Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Research

Safety Concept Evaluation with Failure Tolerance Analysis

2025:01

Author: Gunnar Johanson, Stefan Hjelm,
Bengt Lidh, Tommy Lindholm, Olivia Winestedt, alla AFRY
Date: Febrary 2025
Report number: 2025:01
ISSN: 2000-0456
Available at www.ssm.se

Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Author: Gunnar Johanson, Stefan Hjelm, Bengt Lidh,
Tommy Lindholm, Olivia Winestedt, alla AFRY

2025:01

Safety Concept Evaluation with Failure Tolerance Analysis

Date: February 2025
Report number: 2025:01
ISSN: 2000-0456
Available at www.stralsakerhetsmyndigheten.se

This report was commissioned by the Swedish Radiation Safety Authority (SSM). The conclusions and viewpoints presented in the report are those of the author(s) and do not necessarily coincide with those of SSM.

SSM perspektiv

Bakgrund
Hög funktionssäkerhet uppnås genom att använda redundans. Redundanser (enkelfelstålighet) blir i sin tur effektiva genom att tillämpa ytterligare konstruktionsprinciper såsom fysisk och funktionell separation och diversifiering.

Tillståndshavare av kärnkraftsreaktorer måste visa att krav uppfylls, inklusive kraven på enkelfelstålighet och att konstruktionsprinciper som separation och diversifiering tillämpas i tillräcklig utsträckning.

Sedan 2013 har den finska myndigheten STUK ställt specifika krav på så kallade feltoleransanalyser (FTA). I Sverige finns för närvarande inga sådana uttryckliga krav. FTA skulle dock kunna vara av värde i SSM:s arbete med reaktorsäkerhet. Det är därför av intresse för SSM att studera hur den nuvarande situationen ser ut i Finland samt tillämpning av FTA eller liknande i andra länder och organisationer. En del av studien är också att titta på nuvarande tillvägagångssätt som används av svenska tillståndshavare för att påvisa att säkerhetsfunktionernas funktionssäkerhet uppfyller kraven, inklusive hur det dokumenteras. En specifik fråga är att undersöka potentiell användning av PSA-modeller inom FTA.

Resultat
Studien har granskat de finska FTA-kraven (redundans, funktionell och rumslig separation, diversifiering och oberoende mellan djupförsvarsnivåer) och jämfört med amerikanska, brittiska och svenska krav. Det är bara Finland som har uttryckliga krav, men tolkningen är att de andra länderna har underförstått samma krav, det vill säga det måste visas att funktionssäkerheten och djupförsvarsoberoende så långt det rimligen är möjligt uppfyller kraven. Även svenska tillståndshavare har dokumentation om hur kraven uppfylls. Det är dock inte nödvändigtvis lätt att hitta information om hur krav på funktionssäkerhet och oberoende uppfylls.

En disposition för ett FTA-upplägg har tagits fram och en SWOT-analys avseende FTA är genomförd.

En slutsats från detta arbete är att FTA kan användas för att påvisa efterlevnad av SSMFS 2021:4, 4 kap. 13 § som inkluderar användning av redundans, separation och diversifiering som medel för att uppnå den grad av funktionssäkerhet som uppfyller säkerhetskriterierna så långt det är möjligt och rimligt. Guider och metoder för FTA beskrivs för närvarande inte i litteraturen och det finns ingen internationell konsensus om vad FTA måste innehålla.

Relevans
Denna studie är relevant för eventuell vidareutveckling av SSM krav avseende att påvisa kravuppfyllnad på funktionssäkerhet, inklusive krav på dokumentation av sådan kravuppfyllnad.

Behov av ytterligare forskning
Eventuellt införande av svenska myndighetskrav liknande de finska kraven kommer sannolikt att gynnas av utvecklingen av ett gemensamt angreppssätt avseende FTA.

Projektinformation
Kontaktperson SSM: **Per Hellström**
Referens: SSM2022-5748 / 4530532

SSM perspective

Background
One of the most important design principles to achieve high safety function dependability is the use of redundancy to be single-fault tolerant. In turn, redundancies become effective 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 requirements for single-fault tolerance and that design principles such as separation and diversity are applied to a sufficient extent to meet the overall dependability requirements as reflected by acceptance criteria for deterministic as well as probabilistic safety analyses.

Since 2013, the Finnish authority STUK has set specific requirements on so called failure tolerance analyses (FTA). Sweden currently has no such explicit requirements. However, FTA could be of value in SSM's work with reactor safety. It is therefore of interest to SSM to study what the current situation looks like in Finland as well as current application of FTA or similar in other countries and organizations. Part of the study is also to look at cur-rent approaches, used by Swedish utilities, to show that safety function dependability com-ply with requirements, including how they are documented, One specific issue is to investigate potential use of PSA models in the FTA process.

Results
The study has reviewed the Finnish FTA requirements (redundancy, functional and spatial separation, diversity and independence between Defence-in-Depth (DiD) levels and com-pared with US, British and Swedish requirements. It is only Finland that have explicit requirements but the interpretation is that the other countries have implicit the same requirements, i.e. it has to be shown that safety function dependability and defence-in-depth independence as far as is reasonably achievable meet the requirements. Also Swedish utilities have documentation on how the requirements are met. However, it is not necessarily easy to find information on how dependability and independence requirements are met.

An outline for an FTA approach is developed and a SWOT analysis regarding FTA is performed.

One conclusion from this work is that FTA can be used to 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 as far as is practically achievable. Guides and methods for FTA are not currently described in literature and there is no international consensus of what FTA must contain.

This study is relevant for potential further development of SSM requirements on how dependability requirements are met, including requirements on documentation of such assessments.

Need for further research
The potential introduction of Swedish regulatory requirements similar to the Finnish requirements is likely to benefit from development of a common FTA approach within the industry.

Project information
Contact person SSM: **Per Hellström**
Reference: SSM2022-5748 / 4530532

Safety Concept Evaluation by Failure Tolerance Analysis

Summary

A safety assessment methodology based on the failure tolerance analysis described by the Radiation and Nuclear Safety Authority in Finland (STUK YVL B.1) has been studied.

Since 2013, the Finnish regulatory guides have required failure tolerance analyses (FTA) of safety functions and systems of nuclear power plants. The FTA covers plant level functions instead of individual systems.

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 causes of failures and their effects on structures, systems and components. FTA is thus a set of failure analyses aimed at demonstrating that the NPP design meet failure tolerance requirements - demonstrate sufficient redundancy, separation and diversity - (in Swedish regulations requirements on dependability and application of design principles to reach a dependability as far as is reasonably achievable).

Other countries, 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. In Sweden, the licensees are required to perform all the analyses that make up the basis of an FTA. 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. However, guides and methods for FTA are not currently described in literature and there is no international consensus of what FTA must contain.

A SWOT (Strengths – Weaknesses – Opportunities – Threats) analysis for Failure Tolerance Analysis has been performed. One conclusion is that FTA could be used to demonstrate compliance with Chapter 4 §13 SSMFS 2021:4, 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 (*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)*.

However, possible benefits and drawbacks need to be studied further in order to avoid confusion regarding application of the analysis including potential duplication of requirements and existing SAR content and potential increased burden on resources compared to benefits. The role of quality/qualification requirements needs to be clarified in the light of an FTA.

One interesting observation is that the analyses performed reveal a problem with the requirement of independence of all levels in defense in depths (DiD). It´s a potential safety concern that the solution to this requirement is introduction of more and diverse systems and components making the plant more complex and thus challenging for maintenance, which in turn may become a safety concern. This issue needs further attention.

