nks
Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-223
ISBN 978-87-7893-293-8

Guidance to Risk-Informed Evaluation of Technical Specifications using PSA

Ola Bäckström 1
Anna Häggström 1
Ilkka Männistö 2

1 Scandpower AB, Sweden
2 VTT, Finland

October 2010

Abstract

This report presents guidance for evaluation of Technical Specification conditions with PSA. It covers quality in PSA, how to verify that the PSA model is sufficiently robust and sufficiently complete and general requirements on methods. Acceptance criteria for evaluation of changes in the TS conditions are presented.

As the probabilistic safety assessment (PSA) has developed over the years, it has demonstrated to constitute a useful tool for evaluating many aspects of the TS from a risk point of view. and in that way making the PSAs as well as the decision tools better. This also means that it will be possible to take credit for safety system overcapacity as well as inherent safety features and strength of non-safety classed systems.

However, PSA is only one of the tools that shall be used in an evaluation process of TS changes (strengthening/relaxation). PSA is an excellent tool to be used to verify the importance, and thereby possibly relaxation, of TS requirements. But, since PSA is only one tool in the evaluation, it is not sufficient in itself for defining which equipment that shall or shall not have TS requirements.

The purpose of this guidance document is to provide general require-ments, requirements on methods and acceptance criteria on risk-informed evaluation of TS changes based on PSA. The purpose is not to provide a single solution.

As part of the review of the TS conditions this guidance specify require-ments on:
- Quality verification of the PSA model
- Verification that the PSA model is sufficiently robust with regard to SSCs for which requirements both are and are not defined by the TS
- Verification that the SSCs, for which TS demands are to be evaluated, are modelled in a sufficient manner
- Methods for performing the evaluation
- Which evaluation criteria that shall be used (and how that is verified to be correct)
- Acceptance criteria

This guidance also briefly discusses the documentation of the analysis of the TS changes.

This guidance document is to a large content influenced by the structure and guidance given in the NRC Regulatory Guide 1.174.

Key words

Technical Specifications, PSA, Risk optimisation, Risk evaluation

NKS-223
ISBN 978-87-7893-293-8

Electronic report, October 2010

NKS Secretariat
NKS-776
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@nks.org

Contents

Appendices

Foreword

This guidance document has been developed within the project “Interpretation and Risk Evaluation of Technical Specification Conditions”. The project is financed both by the Nordic Nuclear Safety Research group, NKS, and the Nordic PSA Group, NPSAG (project ID NPSAG #14-002).

Technical Specifications (TS) are part of the safety documentation – FSAR/SAR in Swedish and Finnish NPPs. Any changes therefore have to be reported to and approved by the respective regulatory body in these countries. Risk informed evaluation of TS conditions and changes to these is an area with increased interest.

Phase 1 of the project, finalized in mid 2008, studied several risk-informed TS evaluation projects performed internationally. Several seminars with participants from the Swedish and Finnish nuclear community discussed methods and important aspects on risk-informed TS evaluation.

This guidance document is compiled on the basis of the conclusions from the seminars and answers to the questionnaires sent out to the participants during the second phase of the project.

The report is reviewed by the members of the Nordic PSA group during summer/autumn 2009.

SUMMARY

This report presents guidance for evaluation of Technical Specification conditions with PSA. It covers quality in PSA, how to verify that the PSA model is sufficiently robust and sufficiently complete and general requirements on methods. Acceptance criteria for evaluation of changes in the TS conditions are presented.

I denna rapport presenteras vägledning för hur PSA kan användas vid utvärdering av villkoren i STF. Vägledningen täcker kvalitetsaspekter på PSA, verifiering av PSA modellens robusthet och fullständighet och generella krav på metoder. Slutligen presenteras acceptanskriterier för värdering av förändringar i STF.

As the probabilistic safety assessment (PSA) has developed over the years, it has demonstrated to constitute a useful tool for evaluating many aspects of the TS from a risk point of view. and in that way making the PSAs as well as the decision tools better. This also means that it will be possible to take credit for safety system overcapacity as well as inherent safety features and strength of non-safety classed systems.

However, PSA is only one of the tools that shall be used in an evaluation process of TS changes (strengthening/relaxation). PSA is an excellent tool to be used to verify the importance, and thereby possibly relaxation, of TS requirements. But, since PSA is only one tool in the evaluation, it is not sufficient in itself for defining which equipment that shall or shall not have TS requirements.

The purpose of this guidance document is to provide general requirements, requirements on methods and acceptance criteria on risk-informed evaluation of TS changes based on PSA. The purpose is not to provide a single solution.

As part of the review of the TS conditions this guidance specify requirements on:

- Quality verification of the PSA model
- Verification that the PSA model is sufficiently robust with regard to SSCs for which requirements both are and are not defined by the TS
- Verification that the SSCs, for which TS demands are to be evaluated, are modelled in a sufficient manner
- Methods for performing the evaluation
- Which evaluation criteria that shall be used (and how that is verified to be correct)
- Acceptance criteria

This guidance also briefly discusses the documentation of the analysis of the TS changes.

This guidance document is to a large content influenced by the structure and guidance given in the NRC Regulatory Guide 1.174.

Acronyms and Abbreviations

AOT	Allowed Outage Time
BIR	Burden-to- Importance-Ratio
CCF	Common Cause Failure
CDF	Core Damage Frequency
LCO	Limiting Conditions for Operation
LERF	Large Early Release Frequency
LWR	Light Water Reactor
PSA	Probabilistic Safety Assessment (aka PRA, Probabilistic Risk Assessment)
RAMA	Consequence mitigation systems (in Swedish BWR units)
RG	Regulatory Guide (by NRC)
SAR	Safety Analysis Report
SG	Safety Goal
SR	Surveillance Requirements
SRP	Standard Review Plan (by NRC)
SSC	System, Structures and Components
STI	Surveillance Test Interval
TS	Technical Specifications
URF	Unacceptable Release Frequency (exceeding the limit defined as acceptable in case of a core damage)
Safety object	Object part of safety class 1-3
Non-safety object	Object part of safety class 4 (i.e. not part of safety class 1-3)

Organizations

ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
IAEA	International Atomic Energy Agency
NRC	Nuclear Regulatory Commission (US)
SSM	Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority)
STUK	Säteilyturvakeskus (Finnish Radiation and Nuclear Safety Authority)

1. Introduction

1.1 Background

A nuclear power plant´s Technical Specifications (TS) define the limits and conditions for plant operation to secure the validity of the assessment performed in the Safety Analysis Report (SAR).

The SAR assessment is basically deterministic. The assessment includes risk insights for example by positioning different event into different event classes. Although the SAR assessments include a large degree of conservatism, the conservatism can vary from case to case and is not necessarily proportional to the public risk (risk for core damages or radioactive releases).

The TS are developed for assuring safety during operation and are part of the licensing basis for the plant. The original TS were based on deterministic analyses and engineering judgments (and to some extent risk evaluations).

Specifically, the TS present information on allowed outage times (AOT) and surveillance Test Intervals (STI) for different safety related equipment. The AOT and STI for specific equipment are dependent on the importance of this equipment. The TS also present the actions to be taken in case the AOT cannot be met, e.g. shutting down the plant to hot or cold standby conditions.

As said above, the main purpose of the TS is to guarantee that the basis (initiating data) for the SAR assessment is valid. There is also an expectation that a plants TS conditions imply a certain risk level. This means that the different TS conditions shall represent a similar risk to the public. However, the different TS conditions developed strictly on the existing SAR and its event classification will not necessarily represent the core damage frequency (CDF) and Large Early Release Frequency (LERF) in a balanced and proportional way.

As the probabilistic safety assessment (PSA) has developed over the years, it has demonstrated to be a useful tool for evaluating many aspects of the TS from a risk point of view and in that way contribute to the development of conditions that are balanced and better represent the real risk.

Existing PSAs are not primarily developed to be a basis for TS conditions evaluation. An existing PSA may therefore not include all aspects valid for the TS conditions. It is very important that all such aspects are either included in the plant specific PSA study to be used in TS condition evaluation or taken care of by complementary means.

PSA is an excellent tool to be used to verify the risk importance, and thereby possibly relaxation (or strengthening), of TS conditions. However, PSA is not sufficient in itself for defining which equipment that shall or shall not have TS requirements.

The basic objectives in a PSA based analysis and modification of TS conditions can be summarized as follows [1]:

- to assure that any changes in TS do not compromise the basic intent of the TS in assuring the safety margins during normal and accident conditions
- to obtain a quantitative assessment of the risk impact of the changes and to provide a quantitative basis as a justification
- to make it acceptable and defensible to the regulatory body whose approval is usually required.

The reasons for making changes to the TS conditions may be several, for example plant experience, adaption of standard TS or optimisation of TS conditions with PSA. The purpose of this guidance is to embrace all reasons for an update and to provide a method to evaluate the impact on safety.

1.2 Purpose

No Nordic country has yet developed guidance for risk-informed development and assessment of the TS conditions. In the US several guidance documents exist. These are primarily developed by the PWR and BWR owners groups (BWROG, WOG etc). The NRC Regulatory Guide RG. 1.174 is applied for addressing changes in the TS conditions.

Several different approaches are used for quantifying the importance of changes to the TS conditions. Definition of a new very rigid approach is considered as a potential problem, since this may prevent development of alternative approaches. It is however vital that the characteristics of any method, its results and documentation meet certain minimum requirements.

The purpose of this guidance document is hence to provide guidance and requirements on how risk-informed methodologies are to be used to change existing or specify new AOT and STI TS conditions. The requirements cover input data, methods, results and result presentation, documentation and criteria for introducing changes. The intent is that any method meeting the requirements shall be possible to use.

1.3 Scope

An approach for using PSA for evaluating proposed changes in the TS conditions is described in detail in the RG 1.174 [2]. RG 1.174 states the following requirements for evaluation of TS condition changes:

- The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change
- The proposed change is consistent with the defence-in-depth philosophy
- The proposed change maintains sufficient safety margins

- When the proposed change result in an increase in core damage frequency or risk, the increase should be small and consistent with the Commission´s Safety Goal Policy Statement
- The impact of the proposed change should be monitored using performance measurement strategies

RG.174 then presents a process with four elements as shown in figure 1.

