Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Assessing Regulatory Requirements and Guidelines for the Single Failure Criterion (Research Project R557.1)

Final Report
ENCO FR-(15)-12

June 2015

enco
Provider of independent Nuclear Safety expertise

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Assessing Regulatory Requirements and Guidelines for the Single Failure Criterion (Research Project R557.1)

Final Report
ENCO FR-(15)-12

June 2015

Prepared by:

Prepared for:

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

DOCUMENT REVIEW
AND APPROVAL COVER SHEET

PROJECT Nr.: Research Project R557.1

PROJECT TITLE: Assessing Regulatory Requirements and Guidelines for the Single Failure Criterion

PERFORMED BY: ENCO

TASK: Task 1: Establishing international context regarding Single Failure Criterion (SFC) requirements and comparison to Canadian requirements

Task 2: Consideration of exemptions to SFC requirements for new small reactor designs

Task 3: Recommended improvements to CNSC regulatory requirements related to SFC

DELIVERABLE: D2 Final Report

PREPARED FOR: Canadian Nuclear Safety Commission - Commission canadienne de sûreté nucléaire

DATE released	REVISION	PREPARED/ REVISED by:	REVIEWED by:	APPROVED by:
30.06.2015	Rev. 0	Ivica Basic Ivan Vrbanic (signature on file) Date: 29.06.2015	Maciej Kulig Ioana Popa (signature on file) Date: 29.06.2015	Bojan Tomic (signature on file) Date: 29.06.2015

Distribution: CNSC, ENCO

DISCLAIMER

The Canadian Nuclear Safety Commission is not responsible for the accuracy of the statements made or opinions expressed in this publication and does not assume liability with respect to any damage or loss incurred as a result of the use made of the information contained in this publication.

ABSTRACT

The report provides an overview of the regulatory design requirements for new reactors addressing Single Failure Criterion (SFC) in accordance to international best-practices, particularly considering the SCF relation to in-service testing, maintenance, repair, inspection and monitoring of systems, structures and components important to safety.

The scope of the work included:

- Review and comparison of the current SFC requirements and guidelines published by the IAEA, WENRA, EUR and nuclear regulators in the United States, United Kingdom, Russia, Korea, Japan, China and Finland. This review address the application of SFC requirements in design; considerations for testing, maintenance, repair, inspection and monitoring; allowable equipment outage times; exemptions to SFC requirements; and analysis for SFC application to two-, three- and four-train systems.
- Identification and analysis of any differences in SFC requirements and its application between Canada and the above-mentioned countries.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AOT	Allowable Outage Time
DiD	Defence in Depth
DBA	Design Basis Accident
DBC	Design Basis Condition
DEC	Design Extended Condition
NRC	Nuclear Egulatory Commision
IAEA	International Atomic Energy Agency
WENRA	Western European Nuclear Regulators Associations
RHWG	Reactor Harmonization Working Group
EUR	European Utility Requiremen
SS	Safety Systems
SFC	Single Failure Criteria
RG	Regulatory Guide

LIST OF TABLES

LIST OF FIGURES

N/A

1. INTRODUCTION

1.1 Background

The Single Failure Criterion (SFC) ensures reliable response of safety systems in nuclear power plants in response to design basis initiating events. The SFC, basically, requires that the system must be capable of performing its task in the presence of any single failure.

The capability of a system to perform its design function in the presence of a single failure could be threatened by a common cause failure such as a fire, flood, or human intervention or by any other cause with potential to induce multiple failures. When applied to plant's response to a postulated design-basis initiating event, the SFC usually represents a requirement that each safety system performs all safety functions as designed, and mitigates all of the following:

1. All failures caused by a single failure.
2. All identifiable but non-detectable failures, including those in the non-tested components.
3. All failures and spurious system actions that cause (or are caused by) the postulated event.

In the case of CNSC's regulatory framework, the requirements for SFC are currently addressed in the regulatory documents REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, and RD-367, Design of Small Reactor Facilities.

In order to further improve its regulatory framework concerning the SFC, the CNSC launched a project under which detailed information on the international status of SFC requirements and applications are collected and presented. The project addressed all relevant aspects of SFC application, including also the specifics of new designs of small reactors (as compared to new designs corresponding to "conventional nuclear power plants"), compared Canadian SFC context to international context and provided recommendations regarding the improvements to CNSC's regulatory framework concerning the SFC.

