FTA – Review of Approaches for Verification / Presentation of Failure Tolerance

Per Hellström[a*]
[a]Swedish Radiation Safety Authority, Solna, Sweden

Abstract: The functions of a nuclear reactor shall have a high dependability/availability, i.e.: if needed, the function shall perform as expected. A high dependability/availability is based on a high reliability, high maintainability and high maintenance support performance. Reliability is the mean most important for ensuring a high dependability/availability. Proven technology and simplicity of construction are two basic design principles to achieve a certain reliability (dependability). However, one of the most important design principles to achieve high safety function dependability is the use of redundancy to be single-fault tolerant. Redundancies may be vulnerable to dependencies and thus it becomes very important to be in control of dependencies and limit the negative impact by applying additional design principles such as physical and functional separation and diversity. License holders of nuclear power reactors must demonstrate that requirements are met, including the application of design principles to a sufficient extent (as far as is reasonably achievable in proportion to the function's importance) to meet the overall dependability requirements as reflected by acceptance criteria for deterministic as well as probabilistic safety analyses. Deterministic radiological acceptance criteria are mostly defined in terms of dose limits for event classes with defined frequency bands. Probabilistic criteria are expressed as maximum frequency for core melt, maximum frequency for large or large early release and in some cases maximum frequency to receive a certain dose or fatalities as a result of a radiological accident. It is an important task to show that a design is robust, and in particular that the use of redundant equipment is fault tolerant. The Finnish regulator STUK has implemented in its regulations, a specific requirement for fault tolerance analysis (FTA). A Swedish study performed for SSM in 2022-2023 investigated the STUK requirement in order to learn more and as a basis for potential introduction in Swedish legislation. The focus with FTA is to show the strength of individual defence-in-depth levels (physical, functional and diverse separation) as well as independence between DiD levels. This paper discusses the FTA concept, experiences on the use of FTA and a comparison with other countries approaches in justifying that their designs have the expected fault tolerance. The paper will also discuss dependability requirements, the relation to the defence-in-depth, event classes, quantitative goals, and how dependability requirements are verified/validated and documented.

Keywords: PRA, Defence-in-Depth, Dependability, Failure Tolerance Analysis.

1. INTRODUCTION

The functions of a nuclear reactor shall have a high dependability/availability, i.e.: if needed, the function shall perform as expected. A high dependability/availability is based on a high reliability, high maintainability and high maintenance support performance (see figure 1). Reliability is the mean most important for ensuring a high dependability/availability. However, to start with, the Structures, Systems and Components (SSCs) must have the needed performance in terms of pumping capacity, pressure relief capacity etc., and also be environmentally qualified for both normal operating conditions and for expected accident conditions when the SSCs are expected to do their job, i.e., the chance that this is not the case must be close to zero.

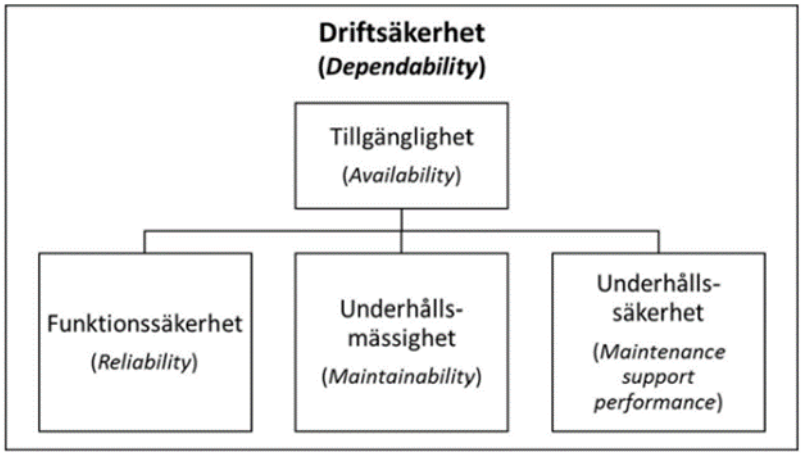

Figure 1. Relationship Between Dependability/Availability and Underlying Factors, from SSMFS 2021:4 [1]

Given that the needed performance and environmental qualification is in place (by design etc.), proven technology and simplicity of construction are two basic design principles to achieve a certain reliability (dependability). However, one of the most important design principles to achieve high safety function dependability is the use of redundancy to be single-fault tolerant. Redundancies may be vulnerable to dependencies and thus it becomes very important to be in control of dependencies and limit the negative dependence impacts by applying additional design principles such as physical and functional separation and diversity.

