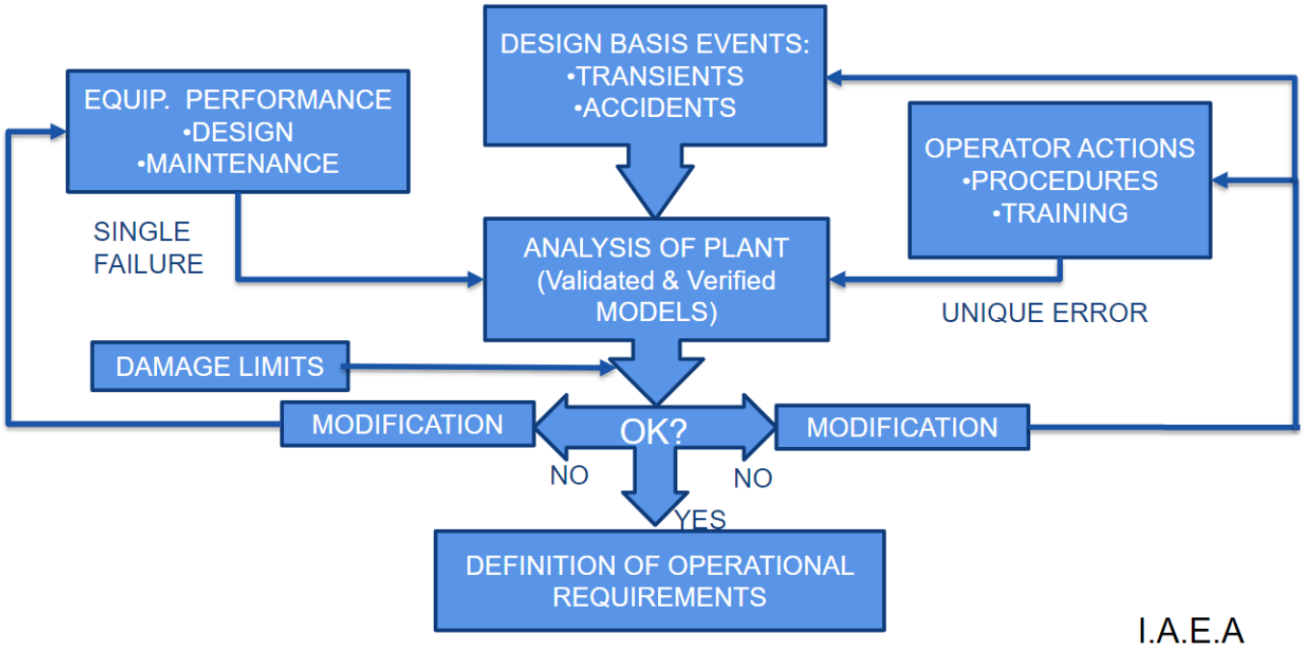

Figure 5: Overview of the deterministic approach [10]

1.7.1 Conservative analysis

The conservative approach in safety analysis for nuclear power plants involves assuming the worst-case scenario and applying significant safety margins to account for uncertainties and potential variations in operating conditions. In other words, any parameter that has to be specified for the analysis should be allocated a value that will have an unfavourable effect in relation to specific

acceptance criteria.
Safety analysis using the conservative approach involve evaluating the plant's response to a variety of hypothetical accidents, including those that are extremely unlikely but still possible. For example, a safety analysis may consider the failure of multiple safety systems simultaneously pr the occurrence of a natural disaster.

By using conservative assumptions and safety margins, safety analysis can ensure that the nuclear power plant is designed to withstand a wide range of potential events and still maintain safety. The conservative approach is a critical component of the licensing and regulatory process.

The conservative approach includes several hypothesis concerning the power plant. Concerning the availability of systems and components, a system or a component should be able to perform its functions in all cases, even in the case of the worst possible single failure, so the worst possible single failure is always assumed. Furthermore, all the common cause failures and the possible consequential failures associated with the postulated initiating event should be considered and availability due to on-line maintenance have to be taken into account. In addition to this, a loss of off-site power should be considered, as appropriate, when analysing design basis accidents. For such cases, the assumption that gives the most negative effect on the margin to the acceptance criterion should be chosen.

