NPP Failure Analyses in Finland

Pia Humalajoki[*a] and Ilkka Niemelä[a]
[a] STUK - Radiation and Nuclear Safety Authority, Helsinki, Finland

Abstract: Since 2013 Finnish Regulatory Guides have required the application of Failure Tolerance Analysis to demonstrate the redundancy, diversity and separation of safety functions and systems of nuclear power plants. Failure Tolerance Analysis consist of a set of already well-known failure analysis methods, demonstrating the tolerance against failures of nuclear power plant. The analysis set pays special attention to relations between different failure analyses and their ability to cover plant level failure tolerance.

Failure Tolerance Analysis can be used to justify the choices of design solutions and to demonstrate the fulfillment of the design requirements of safety systems, support systems or components. Experiences have shown benefits of well-defined analyses set in several stages of life cycle of nuclear power plant in Finland. Failure Tolerance Analysis, Deterministic Safety Analyses and Probabilistic Risk Assessment support each other. Failure Tolerance Analysis also improve coverage of analyses scope by concentrating on effects of failures. Analysis results may affect plant modifications or demonstrate that the plant design is safety despite of some weaknesses.

Keywords: Failure analyses, Failure Tolerance Analysis, Redundancy, Diversity, Common Cause Failures

1. INTRODUCTION

For a long time different failure analyses have been used to prove the safety of nuclear power plants and to recognize potential failures of systems and components. For example Failure Mode and Effects Analyses (FMEA), Common Cause Failure (CCF) analyses, redundancy and diversity analyses, analyses of spurious I&C actuations, human error analyses, initiating event analyses and hazard analyses are well-known failure analyses.

Radiation and Nuclear Safety Authority in Finland (STUK) uses term *'Failure Tolerance Analysis'* to describe a specified collection of failure analyses. Those analyses demonstrate that the plant is tolerant to failures and its safety is confirmed also with defined failures. Individual failure analyses are tools for Failure Tolerance Analysis. This paper concentrates on two points:

- Relations between Failure Tolerance Analysis, other failure analyses, Probabilistic Risk Assessment (PRA) and Deterministic Safety Analyses.
- Coverage and experiences of Failure Tolerance Analysis.

This paper describes motivation and development of clearly defined set of failure analyses utilized as Failure Tolerance Analysis at STUK. Insights of relations between different failure analyses and their coverages are introduced in chapter 3. Finnish regulatory requirements in Failure Tolerance Analysis are presented in chapter 4. Chapter 5 introduces some experiences of Failure Tolerance Analysis in different life cycles of nuclear power plants. Some benefits of defined analysis set are described in chapter 6, based on Finnish experiences.

2. CHALLENGES IN INTEGRATING DIFFERENT ANALYSES TYPES

During the course of time and continuous development of Finnish Regulatory Guides (YVL Guides), plenty of different requirements regarding failure tolerance of systems or functions have been introduced. The problem was, that requirements focused on individual technical disciplines, and the

[*] pia.humalajoki@stuk.fi

general plant level impression of failure tolerance was not considered. Also analyses of failures and failure tolerance, PRA and Deterministic Safety Analyses did not cooperate optimally. Coverages of individual analyses and also whole set of analyses were unclear.

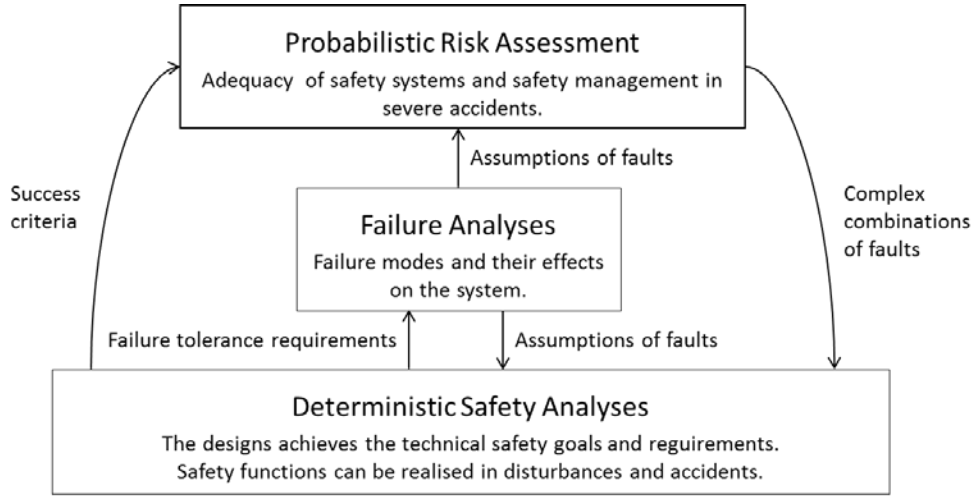
From an authority perspective, analyses overlapping with each other caused extra work. Resources or responsibilities for review of analyses crossing several technical disciplines were unclear. Expectations and acceptance criteria of failure analyses were not clearly defined. Each analysis met its own technical requirements, but relations between analyses were not paid attention to.