1.2 Objectives and Scope

The overall objective of the work under this project is to provide recommendations on regulatory design requirements for new reactors addressing Single Failure Criterion (SFC) in accordance to international best-practices, particularly considering the SCF relation to in-service testing, maintenance, repair, inspection and monitoring of systems, structures and components important to safety.

The scope of the work included in this report covers the following 3 tasks of the overall project:

Task 1: Establishing international context regarding Single Failure Criterion (SFC) requirements and comparison to Canadian requirements

Under this task, a review of the current SFC reactor design requirements and guidelines published by the IAEA, WENRA, EUR and nuclear regulators in the United States, United Kingdom, Russia, Korea, Japan and Finland were performed. France was not used based on

the fact that French Regulatory Body plays the important ruole under WENRA harmonization project and EDF plays the leading role under EUR revision. Specifically, SFC requirements and guidelines for new reactor design were compared against Canadian requirements, with specific consideration to testing, maintenance, repair, inspection, monitoring, and allowable equipment outage times. The probabilistic approaches to grant SFC exceptions (both permanent and temporary) were listed in the cases where they identified. The approach was analysed of each selected country as SFC applies to two-, three- and four-train systems.

Task 2: Consideration of exemptions to SFC requirements for new small reactor designs

Under this task, based on the information collected and comparisons made under T1, address the specifically the following question: "Should exemptions to SFC requirements pertaining to new reactor design differ between small reactors facilities and conventional nuclear power plants?"

The question is approached from all relevant angles and in the light of the approaches identified under T1, including the considerations and any examples of exemptions based on probabilistic or other arguments.

Task 3: Recommended improvements to CNSC regulatory requirements related to SFC

Based on T1 and T2 findings improvements to CNSC regulatory requirements are recommended as relating to SFC in a way to ensure clear interpretation and to reflect best-practices. All recommendations are supported with detailed technical basis and rationale.

The report is organized in a way to present the work done under these tree tasks and to show the results which were obtained.

2. OVERVIEW OF INTERNATIONAL PRACTICE

2.1 IAEA application of Single Failure Criteria (SFC) and allowable outage time (AOT)

IAEA, in the major document related to the design of the nuclear power plants (SSR-2/1 as in the process of post-Fukushima upgrade [1]), defines under section 5 (General Plant Design) the single failure criterion in Requirement 25:

"*The single failure criterion shall be applied to each safety group incorporated in the plant design.*

5.39. Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system.

5.40. The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event."

explaining that "*the single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure*."

Note:

It should be noted that IAEA SSR-2/1 mentions the term "safety group" only in the Requirement 25 without definition and that in all other requirements only term "safety system" is applied. IAEA Safety Glossary [56] defines a "safety system" as a system important to safety, provided to ensure the safe shutdown of the reactor or the 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. Furthermore, IAEA Safety Glossary [56] defines a "safety group" as the assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded. Per our understanding of IAEA glossary, single "safety system" is designed to perform its single safety function e.g. decay heat removal from core while "safety group" covers the few "safety systems" to perform all actions required for a particular postulated initiating event (Large Break LOCA).

Generally, based on the SSR-2/1, IAEA requires application of the single failure criteria (SFC) for all safety systems and it is covered by IAEA NS-G guidelines (e.g. NS-G-1.9, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants or NS-G-1.10 Design of Reactor Containment System for Nuclear Power Plants, etc.). Generally, in applicable IAEA NS-G guides it is discussed that the all evaluations performed for design basis accidents should be made using an adequately conservative approach. In a conservative approach, the combination of assumptions, computer codes and methods chosen for evaluating the consequences of a postulated initiating event should provide reasonable

confidence that there is sufficient margin to bound all possible The assumption of a single failure in a safety system should be part of the conservative approach, as indicated in SSR-2/1. Care shouldbe taken when introducing ad equate conservatism, since:

- For the same event, an approach considered conservative for designing one specific system could be non-conservative for another;
- Making assumptions that are too conservative could lead to the imposition of constraints on components that could make them unreliable.