A potential path forward is to learn more from Finnish experience, promote international consensus regarding the methodology and applicability of FTA and development of guidance before potential introduction of Swedish requirements. One step can be to request an FTA summary in future Periodic Safety Reviews.

Sammanfattning

En analysmetod som baseras på den feltoleransanalys som beskrivs av Strålsäkerhetscentralen i Finland (STUK YVL B.1) har studerats.

Sedan 2013 har de finska regleringsguiderna krävt feltoleransanalyser (FTA) av kärnkraftverkens säkerhetsfunktioner och system. FTA omfattar funktioner på anläggningsnivå istället för enskilda system.

FTA-konceptet, enligt den finska metoden, är att utföra en uppsättning felanalyser och sammanfatta analyserna av redundans, funktionell och fysisk separation och diversifiering för varje säkerhetsfunktion och varje initierande händelse (IE) samt för varje djupförsvarsnivå (DiD). Dessa verifikationer/demonstrationer ska utföras med olika typer av felanalyser i syfte att identifiera orsaker till fel och deras effekter på strukturer, system och komponenter. FTA är alltså en uppsättning felanalyser som syftar till att visa att kärnkraftverkets konstruktion uppfyller feltoleranskraven - uppvisar tillräcklig redundans, separation och diversifiering - (i svenska regelverk finns det krav på tillförlitlighet och tillämpning av konstruktionsprinciper för att nå en tillförlitlighet så långt det är rimligt möjligt att uppnå).

Andra länder, som Sverige, Storbritannien och USA, och organisationer som IAEA använder inte begreppet FTA, men de analyser som omfattas av begreppet FTA är genomförda med vissa skillnader i hur analyssammanfattningen sätts ihop och presenteras. I Sverige är tillståndshavarna skyldiga att utföra alla de analyser som utgör grunden för FTA. Ägare av kärnkraftverk (NPP) använder säkerhetsanalysrapporter (SAR) eller motsvarande för att visa, genom en uppsättning felanalyser, att alla krav är uppfyllda. Guider och metoder för FTA finns dock för närvarande inte beskrivna i litteraturen och det finns ingen internationell konsensus om vad FTA måste innehålla.

En SWOT-analys (Strengths – Weaknesses – Opportunities – Threats) avseende FTA har utförts. En slutsats är att FTA skulle kunna användas för att visa efterlevnad av kap 4 §13 SSMFS 2021:4, som inkluderar användning av redundans, separation och diversifiering som medel för att uppnå den grad av tillförlitlighet som är tillräcklig (*i proportion till deras betydelse för att fullgöra de funktioner som anges i 2–4 §§ vid händelser och förhållanden i händelseklass H1–H5 samt vid scenarier för radiologiska nödsituationer*).

Emellertid måste möjliga fördelar och nackdelar studeras ytterligare för att undvika förvirring när det gäller tillämpningen av analysen, inklusive potentiell dubblering av krav och befintligt SAR-innehåll och potentiell ökad börda på resurser jämfört med fördelar. Kvalitets-/kvalifikationskravens roll behöver förtydligas i ljuset av FTA.

En intressant iakttagelse är att genomförda analyser visar på ett problem med kravet på oberoende för alla nivåer i djupförsvaret (DiD). Det är ett potentiellt säkerhetsproblem att lösningen på detta krav är införandet av fler och olika system och komponenter som gör anläggningen mer komplex och därmed utmanande för underhåll, vilket i sin tur kan bli ett säkerhetsproblem. Denna fråga behöver ytterligare uppmärksamhet.

En möjlig väg framåt är att lära sig mer av finska erfarenheter, främja internationell konsensus om metodiken och tillämpligheten av FTA och utveckling av vägledning inför eventuellt införande av svenska krav. Ett steg kan vara att begära en sammanfattning av FTA i framtida periodiska säkerhetsgranskningar.

Abbreviations and concepts

Acronyms and abbreviations

BDBA – Beyond Design Basis Accident
BESEP – Benchmark Exercise on Safety Evaluation Practices
CCCG – Common Cause Component Groups
CCF – Common Cause Failures
CCI – Common Cause Initiator
DBA – Design Basis Accident
DBC – Design Basis Condition
DEC – Design extension condition
DiD – Defence in Depth
DSA – Deterministic Safety Analysis
FMEA – Failure Mode and Effect Analysis
FT – Fault trees
FTA – Failure Tolerance Analysis
GSR – General Safety Requirements
I&C – Instrumentation and Control
IAEA – International Atomic Energy Agency
IE – Initiating Event
IEC – International Electrotechnical Commission
LCO – Limiting Conditions for Operation
LOCA – Loss of Coolant Accident
MCS – Minimal Cut Sets
NPP – Nuclear Power Plant
NRC – Nuclear Regulatory Commission
ONR – Office for Nuclear Regulation (UK)
PRA – Probabilistic Risk Assessment
PSA – Probabilistic Safety Analysis
RICT – Risk Informed Completion Time
RMTS – Risk-Managed Technical Specifications
R&D – Research and Development
RPS – Reactor Protection System
SA – Severe Accident
SAPs – Safety Assessment Principles
SAR – Safety Analysis Report
SF – Safety Fundamentals
SFC – Single Failure Criteria
SFDP – Safety Function Determination Program
SSC – Structures Systems and Components
SSM – Swedish Radiation Safety Authority (Strålsäkerhetsmyndigheten)
SSR – Specific Safety Requirements
STF – Säkerhetstekniska föreskrifter (Technical Specifications)
STUK – the Finnish Radiation and Nuclear Safety Authority
TAGs – Technical Assessment Guides
TC – Technical Committee
V&V – Verification and Validation
WENRA – Western European Nuclear Regulators Association
WNA – World Nuclear Association
YVL – Finnish Regulatory Guides

Contents

List of Figures

List of Tables

1. Introduction

1.1. Background

Safety analyses are essential for nuclear safety. Safety analyses are performed to confirm that safety functions can be fulfilled, and thus that Structures, Systems, and Components (SSC) and operating actions meet acceptance criteria.

Regulatory requirements and regulatory guidance are developed and published by international nuclear organisations as well as national authorities. It is mandatory for licensees to demonstrate compliance with national regulations. The national authorities can also demand that other analyses need to be performed in order to prove that safety criteria are met.

One fairly new assessment, so called Failure Tolerance Analysis (FTA), was developed in Finland and implemented in the Finnish regulations in 2013. The Finnish nuclear industry together with the regulator STUK has developed the term FTA in different papers and presentations [1], [2], [3]. The Swedish knowledge regarding the concept of FTA is lacking, and therefore this study aims to increase knowledge in the subject.

1.2. Scope and purpose

The scope includes gathering information and defining what Failure Tolerance Analysis is, investigating the international usage of the analysis and other nations and organisations requirements and regulations regarding FTA, with the purpose of broadening the knowledge of FTA and its applicability regarding methods and requirements and providing advice on its use in Sweden including potential requirements on FTA.

1.3. Method

The present report combines a literature study with previous direct experiences of the authors and other experts in Sweden and Finland.

The following references provided with the assignment were:

- Guide YVL B.1 Safety Design of a Nuclear Power Plant, [4]
- NPP Failure Analyses in Finland [3]
- Reliability analysis of safety-related digital instrumentation and control in a nuclear power plant [5]
- Design Basis Analysis [6]

The additional literature investigated in this study is mainly regulations for NPPs obtained from the International Atomic Energy Agency (IAEA), the US Nuclear Regulatory Commission (NRC), the Swedish Regulatory Safety Authority (SSM) and the UK Office for Nuclear Regulation (ONR). A summary overview of the references was gathered before being divided between the participant members to focus a search on different aspects of information needed; delegation to individuals was based on their previous knowledge and experience.