3. DEVELOPMENT OF FAILURE ANALYSES AS A REGULATORY CONCEPT

In the project of new nuclear power plant, Olkiluoto 3, various failure analyses had strongly been applied during plant design and construction, but the entire insight of collection of analyses was unclear. There were many different analyses to demonstrate one section of plant's tolerance against specific failures. For creating the clearly defined analyses set, STUK started a process to define Failure Tolerance Analysis, outline the compiled failure analyses set and clarify the target for these. In this process, a regulatory concept of failure analyses was created, the aim of which is to reach traceability and sufficient coverage of failure analyses without overlapping work. Defined Failure Tolerance Analysis is one part of that concept. As a result of this process, an example of sufficiently comprehensive failure analyses set was introduced in master's thesis work. Also a new guide for reviewing failure analyses was added in the Internal Quality Handbook of STUK. [1,3]

Figure 1 presents relations between failure analyses, PRA and Deterministic Safety Analyses, which all have own different roles to assign the safety of nuclear power plant. Deterministic methods demonstrate that the plant is able to accomplish the safety functions needed, also in case of selected failures. Deterministic Safety Analyses utilize potential failures identified by failure analyses, like FMEA. So does also PRA by compiling the results of Deterministic Safety Analyses and failure analyses to risk model of the plant.

Figure 1 Relations Between Failure Analyses, PRA and Deterministic Safety Analyses



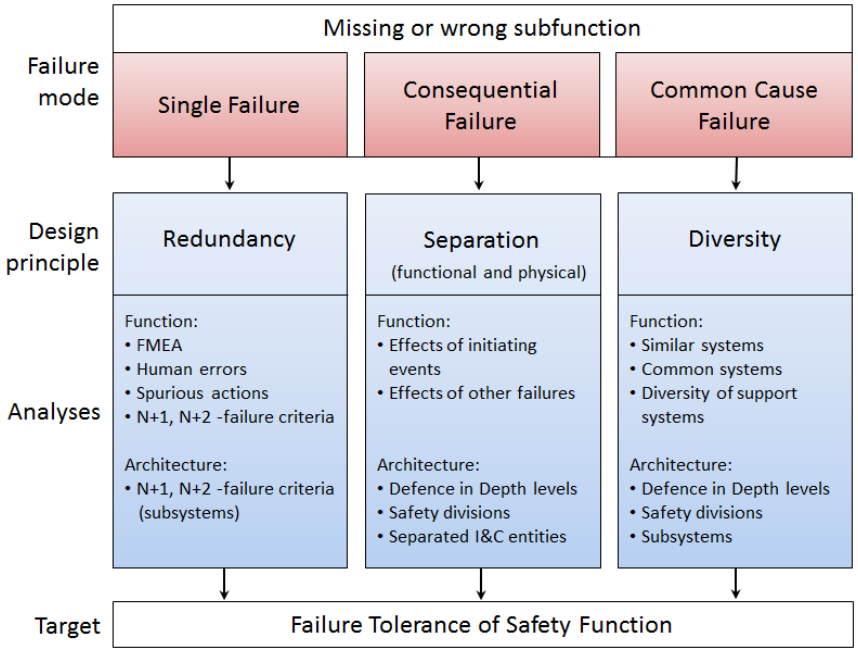
The analysis process is all the time iterative: As well failure analyses utilize results of Deterministic Safety Analyses. In failure analyses, success criteria of systems are based on deterministic studies. Acceptability of consequences of failure combinations can be evaluated with deterministic studies.