Allowable Outage Time (AOT)

Under Requirement 28 in SSR-2/1 (Operational limits and conditions for safe operation) it is stated that the design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant. Para 5.44: The requirements and operational limits and conditions established in the design for the nuclear power plant shall include ([2], requirement 6):

a) Safety limits;

b) Limiting settings for safety systems;

c) Limits and conditions for normal operation;

d) Control system constraints and procedural constraints on process variables and other important parameters;

e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;

f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;

g) Action statements, including completion times for actions in response deviations from the operational limits and conditions.

Furthermore, Requirement 29 (Calibration, testing, maintenance, repair, replacement inspection and monitoring of items important to safety) in para 5.46 requires that where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions. Para 5.47 provides the alternatives if an item important to safety cannot be designed to be capable of being tested, inspected or monitored to the extent desirable. Alternatives include a robust technical justification that incorporates the following approach:

(a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified.

(b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures

Additionally to reqirements from IAEA SSR-2/1 [1], SSR-2/2 [2]((IAEA Safety Standard Series, SSR-2/2, Safety of Nuclear power Plants: Commisioning and Operations, Rev. 1 in preparation, 2014) defines that in, para 4.9, the operational limits and conditions shall include requirements for normal operation, including shutdown and outage stages, and shall cover actions to be taken and limitations to be observed by the operating personnel. Furthermore, para 4.12 requires that the operating organization shall ensure that an appropriate surveillance programme is established and implemented to ensure compliance with the operational limits and conditions, and that its results are evaluated, recorded and retained.

Finally, para 4.15 defines that the operating organization shall not intentionally exceed the operational limits and conditions. Where circumstances necessitate plant operation outside the operational limits and conditions, clear formal instructions for such operations shall be developed, on the basis of safety analysis, if applicable. These instructions shall include instructions for returning the plant to normal operation within the operational limits and conditions. The instructions shall also include specification of the arrangements for approval by the operating organization and the regulatory body, as appropriate, of the changed operational limits and conditions, prior to operation under these changed operational limits and conditions.

IAEA Safety Guide NS-G-2.2 [3] defines the requirements for plant safety limits, limiting safety systems settings, surveillance requirements and limits and conditions for normal operations. Under section 6 the requirements for the limits and conditions for normal operations are described in details. Among others:

> 6.2 The limits and conditions for normal operation should include limits on operating parameters, stipulations for minimum amount of operable equipment, minimum staffing levels, prescribed actions to be taken by the operating staff in the event of deviations from the established OLCs and the time allowed to complete these actions. The limits should also include parameters important to safety, such as the chemical composition of working media, their activity contents and limits on discharges of radioactive material to the environment.
>
> 6.3. Operability requirements should state for the various modes of normal operation the number of systems or components important to safety that should be either in operating condition or in standby condition. These operability requirements together define the minimum safe plant configuration for each mode of normal operation. Where operability requirements cannot be met to the extent intended, the actions to be taken to manoeuvre the plant to a safer state, such as power reduction or reactor shutdown, should be specified, and the time allowed to complete the action should also be stated.
>
> 6.6. When it is necessary to remove a component of a safety system from service, confirmation should be obtained that the safety logic continues to be in accordance with design provisions. The performance of a safety function may be affected by process conditions or service system conditions that are not directly related to the equipment performing the function. It should therefore be ensured that such influences are identified and appropriate limits applied.
>
> 6.7. For the operability requirements for safety related equipment, the provisions in the design for redundancy, the reliability of the equipment and the period over which equipment may be inoperable without an unacceptable increase in risk should be taken into consideration.
>
> 6.8. The allowable periods of inoperability and the cumulative effects of these periods should be assessed in order to ensure that any increase in risk is kept to acceptable levels.

Methods of PSA or reliability analysis should be used as the most appropriate means for this purpose. Shorter inoperability periods than those derived from a PSA may be stipulated in the OLCs on the basis of other information such as pre-existing safety studies or operational experience.

Previously, IAEA had a document Safety Series document 50-P-1 (Application of the Single Failure Criteria, [6]). This document is outdated but there is still no new IAEA document superseded it. However, [6] in section 2 deals with the purpose of the single failure criterion with respect to the safety of a nuclear power plant. It also shows where the criterion has its limitations. The third section explains the difference between active and passive types of failure and the consequences of the failure characteristics for the application of the criterion. Examples are given of simple and more sophisticated component redundancy arrangements in a fluid system. The possibility of fail-safe designs and the role of auxiliary systems are also dealt with. The following section, which is supported by an extensive appendix on various methods to determine allowable outage times for redundant components, treats the important case of the reduction of redundancy during in-service maintenance and repair actions in operating nuclear power plants. Different maintenance strategies are discussed. Section 5 then considers that part of the definition of the single failure criterion which states that consequential effects of a single failure are to be considered as part of the failure.