License holders of nuclear power reactors must demonstrate that requirements are met, including the application of design principles to a sufficient extent (as far as is reasonably achievable in proportion to the function's importance) to meet the overall dependability requirements as reflected by acceptance criteria for deterministic as well as probabilistic safety analyses. Deterministic radiological acceptance criteria are mostly defined in terms of dose limits for event classes with defined frequency bands. Probabilistic criteria are expressed as maximum frequency for core melt, maximum frequency for large or large early release and in some cases maximum frequency to receive a certain dose or fatalities as a result of a radiological accident.

It is an important task to show that a design is robust, and in particular that the use of redundant equipment is fault tolerant. The Finnish regulator STUK has implemented in its regulations, a specific requirement for fault tolerance analysis (FTA).

A Swedish study performed for SSM by AFRY in 2022-2023 investigated the STUK requirement. This paper is based on the report developed by AFRY. The report will eventually be published as an SSM research report.

The focus with FTA is to show the strength of individual Defence-in-Depth (DiD) levels (physical, functional and diverse separation) as well as independence between DiD levels. This paper discusses the FTA concept, experiences on the use of FTA and a comparison with other countries approaches in justifying that their designs have the expected fault tolerance.

2. DEPENDABILITY REQUIREMENTS

2.1 Design Requirements

The IEC definition IEC 60050-192:2015 [2] of fault tolerance is as follows:

"*ability to continue functioning with certain faults present*"

Swedish nuclear legislation and international legislation do not normally use the term "fault tolerance". Instead requirements are on dependability and provides the design criteria to be used to achieve the dependability needed (as far is reasonable and practicable). In terms of fault tolerance, this means that it is required that the fault tolerance is on the right level (as far as is reasonable and practicable). The Swedish design criteria for dependability are expresses as follows (according to chapter 4 12-13 §§ SSMFS2021:5 [3]):

12§ A nuclear reactor shall be constructed so that the functions specified in 2 – 4 §§ can be performed with as high dependability as is reasonably achievable under events and conditions within event classes H1 – H5, as well as under radiological emergency scenarios.

13§ Structures, systems and components that are depended on for safety must be designed in such way that their dependability is proportional to their importance to fulfill the functions specified in 2 – 4 §§ during events and conditions within event classes H1 – H5, as well as under radiological emergency scenarios.

Dependability, must be achieved by applying, to the extent necessary, the following design principles:

1. *proven technology,*
2. *simplicity of construction,*
3. *redundancy,*
4. *diversity,*
5. *physical separation, and*
6. *functional separation.*

When it is neither possible nor reasonable to apply proven technology (as per point 1), structures, systems, and components that are important for radiation safety must be systematically verified and validated according to chapter 3 § 4 in a way that demonstrates that they have the dependability proportional to their importance for the fulfillment of the functions specified in 2 – 4 §§.

In addition, Chapter 4 7 - 8§§ provide requirements on independence between functions in order to achieve a defense-in-depth:

7§ A nuclear power reactor shall, as far as reasonably achievable, be designed that failures in functions contributing to fundamental safety functions during events and conditions in:

1. *event classes H1–H2 do not prevent fundamental safety functions from being fulfilled during events and conditions in event classes H3–H5, and*
2. *event classes H3–H4B do not prevent fundamental safety functions to be fulfilled during events and conditions in event class H5.*

8§ A nuclear reactor shall be designed so that actions to fulfil functions according to 2–4 §§ during events and conditions in event classes H1-H5 and action during radiological emergency situations, interact in a balanced way.

The Swedish event classes are shown in Table 1.

Table 1. Swedish Event Classes

Event class	**Frequency of occurrence [year-1]**
Normal (H1)	1
Expected (H2)	10^{-2}<=H2
Not expected (H3)	10^{-4}<=H3<10^{-2}
Unlikely (H4A)	10^{-6}<=H4A<10^{-4}; External events: 10^{-5}<=H4A<10^{-4}
Special (H4B)	<10^{-4} + CCF; External events: 10^{-6}<=H4B<10^{-5}
Very unlikely (H5)	<10^{-6}
Extremely unlikely (H6)	-

Finnish and other countries requirements for dependability are quite similar.