3.1. Failure Tolerance Analysis Collection and Its Coverage

Failure analyses are descriptive analyses used to recognize failures modes and describe their effects. The results of certain failure analyses can be utilized to demonstrate the failure tolerance of the plant or its systems. These demonstrative analyses are part of defined Failure Tolerance Analysis set.

Failure Tolerance Analysis aim to cover general design principles for nuclear power plants. Different types of analyses are needed to demonstrate each principle: redundancy, separation and diversity. For demonstrating the failure tolerance of the whole plant, every principle needs to be considered individually. The Failure Tolerance Analysis set builds on different types of failure analyses, for example FMEA, CCF analyses, redundancy and diversity analyses, analyses of spurious I&C actuations and human error analyses. Most of these analyses methods are already generally used. Figure 2 presents different types of analyses to demonstrate each design principles. It indicates the need for different types of analyses instead of one analysis of failure tolerance.

Figure 2 Individual Parts of Failure Tolerance Analysis and Their Targets



Next paragraphs introduce shortly methods used for analysis of failure tolerance, considered in this paper.

Failure Mode and Effect Analysis (FMEA) is one of the most used failure analysis. FMEA is used to determine potential individual failure modes and their effects on component or system. The purpose is to find all potential failure modes and to identify the effects on the operation of component, system or safety function to be analyzed. Failure modes include also maintenance and service faults caused by human errors. FMEA is utilized during early design and as a basis for most other failure analyses and also PRA.

From the perspective of I&C systems, potential of wrong or spurious actuations of the system should be identified by failure analyses. Instead of identifying every single signal and it's all effects, it is enough to recognize failures of I&C signals leading to the worst consequence for the plant. It follows that analyses of spurious I&C actuations may deal with I&C entities managed by separation. Results are considered in CCF and diversity analyses as a failure modes of I&C.

Redundancy and diversity analyses demonstrate that safety functions can be executed on demand even in case of inoperability of some of systems or subsystems performing the selected function. A well-

defined analysis set can make individual analyses manageable and yet cover the required entity. For example, a diversity analysis may be carried for process systems and components, demonstrating that CCFs between frontline and backup systems do not endanger safety. Another diversity analysis is then performed for their I&C systems to show that CCFs between them have been excluded. Then it is shown that failures of frontline I&C do not prevent the backup I&C from operating, and vice versa. In this way the demonstration of failure tolerance is divided into manageable parts yet ensuring adequate coverage. Individual analyses utilize failures identified in FMEA and already recognized potential CCFs.

Common Cause Failure (CCF) analyses identify potential CCFs between redundant systems or subsystems. They also recognize shared or type identical systems and components between redundant systems, subsystems or functions. Main target is to identify the CCFs between redundancies, which may lead to spurious actuation or loss of safety function.

4. FAILURE TOLERANCE ANALYSIS IN REGULATORY GUIDES

Reliability of safety function is related to quality of systems implementing the function, but also failure tolerance of function. The quality of system and its components is related to safety class of system: the higher safety importance, the higher quality should be. Compared to failure tolerance, that considers the whole function instead of single systems. Failure tolerance takes into account main systems as well as support systems implementing the function. The purpose of Failure Tolerance Analysis is to demonstrate acceptability of consequences of failures.

To demonstrate acceptability, Failure Tolerance Analysis demonstrates sufficient redundancy, sufficient separation and sufficient diversity of safety functions. Sufficient redundancy means amount of redundant components or systems to meet the specific failure criteria for function performed. Specific criteria for safety functions or systems performing safety functions are presented in YVL Guides [2]. *'Sufficiently diversified'* does not always mean 100% diversification between redundancies, except for severe accident management. If analysis notices a potential of CCF, it needs to be assessed if it is acceptable. CCF potential might be acceptable if there is enough diversity inside the redundancy or the accident is manageable even with CCF, for example. Analysis aim is to ensure that all potential failures and their consequences are recognized and their acceptability is evaluated.