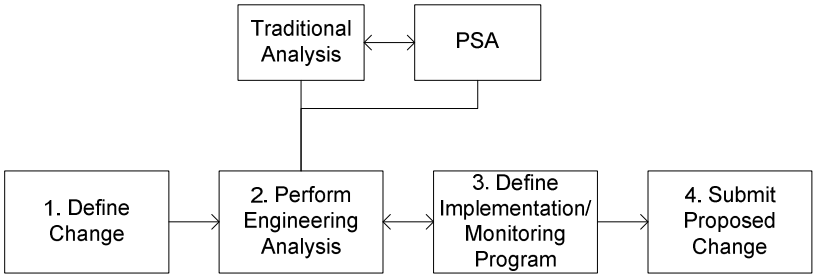


Figure 1 Principal Elements of Risk-Informed, Plant-Specific Decision-Making from RG 1.174 [2].

Briefly the different elements include:

- Element 1: Define the proposed change. All aspects of the proposed change shall be identified. All structures, systems and components (SSCs), procedures and activities that are covered by the proposed change shall be evaluated. Specifically the original reasons for the program (the TS conditions) shall be understood.
- Element 2: Perform engineering analysis. The analyses include traditional engineering analyses and PSA. The licensee shall verify that the fundamental safety principles of the plant are not compromised. Safety margins and defence-in-depth may be affected by the proposed change and the licensee should therefore re-evaluate these to support the licensing basis change. The PSA result changes shall meet defined acceptance criteria and uncertainties shall be evaluated.
- Element 3: Define implementation and monitoring program. The purpose is to avoid an unexpected increase in number of failures due to unanticipated degradation. An implementation and monitoring plan should be developed to ensure that the engineering evaluations conducted remain valid.
- Element 4: Submit propose change.

The NRC procedure described above is considered to be a good outline of the whole TS evaluation process.

The engineering analysis focuses on two main areas; traditional engineering considerations and evaluation of risk impact. Traditional engineering considerations include verifying that the defence-in-depth principle is main-

tained and that the safety margins are as well. For the defence-in-depth for example it must be demonstrated that the balance between prevention of core damage, prevention of containment failure and consequence mitigation is reasonably preserved after changing the TS. The changes should not render simultaneous outages possible that would weaken the principles of system redundancy and diversity.

Regarding safety margins, codes and standards have to be met also after a TS condition change. The SAR acceptance criteria must also still be met. As an example, a new AOT is not allowed to compromise a safety function success criteria.

This guidance focuses on the use of PSA in the risk evaluation part of element 2 in the process.

The use of PSA and PSA methodology can span many types of equipment. A plant specific PSA model is generally focused on the technical safety of the plant, and all equipment is therefore not modelled. PSA can be used to evaluate other types of equipment (not represented in the PSA today). However, the risk measure to be used in the evaluation is likely to be different. This guidance document is restricted to the evaluation of equipment in the PSA that can have effect on the Core Damage Frequency (CDF) and the Unacceptable Release Frequency (URF).

2. Relation to Relevant References

2.1 Relation to Swedish Legislation

The Swedish Radiation Safety Authority statutes SSMFS 2008:1 [3] (chapter 4 §5 including its general recommendations), states that all principal changes in the safety documentation and also all consequences of technical and organizational modifications that can affect the conditions therein should be analyzed with regard to safety. This includes changes to the TS. The documentation to be submitted to the authority should include an assessment of the safety related consequences. This implies use of an existing PSA or adapted PSA application, to demonstrate the safety impact of the change.

SSMFS 2008:17 [4], §16, also defines that exemptions from deterministic requirements only are acceptable if it can be demonstrated that the resulting risk contribution is very small.

The general recommendations to chapter 3 §1 and chapter 3 5§ in SSMFS 2008:13 [5], provides requirements on quantitative methods, e.g. PSA, and describes how PSA can be used in the quantification of relative risk.

2.2 Relation to International Guidance

2.2.1 NRC

The United States Nuclear Regulatory Commission, NRC, adopted already in 1995 a policy statement that in broad outline says that the use of PSA insights should be increased in all regulatory matters and be used in a manner that complements the traditional deterministic approach and supports defence-in-depth. The most important Regulatory Guides with regard to risk-informed TS condition evaluation are:

- RG 1.174 - An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis [2]
- RG 1.175 – An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing [6]
- RG 1.177 – Risk-Informed Decision- An Approach for Plant-Specific, Risk-Informed Decisionmaking:Technical Specifications [7].

RG1.174 forms the basis for risk informed decision making in the reports 1.174-1.177. The basis for evaluation of changes in TS conditions is presented, for example that both CDF and LERF shall be used. It is stated that the accepted changes in risk shall be small and that cumulative effects of several changes shall be considered. The methods used must be well docu-

mented and it shall be possible to perform a normal review of the method. The whole process for evaluation of user initiated plant changes is presented.

Standard Review Plan (SRP) section 16.0 [8] provides general guidance for review of TS. Section 16.1 [9], is used as reference from the SRP 16.0 for review of risk informed applications.

SRP Section 19.1 [10] provides general guidance for evaluating all types of risk-informed regulatory changes and for determining the technical adequacy of PSA results for risk informed activities.

Appendix 3 to this Guidance presents a list of other reference documents published by the NRC that contain interesting information with regard to risk-informed evaluation of TS conditions.

The guidance by ASME [16] sets requirement on PSA with reference to quality aspects on PSA. This is further discussed in section 3.1 of this Guidance.

2.2.2 IAEA

The International Atomic Energy Agency, IAEA, has several publications related to risk based/risk informed analysis of the TS conditions.

IAEA-TECDOC-1200, *Applications of probabilistic safety assessment (PSA) for nuclear power plant* [11], has a section devoted to "Use of PSA in connection with NPP technical specification (TS)" where the use of PSA to support modifications and to AOTs and STIs are discussed.

IAEA-TECDOC-729 [1] discusses how PSA can be used to improve technical specifications, presents an overview of methods and data requirements and provides examples of some applications. The document vas published already in 1993 though, and is considered mainly as orientation.

IAEA-TECDOC-1138 [12] includes several papers discussing the use of PSA for TS conditions evaluation and optimization.

In Safety Standard Series draft DS394 [13] requirements on risk-informed TS are briefly discussed.

A number of other reference documents published by IAEA that could be of interest with regard to risk-informed evaluation of TS are listed in Appendix 3.

2.2.3 STUK

In Finland the Radiation and Nuclear Safety Authority's regulatory guides, the YVL-guides, present requirements on TS and PSA. YVL-1.8 [14] presents how STUK regulates repairs, modifications and preventive mainte-

nance of SSCs at nuclear facilities during operation. The guide further describes the obligations related to this work imposed on power companies.

YVL-2.8 [15] sets requirements for the use of PSA in the safety managements. The Guide states that "*The technical specifications shall be reviewed by PSA in such a way that the coverage and balance of technical specifications are ensured. The review must cover all operating states of the plant. Especially such failure states, in which the change of operating state of the plant may result in a greater risk than the repair of the plant during operation, shall be reviewed with PSA. The results of the review shall be submitted to STUK in conjunction with the application for an acceptance of technical specifications.*"

As such, the STUK guidance does not recommend or require specific methods for the risk-informed TS conditions evaluation. In this way the operators have some flexibility in developing the analysis methodology, but the proposals for any risk-informed TS condition changes naturally are assessed and evaluated by STUK.

3. General Requirements on the PSA model

The PSA model has to meet certain general requirement to be suitable for TS condition evaluation. Quality of the PSA and requirements on modelling of SSCs are discussed below.

3.1 Quality of the PSA

The quality of a PSA analysis used to support an application is measured in terms of its appropriateness with respect to scope, level of detail, and technical adequacy. The scope, level of detail, and technical adequacy of the PSA are to be commensurate with the application for which it is intended and the role the PSA results play in the integrated decision process. The more emphasis that is put on the risk insights and on PSA results in the decision-making process, the more requirements have to be placed on the PSA, in terms of both scope and how well the risk and the change in risk is assessed.

One basic requirement is that the PSA should realistically reflect the actual design, construction, operational practices, and operational experience of the plant and its owner. This should include the licensee's voluntary actions as well as regulatory requirements, and the PSA used to support risk-informed decision-making should also reflect the impact of previous changes made to the licensing basis.

The documentation of the risk-informed TS condition evaluation should include:

- A description of the PSA used, in terms of the process to ensure quality and the scope of the PSA, and how limitations in quality, scope, and level of detail are compensated for in the decision-making process. (List all known conservatism in the study and grade the effects of the conservatism. If the existing conservatism give significantly improper risk estimate for certain functions in the risk evaluation this has to be considered.)
- Reference to process or system based instructions and routines that the licensee follows for risk-informed applications

Neither Sweden nor Finland strictly follows any specific PSA model standard today. In the US the American Society of Mechanical Engineers, ASME, has published the *Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications* [16], applicable for internal events during full power operation. Draft guides for external events and low power and shutdown conditions are under development by ANS, the American Nuclear Society.

NRC has issued a regulatory guide, RG 1.200 [17], describing one acceptable approach for determining whether the technical adequacy of the PSA, in total or partly, that are used to support applications, is sufficient to provide confidence in the results, such that the PSA can be used in regulatory decision-making.

IAEA-TECDOC-1511 [18] describes an approach for determining the quality of PSAs for various applications, including risk-informed evaluation of Tech. Specs. condition changes.

3.2 Requirements on PSA Modelling

One of the requirements for risk-informed TS conditions evaluation is that the PSA model must reflect the SSCs concerned in sufficient ways to be able to use it.. The discussion of SSCs are divided into the following groups:

- SSCs represented in the PSA model
- Safety SSCs not explicitly represented in the PSA model
- Non-safety SSCs not explicitly represented in the PSA model

3.2.1 SSCs Part of the PSA

It is obvious that only SSCs that are represented in the PSA model can be evaluated. It is however not sufficient that the SSCs are represented in the PSA model to state that the SSC is represented in a sufficient way. The representation may be partial, and this must be considered when a TS condition change is being evaluated.

The following questions need to be answered:

- Does the PSA model, with regard to the SSC, represent all functions which are relevant in the SAR? E.g. are isolation valves represented for containment isolation or are they represented only in case of pipe rupture outside the containment? If no, remodel or make separate assessments.
  - Are all functions for the SSCs as stated by SAR represented by the PSA model? If no, is it of significant importance?
  - Is the object(s) being evaluated represented in a manner that is consistent with the SAR? E.g. the consequence mitigation systems may be taken into account in a way that is not in line with the SAR.

The evaluation of the TS conditions shall include documented answers to the above questions.

Some objects are more likely to be consistently represented by the PSA model than others. Normally active components are represented in a detailed way, e.g.