The proposed methodology and the main topics of FTA in chapter 4 is based on general experience of the authors and discussions with relevant experts on failure analysis applications in Sweden and Finland.

In addition, an earlier Finnish survey studied the use of Probabilistic Risk Assessment (PRA[1]) to support failure tolerance analyses [2]. This Finnish survey provides a valuable overview of the applications by the licensees in Finland with respect to YVL B.1 paragraph 351.

[1] The terms PRA and PSA are used interchangeably.

2. Safety assessment with FTA

2.1. Fundamental safety requirements

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.

Credit for a function to be successful in the short-term, requires that enough time is available to the operators to take action. This is often called grace time. For a function to be considered successful in the long-term, the nuclear power reactor needs to reach a steady state that can be maintained for months or years. The division between short- and long-term is a qualitative assessment that may vary from function to function.

2.2. FTA requirement in the Finnish YVL B1

The concept of FTA was introduced by the Finnish Authorities in 2013, and Finland is still the only nation which has developed detailed requirements for FTA. 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]

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).

The YVL B.1 Guide published in 2013 stated in paragraph 354 that Failure Tolerance Analyses should consider human errors and demonstrate that single human errors would not prevent the performance of the safety function concerned. However, in the YVL B.1 Guide published in 2019, requirement 354 regarding human errors were removed. One reason seems to be that human errors are included in failure analyses and other demonstrations.

2.3. FTA definition

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 1, an extended table based on Benchmark Exercise on Safety Evaluation Practices (BESEP) 2.3 [7].

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 1, an extended figure based on ref [3], illustrates the relation between failure analyses making up the FTA and deterministic analysis.

Table 1: Failure analyses.

Topic of plant-level design:	Topics of architecture-level design:	Topics of system-level design:	Examples of failure analyses (some analyses can be classified under several topics)
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)

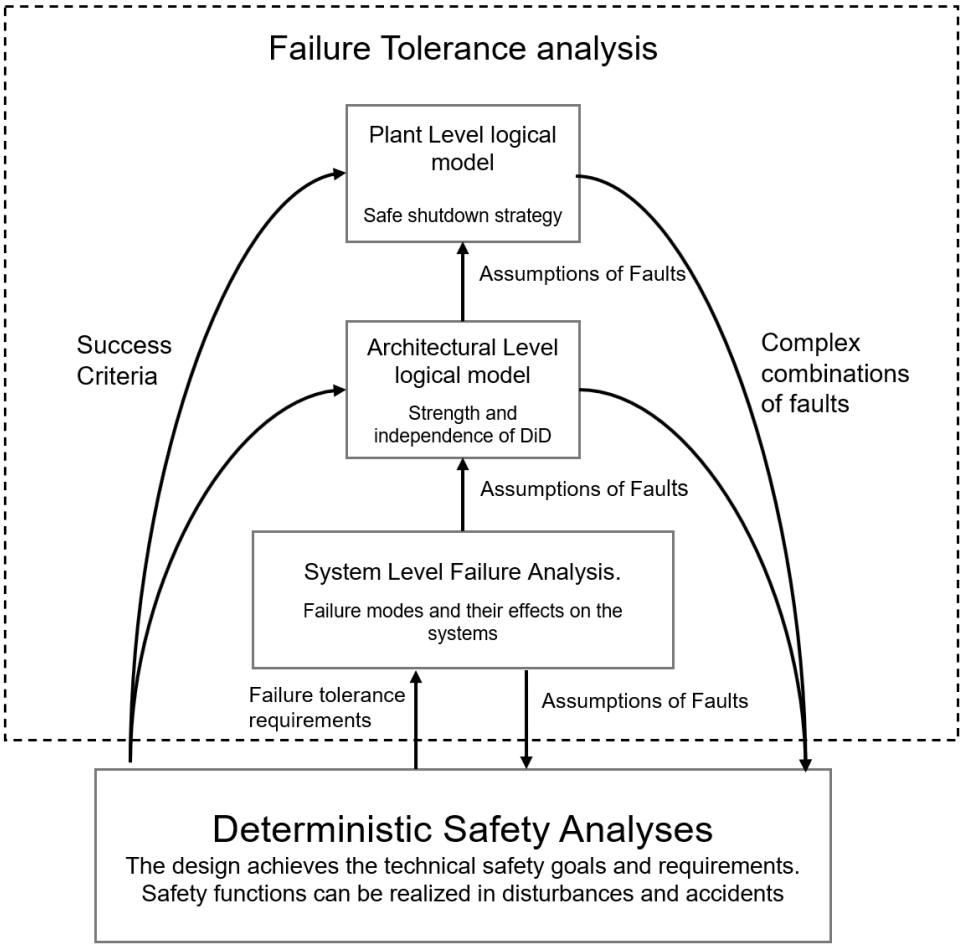

Figure 1: Relation between Failure analysis and Deterministic Safety Analysis (extended figure based on ref [3]).

3. FTA regulatory outlook

This chapter presents a summary of the current requirements, relating to safety functions, in the US, Sweden, the IAEA and the UK. None of the requirements for these nations and organisation include an FTA as defined in YVL B.1.

3.1. The US and NRC's verification of safety functions operability

The Finnish FTA relates to the design of the NPP for verifying the safety functions. The US design requirements are found in GDC 10CFR50 appendix A, GDC criterion 21 Single failures, criterion 22 Diversity and criterion 24 Separation. The Nuclear Regulatory Commission (NRC) have in their regulation NUREG-1431 for Westinghouse reactors [8], defined requirements for different programs related to operation, to verify that the safety functions are operable according to the requirements. In the following sections, the requirements for different programs as defined by NRC are presented, which are the:

- Safety Function Determination Program (SFDP),
- Setpoint Control Program,
- Surveillance Frequency Control Program,
- Risk Informed Completion Time Program.

3.1.1. Safety Function Determination Program (SFDP)

The Safety Function Determination Program (SFDP) ensures that the loss of a safety function is detected and that appropriate actions are taken. Upon the loss of a support system, an evaluation shall be made to determine if a loss of safety function occurred. Additionally, other appropriate limitations and remedial or compensatory actions may be identified to be taken as a result of inoperability of the support system. This includes corresponding exceptions in the Condition and Required Actions for the supported system. The SFDP shall contain the following:

1. Provisions for cross-train checks to ensure that a loss of the capability to perform the safety function assumed in the accident analysis does not go undetected[2],
2. Provisions for ensuring the plant is maintained in a safe condition if a loss-of-function condition exists,
3. Provisions to ensure that an inoperable supported system's completion time is not inappropriately extended as a result of multiple support system inoperability's, and
4. Other appropriate limitations and remedial or compensatory action.

A loss of safety function exists when a safety function assumed in the accident analysis cannot be performed, assuming no concurrent (N+1): single failure, loss of offsite power, or loss of onsite diesel generator(s). For the purpose of the SFDP, a loss of safety function may exist when a support system is inoperable, and:

a. A required system redundant to the system(s) supported by the inoperable support system is also inoperable, or
b. A required system redundant to the system(s) in turn supported by the inoperable supported system is also inoperable, or

[2] E.g. insufficient separation due to an open fire door or inadvertent flooding path

c. A required system redundant to the support system(s) for the supported systems (a) and (b) above is also inoperable.