In addition to PRA and Deterministic Safety Analyses, Failure Tolerance Analysis is required by YVL Guides since 2013 [2]. The Regulatory Guides require the usage of Failure Tolerance Analysis set to demonstrate the redundancy, diversity and separation of safety functions and systems. These analyses can be used to justify the choices of design solutions and to demonstrate the fulfillment of the design requirements of safety systems, auxiliary systems or components. There are three requirements presented below:

"YVL B.1 351. Failure tolerance analyses shall be carried out to demonstrate that

- *all systems performing safety functions and their auxiliary systems satisfy the failure criteria specified in section 4.3 of this Guide;*
- *systems assigned to different levels of defence according to the defence in depth approach have been functionally isolated from one another in such a way that a failure in any one level does not affect the other levels; and*
- *a common cause failure in any single component type (e.g. a similar check valve, same type and manufacturer) will not prevent the nuclear power plant from being brought to a controlled state and further to a safe state."* [2]

Requirement 351 identifies the aim of the Failure Tolerance Analysis. Analysis needs to demonstrate fulfillment of specified failure criteria for systems. Failure Tolerance Analysis can also be used for demonstrating independence of defense in depth levels with Deterministic Safety Analyses.

"YVL B.1 352. 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 failure at a time and examine its impact in terms of the operation of the system." [2]

Requirement 352 describes the content to be covered with Failure Tolerance Analysis set. Individual analyses focus on each safety function or other limited entity at a time taking into account also support systems performing it.

"YVL B.1 353. A common cause failure analysis shall be drawn up for initiating events in design basis categories DBC 2 and DBC 3. For the common cause failure analysis, the implementation of the safety functions shall be presented for each initiating event in a manner that indicates the use of the systems implementing the principles of diversity and redundancy. The common cause failure analysis shall address one safety function, or part of it, at a time with due regard to the systems implementing the function and the related auxiliary systems. The analysis shall address the common cause failures of all components whose common cause failures or spurious actuation may affect the performance of the safety function. The common cause failure analysis shall consider the initiating event, interdependencies between initiating events as well as common cause failures between components sharing a similar property, i.e. components that are similar or contain a significant number of similar parts." [2]

Scope of CCF analysis is defined by requirement 353. It also includes a requirement to identify dependencies between initiating events and safety functions. CCF analysis focus on anticipated operational occurrences (DBC 2) and class 1 postulated accidents (DBC 3). DBC 2 events shall refer to such 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 events shall refer to a deviation from normal operation which is assumed to occur less frequently than once over span of hundred operating years, but at least once over a span of thousand operating years, and which the nuclear power plant is required to withstand without sustaining severe fuel failure, even if individual components of systems important to safety are rendered out of operation due to service or faults. [2]

Acceptance criteria for defined analyses of failure tolerance vary between individual analyses. To demonstrate the failure tolerance of whole plant, acceptance criteria for plant failure tolerance are divided to different analyses which together build the coverage of the whole. Single analysis may demonstrate fulfillment of selected failure criteria, e.g. fulfillment of single failure criteria, fulfillment of required diversification, or prevention of the spreading of failures between defense in depth levels or separated systems. Failure Tolerance Analysis also may demonstrate specific regulatory requirements of design, like *"YVL B.1 435. A failure in a system performing safety functions shall not cause a failure in either any redundant part of the same system or any other system contributing to the same safety function."* or *"YVL B.1 5240. When I&C systems fail, they shall meet the below requirements: ... 8.The severe reactor accident instrumentation and management systems and their auxiliary systems shall be independent from all other I&C systems of the plant unit. The failure of other I&C systems shall not interfere with the management systems for severe accidents."* [2]

Ensuring that each single analysis meets its acceptance criteria, acceptability of plant level failure tolerance will be confirmed as a whole. With well-defined analysis set, the entity can be covered by focusing on the individual analyses.

5. EXPERIENCES OF FAILURE TOLERANCE ANALYSIS IN FINLAND

Since 2013, Failure Tolerance Analysis is required for every nuclear power plant in Finland: for units under design, units under construction and operating units. In Olkiluoto 3 and Hanhikivi 1 projects

Failure Tolerance Analysis is part of the design process. STUK has already commented Fennovoima's plans of Failure Tolerance Analysis concept required for construction license for Hanhikivi 1 unit under design.

For example a comprehensive diversity analysis was performed for Olkiluoto 3 unit. The analysis covered every system performing safety functions and their support systems. The results caused some modifications to the plant design. Chapter 5.1 introduces some experiences of diversification and CCF analysis for Olkiluoto 3, during plant design and construction.