2.2 Acceptance Criteria

The design of a nuclear power plant is developed so that the plant on high level meet deterministic radiological acceptance criteria and probabilistic acceptance criteria. The radiological acceptance criteria are many times expressed in terms of a maximum individual effective dose to a representative member of the public and different dose values are defined for different frequency bands (frequency of occurrence for events and conditions) where expected events and conditions are allowed to result in smaller dose levels and less frequent events and conditions are allowed to result in higher dose levels.

Technical criteria on performance and environmental qualification including dependability requirements need to be identified during the design process including the use of various design principles. Justification on how design principles are applied to meet requirements is needed and this is where Fault Tolerance Analysis (FTA) plays a role.

3 FAULT TOLERANCE ANALYSIS

3.1 Fault Tolerance Analysis in Finland

The concept of FTA was introduced by the Finnish Authorities in 2013. The FTA requirements in YVL B.1 [4] defines input data, scope and purpose of FTA. YVL B.1 351 and 352 describes that failure tolerance analysis shall be used:

> *351.The fulfilment of the failure criteria of systems implementing safety functions and their support systems as well as common cause failures shall be assessed by means of failure tolerance analysis when designing the systems or their modifications. If necessary, analyses shall be performed in more detail in different stages of design. [2019-06-15]*
>
> *352.A failure tolerance analysis shall assess one functional complex at a time, with due regard both to the system that performs a safety function and its auxiliary systems. The analysis shall address each component that, in the event of a failure, may affect the successful execution of the safety function performed by the system following a specific initiating event. The analysis shall address all modes of failure for all the components affecting the system performing the safety function. Depending on the applicable failure criterion, the analysis shall focus on one or multiple failures at a time and examine their impact in terms of the operation of the system. [2019-06-15]*

In modern safety assessments each safety function can be evaluated based on the three following aspects:

- Redundancy
  Does the safety function have redundant components, i.e., is the safety function resilient to a "single failure" – a postulated failure in the most critical component.
- Separation
  Are the redundant components functionally and physically separated, i.e., are there barriers that prevents redundant equipment from being exposed from the same hazard at the same time and that prevents failure in one component to spread to other components. The physical separation principle ensures that the safety function is resilient to spatial dependencies.
- Diversity
  Is the safety function diversified, i.e., can the safety function be performed in more than one manner? The diversity principle ensures that the safety function is resilient to "common cause failure" – a postulated failure in more than one component by the same cause.

A system is regarded as "single failure tolerant" if failure in any one component does not hinder the system function.

The methodology gives tools to check the correctness of NPP design regarding functional architecture. In particular, the following properties of NPP safety functions are analysed as part of FTA:

- Single failure (redundancy sufficiency) (YVL-B.1-4.3.1 432, 433, 435, YVL B.1-4.3.5-456, 456a, 456b, 456c, 456d, 456e, 457)
- Independence of Defence-in-Depth (DiD) levels (YVL-B.1-4.3.1 425, 426, 428, 429, 431),
- Functional analyses of each component or part that can affect the successful performance of a safety function or it´s support system (YVL-B.1-3.6-352), and
- Tolerance to common cause failures during Anticipated Operational Occurrences and postulated accidents (YVL-B.1-3.6-353).

Given the requirements above, failure tolerance analysis can be defined as a set of failure analyses to study the failure tolerance of an NPP, instead of treating the different systems and aspects of the plant as separate entities.

Failure tolerance is demonstrated through sufficient redundancy, diversity, and separation of safety functions. Various types of failure analyses are listed in Table 2, an extended table based on Benchmark Exercise on Safety Evaluation Practices (BESEP) [5].

The concept of FTA is thus to summarise results from the Deterministic Safety Analyses (DSA) for each safety function and each Initiating Event (IE) as well as for each Defence-in-Depth level (DiD). These verifications/demonstrations need to be performed by different types of failure analyses where the purpose is to identify causes of failure and their effects on structures, systems or components.

A plant level logical model can be used to analyse the defined initiating events and functions according to a defined safe shutdown strategy to verify the plant level architecture. Figure 2, an extended figure based on ref [6], illustrates the relation between failure analyses making up the FTA and deterministic analysis.

