Peer review of theoretical report by Group 1 on the concept of nuclear safety - Jaslovské Bohunice

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 8, 2023

Contents

1 Overview on safety theory of NPPs

In this section we found no unclear informations or statements. Nice introduction.

1.1 Safety objectives

In this section the example of problematic interpretation of risk in normal life is discussed. The risk definition is added. In the fourth block, it seems that ... (Quentin's comment)

1.2 Operational and accident conditions

In this section different operational and accident conditions are discussed. It is good to structuralize the theory to get better overview, als. There is an unclear statement or a bit strange formulation of words. In the normal operation condition block, you say "All those parameters are carefully monitored and in case of their deviation needed steps have to performed to keep the reactor safe." I do not know what is meant by steps, but maybe it would be better to mention also the word "design", because "steps" seems only like a action, that need to be performed. In this case, reactor design can also very often help to maintain the reactor parameters in the normal operation limits.

Overall this section is carried out quite well, it has correct structure and more or less right formulations.

1.3 Defense in depth

Prevention of abnormal conditions

In this block, ... (Quentin's comment)

Abnormal conditions control and fault detection

This text the authors describe ... (Quentin's comment)

DBA control

In this part of the work, ... (Quentin's comments)

Control of BDBA and SA

In this subsection, several unclear statements can be found.

The first two sentences, it is said that "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." The question might be, is it that they WERE NOT, but now they ARE taken into account? Or is that BDBA are not incorporated and taken into account when designing the reactor? If so, you say in the following block, that SA are cnsidered when designing a NPP. The design incorporates e.g. core catcher. So BDBA are not taken into account, but SA are?

The end of the sentence "so no system has been incorporated in the plant to deal with it" says that there are no systems that help to deal with BDBA, but what about the contaiment sprayers? Or the cooling of the condensation tank? For example when LOCA happens, these systems are activated during the process. This

In the second block of this subsection ... (Quentin's commentary)

1.4 Acceptance criteria

In this section the topic of acceptance criteria is discussed. The informations about different key players involvement in the NPP lifetime is realy interesting and gives the author nice overview. (Quentin's comment on figure)

In the last block on page 5, the single failure and acceptance criteria are mentioned, but they nowhere in the subsection about the topic of acceptance criteria are defined or explained. I twould be nice to actually see what the acceptance and single failure criteria are.

Quentins commentary.

1.5 Safety assesment

1.6 Safety analysis

Quentin's commentary

1.7 Deterministic safety analysis

1.7.1 Conservative analysis

In the second block, there is a bit strange formulation, it is said that SA includes evaluation of the plant response to hypothetical accidents, even ones that are extremely unlikely to happen. What does extremely unlikely means? In section 1.3 Defense in depth, it is postulated that BDBA and SA are not discussed when designing the NPP. But here, it says it involves "extremely unlikely, but still possible" accidents. This looks like BDBA and SA are not even possible. Or was it that in section 1.3 it was mentioned that they WERE not incorporated? If so, it should be said that they are discussed when designing the NPP, like was said before in this text.

1.7.2 Best estimate analysis

1.8 Probabilistic safety analysis

1.9 Computer codes

Maybe it would be worthy to mention a bit more about the system codes discussed during in the lectures. Overall, the general description of the computer codes is given.

1.10 Verification and validation

The block about verification has a false statement. A code can not be verified using benchmark task. It is validated using benchmark. This is clearly wrong. Also, verification is not only compared to other codes. What would one do, if the first on code for a specific application was created? It would not be validated? Validation also includes checking the usage of the right models, code structure, and right differential equations solvers, checking the robustness of the code etc.

2 NPP Jaslovské Bohunice A1

2.1 First accident

In the detailed description of the first accident, some comments might be made. The part from "The reactor power is being ..." to "..., CO_2 is being released." should be described as a failure of the safety assessment of the screw and filling procedure. Up to this point, it should not be addressed as a human error. For example, if the PSA recognized and pointed out the possible failure of the screw, consistent procedures could have avoided the accident.

Maybe it should be nice to also point out the lack of given procedures and emergency planning. This way the first accident looks like it was caused only by human errors, which is clearly not true. Still, significant human error and unpreparedness can be recognized and it is good it is adressed.

2.2 Second accident

The text about second accident describes the event generally, but here are few comments.

In the second block of the detailed description, it is said that a "technical worker reconnected the sensor to standard at power measuring". What does it mean, that he switched the sensor to standardd Why did he do that? Maybe something similar to recalibration? This could definitely be marked as a huge error from the operators. They probably should have SCRAMed the reactor, but they wanted to maintain the normal operation.

In the consequences part, there are two things worth discussion. The first sentence shows a typical single failure, right? The silica gel, which has no functional connection to the cooling ability of the flow channel has caused the blockage, increase in temperature, melting of the fuel and cladding, and moreover resulted in contamination. This should have been mentioned when speaking about the acceptance criteria and pointed out.

Another thing is the statement about the silica gel removal. Is there a detailed description of how did that happen? Why did they put the fuel assembly in the core even though they did not succeed in removing the sack?

Was it that they knew that the silica gel can't be put in the core, but had no clue that it still might be there? And why did they did not investigated it more, to see if there is still some gel left in the fuel assembly?

Or was it that they did not think the silica gel is an issue and they just put the FA in the core?

If it was the first case, it is definitely a breach of safety culture, when people just have low awareness of possible safety outcomes and did not care much.

If it was the second case, it is more likely to be a human error. Non-recognition of crucial errors like this definitely points out the incompetence of the operators.

Overall, this could have been discussed in more detail in the terms of nuclear safety.

3 Conclusion

Some comments should be made about certain parts of the text.

It is said, that "2 workers died because there was no procedure urging them to leave the reactor because CO2 is a toxic gas." According to literature (*Kuruc and Matel, Thirtieth anniversary of reactor accident in A-1 Nuclear Power Plant Jaslovske Bohunice*), carbon dioxide, which was used for cooling, spewed out of the twelve-meter long fuel assembly into the reactor hall. Nobody was irradiated or injured immediately. However, two men outside of the hall who **did not** respond to emergency signal were stifled by the carbon dioxide. This points out, that they ignored the signal warning.

If the second block, it is said that the lack of safety culture explained the quasi-absence of safety assessment. Is it true, that the lack of sufficient safety assessment was caused by the insufficient safety culture? Isn't safety culture related to the behavior, thinking and acting in the organization as NPP? Maybe it can be formulated, that in that time, nuclear safety was less emphasized, and therefore more vague assessment was performed.

4 Reviewer commetary

Overall we miss a bit of some discussion about the possible safety analysis that could have been performed (PSA and DSA) and how it could prevent/mitigate the accidents. Also, some further description on how the DiD breached, and what was the single failure that caused the accidents would be brilliant. It would be also interesting if some additional discussion about the assessment of the government was added because this accident was "hushed".

Overall we like the nice description of the concepts of nuclear safety. The concepts of safety objectives, DiD and reactor conditions were nicely described. Maybe we would add some references for further reading.

Appendix