The SFDP identifies where a loss of safety function exists. If such a loss is determined to exist, the appropriate conditions and required actions of the Limiting Conditions for Operation (LCO) in which the loss of safety function exists must be put in place. When a loss of safety function is caused by the inoperability of a single Technical Specification support system, the appropriate conditions and required actions to put in place are those of the support system.

3.1.2. Setpoint Control Program

The Setpoint Control Program shall establish the requirements for ensuring that setpoints for automatic protective devices are initially within and remain within the assumptions of the applicable safety analyses, provides means for processing changes to instrumentation setpoints, and identify setpoint methodologies to ensure instrumentation will function as required. The program shall ensure that the testing of automatic protective devices related to variables that have significant safety functions verifies that instrumentation will function as required.

3.1.3. Surveillance Frequency Control Program

The Surveillance Frequency Control Program provides controls for surveillance frequencies. The program shall ensure that surveillance requirements specified in the technical specifications are performed at intervals sufficient to assure the associated LCO are met.

1. The Surveillance Frequency Control Program shall contain a list of frequencies of those surveillance requirements.
2. Changes to the frequencies listed in the Surveillance Frequency Control Program shall be made in accordance with NEI 04-10, "Risk-Informed Method for Control of Surveillance Frequencies", Revision 1. [9]
3. The provisions of surveillance requirements are applicable to the frequencies established in the Surveillance Frequency Control Program.

3.1.4. Risk Informed Completion Time Program

The Risk Informed Completion Time Program provides controls to calculate a Risk Informed Completion Time (RICT) and must be implemented in accordance with NEI 06-09-A, Revision 0, "Risk-Managed Technical Specifications (RMTS) Guidelines [10]".

3.2. Swedish regulations

The regulations issued by the Swedish Radiation Safety Authority (SSM) require the licensee to show compliance with (amongst many others) the use of the three main principles redundancy, separation and diversity in achieving a dependability as far as is reasonably achievable. A new set of regulations were published by SSM in 2021 and in effect from 1st March 2022 with some of the requirements having a transition period before they are fully in effect (in January 2027). This means that all Swedish licensees are undergoing a period of sequential implementation of requirements.

Until 2022, the main framework regarding safety in nuclear facilities consisted of two regulations:

- SSMFS 2008:1 “The Swedish Radiation Safety Authority’s Regulations concerning Safety in Nuclear Facilities”, and
- SSMFS 2008:17 “The Swedish Radiation Safety Authority’s Regulations concerning the Design and Construction of Nuclear Power Reactors”.

Upon implementation of SSMFS 2008:17, licensees had to perform several new analyses to show compliance. The requirements that make up the basis of the FTA-concept, §§9-11, were subject to major evaluations.

Following the implementation of new regulations in 2022, the framework is now shared between three regulations:

- SSMFS 2021:4 “The Swedish Radiation Safety Authority’s Regulations concerning Construction of Nuclear Power Reactors” [11]
- SSMFS 2021:5 “The Swedish Radiation Safety Authority’s Regulations concerning Analysis of Radiation Safety for Nuclear Power Reactors” [12]
- SSMFS 2021:6 “The Swedish Radiation Safety Authority’s Regulations concerning Operation of Nuclear Power Reactors”. [13]

The requirements in the newer (SSMFS 2021:4-6) regulations describe three fundamental safety functions; reactivity control, heat removal and activity confinement. Swedish licensees perform their safety analyses based on “basic safety functions”, (Reactivity control, Protection of the primary system integrity, Emergency core cooling, Residual heat removal and the Containment function) that were described in the older (SSMFS 2008:1 and 2008:17) regulations. For the purpose of this report, the structure of safety functions can be considered equal.

The design and analysis requirements in the old (primarily SSMFS 2008:1 and SSMFS 2008:17) and new (SSMFS 2021:4, SSMFS 2021:5 and SSMFS 2021:6) regulations are in most aspects similar – the main differences lie in how requirements are structured. Requirements regarding the operation of nuclear power reactors, such as measures to mitigate human errors, are mainly described in SSMFS 2021:6.

The requirements that make up the Failure Tolerance Analysis as described in Section 2 (redundancy, separation, and diversity) were previously described in SSMFS 2008:17 §§9-11, but are now divided between Ch.4 §§12-13 SSMFS 2021:4 (design) and Ch.3 §14 SSMFS 2021:5 (analysis).

3.2.1. Requirements regarding design

An extract of chapter 4 12-13 §§ SSMFS 2021:4 are presented below (non-official translation from Swedish to English).

> *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§§ SSMFS 2021:4 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.

Briefly, the purpose of Ch. 4 §12 SSMFS 2021:4 [11], is that 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 2.

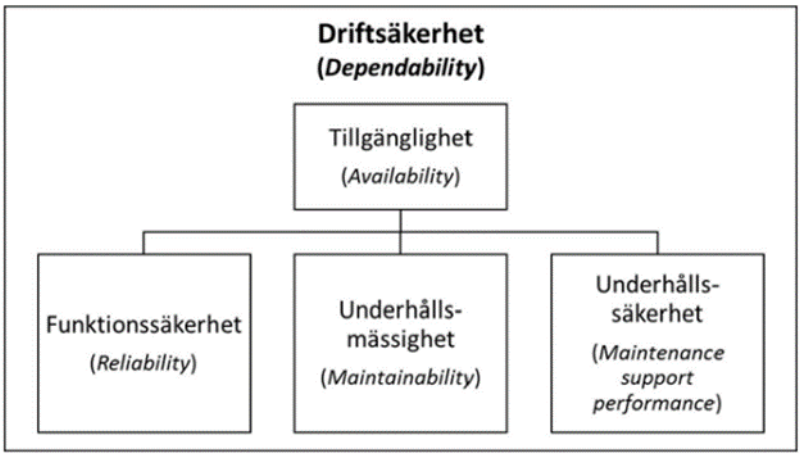

Figure 2: Relationship between Dependability/Availability and underlying factors, from SSMFS 2021:4 [11].

The purpose of Chapter 4 §13 SSMFS 2021:4 is to describe the means which are important for ensuring a high dependability/availability mainly through ensuring a high reliability. The paragraph also clearly states that the means taken to ensure high reliability shall stand in proportion to the function's importance.

When assessing which measures need to be included in the construction, requirements on redundancy, diversity and separation can in some cases be exempt or partially applied, as long as the overall goal to ensure a high dependability is sufficiently met.

Redundancy
In some cases, redundancy requirements may be excluded. For example, in some cases adding redundant components in a robust system can introduce new failure modes and/or dependencies, which in turn can reduce the overall reliability. Other cases can be when components have such proven and simple design that added redundancy does not add to the overall safety.

Physical and Functional Separation
Physical separation can be achieved by distance, shielding or combinations of both. Functional separation can be achieved by, for example, use of isolating devices and through diversity. It is important to note that requirements on separation are not only for protection from internal events (room events, such as fire and flooding), but also external events (such as weather events and antagonists).

Diversity
The fulfilment of diversity requirements on construction shall be in proportion to the function's importance. Diversity can also be applied on maintenance and testing to further decrease the risk of introducing common cause failures, however this is currently not required in Chapter 4 §1 SSMFS 2021:4.

3.2.2. Requirements regarding analysis

The purpose of Chapter 3 §14 SSMFS 2021:5 [12] is to set a basis/framework for analysis of the nuclear reactor's ability to reach a safe state following an initiating event. The paragraph adds background to how deterministic analyses shall be performed and thus completes the requirements on redundancy and diversity in Chapter 4 §13 SSMFS 2021:4. Besides setting a basis/framework for analyses, the regulation also states what results shall be justified. For example, the single failure used in an analysis shall be demonstrated to be the most challenging. Important to note is that the paragraph states that requirements shall be interpreted "as far as reasonably achievable", which means, for example, that single failures can be exempt for functions with very high dependability. However, such cases must be justified through specific evaluations.