Table 2. Failure Analyses

Plant level	**Architecture level**	**System level**	**Example failure analyses**
Safe shutdown level	Strength of DiD levels	Redundancy	Failure mode and effect analysis. Spurious actions, N+1, N+2 failure criteria,
		Physical Separation	Physical separation of redundant components
		Functional Separation	Functional separation of redundant components
		Diversity	Common cause failure analysis, Diversity analysis (of systems, automation, measurement systems)
	Independence of DiD levels	Physical Separation	Physical separation of safety divisions, internal hazard analysis, external hazard analysis
		Functional Separation	Initiating event effect analysis, Common Cause Initiators (CCI), consequential failures, independency of electric systems, I&C separation
		Diversity	Common cause failure analysis, Diversity analysis (of systems, automation, measurement systems)

Note that complete independence of DiD levels is quite impossible and that the requirement is that independence shall be sufficient (as far as is reasonably achievable), and this is what the FTA shall show.

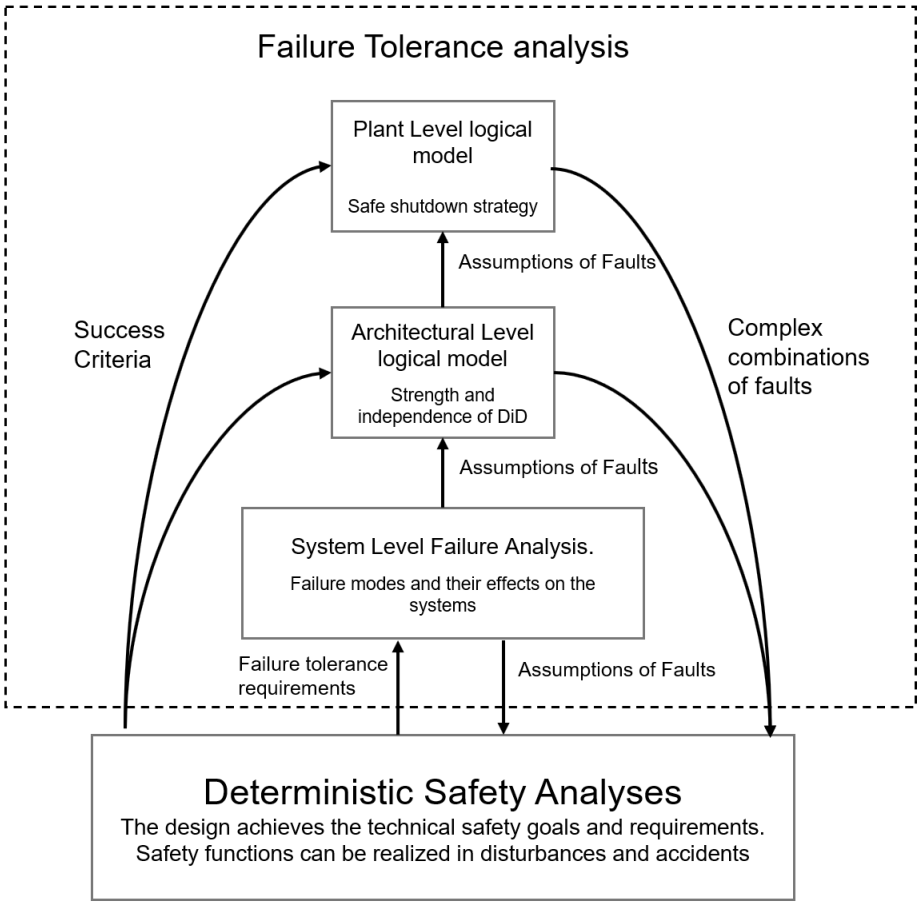

Figure 2. Relation Between Failure analysis and Deterministic Safety Analysis (Extended Figure Based on [6]).

3.2 FTA in Swedish Regulations

The Swedish regulations do not provide any specific requirements on how to show that the single failure and following design principles are implemented - presented and/or structured. While analyses shall be performed in such a way that the plant response can be evaluated and assessed for all relevant initiating events, criteria are evaluated individually. The presentation of analyses and results in the safety analysis reports of the current licensees are generally grouped on initiating events, and the fundamental safety requirements are considered in the separate analyses. There is no formal presentation of compliance with each separate fundamental safety requirement.

The licensee is not required to perform an overall assessment such as the FTA concept required in Finland. However, the licensee is required to perform all the analyses that make up the basis of an FTA.

The US and the UK have similar requirements or expectations that it is shown that the plants functions have the needed dependability / fault tolerance making the nuclear power plant being safe enough.