Concerning the operators, conservative assumptions should be made. It should not be assumed that operators will take efficient measures to limit the evolution of a design basis accident within a short enough period of time.

Particular attention should be put into the model itself, and the choice of some of its parameters like the number of nodes that are used, as it can have a large influence on the results of the analysis.

1.7.2 Best estimate analysis

Best-estimate approach has more realistic description of physical phenomenons. This approach has to assure, that all important factors and uncertainties are being correctly assumed.

Correct calculation of uncertainties is significantly important when it comes to best-estimate approach. In a computer model there are various causes of uncertainties, those could be:

- **Input data** (the physical data, which are given by user always has an uncertainties, that have to be assumed. The process of input error uncertainty is called sensitivity analysis)
- **Model itself** (the model describing a real incident/event is usually simplified. Model re-nodalization methods are checked, if giving the same results)
- **Unpredictable events** (as it was explained, there could still be physical phenomena, that are not fully understood)

Main disadvantages of both deterministic approach are limitation on DBA (there could always be assumed a worse accident), doesn't take into account partial system functionality (can make the situation better) and it doesn't take into account the probability of system functionality.

For this purpose probabilistic safety analysis has to be carried out.

1.8 Probabilistic safety analysis

Probabilistic safety analysis (PSA) is based on DSA, but combines its results with probabilities. When evaluating the safety analysis probabilities of devices working properly and staff correctly recognizing the incident are taken into account.

The first mention of PSA concept may be found in Rasmussen report ([4]) from 1975.

In practice, PSA aims at: [6]

- Identifying and delineating the combinations of events that may lead to a severe accident,

– Assessing the expected probability of occurrence for each combination,
– Evaluating the consequences.

In order to perform these tasks, PSA methodology integrates information about plant design, operating practices, operating history, component reliability, human behaviour, accident phenomena, and (in its widest application) potential environmental and health effects.

Three levels of PSA may be distinguished.

– PSA 1. evaluates the probability of core damage frequency (CDF)
– PSA 2. determines the probability of large release frequency (LRF)
– PSA 3. calculates the probability of undesirable effects on public and environment

For graphical visualization of PSA a binary logical techniques are used, namely:

– **Event tree diagram** starts with postulated initiated event and the sequence of future events is examined. All possible combination are modelled and each "branch" is described by its probability. Using this approach the total risk can be determined.
– **Fault tree diagram** is linked to event tree and examines the potential of component failure.