3.2.3. Summary

The Swedish regulations do not provide any specific requirements on how results shall be 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 as described in section 2. However, the licensee is required to perform all the analyses that make up the basis of an FTA.

For future Periodic Safety Reviews (PSR) for existing plants or SAR for new plants an FTA summary could be valuable in providing an overall assessment and comprehensive presentation of the plant failure tolerance from the viewpoint of fundamental safety requirements rather than from initiating events.

3.3. International Atomic Energy Agency – IAEA

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). 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 [14], should confirm that the requirements for NPP design according to SSR/1 [15] are met. Recommendations and guidance on DSA are provided in IAEA Safety Standards Series No. SSG-2 (Rev. 1) [16] and recommendations on PSA are provided in IAEA Safety Standards Series No. SSG-3 and No. SSG-4, [17], [18].

Those SARs are organised in a standard format based on SAR guides such as IAEA Specific Safety Guide No. SSG-61 [14]. 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” [15]. 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. United Kingdom, Office for Nuclear Regulation – ONR

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 Licence Condition Handbook [19], followed by Safety Assessment Principles (SAPs) [20] 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 [20].

Safety measures are defined in the TAG for Design Basis Accident (DBA) analysis [6]:

- 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 [6] 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 [21], [22]. 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.

3.5. Overview of studied requirements

In addition to the FTA requirement in the Finnish YVL B.1, the requirements presented in Table 2 have been reviewed.

Table 2: Summary of the studied requirements.

Regulations	**Redundancy** (Single failure)	**Diversity** (Common Cause Failure)	**Separation** (Consequen-tial failure)
SSMFS 2008:17	§9	§10	§11
SSMFS 2021:4	Ch.4, 12-13§§	Ch.4, 12-13§§	Ch.4, 12-13§§
SSMFS 2021:5	Ch.3, 14§	Ch.3, 14§ (Ch.2, 8§)	N/A
IAEA, SSR-2/1 rev 1	Req 25	Req 24	Req 21
ONR, SAP	EDR.4 NS-TAST-GD-036	162, 180, EDR.2, EDR.3, EMC.29, 309, ESS.7, NS-TAST-GD-036	Segregation 180, EDR.2, 187, 244, 273, ESS.18, 413, NS-TAST-GD-036
NRC/GDC 10CFR50 App A	Criterion 21	Criterion 22	Criterion 24

4. FTA – Proposed Methodology

Verification and Validation (V&V) activities take place on all levels in an NPP design engineering process. An outline for a methodology is presented in the following sections.

4.1. Verification and validation of plant level safety requirements

An NPP engineering design process starts with a set of requirements to be fulfilled by the designers, including everything needed to form a system, structure or component. The V&V process, as part of NPP engineering design process, handles all requirements addressed as design requirements. Those requirements include functional requirements as well as non-functional requirement. Functional requirements specify particular performance attribute when a pump is started. For example, a certain flow rate should be reach at a certain pressure. Non-functional requirements are often referred to as quality requirements even if that is a simplification. Non-functional requirements properties of a design entity cannot always be verified for individual components in a measurable way. As for the example above related to functional requirements. Safety class, diversity, reliability, failure tolerance and environmental qualification are example of non-functional requirements. Among all those design requirements, only a sub-set are related to safety in terms of the plants abilities to handle the Design Basis Accidents (DBA). Even systems, structures, or components with no relevance to safety may have requirements related to redundancy, separation and diversity for reasons other than reactor safety requirements.

The V&V process for an NPP project can be visualised as in Figure 3. The figure visualises a top-down and bottom-up design approach. The top of the left leg symbolizes high level plant design that is broken down to more and more detailed level design as architecture, system/component detail design. The right leg visualizes a validation of the design from bottom level with components that are put together in systems and form the architecture of systems that finally forms the plant itself.

The plant level safety analysis (SAR chapter 15, [14]) can be seen as an aggregation of all V&V activities performed in a system engineering design process to qualify the SSC's. The purpose is to ensure that reactor safety requirements are handled for those IE's stipulated in the DBA scenarios for the plant. This means to demonstrate the fulfilment of safety functions by the design, to ensure that barriers to the release of radioactive material will prevent an uncontrolled release to the environment for all states of the plant, and to demonstrate the validity of the operational limits and conditions.

There exist different analysis methods which can be used on plant level to verify or demonstrate that fundamental safety requirements are met. DSA and PSA are common methods used in the nuclear industry to demonstrate that safety requirements are met.

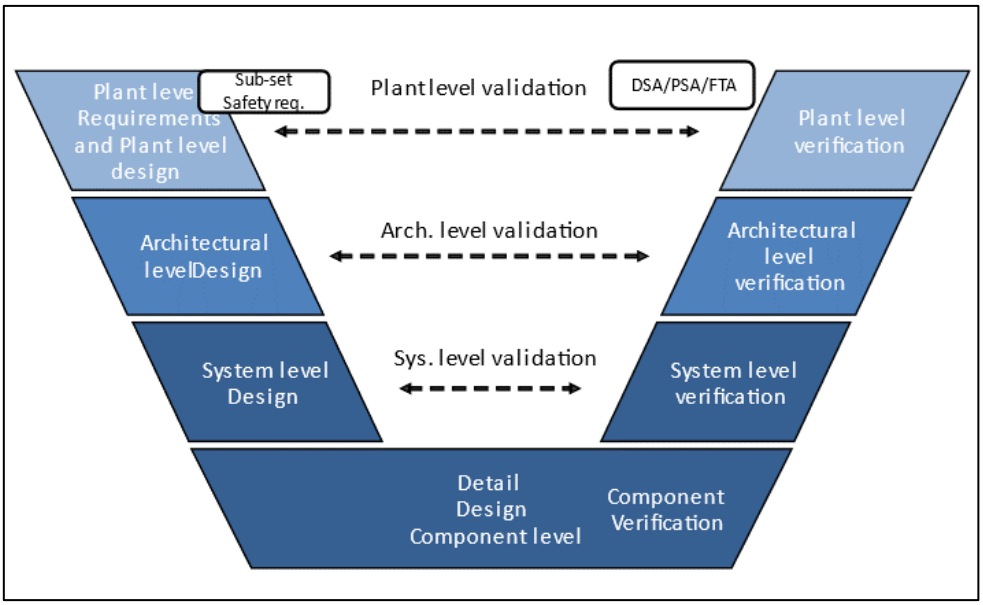

Figure 3: Sketch of a Verification and Validation (V&V) model.

4.2. Perspectives relating to the implementation of FTA

4.2.1. FTA as a safety engineering activity during the design of an NPP

General

Applying FTA in the design phase leads to different challenges than when FTA is applied on an existing NPP.

FTA as a safety engineering activity during design is more challenging since it takes time to develop a final design. Typically, the design is an iterative process, which will lead to many updates of the initial FTA. The top-down vs. bottom-up approach has certain implications for the FTA. FTA as a safety engineering activity has been practiced in Finland. There is ongoing work in an European R&D project to develop such an approach further based on the Finnish experience, "Best Safety Engineering Practices for Nuclear Safety - BESEP" [7]. The work presented in chapter 5 in [7] address the topic "Failure tolerance analysis as safety engineering activity", which in some way aims to develop an approach to fulfil the YVL B.1.351 requirement during the design phase.