- Pumps

- Motor operated and Pneumatic Valves
- Diesel generators
- Fans
- Compressors

Some objects may only be represented in the PSA model for limited parts of the functions they represent. These are usually not relevant to analyze with PSA. Examples of such objects are :

- Instrumentation
- Indication
- Relays

This equipment can be analyzed with PSA but that would require a thorough investigation to verify that the functions for the objects are represented in a sufficient way. Example, level measurement is used in the control room by the operators and this is generally not represented by the PSA model (in a quantifiable way).

Passive components can also be analyzed with PSA, but they are normally only modelled indirectly and would require an additional effort. Testing of passive components is not part of the TS conditions.

3.2.2 Safety Objects Not Part of the PSA

Generally, if an object is not part of the PSA it cannot be evaluated with PSA.

However, the PSA model normally groups several mechanical objects/components into larger groups of objects (main components), e.g. diesel generator. If the subcomponent is part of a “main component” then the evaluation can still be performed as described in the previous section. The subcomponent shall be represented by one main component and it must be clearly stated which main component that is used.

In some cases it is also possible to group a series of component as one component. An example is a set of valves in a pump line, where the PSA does not explicitly represent these objects individually. Also in this case it is needed to define and describe which main component that can be used and why it is relevant to use that main component.

3.2.3 Non-Safety Equipment and Not Part of PSA

Non-safety equipment (safety class 4) is not necessarily part of the TS.

There are also cases with non-safety systems that are covered by the TS conditions due to their overall importance for safety. Examples are the conse-

quence mitigation systems. Non-safety systems that are part of the TS shall be evaluated with the same requirements as are applied for the evaluation of safety related objects/equipment.

3.3 Summary – Component Categorization

The first step in the component categorization is to list all SSCs being addressed in the evaluation. This list gives an overview of the scope and will also facilitate the review. It must be possible to review the evaluation without being familiar with the PSA models' limitations.

The list(s) is used in support of verifying robustness and completeness.

1. **Robustness:** There is a risk that TS conditions are relaxed when the analysis is based on the assumption of availability of certain SSCs that not have any TS condition (operability requirements, test frequency, allowed outage time).. The results of the Tech. Specs. evaluation can then be questioned. The basis for the evaluation must be robus.
2. **Completeness with regard to the evaluated SSC:** The SSCs being evaluated requires all relevant aspects to be taken into account in the analysis, i.e. the SSCs are represented in a sufficient manner (see description in SSCs part of the PSA section 3.2.1)

Some more comments on robustness and completeness are given below.

Robustness of the analysis

Generally, the evaluation of the TS conditions shall be based on the full scope PSA, including safety and non-safety systems (including mitigation systems). However, this requires that the robustness of the model can be verified.

This means to verify that changes in assumptions with regard to system availabilities will not significantly change the results of an evaluation. The list of important SSCs gives an overall overview of the content in the current PSA and also an indication of which SSCs that are of significance for the overall plant safety level from a PSA point of view.

The evaluation shall be made on a sufficiently detailed level to determine if the relevant SSCs of importance are covered by the TS conditions. This means for example that an evaluation can first be made on system level, and if a system has a significant safety importance (above 1% importance with regard to the chosen risk measure) a refined study is required of the system. This refined study of the system (and functions within that system) should ensure that relevant requirements are set on the system (parts of the system).

The evaluation may show that SSCs being part of the PSA but not the TS have a high safety significance. It should then be considered to add these

SSCs to the TS. If this is not done – the analysis must be complemented with a justification with respect to that SSC and the robustness of the model used for the TS condition evaluation.

Completeness with regard to the evaluated SSC
When the robustness of the PSA model is established, the completeness of the model with regard to the current TS condition evaluation must be shown. This means a verification that all relevant functions described by the TS conditions for the SSCs, are represented by the PSA in a sufficient manner. This can be very difficult for a reviewer to verify without a significant effort and hence this information must be provided in the documentation of the analysis.

The definition of the SSCs being evaluated must include the following:

1. The functions for which it is required according to the TS
2. Which of these functions that are represented by the PSA model.
3. A statement whether the function is represented completely or only partially by the PSA.
4. The type of criteria that have to be used to verify the system function, i.e. the PSA end state (CD/UR) that represents the function in the evaluation.

Using the containment isolation valves as an example SSC, the functions are:):

- Isolation of containment in case of feed water pipe rupture outside the containment
- Isolation of containment in case of core damage (PSA level 2)

It is not necessary that all functions , for which the SSC is used, are represented in the PSA model. A decision to leave out functions shall be justified in the documentation of the analysis. An example is presented below:

SSC	TS Function	In PSA	Consequence	Comment
415Vx	Main feed water isolation (pipe rupture)	X	Core damage	
	Containment isolation	(X)	Unacceptable release	Not fully represented, only in case if pipe rupture in 415. No release through system is assumed in PSA (if no pipe rupture). PSA is therefore acceptable.

4. Properties of Methods for Risk Informed TS Condition Evaluation

First some general requirements on methods are discussed and then specific requirements for evaluation of Surveillance Test Intervals (STIs) and Allowed Outage Times (AOTs) respectively are discussed.

Examples of methods for STI and AOT analysis are presented in appendix 1.

4.1 General Requirements on Methods

An evaluation of TS condition changes must meet some basic requirements:

- The evaluation shall be transparent and easy to communicate.
- The evaluation shall be based on known principles.
- The model must reflect the different aspects related to the TS condition being evaluated

This means that the method(s) used for evaluation shall be based on known principles and possible to understand and communicate, both for plant management and the authority. If the methods are newly developed a sufficient time must be considered for the acceptance of the method.

The method must also be able to calculate the change in the overall plant risk taking into account all concurrent changes to the STIs and AOTs.

4.1.1 Plant Operating Mode (POM)

Normally the plant operating mode for which a change to a STI or an AOT is proposed should be evaluated. TS condition changes related to full power should be evaluated using the full power PSA and changes related to shutdown using the shutdown PSA. However, if for example, changes are proposed for any SSC with significant importance for both full power and shutdown, the effect on both operating modes must be addressed.

4.1.2 Initiating Events (IE)

Generally all initiating events in the full scope PSA should be included in the evaluation. This means a full set of internal, external, and area events. However, if there is a large contribution to the overall CDF/unacceptable release frequency from area and/or external events, a sensitivity study may be performed covering these issues instead. Conservatisms in the area and/or external event analysis should then be evaluated and their effect on the result commented.

A screening approach may be used to screen out initiators that have no effect on the results. This screening process should then be documented.

4.1.3 Sensitivity and Uncertainty Analyses

Sensitivity studies are required. An important part of the TS condition evaluation is to identify the areas for which sensitivity studies are required. A decision to not perform sensitivity studies and the justification shall be stated in the documentation of the evaluation.

Parametric uncertainty analyses are not required.

For STI changes, the possible effect on failure data used must be addressed, see section 4.2 below.

4.2 Evaluation of Surveillance Test Intervals

When evaluating a STI the significant SSCs that are affected by that test shall be listed. The SSCs in the PSA model that have a relation to the test shall be stated. Example:

STI	SSC affected	PSA model representation	Comment	Can be evaluated
Start test ECC	323P1	323P1		Yes
Capacity test ECC	323P1, 323V1, 323V3	323V1, 323V3	323P1 is represented by start test.	No (without further justification)

The following should especially be considered when evaluating changes to the STIs:

- Modelling of test types

  For an evaluation of a STI the test must be represented in the PSA model in a sufficient way. Normally one test is chosen as representative in the PSA and this is hence the one that can be evaluated without further evaluation (see table above for example and next bullet for relation between different tests).

- Relation between different test types

  In cases where there are several different test types for a component where only one is represented fully in the PSA, a justification of changes in the test types that not are represented by the PSA shall be provided (e.g. the relative displacement of the tests must be preserved in case of a prolonged interval).

- SSCs with small importance in the PSA model

  If the object(s) involved in a test has a low significance in the PSA, the test interval can be prolonged indefinitely with very small effect on the PSA results. The evaluation should therefore consider the use of an appropriate maximum test interval. This issue is also related to effects on failure data, see below.

- Effects on failure data

  A change of a test interval must include an analysis of effects on the failure data used. If the failure data not is affected when prolonging or shortening an interval, it must be clearly stated why the data is still applicable. Prolonged intervals for example can have an effect on component lubrication while shortened intervals, on the other hand, may lead to test wear-out of the component. If the test types are changed it should be demonstrated that the new test types are at least as efficient as the previous and that component availability not will be degraded. Principles for experience feedback and collection of new empirical data have to be documented if new data are used during the evaluation.

- Effects of Common Cause Failures, CCF

  The potential effect on common cause failures shall be discussed.

- Unavailability during test

  Unavailability during test should normally not be considered as a reason for prolonging the test interval without a separate discussion. Personnel is available and it can be assumed that the equipment can be made operable if needed. However, if a SSC is tested very often, unavailability during that test might be relevant to consider.

- Influence on initiating events

  The possibility that certain tests may have influence on initiating events and initiating event frequencies must be taken into consideration when proposing changes to STIs.

- System configurations

  If different system configurations are possible, the analysis shall take this into consideration.

- Testing schemes

  The use of sequential or staggered testing schemes shall be reflected in the analysis.

4.3 Evaluation of Allowed Outage Times

In the evaluation of an AOT the SSC outage must be represented in the PSA model in a sufficient way. It must be demonstrated how this is represented and also how the length of the outage time has been estimated and the effect the change has on the SSC unavailability.