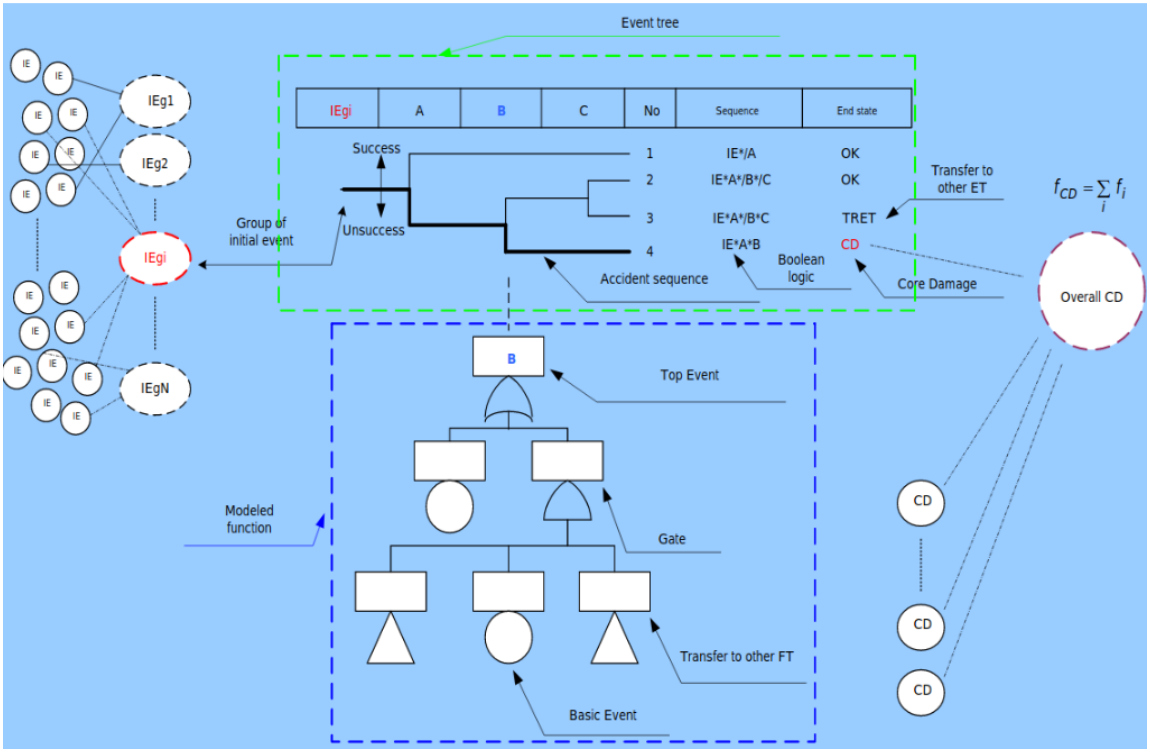

Figure 6: A graphical visualization of event tree and fault tree diagrams [6]

A complete safety analysis should always contain a combination of conservative, best estimate deterministic and probabilistic analysis!

1.9 Computer codes

When it comes to performing safety analysis, computer codes are absolutely essential. They represent a collection of models that are needed to simulate every part of a nuclear power plant during a transient or an accident. Those models differ from the conservative deterministic safety analysis and the best-estimate safety analysis. Of course, for conservative DSA, for example, conservative codes are used. Those are codes that use pessimistic models, with pessimistic assumptions.

Among the main different types of computer codes, we can distinguish :

- **System codes**, that can model the entire power plant to simulate certain accidents.
- **Reactor dynamic codes**, which purpose is to focus on the reactor core and simulate the neutron kinetic response of the plant.
- **Severe accident codes**, designed to analyse beyond design basis accidents.

In the text below details about those different codes are given.

The most common type of system codes is thermal-hydraulic system codes, used for analysis of LOCAs. Experimental data is necessary to create efficient codes, and that is why those codes have improved a lot and keep improving since the first system codes, which were quite limited. Of course, this improvement is also related to the better quality of today's computers. Experimental correlations are incorporated to accurately describe the needed boundary conditions for each phase, and more experimental data is a synonym of more accuracy.

All the progress that has been made in the field has enabled nuclear engineers to have realistic codes such as APROS, ATHLET or TRACE, but always with quite simple neutronics models, and there is today a strong need for coupling system codes and neutronics codes. This would allow for a more comprehensive and accurate analysis of nuclear systems, as a code that couples neutronics and the behavior of coolant, structures, etc... would take into account the interactions between the neutronics and thermal-hydraulic behavior of the system. For example, the feedback effects of temperature and coolant flow on the neutron behavior can have a significant impact on the behavior of the system as a whole. This more accurate description of the phenomena that occur in the power plant is particularly important when accidents are simulated, as more complex phenomena occur during accidents, involving micro scale and multidimensional features too complex to be described without coupling. IAEA gives examples of transients which consequences would be more accurately described thanks to coupled codes :

- Inadvertent control rod withdrawal
- Control rod ejection
- Severe accident progression and radioactive material transport in the containment
- LOCA with strong influence from containment processes

As system codes often don't include a complex neutronics model, reactor dynamic codes rarely include detailed thermal-hydraulics. They simulate transients and accidents with criticality concerns. Examples of these codes are PARCS, SIMULATE3K and POLKA7.

Finally, severe accident codes such as MELCOORE, MAAP or ASTEC are deterministic as they aim to describe physical phenomena with much detail. Since the development of the first severe accident codes, realistic modelling has been the strategy of development.

1.10 Verification and validation of computer codes

There cannot be used just an arbitrary computer code for safety analysis purposes. Each code, that has the approval to be used for safety analysis has to verified and validated.

Verification and validation of computer codes are important stepsa of quality assurance procedure for successful application.