For operating units Failure Tolerance Analysis has not been part of the original safety analyses concept even though issues to be considered in these analyses have already mostly been included in the existing safety analyses. Specific Failure Tolerance Analysis is required when renewing operating license or during the significant plant modifications. Chapter 5.2 introduces two different situations of Failure Tolerance Analysis for operating units. First one presents I&C architectural level CCF analyses in Loviisa 1 and 2 units associated with I&C renewal process. Another example presents coverage of analysis set in Olkiluoto 1 and 2 units, based on existing failure analyses developed during the lifetime of the plant.

5.1. Units Under Design or Under Construction

Diversity and CCF analysis for unit under construction

Olkiluoto 3 "Diversity and Common Cause Failure analysis" describes safety functions on the component level, looking for CCF potentials, which may lead to the failure of safety function. For this purpose, the analysis presents components used in frontline and backup functional chains for every safety function. It concentrates on the functions, and their necessary support systems, coping with DBC 2 or frequent DBC 3 events. Term *'frequent DBC 3 events'* means a limited part of DBC 3 events. The term was only used in Olkiluoto 3 before official definition of failure analyses and definition of DBC events in renewed YVL Guides [2].

Developed methodology of diversity and CCF analysis includes steps to identify and compare frontline and backup functional chains on the component level. It identifies shared and type identical components between chains. Analysis contains the evaluation of physical dependencies and dependencies of necessary common support systems, i.e electricity and I&C regarding activation of active components.

Analysis results demonstrate that the frontline chain and the redundant backup chains are sufficiently diversified. It is possible to cope with DBC 2 or frequent DBC 3 events even with CCF. Some lack of diversity was recognized with the analysis: noticed weaknesses caused some modifications in plant design. One example of recognized weakness of diversity were the check valves in emergency cooling pipelines. The design was not changed, but with analyses it has been demonstrated that DBC 2 and frequent DBC 3 events can be coped even with CCF in these valves.

During plant design phase, the design basis for I&C was clarified to include also spurious actuations of entire I&C systems or platforms. Initially, it contained spurious actuations of individual functions. Including spurious worst-case failures of large I&C entities into design base caused wide modifications to I&C architecture. Failure Tolerance Analysis was utilized for demonstrating the protection against such complex failure modes.

During construction, Failure Tolerance Analysis was refined with finer details, and they caused still some modifications of design: e.g. I&C signals were arranged so that diverse signals were moved from some output cards to another so that they do not weaken the diversity principle.

Diversity and CCF analysis can be also seen as an example of practical elimination concept. Early recognition of I&C CCF potentials managed to eliminate "loss of"-type failures in practice. Practical

elimination of spurious automation failures was demonstrated by a set of failure analyses, diversity analyses, separation analyses, robustness analyses etc. Analysis showed that it is possible to cope with DBC 2 or frequent DBC 3 events even with assumed worst-case failures of digital I&C systems.

5.2. Operating Units

CCF analysis for plant modification

Failure Tolerance Analysis is required also for plant modifications. One target of this analysis is to prove that the modification follows the principle of continuous improvement. That is a reason why it is not enough to make analysis only limited to renewed part of the plant. The analysis should consider every part of the plant on which the modification might affect. Failure tolerance is assessed based on plant level impacts function by function. If the Failure Tolerance Analysis already exists for current plant design, the analysis update process would be easy.

Loviisa 1 and 2 I&C renewal process is about to be completed in annual outage 2018. Part of the process is the plant level Failure Tolerance Analysis, from view of new I&C. Plant level analysis consist of single and CCF analyses, separation analyses and systems boundary analyses. Analyses support each other, for example CCF analyses utilize results of boundary and separation analyses.

CCF analyses focuses on new I&C components, systems, functions actuated by new I&C signals and new I&C platforms. Original hardwired I&C does not include components, systems or platforms similar to those in renewed digital part, so component level analyses do not need to include retained former parts. At functional level some functions need both new and old I&C. In these cases analysis boundaries are extended to include possibilities of original I&C prevent renewed systems from accomplishing their functions. Also effects of new signals to original parts are considered.

Demonstration of coverage of Failure Tolerance Analysis for operating unit

One example of analysis made afterwards is a Failure Tolerance Analysis for Olkiluoto 1 and 2. For these units, Failure Tolerance Analysis was made as a part of application for the operating license renewal in 2017.