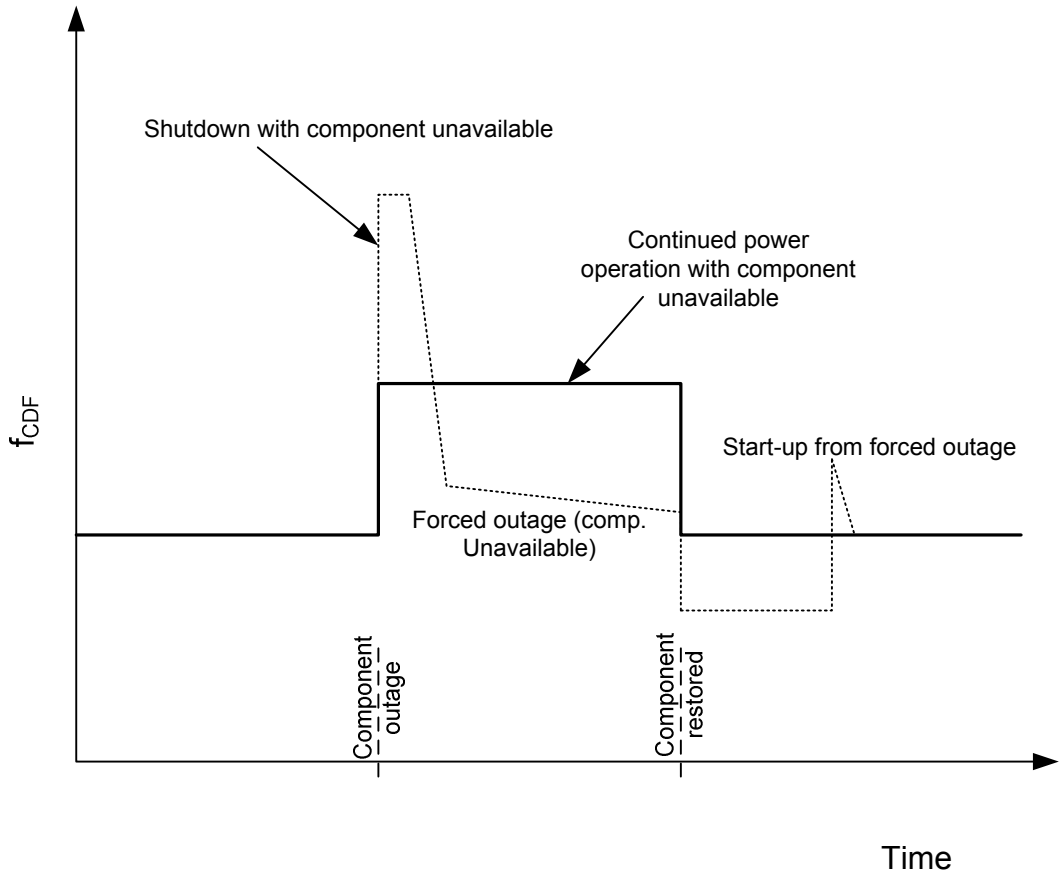


Figure 2 Two different strategies with component unavailable illustrated, continued power operation or shutdown and repair at forced outage and then start-up again. The total risk is the accumulated risk below each line (area).

The evaluation shall focus on the risk of continued operation at the same plant operating mode (see figure 2 above). If a prolonged AOT means an increase in risk that is small (see section on acceptance criteria), then the change in AOT is acceptable. If the change in AOT is not acceptable only by looking at continued operation of the plant, the change may be justified if it can be shown that the increase in risk during power operation can be motivated by a decrease in risk taken in the low power phase. This will however require that the low power include LCO induced shutdown. It shall be possible to quantify a total risk measure (e.g. core damage frequency) for all operational modes separately before and after the changes.

As a sensitivity analysis a bounding assessment using the full AOTs should be considered. This might be a somewhat conservative approach but will give an upper-bound estimate of the risk impact from AOT changes.

Some areas that need special attention are:

- Evaluation of expected real outage times

  Prolongation of AOTs must include an evaluation of effects on the expected real outage times in case this is based on statistics in the PSA. A prolonged AOT may for example involve changes in stock-keeping of spare parts.

- Mitigating/compensating actions

  Compensating actions may be taken into account. A compensating action may for example be a redesign of the system or test of redundant equipment. The importance of compensating actions shall be discussed.

- System configurations

  If different system configurations are possible, the analysis shall take this into consideration.

- Effect on Common Cause Failures, CCF

  The potential effect on common cause failures shall be discussed, so that the risk for a situation where redundant equipment is unavailable due to the same reason can be ruled out. This is e.g. achieved by testing of redundant equipment.

- Simultaneous AOTs

  Cases where the proposed change in AOT significantly increases the risk for simultaneous failures (and thereby force the plant into shutdown with more than one component unavailable) shall be discussed.

4.4 Define Risk Measures to be Used

For each STI or AOT (and hereby SSC) included in the analysis the evaluation criteria must be defined,i.e. if the change shall be evaluated with regard to its impact on CDF, URF or other PSA model results. This is decided in accordance with section 3.3.

For most SSCs the CDF constitutes the main risk measure and the proposed changes can be considered acceptable if they do not significantly affect the CDF. It then has to be demonstrated that these SSCs do not perform or support a safety function of importance to the prevention of radioactive release during severe accidents. If they do, the URF must be evaluated as well (see discussion in section 3.3). The unacceptable release is in Sweden defined as a release larger than 0.1 % of the core inventory of a 1800 MW reactor. This criterion was originally established when designing and installing the consequence mitigation systems in the Swedish BWR units. The corresponding requirement in Finland is expressed as 100 TBq Cs-137.

SSCs only relevant for severe accident management should be evaluated with URF as the main risk measure and if the frequency is not significantly affected, then the changes accordingly can be considered acceptable.

It is not certain that the CDF or the URF represents a relevant risk measure for the actual SSC being evaluated. Other risk measures may therefore have to be defined, for example in an STI evaluation for isolation valves the availability of the system function may constitute the main risk measure.

5. Change Acceptance Criteria

If it can be demonstrated that the proposed changes do not significantly affect the identified risk measure (i.e. in most cases the core damage frequency (CDF) or Unacceptable Release Frequency (URF) the proposed changes can be considered acceptable.

- The definition of a significant change is based on value of the absolute frequency and the change in frequency.

Generally, a best estimate of the CDF less than 10 times of the safety goal[1] for the core damage frequency per year is considered acceptable from a PSA point of view. Accordingly, a best estimate of the URF less than 10 times the unacceptable release frequency defined as the safety goal is considered acceptable. The acceptance criterion applies to the total CDF/URF, i.e. including all plant operating modes and all initiating events. Any missing contributors to the total CDF/URF, for example excluded area and/or external events, have to be estimated and added or their exclusion being justified.

There may be cases with frequencies above the CDF/URF target values (safety goals). One reason for allowing that the frequencies exceeds the safety goals for core damage and unacceptable release respectively is that all changes are not possible to quantify with the PSA methodology. Not all safety improvements are possible to represent with PSA. The documentation of a TS condition change therefore also has to consider other relevant qualitative and quantitative information – e.g. improved maintenance and test instructions and other compensatory measures.

In addition to the absolute frequency, the change in risk shall be presented. The change is quantified as the risk after the change subtracted with the risk prior to the change(s). If there is an increase in risk above 10% of the safety goal for CDF and URF, the increase is considered significant. An increase in risk is acceptable if it can be based on other motives than PSA. That is, an increase in risk solely based on PSA optimization is generally not acceptable.

This combination of absolute risk and relative risk criteria is similar to what is stated in RG 1.174 [2]. The limits have however been adapted to what is considered acceptable in the Nordic countries). The idea is to have both an absolute criterion, so that many small steps will not automatically be considered acceptable and also so that the initial state for the plant is taken into

[1] Safety Goal – in this guidance document the safety goal numbers are those that are officially declared by the management of the Nordic NPPs and those declared by the regulatory bodies SSM and STUK. This guidance does intentionally not interpret the safety goals described in INSAG 3, INSAG 8, INSAG 12/75 INSAG 3 and in the older CB3 and CB5 documents of IAEA.

consideration, and a delta criterion, to identify when one change is very significant and may require a thorough discussion.

The figures 3a and 3b below presents the acceptance criteria.

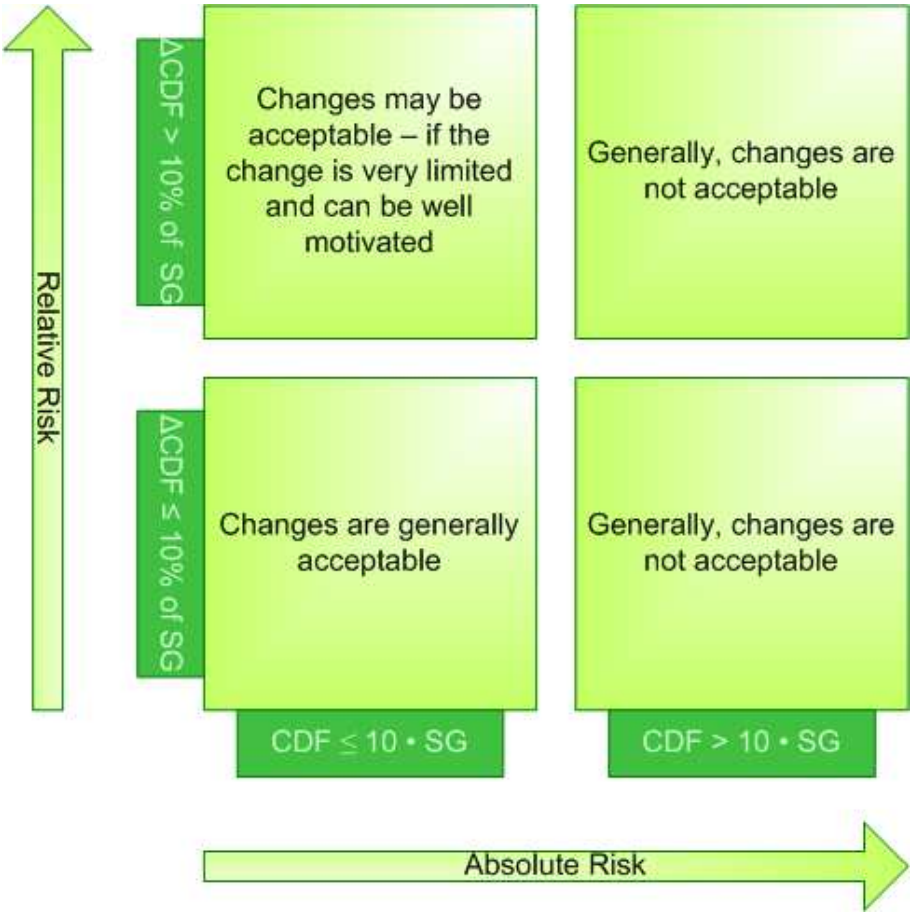


Figure 3a Acceptance criteria for CDF (core damage frequency). SG means Safety Goal for CDF.