Verification means a detailed check of all code function agings other code. During this process the structures of an examined code are tested and an assurance is done to meet the defined requirements. A code could be verified throughout a so called benchmark task.

Validation aims to check an examined code against experimental data. For the purpose of validation a suitable physical experiment is required to compare experimental and computational data. Chronologically validation should be performed after verification is finished.

The whole process of verification and validation should contain:

– Comparison of results with a similar model/code
– Comparison of results with an experimental data on a miniature of tested devices,
– Comparison of results with an experimental data on a real nuclear power plant.

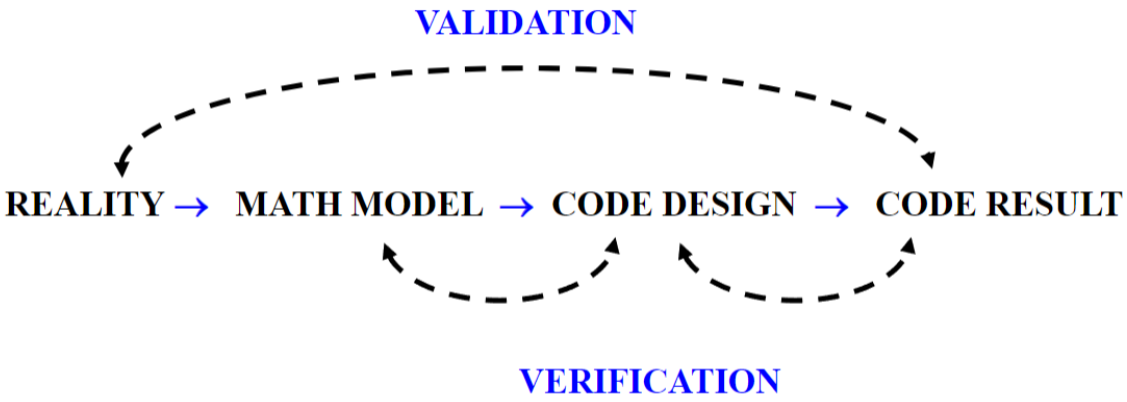

Figure 7: A graphical visualization of verification and validation process [11]

2 NPP Jaslovské Bohunice A1

Jaslovské Bohunice A1 was the first commercial nuclear power plant on the territory of former Czechoslovakia (ČSR). The accidents description was inspired by a presentation [3].

NPP timeline:

– 1955 a cooperation agreement on the peaceful uses of nuclear energy was signed,
– 1958 the construction began,
– 1972 the first critical state achieved,
– 5.1. 1976 first major accident,
– 1.6. 1976 reactor restarting,
– 22.2. 1977 second major accident,
– 1979 definite shutdown,
– 2050? final NPP decommissioning.

The whole operation time NPP was in an experimental operation to demonstrate the possible use of natural uranium.

Reactor KS-150

Reactor KS-150 with thermal power 150 MWe, consisting of 6 loops, the reactor vessel is formed by pressure channels. Heavy water is used as moderator with combination of natural uranium[2] as a fuel. The system was cooled by CO_2 (flowing from the top to the bottom). Primary system pressure 6.5 MPa. Regulation was performed by control rods (40) inserted from above.

The core was 5.1 m in diameter and 20.1 m in height. Online refueling is performed using quite complicated reactor crane. Maximum fuel burn-up (being only) 4500 MWd/tU.

A visualization of fuel pin is presented in Figure 9. It can be seen that the fuel pin has "teeth" around the perimeter to increase the heat transfer from cladding to flowing gas.

[2]Natural uranium was mined in ČSR and than transported to SSSR, where the fuel assemblies were assembled and brought back.