Section 6 provides an introduction to the problem of common cause failures. While the single failure criterion may be satisfied by redundancy of identical components, the common cause failure of such components would nullify this redundancy. Exemptions from the application of the criterion are related to failure occurrence probability in Section 7. The methodology and the individual steps involved in a single failure analysis (SFA) are explained in the last section. A short commentary on the complementary use of probabilistic safety assessment (PSA) methods is also given. Permissible outage time in the context of single failure criteria is discussed in section 4.1.3. The basic requirements concerning permissible maintenance, test and repair times should be considered. They can be summarized as follows:

(a) If during maintenance, test or repair work, the assumption of a single failure would lead to a failure of the safety features, these activities are only permissible within a relatively short period without special measures being taken (e.g. replacing the function or rendering its operability superfluous). In most cases the time involved in the maintenance, test or repair procedure is so short as to preclude any significant reduction of the reliability of the safety feature concerned. Various methods (including probabilistic) can be used to determine an admissible outage period.

(b) If the resultant reliability is such that the safety feature no longer meets the criteria used for design and operation, the nuclear power plant shall be shut down or otherwise placed in a safe state if the component temporarily out of service cannot be replaced or restored within a specified time (stated in the technical specifications).

(c) Maintenance procedures on safety features over a longer period, during which the component concerned is not operable, are only admissible without special measures if in addition to the maintenance a single failure can be assumed without preventing the safety feature from fulfilling its safety function or if another available system can adequately replace the impaired function.

(d) Even if the single failure criterion is fulfilled during the maintenance procedure, the time for this procedure should be reasonably limited. (e) A PSA can be used to define the maintenance and repair times (time from the detection of the failure until the completion of the repair procedure), as well as the inspection concept. If this is done, the maintenance

procedures should be defined so that they do not reduce the reliabilities of the safety features below the value required for the relevant PIEs and so that the probabilistic safety criteria, if established, are met.

Several methods can be used for the determination of permissible outage times. Important parameters are the degree of redundancy of the components or systems and the failure rate. The final goal is always the performance of a certain safety function, not primarily the availability of a particular component. The determination of the required degree of redundancy has to take this into account. It allows, therefore, not only for parallel trains of identical configuration but also for other systems which could perform the same function. Taking into account the need for reliability of safety systems and the desire for high operational availability, some countries consider it necessary in ensuring plant safety to require, along with the single failure criterion, additional redundancy for some specified safety functions in order to be able to cope with both ongoing maintenance or repair work and a simultaneous single failure. This requirement leads to an n + 2 degree of redundancy, for example 4 X 50% or 3 X 100% redundancy concepts. Another method used in many countries is to increase the redundancy of active components (e.g. pumps, valves) which require the most frequent maintenance. This leads in general to a 4 x 50% or a 4 x 100% redundancy concept for such components. It should also be noted that some countries as a result of probabilistic considerations introduce further equipment in addition to the single failure criterion requirements. This increases the level of redundancy of some safety groups required to cope with the relevant PIEs.

The question of common cause failure must also be considered, as described in Section 6 of [6]) . The advantage of applying these concepts is not only a higher reliability of the safety systems but also a higher availability of the plant, because in the event of longer lasting repair activities additional measures such as power reduction or plant shutdown are not necessary. The choice between the possibilities is then also an economic matter; the investment costs must be compared with the anticipated savings connected with the improved availability of the plant.