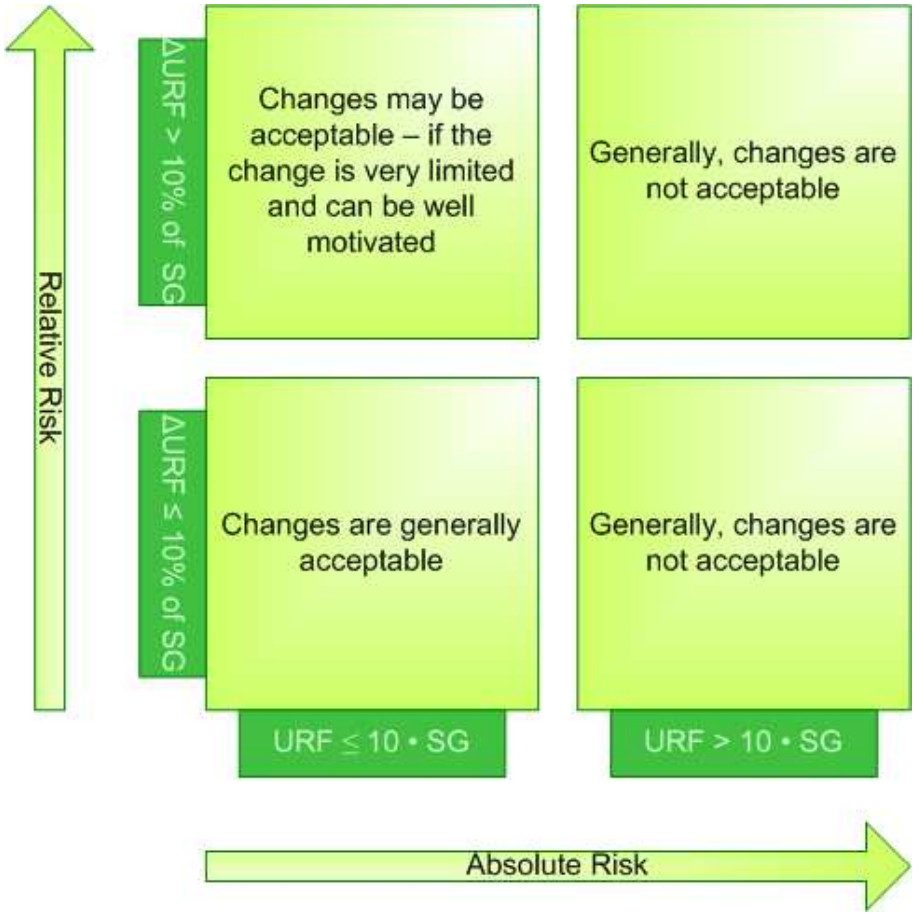


Figure 3b Acceptance criteria for URF (Unacceptable Release Frequency). SG means Safety Goal for URF.

6. How shall an Analysis be Documented

The requirements on documentation stated in this guidance are only for the process element that is related to the PSA evaluation.

The documentation of a TS evaluation with PSA shall comprise at least the following:

- Description and background to the proposed change(s). The presentation should cover the present and changed TS condition as well as the stated demands in the SAR and possible changes in the safety documentation.
- Statement on the applicability of the PSA for the intended evaluation
- Verification of important SSCs (see section 3.3)
- Analysis of relevant SSC implementation in PSA (see section 3.3)
- Definition of risk measure to be used (based on previous)
- Presentation of method
- Discussion about important issues for the evaluation (see examples in section 4.2 and 4.3)
- Pre-analysis (including effect on data, CCF, model etc). Special emphasis shall be put on verification of data when e.g. STIs are changed.
- Analysis, considering the issues discussed.
- Sensitivity analyses (if considered not necessary, this shall be stated, and the reasons for this)
- Evaluation of results and comparison with acceptance criteria. The result presentation should show the result before and after the Tech. Specs. condition modification.

Guidance on what a US licensee is expected to present to NRC in a risk-informed application is presented in Standard Review Plan section 16.1 and 19.1 ([9] and[10]).

7. Requirements on Implementation and Monitoring Program

It is important to closely monitor components for which the STIs are changed when a new test plan is implemented. The monitoring program shall be able to detect, as early as possible, any test cycle related effects on the performance of the components.

Significant changes in AOT shall be monitored via a yearly risk follow up.

Specifically changes that are related to the risk for common cause failures (CCF) shall be monitored.

8. References

[1] IAEA TECDOC Series No. 729, Risk Based Optimization of Technical Specifications for Operation of Nuclear Power Plants, December 1993

[2] NRC Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, November 2002

[3] SSMFS 2008:1, The Swedish Radiation Safety Authority's Regulations concerning Safety in Nuclear Facilities, December 2008

[4] SSMFS 2008:17, The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power reactors, January 2009

[5] SSMFS 2008:13, Strålsäkerhetsmyndighetens föreskrifter om mekaniska anordningar i vissa kärntekniska anläggningar. Strålsäkerhetsmyndighetens allmänna råd om tillämpning av föreskrifterna (SSMFS 2008:13) om mekaniska anordningar i vissa kärntekniska anläggningar, January 2009

[6] NRC Regulatory Guide 1.175, An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing, August 1998

[7] NRC Regulatory Guide 1.177, An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications, August 1998

[8] U.S. Nuclear Regulatory Commission Regulatory Standard Review Plan Section 16.0, Revision 2, Technical Specifications, March 2007

[9] U.S. Nuclear Regulatory Commission Regulatory Standard Review Plan Section 16.1, Revision 1, Risk-informed decision making: Technical Specifications, March 2007

[10] U.S. Nuclear Regulatory Commission Regulatory Standard Review Plan Section 19.1, Revision 2, Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, June 2007

[11] IAEA TECDOC Series No. 1200, Applications of probabilistic safety assessment (PSA) for nuclear power plant, February 2001

[12] IAEA TECDOC Series No. 1138, Advances in Safety Related Maintenance, March 2000

[13] IAEA Safety Standard Series DS394, Draft 2, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, June 2007

[14] YVL-1.8, Repairs, modifications and preventive maintenance at nuclear facilities, October 1986

[15] YVL-2.8, Probabilistic safety analysis in safety management of nuclear power plants, May 2003

[16] ASME Standard RA-S-2008, Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications (an addenda RA-Sa-2009 is also available)

[17] NRC Regulatory Guide 1.200, An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities, March 2009

[18] IAEA-TECDOC-1511, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants, July 2006

[19] NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications, 1994

[20] Optimization of Allowed Outage Times using PSA, STUK, I. Niemelä, presented at Slottsmöte 2003, Naantali, June 10-11 2003

[21] Evaluation of Olkiluoto BWR techspecs by using plant specific PSA, R. Himanen, J. Pesonen, P. Pyy, M. Tupala and J. Holmberg, presented ANS PSA 2008 Topical Meeting at Knoxville, Tennessee, September 7-11 2009

[22] W.E. Vesely, Principles of resource-effectiveness and regulatory-effectiveness for risk-informed applications: Reducing burdens by improving effectiveness, Reliability Engineering and System Safety 63, pages 283-292, Elsevier Science, 1999

Appendix 1 – Description of Technical Specifications and definition of terms

Information summed up in this attachment is written by the Dept. of Nuclear Power Plant Safety at Swedish Radiation Safety Authority (SSM)

Technical Specifications (TS) for the Nordic light water reactors (LWR) define the limits and conditions for operation, and assure that they fulfil the safety levels for which they were originally designed. The current TS were originally developed using engineering and deterministic considerations.

TS are part of the safety documentation – FSAR/SAR in Swedish and Finnish NPPs. Any changes have therefore to be reported to and approved by the respective regulatory body in these countries.

The Swedish and Finnish BWR TSs are built according to a traditional Swedish TS standard, developed at the time when the first ASEA ATOM reactors were designed.

The Swedish PWR TSs are nowadays built according to the Westinghouse standard TS (STS), documented in the NUREG-1431 (see Appendix 3 for information about reference).

The TS for the 5th Finnish NPP will also be built according to a STS format.

Structure of Nordic conventional LWR TS is to present the licensed requirements for:

- safety limits
- limiting conditions for operation (LCO), which includes the AOT or CT for required actions for maintenance, repair and surveillance requirements (SR)
- design features
- administrative controls

TSs of today are increasingly being adjusted using insights from probabilistic or risk-based analysis. Risk-based applications and reviews have mainly focused on risk evaluation of LCOs and SRs, which are important part of the TS requirements to ensure safe operation and they are also more prone for risk evaluations than other parts of the TS.

At modernization project of e.g., Swedish NPPs due to requirements in the SSMFS regulations on defences against CCFs, increased safety redundant

and/or diversified trains are installed. These plant modifications will affect the content of the present TSs, especially the requirements on AOTs and STIs due to that more components have to be tested and maintained and also that there might be multiple unavailabilities due to testing and equipment failures.

PSAs for the shutdown operating mode performed so far, indicates that the CDF is at about the same level or above as the CDF for the full power mode. This fact stresses the need of a good PSA for low-power modes and that LCOs in the TSs for all operational modes are thoroughly analyzed with regard to risk. It can therefore also be assumed that the risk impact of LCO changes important for low power modes also will have high risk impact. The TS for low-power and refuelling mode should therefore also reflect all safety important LCOs, AOTs, STIs and administrative controls.

This guidance explains how an affected LCO requirement is risk evaluated with PSA methods, e.g., which risk measures are recommended, risk evaluation of the LCO condition for all plant operating modes, data impact, CCF considerations, needed qualitative information to be documented.

At the time for a TS application e.g., in Sweden to the SSM, the application has to include a preliminary documentation and revision pages on the affected FSAR/SAR and TS chapters describing the changes of e.g., requirements, systems analyses. The IAEA TECDOC-1200 [11] gives a good explanation of what is basically ruled in TS. If not clearly stated elsewhere, the Standard Review Plan (SRP) section 16 [9] and 19 [10] give good information on what should be submitted in a risk-informed TS application.