3.3 IAEA on FTA

The structure used by the IAEA for its safety standards is hierarchical starting with Safety Fundamentals (SF) which have been broken down to a collection of Requirements standards:

- Safety Requirements (NS-R)
- Specific Safety Requirements (SSR)
- General Safety Requirements (GSR)

Those requirements are directed to specific areas of the nuclear field, for which different types of safety guides are published to guide how to fulfil the requirements.

For NPPs, specific safety requirements related to failure tolerance can be traced into Specific Safety Requirements SSR-2/1(Rev.1) [7]. Requirements related to Single Failure (SF), Separation and Common Cause Failure (CCF) can be found as req. 25, 21 & 24, which are to be fulfilled from a design and construction perspective.

From a SAR perspective, Deterministic- and Probabilistic Safety Analysis (DSA and PSA, respectively), in chapter 15 [8], should confirm that the requirements for NPP design according to SSR2/1 [7] are met. Recommendations and guidance on DSA are provided in IAEA Safety Standards Series No. SSG-2 (Rev. 1) [9] and recommendations on PSA are provided in IAEA Safety Standards Series No. SSG-3 and No. SSG-4, [10], [11].

Those SARs are organised in a standard format based on SAR guides such as IAEA Specific Safety Guide No. SSG-61 [8]. Chapter 15 of SSG-61 covers the analyses that demonstrate that the safety of NPPs are covering the requirements addressed in "IAEA No. SSR-2/1 (Rev. 1) Safety of Nuclear Power Plants: Design, Specific Safety Requirements" [7]. In addition to elements relevant for SAR, IAEA No. SSR-2/1 (Rev. 1) covers other FTA elements (as defined by Finnish nuclear industry/STUK).

3.4 UK Regulations Related to FTA

In the UK, the regulation starts with the Nuclear Installations Act, 1965, which is guided by lower-level regulations. These start with the Office for Nuclear Regulation (ONR) publication: the License Condition Handbook [12], followed by Safety Assessment Principles (SAPs) [13] and on the next level there exists a collection of Technical Assessment Guides (TAGs) which provide guidance to ONR inspectors on the interpretation and application of the SAPs.

The UK regulation applies the Safety Standards from the IAEA and ensures that its own set of regulatory documents are consistent with IAEA guidelines. UK, as a member of Western European Nuclear Regulators' Association (WENRA), also supports the Reference Levels as relevant good practices and references them explicitly in the TAGs. Safety assessment principle-related fault analyses are outlined in items 605 to 694 [13].

Safety measures are defined in the TAG for Design Basis Accident (DBA) analysis [14]:

- EKP.4 and EKP.5 on safety function and safety measures
- EDR.1 to EDR.4 on design for reliability
- ERL.1 to ERL.4 on reliability claims
- EHA.1 to EHA.18 on external and internal hazards
- ESS.1 to ESS.27 on safety systems
- ERC.1 to ERC.4 on reactor core
- EHT.1 to EHT.5 on heat transport systems
- EHF.1 to EHF.12 on human factors
- ECR.1 and ECR.2 on criticality safety

The DBA TAG [14] is focused on the high-level principles and concepts of DBA and does not generally go into the detail associated with these engineering SAPs. However, most of these SAPs have their own TAGs:

- NS-TAST-GD-013: External Hazards
- NS-TAST-GD-014: Internal Hazards
- NS-TAST-GD-003: Safety Systems
- NS-TAST-GD-036: Redundancy, Diversity, Segregation and Layout of Mechanical Plant
- NS-TAST-GD-041: Criticality Safety
- NS-TAST-GD-060: Procedure Design and Administrative Controls
- NS-TAST-GD-075: Safety of Nuclear Fuel in Power Reactors.

How the nuclear industry in UK have handled the fault tolerance aspects can partly be reviewed in the public versions of safety analysis reports for Hinkley Point C nuclear power station [15], [16]. An example is that the

deterministic approach to diversity analyses has been completed by a probabilistic assessment of the design. Indeed, Common Cause Failures is being introduced in the PSA model, based on OPEX in order to evaluate the risk and confirm the adequacy of the design regarding diversity.

5. CONCLUSIONS

The IEC has a definition for fault tolerance:

"*ability to continue functioning with certain faults present*"

However, in international and national requirements regarding nuclear safety, the term FTA seem only to be used in the Finnish regulatory guides since 2013, when they first presented the concept of FTA, for which the approach is clarified in YVL B.1.