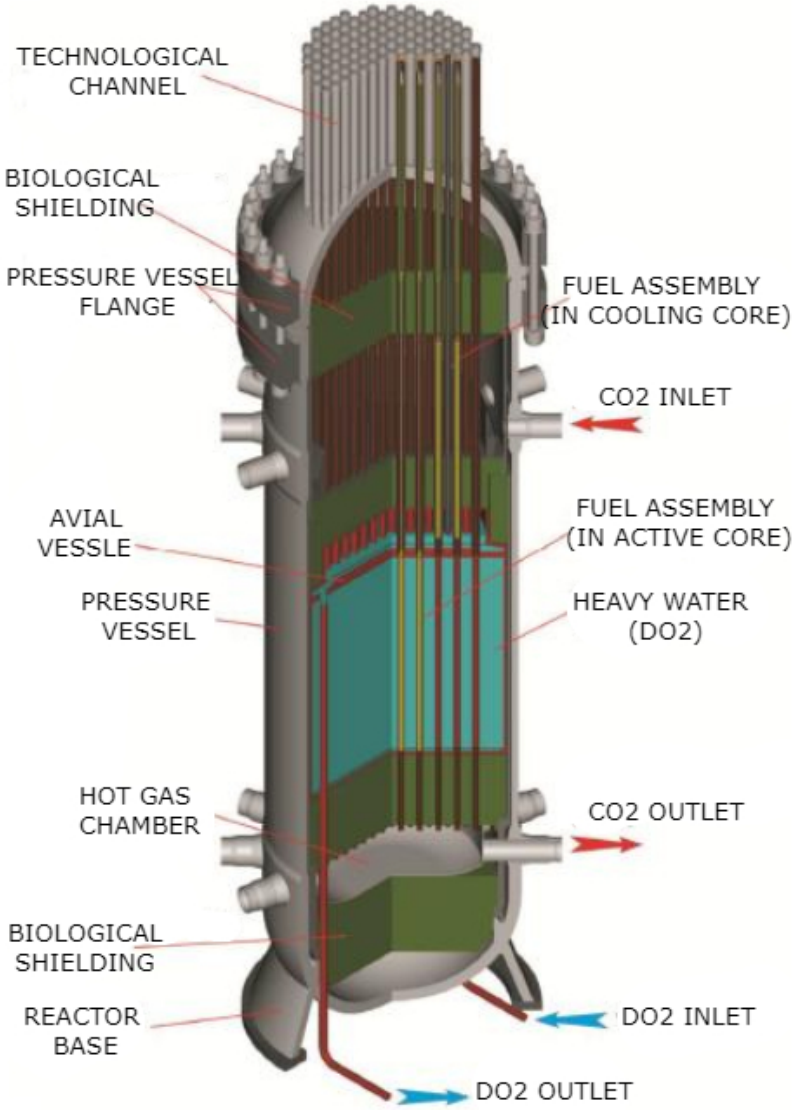

Figure 8: Schematic representation of KS-150 nuclear reactor [1] (modified)

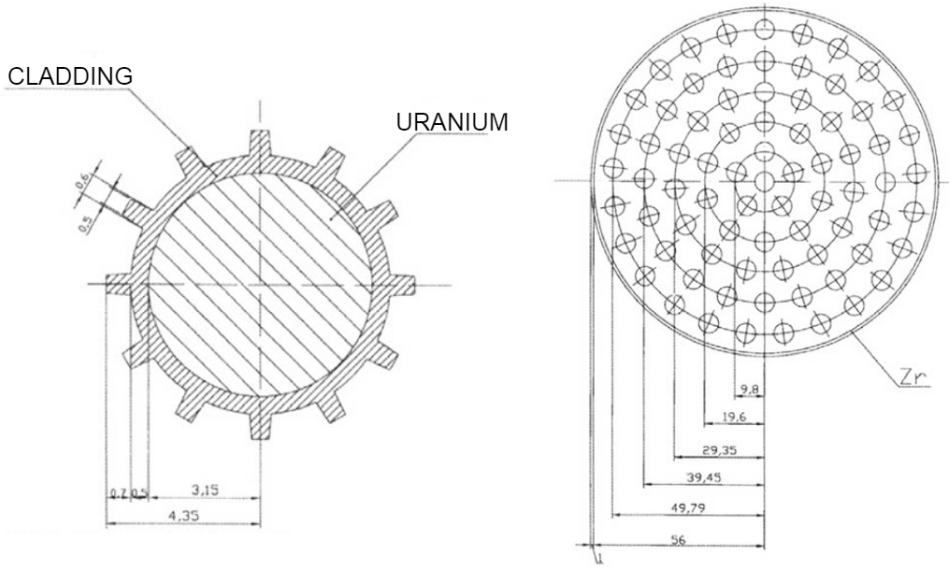

Figure 9: Schematic representation of fuel pin of KS-150 nuclear reactor [1] (modified)

2.1 First Accident

On 5.1.1976 while refueling, one FA sealing plug didn't plug properly. After disconnecting the loading machine the FA was shot up to the ceiling and CO_2 started to leak out.