Definition of TS terms

Some of the most common terms expressed and used in the TS are described below.

allowed outage time. Allowed outage time (AOT) gives the maximum time for repair of safety related equipment in a given operational state. The plant must usually be placed to in safer operational state, if the operability of the faulty equipment is not reached within its AOT. For the faults detected in the power operation state, any repair time exceeding the AOT will require a controlled shutdown in order to complete the repair (usually cold shutdown state). AOT is often also called for the allowed completion time (CT). **Source:** IAEA TECDOC 729

baseline risk. This is the risk level of the plant during power operation assuming that no failures are detected in safety systems and no subsystems are isolated for maintenance. If a demand occurs during the baseline state, the latent or undetected faults in the standby period and failures during the mission time still contribute to the overall system failure probability, and to the baseline risk level. Temporary outages of equipment in safety systems will increase the total plant risk level over the baseline risk level. **Source:** IAEA TECDOC 729

corrective maintenance. Corrective maintenance (CM) is unscheduled maintenance to repair any random failures or degradations. **Source:** IAEA TECDOC 729

in-service inspection. Inspection of structures, systems and components undertaken over the operating lifetime by or on behalf of the operating organization for the purpose of identifying age related degradation or conditions that, if not addressed, might lead to the failure of structures, systems or components. **Source:** IAEA Safety Glossary 2007

inspection. Actions which by means of examination, observation or measurement determine the conformance of materials, parts, components, systems and structures, as well as processes and procedures, with defined requirements. **Source:** IAEA Safety Series Report nr 110

item important to safety. An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. **Source:** IAEA Safety Glossary 2007

limiting condition for operation (LCO). The limiting conditions for operation (LCOs) are a part of the plant's technical specifications. These rules are designated to maintain the plant operation within the bounds of safety analyses. The LCOs specify requirements on the number of subsystems that should be operable at different operational states and the allowed outage times for inoperable equipment. These also define specific action statements if such requirements cannot be met. **Source:** IAEA TECDOC 729

Limiting Conditions for Operation (LCOs) specify minimum requirements for ensuring safe operation of the unit. The ACTIONS associated with an LCO state Conditions that typically describe the ways in which the requirements of the LCO can fail to be met. Specified with each stated Condition are Required Action(s) and Completion Time(s). **Source**: NUREG-1431

maintenance. The organized activity, both administrative and technical, of keeping structures, systems and components in good operating condition, including both preventive and corrective (or repair) aspects. **Source:** IAEA Safety Glossary 2007

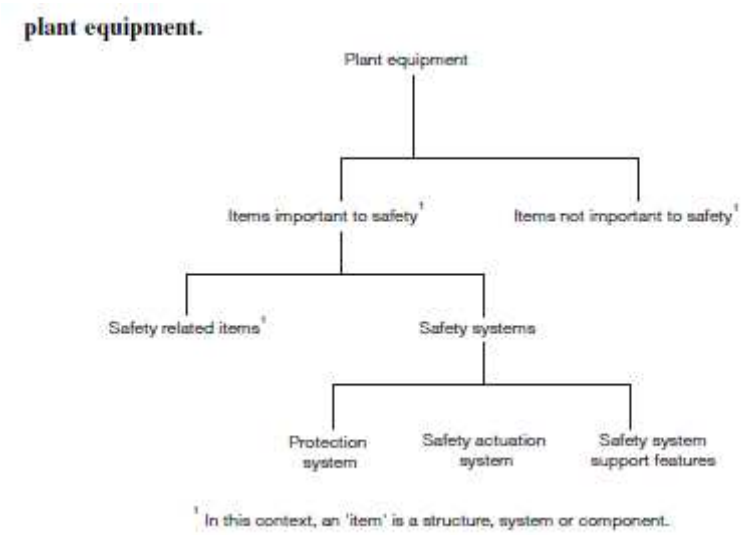
operation. All activities performed to achieve the purpose for which a facility was constructed. For a nuclear power plant, this includes maintenance, refuelling, In-service inspection and other associated activities. **Source**: IAEA Safety Reports Series 110

operational limits and conditions. A set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the regulatory body for safe operation of a nuclear power plant. **Source**: IAEA CB5

periodic maintenance. Form of *preventive maintenance* consisting of servicing, parts replacement, surveillance or testing at predetermined intervals of calendar time, operating time or number of cycles. Also termed *time based maintenance*. **Source**: IAEA Safety Glossary 2007

planned maintenance. Form of preventive maintenance consisting of refurbishment or replacement that is scheduled and performed prior to unacceptable degradation of a structure, system or component. **Source**: IAEA Safety Glossary 2007

plant equipment.



Source: IAEA Safety Glossary 2007

preventive maintenance. Actions that detect, preclude or mitigate degradation of a functional structure, system or component to sustain or extend its useful life by controlling degradation and failures to an acceptable level. **Source**: IAEA Safety Glossary 2007.

protection system. System which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition. **Source**: IAEA Safety Glossary 2007

safety actuation system. The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system. **Source**: IAEA Safety Glossary 2007

safety related item. An item important to safety which is not part of a safety systems. **Source**: IAEA Safety Glossary 2007

safety system support features. The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems. **Source**: IAEA Safety Glossary 2007

safety system. A system important to safety, provided to ensure the safe shutdown of the reactor or residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some plant operational states

and non-safety functions in other operational states. **Source**: IAEA Safety Glossary 2007

surveillance requirements (SR). Surveillance requirements (SRs) in nuclear power plant technical specifications define the tests to be performed on safety system components and specify the intervals at which they should be performed. But the strategy to be followed in scheduling the tests, i.e. the actual placement of tests in relation to each other, is often not specified. In deciding on modifications to surveillance test intervals (STIs), the test strategy to be employed also needs to be considered as it is an important element in defining the risk that is being accepted due to the modifications. **Source**: IAEA TECDOC 729

technical specification. The technical specifications (TS) are safety rules, approved by the regulatory authority, defining the limits and conditions for safe operation of a nuclear power plant. **Source**: IAEA TECDOC 729

test strategy or scheme. The test strategy is concerned with the choice of surveillance test methods and placement (relative timing scheme) of the tests within a group of redundant components or in relation to functionally related systems. In the test scheme, also the relative timing with respect to scheduled maintenance or overhaul outages may be defined. In many cases, several different types of tests are used in combination with a specific timing scheme in order to cover different kind of components in a system, and their different failure modes. The test strategy may define also the procedure for additional tests of redundant equipment in a failure situation until the elimination of the root cause is verified. **Source**: IAEA TECDOC 729

Appendix 2 – Example of Methods for Analysing of TS Changes

1. Example of Methods for Analysing TS Changes

There are different methods to be used when analysing changes to the TS requirements. There is a distinction between analysis/optimisation and evaluation. This appendix is describing methods that can be used both for optimisation and evaluation. The guidance is focused on the evaluation and the methods presented in this appendix may therefore not necessarily be fulfilling the requirements.

The analysis/optimization may be done in different ways, and with different goals, and most methods presented are mainly focused on the analysis/optimisation phase. The analysis and optimisation phase is in most cases performed before this guidance is relevant.

It has been considered relevant to present some of the methods available for analysis/optimisation. It should also be emphasized that the methods presented in this appendix only is a selection from available ones. Other methods exist and may be used.

Evaluation means a verification that all of the different changes do not affect the overall risk. The evaluation requires that it shall be possible to quantify the situation before the change(s) and after the change(s) for the whole plant. It is not acceptable just to look at each individual change. Based on this requirement, it can be concluded that, some of the presented methods may be useful in the process, but is not sufficient in the evaluation phase in the end.

The method applied by TVO recently is presented in section 2 of this appendix.

The methods that are recommended by this guidance in the evaluation phase are:

- STIs: Evaluation on Plant Level. Change all affected test intervals and quantify the top CDF/URF.

- AOT: Quantification of the total CDF/URF at continued power operation. Each change in AOT affects the change of component unavailability due to maintenance and hence a total CDF/URF is possible to quantify. If the increase in risk, considering only continued power operation, is too high, it can be acceptable to also consider the change in risk when performing shutdown to forced outage. The method shall be able to present a total CDF/URF frequency.

1.1 Evaluation of STIs

1.1.1 Evaluation on Component Level

According to *Handbook of Methods for Risk-Based Analyses of Technical Specifications* [19] the total risk impact from a test can be expressed:

$$R_T = R_D + R_C$$

Where:
R_T = Total risk for the test
R_D = Risk contribution detected by the test (test-limited risk)
R_C = Risk contribution caused by the test (test-caused risk)

The risk contribution caused by the test can be divided in several parts according to:

$$R_C = R_{Trip} + R_{Wear} + R_{Config} + R_{Down}$$

Where:
R_{Trip} = Risk that the test causes an initiating event
R_{Wear} = Risk of wear out of the equipment
R_{Config} = Risk that the plant configuration is incorrect when the test has been performed (causing an increased risk)
R_{Down} = Risk due to component unavailability during the test

By comparing the risk contribution detected by the test with the risk contribution caused by the test the effectiveness of a single test can be evaluated, i.e. if:

$R_D > R_C$ the test is risk-effective

Based on this an optimal test interval

$$\text{MIN } R_T = R_D + R_C$$

In figure 1 a plot of the risk contribution detected by the test, caused by the test, and their corresponding total risk is depicted.

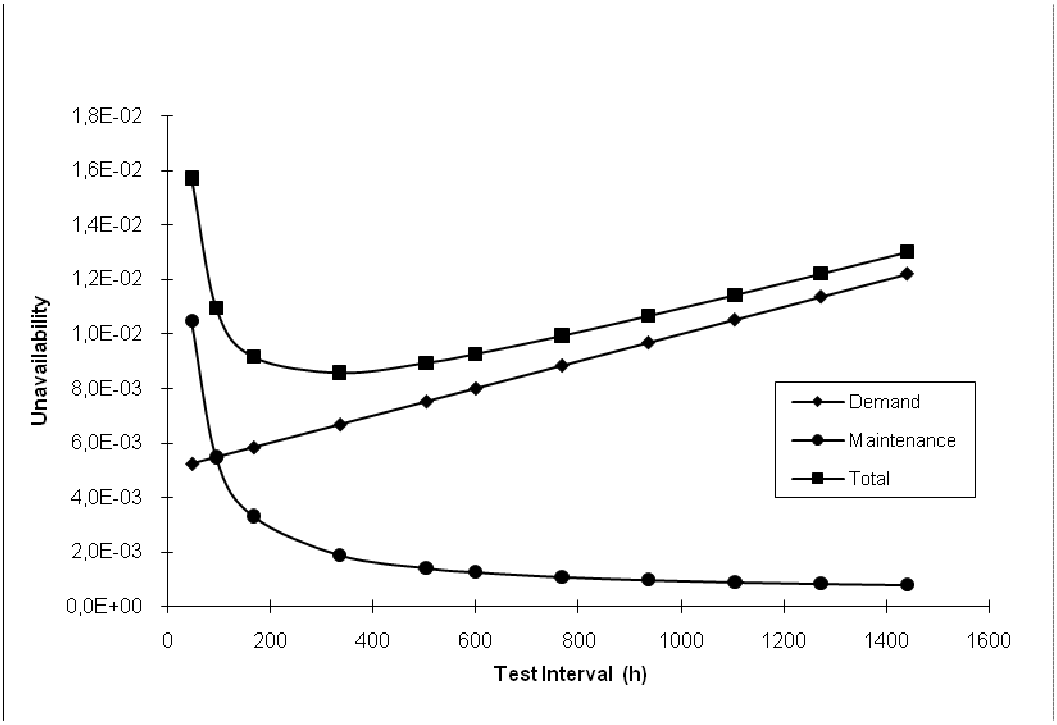


Figure 1 Risk contribution of surveillance testing versus test interval. RD is denoted Demand, RC Maintenance and RT Total [19]

1.1.2 Evaluation on Plant Level

The other perspective is to view all changes in a test program in one analysis on plant level. The methods for this are normally based on the formula for R_T above. In most cases R_C is neglected, i.e. the risk for shutdown, wear out etc. is considered not to be affected by the test frequency. Prolonging of one component/system STI may for example be acceptable if another component/system has a reduced STI. This idea is based on:

$$R_{Tot} = \sum_{j=1}^{n} R_{Dj}$$

Where:

R_{Tot} = Total change in risk of a complete test program

R_{Dj} = Change in risk due to change in one test interval

It can be noted that the above formula is simplified, since relations between different tests are not taken into account. The idea that is shown by the formula is that tradeoffs can be made between different tests. If R_{Tot} is zero, then the new test program neither increases nor decreases the overall risk.