Many analyses supporting Failure Tolerance Analysis requirements have already been performed earlier. In this case, the analysis set can be performed on the basis of existing analyses. These existing analyses have been updated during plants lifetime. The major reference analyses are FMEAs made in the early times of the plant. PRA documentation also includes events analyses and consequential failures caused by events. Initiating event analyses identify the consequences and failures imposed by initiating events. PRA also indicates the safety importance of CCFs and failures related to human performance. Deterministic Safety Analyses have been performed to fulfill the failure criteria and CCF of safety systems combined with initiating events.

Based on these probabilistic and deterministic existing analyses a demonstrative analysis report of plant level diversity was created. It utilizes the diversity principle on three different levels: main safety functions, system level and component level. This summary report did not reveal any new vulnerability. There were already some issues known to be failure tolerant not enough, and these analyses verified the need for plant modifications related to those issues.

Although no new vulnerabilities were recognized, analysis is considered useful. Analysis report helps to consider effects of diversity in plant modifications in the future.

6. BENEFITS OF DEFINED FAILURE ANALYSES SET

According to Finnish experience, different failure analyses, Deterministic Safety Analyses and PRA support each other. As a well-designed set failure analyses and Failure Tolerance analysis can save a

lot of analysis work while ensuring sufficient coverage. Review of well-defined failure analyses saves time and gives a good understanding of failure modes and effects for PRA review. On the other hand, PRA review supports recognition of objects important to safety for considering with more attention in failure analyses.

Comparing of results of PRA, Deterministic Safety Analyses and failure analyses helps to convince of the coverage of the analyses set. Different analyses producing systematically similar results support validity of results. Differences between analyses results raise evidence to question the validity or conclusions of analyses.

Failure analyses are a systematic and effective way to analyze amount of failure potentials. Optimally they should not be used as individual analyses, but as parts of a set, whose coverage is assured without overlapping work. If any failure potentials are excluded from analyses scope, the risk is accepted without evaluating its importance. If analyses consider the potential of failure, the opportunity is to prevent it or accept it.

Failure analyses, Deterministic Safety Analyses and PRA together create also a base for practical elimination concept In Finland. Practical elimination in practice in Finland is presented more detailed in reference [4]. With failure analyses it is possible to recognize failure potentials which should be practically eliminated. On the other hand, failure analyses may demonstrate that failure potentials are sufficiently eliminated.

From regulatory perspective, unified concept of failure analysis set has already given considerable benefits. STUK has developed a new guide in its Internal Quality Handbook [3]. This has created a common understanding and application of failure analyses and Failure Tolerance Analysis between technical disciplines. The review efficiency of analyses has increased. The guide also includes graded approach principle to emphasize the review efforts.

7. CONCLUSION

In nuclear power plants, it is not possible to prevent all failures of components, systems or structures, but the impact of the failures can be limited. Failures excluded from analyses scope without any analysis, takes a risk without knowing its significance. Failure analyses are effective methods to analyze amount of failure potentials systematically. *Failure Tolerance Analysis* utilizes well-known analysis methods to demonstrate that the plant is tolerant to failures and its safety is confirmed also with defined failures. Failure Tolerance Analysis considers to plant level functions instead of only individual systems.

Clearly defined set of failure analyses and Failure Tolerance Analysis improve the coverage and scope of deterministic and probabilistic analyses. Paying attention to relations between analyses helps to ensure a plant level coverage of analyses. Defining of Failure Tolerance Analysis set as a plant level collection, it also may decrease overlapping work between technical disciplines.

References

[1] P. Humalajoki. *"Ydinvoimalaitoksen vika-analyysit"*. Master's Thesis, Tampere University of Technology, pp. 82, (2016).
[2] Radiation and Nuclear Safety Authority (STUK). *"Safety design of a nuclear power plant"*, Regulatory Guide YVL B.1, 15.11.2013, Helsinki. https://www.stuklex.fi/en/ohje/YVLB-1
[3] Radiation and Nuclear Safety Authority (STUK). *"Vika-analyysit"*. Internal Quality Handbook YTV 3.b.3, 22.8.2017, Helsinki.
[4] I. Niemelä, N. Lahtinen and M. Marjamäki. *"Practical Elimination - Experiences for Units in Use, in Construction and in Design"*, Probabilistic Safety Assessment and Management PSAM 14, 2018, Los Angeles, CA.