Figure 10: Crushed fuel assembly, after being shot up the reactor [5]

Detailed description

One day before the accident reactor was shut down by CR insertion. Burned fuel assembly was moved to cooling core and it was replaced by a fresh FA. The reactor power is being increased, but the FA plug wasn't properly plugged due to an allen screw blocking the plug to close. The FA was shot up, hitting the loading machine and dropping to the ground (see Figure 10).

From the open slot, CO_2 is being released. Operators reacted by reducing the coolant flow by disconnecting 3 loops → pressure decreases and heat transfer is worsened.

After 55 minutes the hole, from which CO_2 was released is sealed. The reactor cooling was restored.

Consequences

No significant radioactivity was released, the FA was a fresh one. Two people were killed by inhaling CO_2.

By disconnecting 3 cooling loops the operators tried to reduce the CO_2 release, but this eventually lead to partial core melt. The cladding melting temperature was exceeded by 34 center-most FA and the cladding partly melted down.

The most significant error and learned lesson was incompetence of reactor operators. No defined plans were recognized → operators were forced to improvise.

INES 4

2.2 Second Accident

On 22.2. 1977 an inserted FA has a impurity inside which caused partial core melt. Primary circuit and part of secondary circuit were contaminated by fission products.

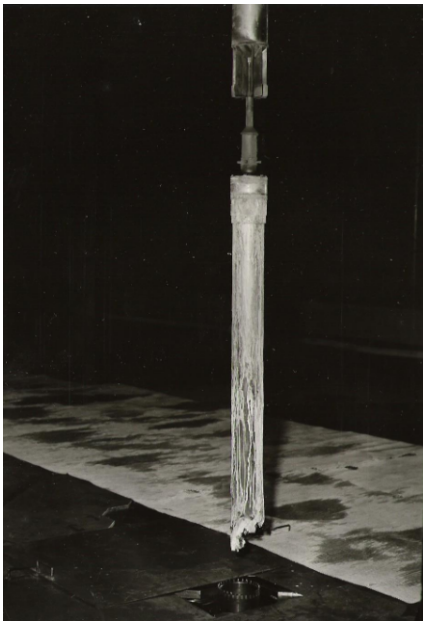

Figure 11: Melted FA after partial core meltdown [5]

Detailed description

This time reactor was at power level of 421 MWt and change of FA was planned.

A fresh FA was prepared to be inserted to the core (online fuel change). After 5 minutes operators recognized a higher temperature in the core → power was reduced to 213 MWt.

Then a technical worker reconnected sensor to standard at power measuring → operator increased power to avoid iodine pit. (The last measured temperature was 363 °C.) Sensors measured fission products in secondary circuit → reactor was shut down!

The whole accident duration was 10 minutes.

Consequences

Latter it was discovered, that the mentioned impurity was a sack of silica gel[3] (100 g). The worst thing is, that the workers noticed the sack when assembling the FA, tried to remove it, but didn't entirely succeed (didn't have a clue about the possible consequences)

The silica gel balls stick to spacers and block the coolant flow. After analysis showed the possible temperature exceeding 650 °C (melting temperature of cladding was 550 °C). The partially melted FA in presented in Figure 11

The total activity of released FP in primary circuit is 550 TBq. No significant activity was released to the atmosphere.

The accident was a certain human error and lack of information about the possible danger. No one died during this event!

INES 4

3 Conclusion

This section aims to discuss the lessons that can be learned from those two accidents in terms of nuclear safety, in light of the theory outlined above.