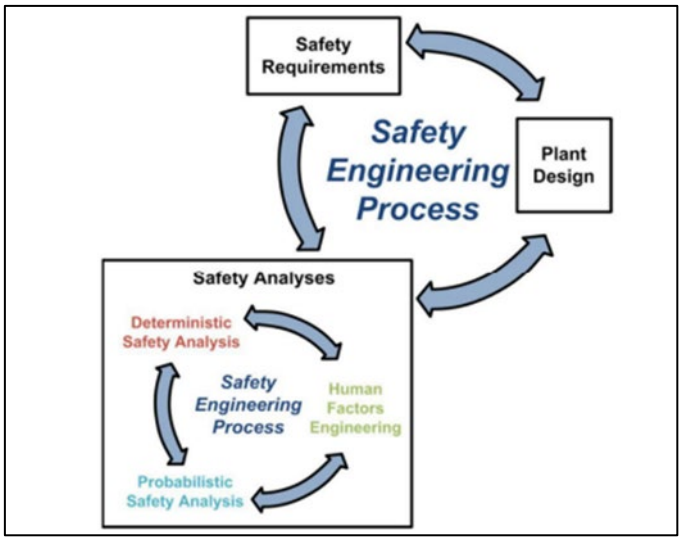

Figure 4: Description of the FTA as a safety engineering activity as interpreted in chapter 5 in [7], addressing YVL B.1.351 during the design phase.

I&C systems

Note that the Instrumentation and Control (I&C) design has many aspects of failure tolerance assessments in its design process, especially for an NPP. “Production excellence” is the demonstration of excellence in all aspects of production, from the initial specification through to the final commissioned system. The International Electrotechnical Commission (IEC) standards apply to the production excellence for I&C systems in which IEC 61513 [23] gives guidance about “production excellence” (by IEC SC 45A “Instrumentation and control of nuclear facilities” being part of IEC TC 45 “Nuclear instrumentation”). By fulfilling the quality aspect during the design of I&C systems in accordance with IEC/TC 45 standards, there will be overlapping analysis to the FTA. The scope of analyses to meet IEC/TC 45 standards will be larger than performing an FTA from a purely nuclear reactor safety perspective. The rigor of the standards (IEC/TC 45) and practices applied should be commensurate with the level of reliability required. The standards and practices should demonstrate ‘production excellence’ and, through the application of ‘confidence-building’ measures, provide proportionate confidence in the final design.

4.2.2. During operation of an NPP

General

During the operation of a nuclear power plant, the design is well-defined, and the construction is completed. All V&V activities specified for the design and constructions should have been successfully performed, given that this was a requirement during the construction phase of the NPP. Over time, new requirements may have been addressed by the design, which can be checked during typical re-assessment activities of the nuclear safety (case). During a re-assessment of an operating nuclear plant, “production (or design) excellence” aspects are excluded, and the FTA can be treated purely as an analytical tool to verify that all prior analyses cover all aspects of the plant's failure tolerance, from a nuclear safety perspective.

At plant-level, the FTA has similarities with the safe shutdown analysis, in which the safe shutdown equipment list is defined. Thereafter, the failure tolerance of the equipment in the list is analysed to identify weak points in terms of single failures, spatial dependencies, and common cause failures (CCF).

I&C systems
New types of digital I&C systems are a specific area of interest for an FTA. The strategies to handle I&C related analysis become more complex by the changeover from analogue to digital automation technology. The quality and qualification requirements in I&C systems often require failure analysis to assess their reliability. Such quality and qualification requirements are often addressed to systems that are not needed for a safe shutdown, from a reactor safety perspective. To avoid confusion amongst the designers, it is important that the regulatory requirements address the execution of the FTA from a reactor safety perspective. The role of quality/qualification requirements needs to be clarified in the light of an FTA.

In the digital I&C systems there are many I&C functions that by quality and qualification requirements, need to be analysed from an FTA perspective. The terms used and in-depth comparison of definitions of key concepts in the I&C area related to diversity and defence have been outlined in different working group reports from the World Nuclear Association (WNA) [18, 20 (Appendix B)], presenting challenges related to I&C Architecture. From the reports it can be noted that there are common terms (e.g. Defence-in-Depth, Diversity, Separation, Redundancy, Reliability) used with different meanings, not only across engineering disciplines, such as I&C disciplines and nuclear safety disciplines, but also within the industry, between different countries and by different regulatory bodies.

4.3. General scope and main topics of FTA

Failure tolerance is demonstrated through sufficient redundancy, diversity, and separation of safety functions as listed in Table 1. The plant safety analyses include a thorough identification of both functional and spatial dependencies. The safety analysis must identify all important dependencies.

Functions and systems designed for plant control under Design Basis Conditions and Design Extension Conditions - DBC2, DBC3, DBC4, DEC - and Severe Accident (SA) conditions, and envisaged at DiD levels 2, 3a, 3b and 4 are analysed within FTA. DBC and DiD levels are further explained in Appendices A.2 and A.3.

An FTA is executed for functions and systems required to perform the following fundamental safety functions needed to bring the plant to a controlled or safe state:

- Reactivity control,
- Heat removal from the nuclear fuel,
- Confinement of radioactivity.

The Reactor Protection System (RPS) and automated safety functions needed during short-term management (DiD3a according to appendix A.2) shall meet N+2 redundancy criteria[3]. Safety functions needed during long-term management shall meet N+1 redundancy criteria[4].

FTA can be used to demonstrate compliance with SSMFS 2021:4, Chapter 4 §13 that includes use of redundancy, separation and diversity as means to achieve a reliability, to the extent necessary (*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)*.

[3] The N+2 failure criterion means that it must be possible to perform a safety function even if any single component designed for that function fails and any other component or part of a redundant system is simultaneously out of operation.
[4] The N+1 failure criterion means that it must be possible to perform a safety function even if any single component designed for the function fails.

Safety functions under DBC2 and DBC3 and which shall meet diversity requirements are analysed by common cause failure tolerance analysis to demonstrate diversity between groups of redundant components.

4.3.1. Topics of function and system-level design

Deterministic Safety Analyses (DSA) demonstrate the capability of the safety functions based on Functional FMEA and System FMEA.

To complete an FTA, it is necessary to define, for each postulated IE, the list of safety functions and corresponding safety systems and to determine the relevance of each safety function to the FTA.

In the system analysis, all failure modes of system components that may affect the performance of a safety function shall be identified.

More specifically, an FTA shall verify that the design of all safety functions of relevance for the FTA satisfies their requirements on:

- Sufficiency of functional redundancy (single failure, N+1, N+2 criteria),
- functional independence between DiD levels,
- diversity (main safety function and its diverse function are tolerant to CCF),
- physical separation

4.3.2. Topics of architecture-level design

Strength of DiD levels. The System level failure analysis demonstrate the strength of an individual DiD with regard to the fundamental safety requirements, i.e. sufficient redundancy, separation, and diversity.

Independence of DiD levels. In the case of a failure of a DiD3 safety function, the DiD4 safety functions should be proven to be unaffected as far as reasonably achievable, i.e. sufficient functional and spatial independence. Actual analyses performed reveal a problem with the requirement of independence of all levels in defense in depths (DiD). The result can be introduction of more systems and components to the extent that the complexity increases which in turn is a challenge for maintenance and thus the maintainability will be jeopardized. This issue needs further attention in terms of how “reasonably achievable” shall be interpreted.