1.2 Evaluation of AOTs

1.2.1 Methods for Evaluating Single AOTs

There are several methods that may be used for evaluation of the specific AOTs. Three main methods are:

1. Risk of continued operation with objects unavailable compared with an accepted frequency
2. Risk of continued operation with objects unavailable compared with an accepted probability (risk budget)
3. Risk of continued operation compared to plant shutdown (with objects unavailable)

These are the three main alternatives, but there are several variants based on these two methods.

The methods are described briefly by following chapters.

1.2.1.1 Frequency that May not be Exceeded

The methods that use this approach indicate which AOTs that may be relevant to be considered in further studies. The measures used can e.g. be the risk increase factor or an absolute risk increase frequency, compared to the nominal risk.

The method does not give any guidance to the length of the AOT, but it can be an indication where it might be acceptable to perform maintenance at power operation (preventive or corrective). The method can hence be considered a way to avoid risk peaks at power operation, due to maintenance activities.

The guidance on AOT length is simple: if the risk frequency is close to the nominal risk frequency, the AOT can be long, and if the risk is increased significantly the AOT must be short.

1.2.1.2 Risk Budget

There are some alternative ways to use a risk budget method, but the basic idea is to compare the conditional risk probability with an accepted risk probability. There are two main principles:

- AOT based on a single event in a system
- AOT based on accumulated risk contribution from a system

In the first case a single repair is studied (assumed to occur) and compared with the accepted risk probability:

$$AOT_x = \frac{P_{Acceptedriskprobability}}{f_{power,x}}$$

In this case the $P_{acceptedriskprobability}$ means the accepted probability per occurrence. If the expected number of occurrences are taken into account the formula would be:

$$AOT_x = \frac{F_{Acceptedriskprobability}}{f_{power,x} \cdot \lambda_x}$$

In this case $F_{acceptedriskprobability}$ means the yearly accepted risk probability and the λ_x means the failure rate of the equipment.

The acceptable, e.g., conditional core damage probability can be determined by different methods. For example, the acceptable conditional core damage probability due to maintenance can be distributed among all possible maintenance activities.

It can be noticed that the method described in RG1.174 [2] constitute a combination of a frequency that must not be exceeded and a conditional core damage probability.

1.2.1.3 Continued Operation versus Shut Down

The previously described methods presuppose continued operation of the plant. These methods do not take into account that shut down may be a risk itself. Shut down from power operation with unavailable components is normally though not to be insignificant from a risk perspective.

A method taking this into account is the comparison of the risk for continued operation with unavailable equipment versus the risk of shutting the plant down (degraded).

Figure 2 below describes a risk curve for staying in power operation conditions with unavailable equipment and a risk curve presenting the shut down risk with unavailable equipment.

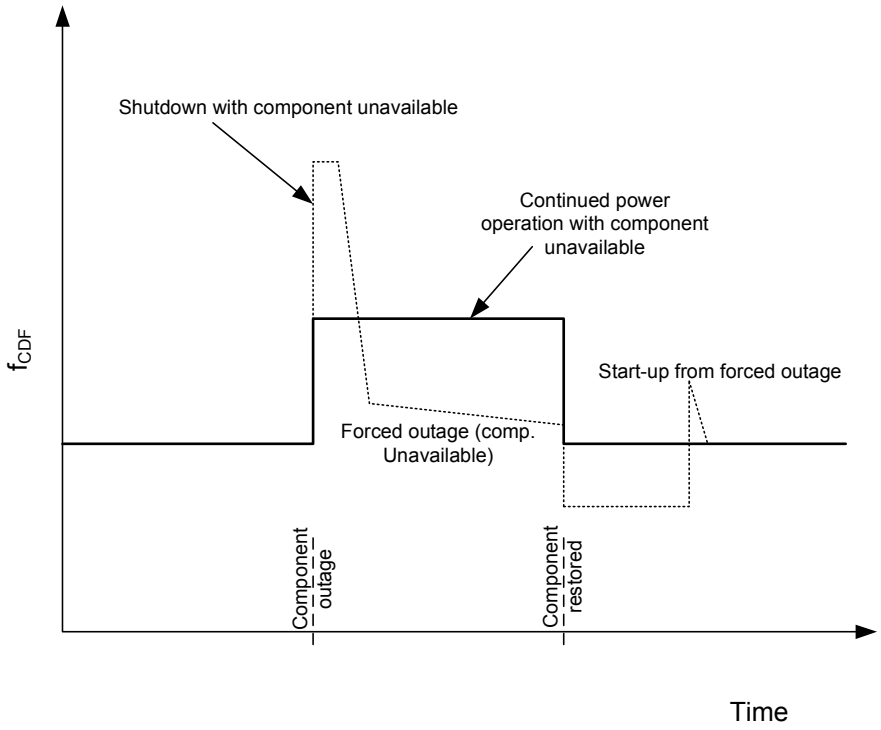


Figure 2 Example of two risk curves: One representing continued power operation with unavailable equipment (solid) and one representing shut down with unavailable equipment (dashed).

In its simplest form, the AOT could be computed according to:

$$AOT \cdot f_{power,x} = P_{SD,x} + P_{forcedoutage} + P_{startup}$$

Where $f_{power,\,x}$ represents increase in risk at power operation with unavailable equipment x, $P_{SD,x}$ represents the shut down risk with equipment x unavailable, $P_{forcedoutage}$ and $P_{startup}$ represents the frequency at cold/hot standby and start up risk respectively.

A development of this method that has been used by both TVO and Ringhals (not exactly in the same way, but similarly) is to include the probability of repair into the equation. The equation could then be written as:

$$\Delta CD_{AOT} = P_{>aot,x} \cdot \left(P_{SD,x} + P_{forcedoutage} + P_{startup}\right) + f_{power,x} \cdot AOT$$

Where ΔCDF_{AOT} means the total increase in core damage probability, $P_{SD,x}$, $P_{forcedoutage}$ and $P_{startup}$ as in previous formula. $P_{>aot,x}$ represents the probability that AOT cannot be met and the plant needs to shut down.
In this case the $P_{>aot,x}$ needs to be determined. One proposed way of doing this is do analyze the existing statistics for repairs, and to develop a repair

time distribution. The length of the AOT and the probability of shut down will hence be dependent. The formula will hence have a minimum. This can be exemplified with Figure 3, which shows the minimum for two and three diesels unavailable.

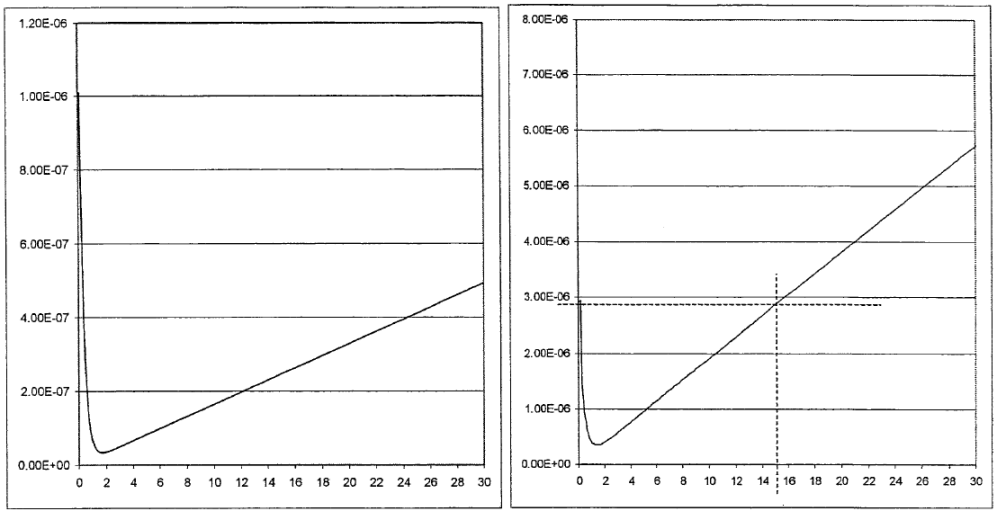


Figure 3 Risk curve for two and three diesels unavailable [20]

1.2.1.4 Comment to Methods

It can be realized that the formula

$$\Delta CD_{AOT} = P_{>aot,x} \cdot \left(P_{SD,x} + P_{forcedoutage} + P_{startup}\right) + f_{power,x} \cdot AOT$$

is a generic formula representing the various methods presented above. The difference lies in the treatment of $P_{>aot,x}$.

The difficulty is hence to determine $P_{>aot,x}$ in an acceptable way. It is not obvious how this probability distribution should be calculated. There are many different aspects to this, for example if it only is the repair time of the component that should form the basis for the usage of the AOT and how the repair time is affected by changes in the AOT.

2. Method applied in complete TS update by TVO

In recent years TVO has performed risk informed evaluations of both the STI and AOT requirements in the technical specifications for the BWR units Olkiluoto 1 and 2. The methods used for the evaluations are described here, based on a paper [21], presented at ANS PSA 2008 topical meeting.

2.1 Method overview

Risk informed evaluation of the TS covered three chapters of the Olkiluoto TS:

- Allowed outage times for power operation (AOTs)
- Surveillance test intervals (STIs)
- Requirements for shutdown states (for refuelling outages)

Each of these chapters was analyzed independently with a similar overall analysis methodology and process. The process used in the evaluation consisted of seven steps:

1. TVO specific **method description** (including objectives and limitations of the analysis).
2. **Screening** of the contents of the TS chapter from a PSA point of view to select items for PSA calculations. Evaluation of the PSA's suitability for the analysis and required modifications and improvements to the PSA are included in this step.
3. **Quantitative assessments** using the plant-specific PSA. The specific quantitative methods and risk measures are detailed in the following section below.
4. **Preparation of the material for an expert panel**. This includes preparing concrete options for the panel with their risk insights and basic information about the test burden defined in the TS.
5. **Expert panel** to comment the results and to propose changes in the TS During commenting rounds a range of factors, including operability, testability and maintainability are considered with the quantitative risk results to form a comprehensive basis for risk-informed decisions.
6. **Documentation** of the results in a working report. As this phase is often left too short and shallow, the basis for any and all decision shall be documented as well.
7. **Preparation of the TS change proposals** to be discussed with the regulatory body.