[3]Silica gel is for example used as humidity absorber in shoes

What these two accidents have in common is the importance of human errors. In a conservative safety analysis, it is never assumed that operators will take efficient actions in case of an accident, and that is why clear procedures are needed to indicate to operators how to react during every type of accident. This is one of the reasons why safety assessment is extremely important. Its main goal is to identify potential hazards to make sure that adequate measures are in place to prevent accidents, and this includes assessment of human factors. Operators, and more generally workers of the power plant should know and have available procedures to respond to different kinds of accidents. For instance, during the first accident, 2 workers died because there was no procedure urging them to leave the reactor because CO_2 is a toxic gas. Moreover, if safety procedures existed, if workers were more aware of the safety issue, they would have known that the silica gel couldn't be left in the core. Moreover, during the first accident, the incompetence of the operators was pointed out because they chose to disconnect cooling loops, which caused partial meltdown of the core, but the main problem is that no procedure existed to tell them how to react.

If no procedure existed for those accidents, it's because of the lack of a safety culture, which explains the quasi absence of safety assessment. Operators didn't react in the best manner during those accidents because they haven't been predicted while designing the nuclear power plant. Nowadays, in a nuclear power plant, every part of the design has to be conceived in a way that takes into account the accidents that could occur, and the safety assessment and safety analysis are performed to identify failures or weaknesses in safety functions that could lead to accidents so that these weaknesses can be mitigated. Here, it wasn't the case, the design of the plant was very complex, increasing the risk of failure, and as those failures and weaknesses weren't identified because no safety assessment was led, no safety system was preventing some accidents to happen.
The level of Defense In Depth was not sufficient in the plant, and the obstruction of one plug was enough to cause an accident. Some of the requirements of DID were not satisfied, such as the prevention of abnormal conditions: the design should be robust, which is not the case since a simple screw caused the first accident. Concerning fault detection, periodic control should be performed, and in this case the plugs should be checked when replacing a fuel rod. Also, the level of redundancy was too low since the failure of a single plug was enough to cause the accident.

Finally, it appears that this reactor was unsafe from its inauguration. The lack of a safety culture contributed to the accidents that occurred, with the absence of procedures and awareness about safety and how to react to the accidents that can occur, but the main cause of those accidents is the fact that no safety assessment was performed while conceiving the plant. The design of the plant was too complex and its weaknesses have not been studied.

References

[1] VUJE a.s. Významné havárie na jadrovo-energetických zariadeniach všeobecná priloha k učebným textom pre i. kategóriu zamestnancov jz v-2. 2018.

[2] Boros Aszódi. Elektrotechinka: A magyar elektrotechnikai egyesület hivatalos lapja. 2012. URL: `https://www.mee.hu/files/images/files2/u9/Elektrotechnika-2012-01.pdf`.

[3] Lenka Frýbortová. Analýza vybraných havárií: A-1 jaslovské bohunice. 2022.

[4] C.P. GILBERT. A review of the rasmussen report (wash-1400). 1979. URL: `https://inis.iaea.org/collection/NCLCollectionStore/_Public/10/482/10482214.pdf`.

[5] Hezučký, Jarmich, Grjbár, Kmošena, Penténvi, Rohár, and Hodul. Dve vážné havárie na jadrovej elektrárni a-1. 2008.

[6] IAEA. Probabilistic safety assessment. 1992. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub916e_web.pdf.

[7] IAEA. Licensing process for nuclear installations. 2010. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1468_web.pdf.

[8] IAEA. Safety assessment for facilities and activities. 2016. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1714web-7976998.pdf.

[9] IAEA. Deterministic safety analysis for nuclear power plants. 2019. URL: https://www-pub.iaea.org/MTCD/publications/PDF/PUB1851_web.pdf.

[10] IAEA. Deterministic safety analysis for nuclear power plants. 2019. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1851_web.pdf.

[11] Sean Roshan. Computer codes, validation and verification. 2023.

[12] Sean Roshan. Safety margin, single failure and acceptance criteria. 2023.

[13] Ian Savage. Comparing the fatality risks in united states transportation across modes and over time. 2013. URL: https://www.sciencedirect.com/science/inproceedings/pii/S0739885912002156, doi:https://doi.org/10.1016/j.retrec.2012.12.011.