Other countries than Finland, such as Sweden, the UK and the US, and organisations such as IAEA do not use the terminology of FTA, but the analyses covered in the term FTA are made with some differences in how the summary of analyses are put together and presented. Nuclear Power Plant (NPP) owners use Safety Analysis Reports (SAR) or equivalent to demonstrate, by a set of failure analyses, that all requirements are met. In Sweden, the licensee is required to perform all the analyses that make up the basis of an FTA.

The concept of FTA, according to the Finnish approach, is to perform a set of failure analyses and summarize the analyses on redundancy, functional and physical separation and diversity for each safety function and each Initiating Event (IE) as well as for each Defence in Depth (DiD) level. These verifications/demonstrations must be performed by different types of failure analyses with the purpose to identify cause of failure and their effects on structures, systems or components. FTA is thus a set of failure analyses aimed at demonstrating that the NPP design fulfils failure tolerance requirements.

The Finnish FTA approach could in Sweden be used as a structure that demonstrate compliance with SSMFS 2021:4, Chapter 4 §13 that includes use of redundancy, separation and diversity as means to achieve the degree of dependability that meet the safety criteria and is practically achievable.

Examples from the UK show that PSA can be used to show compliance with single failure, separation and diversity requirements.

The study describes that actual failure tolerance analyses performed in Finland reveal a problem with the requirement of independence of all levels in defense in depths (DiD). It´s a safety concern that this requirement may result in the introduction of many more systems and components that the complexity and maintainability will be jeopardized.

Guides and methods for FTA are not currently described in literature and there is no international consensus of what FTA must contain. Possible benefits and drawbacks need to be studied further in order to avoid confusion regarding application of the analysis including consideration of duplication of requirements and existing SAR content. What are the lessons learned, what are the positive aspects? What are the challenges and how they have been tackled? Such information can be the basis for further development and introduction of this kind of analysis / documentation of how a plant meet the requirements on application of design principles to meet the overall goal of being safe as far as is reasonably achievable.

Acknowledgements

The author acknowledges the work by AFRY in developing the report on failure tolerance concept, requirements and how failure tolerance is proven.

References

[1] U. Yngvesson, The Swedish Radiation Safety Authority´s Regulations concerning Construction of Nuclear Power Reactors, SSMFS 2021:4, SSM, December 2021.
[2] IEC 60050-192:2015, International Electrotechnical Vocabulary (IEV) - Part 192: Dependability.

[3] U. Yngvesson, The Swedish Radiation Safety Authority's Regulations concerning Analysis of Radiation Safety for Nuclear Power Reactors, SSMFS 2021:5, SSM, December 2021.
[4] STUK, Safety Design of a Nuclear Power Plant, YVL B.1 15.6.2019, 2019.
[5] J. Linnosmaa, Deliverable 2.3: Specification on the key features of efficient and integrated safety engineering process, V:1.2, BESEP, August 2021.
[6] P. Humalajoki and I. Niemelä, NPP Failure Analyses in Finland, Los Angeles: Probabilistic Safety Assessment and Management PSAM 14, 2018. Ref 3
[7] IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements SSR-2/1(Rev.1), Vienna, 2016.
[8] IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, SSG-61, Vienna, 2021.
[9] IAEA, Safety of Nuclear Power Plants: Design, Vienna: International Atomic Energy Agency, 2016.
[9] IAEA, Deterministic Safety Analysis for Nuclear Power Plants, No. SSG-2 (Rev. 1), Vienna, 2019.
[10] IAEA, Development and Application of Probabilistic Safety Assessment for Nuclear Power Plants, No. SSG-3, Vienna, 2010.
[11] IAEA, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, No. SSG-4, Vienna, 2010.
[12] Office for Nuclear Regulation (ONR), Licence condition handbook, February 2017.
[13] Office for Nuclear Regulation (ONR), Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Rev.1, January 2020.
[14] Office for Nuclear Regulation (ONR), Design Basis Analysis, NS-TAST-GD-006 Revision 5, 2020.
[15] NBB Generation Company (HPC) Ltd, Sub-chapter 3.7 – Diversity Design Principles, HPC PCSR3.
[16] NNB Generation Company (HPC) Ltd, Sub-chapter 15.3 – Supporting Analysis for the HPC Design, HPC PCSR3.