Olkiluoto 1 and 2 have different methods for evaluation of STIs and AOTs. Both methods are described below.

2.2 Quantitative assessment method for allowed outage times

There are several ways to perform comparison of risk of continued operation to risk of shutdown, and it was decided to use two methods to reflect different aspects of AOTs:

1. An evaluation of the duration of the continued operation when its risk is equal to risk of shutdown.
2. Minimisation of the maximal AOT from risk point view by assuming that the AOT will be fully used and that if the repair will take longer time than AOT the plant will be shutdown.

In the method 1, the AOT is evaluated by the formula:

$$\tau^1 = (\Delta P + P(SD \mid x)) / \Delta f(x), \qquad (1.)$$

if the component can be repaired during full power operation, or:

$$\tau^1 = \Delta P / \Delta f(x), \qquad (2.)$$

if the component cannot be repaired during full power operation, i.e., a shutdown cannot be avoided.

$\Delta f(x)$ is the momentary risk increase caused by the configuration x [1/time-unit]. $P(SD \mid x)$ is the shutdown risk given the configuration x. ΔP is a risk parameter to account for the economical benefits of continued operation. A small additional risk ΔP can be temporarily accepted. The value of P = 1E-7 (core damage risk) was chosen equal to the risk criterion used for plant modifications in an internal TVO guide for PSA applications.

Method 2 is an optimization problem, where the following equation is minimised with respect to the AOT τ:

$$\Delta P(x,) = \Delta f(x) * \tau + (1 - G(x,\tau)) P(SD \mid x)). \qquad (3.)$$

The first term of the formula represents the risk of continued operation and the second term the risk of shutdown of the repair time being longer than τ. $G(x, \tau)$ is the cumulative probability distribution of the repair time for the configuration x. Assuming an exponentially distributed repair time with mean repair time $MTTR_x$, and including the acceptable continued operation risk parameter P, the following equation is obtained for an optimal AOT

$$\tau^2(x) = \max \{-ln\{\Delta f(x) \cdot MTTR_x / P(SD \mid x)\} \cdot MTTR_x, \Delta P / \Delta f(x)\}. \qquad (4.)$$

Method 1 gives longer AOTs than the method 2. It is simple and it reflects well the operative decision making situation when a failure situation is observed. The drawback is that the method 1 does not account uncertainties in the repair time.

The benefit of the method 2 is that it controls the maximal risk allowed by the Tech. Specs.. Since, in reality, AOTs are not fully used, the method does not reflect the reality. Therefore the method 2 can suggest quite short repair times for small risk increase configurations. AOTs proposed by the method 2 should be considered bottom lines, and shorter limits should not be proposed from risk point of view.

AOTs proposed by methods 1 and 2 can be used as a reference range in the assessment of the appropriateness of Tech. Specs. requirements. The range [2, 1] can be broad but is sufficient to detect anomalies in the TS.

2.3 Quantitative assessment method for surveillance test intervals

The assessment of surveillance test intervals is based on the use of the Burden-to- Importance-Ratio (BIR) –measure, developed by Vesely [22], to identify which components have too long or too short test interval relative to the risk importance of the set of components selected for the assessment. BIR-measure is the ratio of relative resources C_i and relative risk importance R_i of the item *i:*

$$BIR(i) = \frac{C_i \Big/ \sum_j C_j}{R_i \Big/ \sum_j R_j}, \qquad (5.)$$

where the sum is over all the components and systems which are part of the STI requirements.

In the case of surveillance test intervals, the resources are assumed to be equal to man-hours spent for testing, which is dependent on man-hours per test and test interval. In certain cases, a test requires reduction of reactor power causing production losses, which must be accounted for as well. Testing of isolation valves in the steam lines and the feed water lines are examples of tests with production losses.

A suitable measure for risk importance of a test is the Fussell-Vesely (FV) risk importance measure. FV measure is approximately linearly dependent on the test interval of a component, at least for components for which the so called "$q + \lambda \cdot TI$" unavailability model is applied. In few cases, there may be a transient risk associated with the test, which must be accounted for as well. Testing of scram system valves is an example of this.

In an optimal situation *BIR(i)* is equal to 1 for all items. *BIR > 1* indicates too much testing with respect to the risk importance, and vice versa for *BIR < 1*.

In the practical application, BIR-measures are not calculated for individual components but for a group of components whose testing is performed simultaneously, e.g. a pump and a motor-operated valve in the system. The component groups are defined in the testing procedures.

In order to further assess the risk importance of the possible imbalance in the test interval, the absolute impact on CDF of changing of the test interval to two times longer (if BIR > 1) or two times shorter (if BIR < 1) was calculated. The idea here is that the test interval should not be changed by more than a factor 2. These changes were used as part of the options presented for the expert panel.

Appendix 3 – Reference Documentation

1. Introduction

In addition to the reference documents listed in the report, this appendix lists some other references that could be of interest with regard to risk-informed evaluation of TS.

2. Publications from the NRC

NRC 10CFR50.36, “Technical Specifications on Effluents from Nuclear Power Reactors”

NRC RG 1.70, “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants”

NRC RG 1.93, “Availability of electrical power sources”

NRC Information Notice 84-42, “Equipment Availability for Conditions During Outages not Covered by Technical Specifications”

NUREG-1024, “Technical Specifications — Enhancing the Safety Impacts "NUREG 1024, November 1983”

NUREG/CR-4810, “Evaluation of Diesel Unavailability and Risk Effective Surveillance Test Interval, W.E. Vesely et al., NUREG/CR-4810, Brookhaven National Laboratory, May 1987”

NUREG/CR-5200, “Evaluation of Risks Associated with AOT and STI Requirements at the ANO- Nuclear Power Plant. P.K. Samanta, S. Wong, and J.Carbonaro, NUREG/CR-5200, BNL-NUREG 52024, August 1988”

NUREG/CR-5425, “Evaluation of Allowed Outage Times AOTs from a Risk and Reliability Standpoint, W.E. Vesely, NUREG/CR-5425, Brookhaven National Laboratory, August 1989”

NUREG/CR-6141, “Handbook of Methods for Risk-Based Analyses of Technical Specifications, Rep. NUREG/CR-6141, Washington, DC (1994)”

NUREG/CR-6172, “Reviewing PSA Based Analyses to Modify Technical Specifications at Nuclear Power Plants, Rep. NUREG/CR-6172, Washington, DC (1995)”.

NUREG/CR-4810, “Evaluation of Diesel Unavailability and Risk Effective Surveillance Test Interval”

NUREG/CR-5425, “Evaluation of Allowed Outage Times AOTs from a Risk and Reliability Standpoint”

NUREG/CR-6172, “Reviewing PSA Based Analyses to Modify Technical Specifications at Nuclear Power Plants”

The NRC has also published standard TS. in the U.S.:

- NUREG-1024, “Technical Specifications — Enhancing the Safety Impacts”
- NUREG-1430, “Standard Technical Specifications Babcock and Wilcox Plants, Specifications”
- NUREG-0452, “USNRC, Standard Technical Specifications for Westinghouse Pressurized Water Reactors, NUREG 0452, Revision 3 (1980)”
- NUREG-1431, “Standard Technical Specifications Westinghouse Plants Specifications”
- NUREG-1432, “Standard Technical Specifications Combustion Engineering Plants Specifications”
- NUREG-1433, “Standard Technical Specifications General Electric Plants, BWR/4 Specifications”
- NUREG-1434, “Standard Technical Specifications General Electric Plants, BWR/6 Specifications”

3. Publications from IAEA

IAEA-TECDOC-599, “Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications”

IAEA-TECDOC-699, “Case study on the use of PSA methods: Assessment of technical specifications for the reactor protection system instrumentation”

IAEA-TECDOC-729, “Risk Based Optimization of Technical Specifications for Operation of Nuclear Power Plants”

IAEA-TECDOC-740, “Modelling and data prerequisites for specific applications of PSA in the management of nuclear plant safety”

IAEA-TECDOC-873, “Application and Development of Probabilistic Safety Assessment for Nuclear Power Plant Operations”

IAEA-TECDOC-1138, “Advances in Safety Related Maintenance”

IAEA-TECDOC-1436, “Risk informed regulation of nuclear facilities: Overview of the current status”

Title	Guidance to Risk-Informed Evaluation of Technical Specifications using PSA
Author(s)	Ola Bäckström 1, Anna Häggström 1, Ilkka Männistö 2
Affiliation(s)	1 Scandpower AB, Sweden and 2 VTT, Finland
ISBN	978-87-7893-293-8
Date	October 2010
Project	NKS-R RiskEval
No. of pages	49 text and appendices, 58 in total including SSM perspective etc.
No. of tables	2
No. of illustrations	8
No. of references	22

Abstract

This report presents guidance for evaluation of Technical Specification conditions with PSA. It covers quality in PSA, how to verify that the PSA model is sufficiently robust and sufficiently complete and general requirements on methods. Acceptance criteria for evaluation of changes in the TS conditions are presented.

As the probabilistic safety assessment (PSA) has developed over the years, it has demonstrated to constitute a useful tool for evaluating many aspects of the TS from a risk point of view. and in that way making the PSAs as well as the decision tools better. This also means that it will be possible to take credit for safety system overcapacity as well as inherent safety features and strength of non-safety classed systems.

However, PSA is only one of the tools that shall be used in an evaluation process of TS changes (strengthening/relaxation). PSA is an excellent tool to be used to verify the importance, and thereby possibly relaxation, of TS requirements. But, since PSA is only one tool in the evaluation, it is not sufficient in itself for defining which equipment that shall or shall not have TS requirements.

The purpose of this guidance document is to provide general require-ments, requirements on methods and acceptance criteria on risk-informed evaluation of TS changes based on PSA. The purpose is not to provide a single solution.

As part of the review of the TS conditions this guidance specify require-ments on:
- Quality verification of the PSA model
- Verification that the PSA model is sufficiently robust with regard to SSCs for which requirements both are and are not defined by the TS
- Verification that the SSCs, for which TS demands are to be evaluated, are modelled in a sufficient manner
- Methods for performing the evaluation

- Which evaluation criteria that shall be used (and how that is verified to be correct)
- Acceptance criteria

This guidance also briefly discusses the documentation of the analysis of the TS changes.

This guidance document is to a large content influenced by the structure and guidance given in the NRC Regulatory Guide 1.174.

Key words Technical Specifications, PSA, Risk optimisation, Risk evaluation

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@nks.org, www.nks.org