4.3.3. Topic of plant-level design

The plant level assessment is a combination of qualitative analysis (in the same manner as FMEA) and then the construction of a logical model based on this information.

The logical models (fault trees) of safety functions and systems take into consideration the impact of events and component failures on safety functions performance, including support and control systems. Analysis cases (top events in fault trees and associated data) are developed based on the model to analyse the defined IEs and functions according to the defined safe shutdown strategy to capture complex combinations of faults.

The fault tree logic combines all the information from the failure analyses together to a plant fault tree model, in order to enable plant-level failure tolerance analysis to be performed by analysing

Minimal Cut Sets (MCSs). An MCS is a minimal combination of basic events (failure events) resulting in an undesired top event.

MCSs will be generated and analysed, upon which it will be assessed whether the requirements are met to verify the plant level design. Low order cut sets are evaluated in order to confirm the qualification of cut set elements. In the case that an FTA problem is identified, this observation should be clearly documented and explained.

4.3.4. Human errors

A human error criterion can be applied, in a deterministic manner, to plant design, in order to ensure a sufficient tolerability of human errors.

In terms of failure tolerance analysis, human actions are assessed similarly to component failures. All relevant human errors could be identified for an FTA. A PSA model can be used as a source for the identification of human errors, and the assessment could take all relevant human errors into account.

Initially, the Finnish YVL guides also included Human Error Analysis as part of the FTA, but this has been excluded in later versions of the YVL, see section 2.2.

4.3.5. Evaluation of compliance with requirements

In an FTA summary, the results of the analyses carried out in thematic reports (redundancy, DiD levels, independence, diversity, human factors tolerance) are used to check the compliance of NPP design to the requirements.

In the summary, analysis results are grouped by requirement. Based on this presentation, each requirement can be assessed to demonstrate how the design principles are applied on the system-level design and to summarize functional evaluations and the “Strength of DiD”, i.e. all safety functions satisfies their failure tolerance requirements.

5. SWOT- analysis

It can be noted that Sweden, the UK, the US and the IAEA address the topic of failure tolerance in different ways. Finland has been using FTA since 2013, when they first presented the concept of FTA, for which the approach is clarified in YVL B.1. The UK approach to cover the FTA topics differs from the Finnish approach. It is also identified that IAEA guidance regarding FTA is limited.

Introduction of Swedish regulatory requirements similar to Finnish requirements is likely to benefit from development of a common FTA approach within the industry. A SWOT (Strengths – Weaknesses – Opportunities – Threats) analysis for Failure Tolerance Analysis is presented in Table 3.

Table 3: SWOT – Failure Tolerance Analysis.

Strength	Weakness	Opportunities	Threats
General issues			
FTA can fulfil the purpose of SSMFS 2021:4, Chapter 4 §13.	Guides and methods for FTA are not described in literature.	For operating plants FTA is a new compilation of existing analysis	Difficult implementation due to low experience and no current support from guides.
Can describe important means of ensuring a high dependability/availability through ensuring a high reliability by demonstrating how the design principles are applied	There is no consensus in what an FTA is		No new insights compared to existing DSA
	If an FTA is limited to “Strength of DiD” the gap on plant level needs attention	Validation of fundamental safety requirements	Added value of FTA can be questioned since FTA more or less is just another way to present results
FTA will provide for a Safety assessment overview. Plant, Functions, Systems and Sub systems. FTA can be used for High level demonstration		Dependent on scope will the FTA validate the fundamental requirements on, Plant level, Architectural level and System level	
FTA can be used to take advantage of both DSA and PSA simultaneously in the High-level demonstration			
Topics of plant-level design			
Fault tree-model can be used on plant level to analyse the defined IEs and functions according to the defined safe shutdown strategy		Combine all the information from the failure analyses together to a plant fault tree model, in order to enable plant-level failure tolerance analysis. Fault trees can capture complex combinations of faults	
		Verification and Validation (V&V) activities take place on all levels in an NPP design engineering process	
Topics of architecture-level design			
All main components in primary or diverse safety functions used to provide a main or support function, including their subcomponent, are identified and represented by Common Cause Component Groups		By assuming a complete CCF of the Common Cause Component Groups to ensure there is a sufficient diversity of safety features in case of a DBC2 or DBC3 event.	
Topics of system-level design			
Qualitative analysis of safety functions is carried out to prepare a complete list of safety functions in order to be assessed with FTA postulates and to determine the relevance of each safety function to the FTA		To complete an FTA, it is necessary to define, for each postulated IE, the list of safety functions and corresponding safety systems in a functional connection diagram based on fundamental safety requirements.	

6. Conclusions

The term FTA is only used in the Finnish regulatory guides.

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 (in Swedish regulations requirements on dependability and application of design principles to reach a dependability as far as is reasonably achievable).

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 fulfilled. In Sweden, the licensee is required to perform all the analyses that make up the basis of an FTA.

FTA could be used to 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.

Guides and methods for FTA are not currently described in literature and there is no international consensus of what FTA must contain.

Strength and weaknesses are illustrated in the SWOT-analysis. 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.

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. This issue needs further attention.

7. Recommendations

The performed work has identified several issues for further studies. The method, approach and applicability of FTA needs to be researched and developed more by international organisations and the industry before any implementation of requirements in Swedish regulations.

SSM is recommended to collect more information from Finnish industry and authority on experiences from FTA – lessons learned, what are the positive aspects? What are the challenges and how they have been tackled?

When international consensus regarding the methodology and applicability of FTA has been reached, and if it is proven that FTA leads to increased safety, the following proposals could be taken into consideration

- Introduction of requirement on FTA similar to Finland including development of guides and methods for FTA.
- Inclusion of a requirement for an FTA summary in future Periodic Safety Reviews (PSR) to be reported to SSM.

8. References

[1] P. Humalajoki and I. Niemelä, *NPP Failure Tolerance Analyses,* Porvoo: STUK, 2015.

[2] I. Karanta and K. Björkman, *A survey on the use of PRA to support failure tolerance analyses,* VTT Research Report No. VTT-R-00192-20: VTT Technical Research Centre of Finland, 2020.

[3] P. Humalajoki and I. Niemelä, *NPP Failure Analyses in Finland,* Los Angeles: Probabilistic Safety Assessment and Management PSAM 14, 2018.

[4] STUK, *Safety Design of a Nuclear Power Plant, YVL B.1 15.6.2019,* 2019.

[5] J. Gustafsson, *Reliability analysis of safety-related digital instrumentation and control in a nuclear power plant,* Royal Institute of Technology (KTH), May 2012.

[6] Office for Nuclear Regulation (ONR), *DESIGN BASIS ANALYSIS,* NS-TAST-GD-006 Revision 5, 2020.

[7] J. Linnosmaa, *Deliverable 2.3: Specification on the key features of efficient and integrated safety engineering process, V:1.2,* BESEP, August 2021.

[8] United States Nuclear Regulatory Commission (USNRC), *Standard Technical Specifications Westinghouse Plants, NUREG-1431 Revision 5 Volume 2,* Office of Nuclear Reactor Regulation, September 2021.

[9] *NEI 04-10, "Risk-Informed Method for Control of Surveillance Frequencies", Re-vision 1..*

[10] *NEI 06-09-A, Revision 0, "Risk-Managed Technical Specifications (RMTS) Guidelines.*

[11] U. Yngvesson, *The Swedish Radiation Safety Authority´s Regulations concerning Construction of Nuclear Power Reactors, SSMFS 2021:4,* SSM, December 2021.

[12] U. Yngvesson, *The Swedish Radiation Safety Authority's Regulations concerning Analysis of Radiation Safety for Nuclear Power Reactors, SSMFS 2021:5,* SSM, December 2021.

[13] U. Yngvesson, *The Swedish Radiation Safety Authority's Regulations concerning Operation of Nuclear Power Reactors, SSMFS 2021:6,* SSM, December 2021.

[14] IAEA, *Format and Content of the Safety Analysis Report for Nuclear Power Plants,* Vienna: International Atomic Energy Agency, 2021.

[15] IAEA, *Safety of Nuclear Power Plants: Design,* Vienna: International Atomic Energy Agency, 2016.

[16] IAEA, *Deterministic Safety Analysis for Nuclear Power Plants, No. SSG-2 (Rev. 1),* Vienna: International Atomic Energy Agency, 2019.

[17] IAEA, *Development and Application of Probabilistic Safety Assessment for Nuclear Power Plants, No. SSG-3,* Vienna: International Atomic Energy Agency, 2010.

[18] IAEA, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, No. SSG-4,* Vienna: International Atomic Energy Agency, 2010.

[19] Office for Nuclear Regulation (ONR), *Licence condition handbook,* February 2017.

[20] Office for Nuclear Regulation (ONR), *Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Rev.1,* January 2020.

[21] NBB GENERATION COMPANY (HPC), *SUB-CHAPTER 3.7 - DIVERSITY DESIGN PRINCIPLES,* HPC PCSR3.

[22] NNB GENERATION COMPANY (HPC) LTD, *SUB-CHAPTER 15.3 - SUPPORTING ANALYSIS FOR THE HPC DESIGN,* HPC PCSR3.

[23] IEC, *Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, IEC 61513:2011,* TC 45/SC 45A, 2011.

[24] Reactor Harmonization Working Group (RHWG), *Report - Safety of new NPP designs,* WENRA, March 2013.

[25] World Nuclear Association, *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture, No. 2018/003,* April 2018.

[26] World Nuclear Association, *Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts, No. 2019/008,* October 2019.

Appendix A

A.1 Safety Concept Basis

To ensure that Design Basis Conditions at different levels do not lead to unacceptable consequences, nuclear facilities are equipped with safety functions. The safety functions are divided into three main groups of fundamental safety functions with different objectives. The three fundamental safety functions and their respective objectives are:

- Reactivity control,
  which ensures that the core is and remains subcritical.
- Heat removal,
  which cools the fuel and transfers the heat to an ultimate heat sink.
- Activity confinement,
  which contains radioactive substances inside the facility.

Each fundamental safety function is divided into basic safety functions that have more specific objectives, see Table 3. One component or system in the facility may belong to more than one basic safety function.

Table 3: Fundamental safety functions

	Fundamental safety functions		
	Reactivity control	**Heat removal**	**Activity Confinement**
Basic safety functions	Fission reaction termination and subcriticality assurance	Maintaining the primary coolant inventory	Limitation of pressure inside the containment and heat removal from the containment
		Heat removal from the primary coolant (including transfer to the ultimate sink)	Confinement inside the containment/waste pit
		Primary loop integrity assurance	Confinement outside the containment
		Secondary/tertiary loop integrity assurance	Confinement in secondary/tertiary loop
			Confinement in the auxiliary systems and experimental systems
		Cooling of the spent fuel (including transfer to the ultimate sink)	Fuel handling

A.2 Defence-in-Depth levels

The primary means of preventing accidents in a nuclear facility and mitigating the consequences of accidents is the application of the concept of Defence-in-Depth (DiD). The concept is based on the idea that a failure in one level of defence should be handled by the next level. This concept should be applied to all safety related activities to ensure that all safety related activities are subject to independent layers of provisions. The Reactor Harmonization Working Group (RHWG) in WENRA have discussed whether a new level of defence should be defined for multiple failure events, because safety systems which are needed to control postulated single IEs are assumed to fail, and thus another level of defence should take over. However, the single IEs and multiple failure events are two complementary approaches that share the same objective [24]. Therefore, the RHWG have proposed to treat the multiple failure events as part of the third level of DiD. The refined structure of the levels of DiD, proposed by RHWG is presented in Table 4.

Table 4: Refined structure of the levels of DiD, from WENRA RHWG in [24].

DiD level		Objective	Means	Plant condition categories
1		Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation.	Normal operation
2		Control of abnormal operation and detection of failures.	Control and limiting systems and other surveillance features	Anticipated operational occurrences
3	a	Control of accident to limit radiological releases and prevent escalation to core melt conditions	Reactor protection systems, accident procedures	Postulated single initiating events
	b		Additional safety features, accident procedures	Postulated multiple failure events
4		Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.	Complementary safety features to mitigate core melt, management of accidents with core melt	Postulated core melt accidents
5		Mitigation of radiological consequences of significant releases of radioactive material.	Off-site emergency response. Intervention levels	-

A.3 Design Basis Conditions

IEs are events that could challenge the safety of the facility by initiating an accident scenario. To make the list of IEs manageable, they are grouped by their expected effect on the facility. The groups are called Design Basis Conditions (DBC), i.e., the conditions that are expected to occur for a group of IEs. Depending on the frequency of the constituent events, different consequences can be accepted and therefore different safety objectives are defined. The DBC levels and safety objectives, as well as expected occurrences and examples of IEs, are summarised in Table 5.

For the scope of this report no frequency analysis of the initiating events was done and therefore the SAR definition of Design Basis Accident (DBA) IE group has been used as per DBC-3. Beyond DBA (BDBA), which is defined as DBA without containment ventilation isolation, is used as per DBC-4.

Table 5: Design Basis Conditions (DBC 1-4)

DBC	**Safety Objectives**	**DBC occurrence** *Finnish guidelines (YVL)*
DBC 1 *Normal operation*	Normal operation should not lead to yearly effective doses to the public above 1 mSv/year (5 mSv/year is allowed under special circumstances).	Normal operation shall refer to the planned operation of a nuclear power plant according to the Operational Limits and Conditions and operational procedures in place. These also include testing, plant startup and shutdown, maintenance and refuelling.
DBC 2 *Anticipated operational occurrence*	Anticipated operational occurrence should not lead to yearly effective doses to the public above 1 mSv/year (5 mSv/year is allowed under special circumstances).	Anticipated operational occurrence shall refer to a deviation from normal operation that can be expected to occur once or several times during any period of a hundred operating years.
DBC 3 *Design Basis Accidents (LOCA)*	Design Basis Accidents (DBA). LOCA with failure in emergency cooling are subject to the same requirements to dose limitation to the public as under normal operation.	Postulated accidents, which can be assumed to occur less frequently than once over a span of one hundred operating years, but at least once over a span of one thousand operating years.
DBC 4 *Beyond Design Basis Accidents (failed containment isolation)*	Beyond DBA (BDBA) shall not lead to effective doses to the public higher than 10-50 mSv/year.	Postulated accidents which can be assumed to occur less frequently than once during any one thousand operating years.

The Swedish Radiation Safety Authority (SSM) works proactively and preventively with nuclear safety, radiation protection, nuclear security, and nuclear non-proliferation to protect people and the environment from the harmful effects of radiation, now and in the future.

You can download our publications from www.stralsakerhetsmyndigheten.se/en/publications. If you need alternative formats such as easy-to-read, Braille or Daisy, contact us by email at registrator@ssm.se.

Strålsäkerhetsmyndigheten
SE-171 16 Stockholm
+46 (0) 8-799 40 00
www.stralsakerhetsmyndigheten.se
registrator@ssm.se

Scandinavian Print Group Sweden AB, 2025