Exception during testing and maintenance - Allowable Outage Time (AOT)

Detailed methodology for determination the surveillance test intervals and allowed outage times (AOT) of systems and components important to safety are not discussed in IAEA guides. However, under IAEA SSG-3[4] is discussed that the results of the PSA should be used in developing emergency procedures for accidents and to provide inputs into the technical specifications of the plant. In particular, the results of the PSA should be used to investigate the increase in risk after the removal from service of items of equipment for testing or maintenance and the adequacy of the frequency of surveillance or testing. The PSA should be used to confirm that the allowed outage times do not contribute unduly to risk and to indicate which combinations of equipment outages should be avoided. In the chapter „Risk Informed Technical Specifications (bullets 10.28 to 10.35) “ it is discussed that The limiting conditions for operation give, for example, the requirements for equipment operability, the allowed outage times and the actions required (e.g. the testing requirements for redundant equipment). The allowed outage time for a particular system or component is the period of time within which any maintenance or repair activity should be completed. If the allowed outage time is exceeded, the technical specifications specify the actions that the plant operators should take. For example, if an allowed outage time is exceeded during operation at power, the requirement may be for the operators to reduce power or to shut down the plant. In addition, the requirements for equipment operability usually include limits

on the combinations of equipment that can be removed for maintenance at the same time (usually referred to as configuration control). Insights from PSA can be used as an input to justify limiting conditions for operation and allowed outage times. Similarly it is discussed also for surveillance test periods, etc. Some details about practice of risk based AOT optimization is given in few older IAEA-TECDOCs documents [8], [10] and [10].

2.2 WENRA RHWG Safety Reference Levels related to SFC and AOT

A principal aim of the Western European Nuclear Regulators' Association (WENRA) is to develop a harmonized approach to nuclear safety within the member countries. One of the first major achievements to this end was the publication in 2006 of a set of safety reference levels (RLs) for operating nuclear power plants (NPPs) [28] . After the TEPCO Fukushima Daiichi nuclear accident, they have been further updated to take into account the lessons learned, including the insight from the EU stress tests. As a result a new issue on natural hazards was developed and significant changes made to several existing issues.

WENRA Rls cover the following areas:

01 Issue A:Safety Policy

02 Issue B:Operating Organisation

03 Issue C:Management System

04 Issue D:Training and Authorization of NPP Staff (Jobs with Safety Im-portance)

05 Issue E:Design Basis Envelope for Existing Reactors

06 Issue F: Design Extension of Existing Reactors

07 Issue G: Safety Classification of Structures, Systems and Components

08 Issue H: Operational Limits and Conditions (OLCs)

09 Issue I: Ageing Management

10 Issue J: System for Investigation of Events and Operational Experience Feedback

11 Issue K: Maintenance, In-Service Inspection and Functional Testing

12 Issue LM: Emergency Operating Procedures and Severe Accident Manage-ment Guidelines

13 Issue N: Contents and Updating of Safety Analysis Report (SAR)

14 Issue O: Probabilistic Safety Analysis (PSA)

15 Issue P: Periodic Safety Review (PSR)

16 Issue Q: Plant Modifications

17 Issue R: On-site Emergency Preparedness

18 Issue S: Protection against Internal Fires

19 Issue T: Natural Hazards

Single Failure Criterion is considered in several safety reference levels under Design Basis Envelope for Existing Reactors (Issue E), as shown below.

Demonstration of reasonable conservatism and safety margins

E8.2 The worst single failure (A failure and any consequential failure(s) shall be postulated to occur in any component of a safety function in connection with the initiating event or thereafter at the most unfavourable time and configuration.) shall be assumed in the analyses of design basis events. However, it is not necessary to assume the failure of a passive

component, provided it is justified that a failure of that component is very unlikely and its function remains unaffected by the PIE.

Reactor and fuel storage sub-criticality

E9.7 At least one of the two systems shall, on its own, be capable of quickly rendering the nuclear reactor sub critical by an adequate margin from operational states and in de-sign basis accidents, on the assumption of a single failure.

Heat Removal Functions

E9.9 Means for removing residual heat from the core after shutdown and from spent fuel storage, during and after anticipated operational occurrences and design basis acci-dents, shall be provided taking into account the assumptions of a single failure and the loss of off-site power.

Reactor protection system

E10.7 Redundancy and independence designed into the protection system shall be sufficient at least to ensure that:

- no single failure results in loss of protection function; and
- the removal from service of any component or channel does not result in loss of the necessary minimum redundancy.

Emergency Power

E10.11 It shall be ensured that the emergency power supply is able to supply the necessary power to systems and components important to safety, in any operational state or in a design basis accident, on the assumption of a single failure and the coincidental loss of off-site power.

Alowable Outage Time (AOT)

The whole Issue H (Operational Limits and Conditions (OLCs)) deals with demonstration of OLCs to ensure that plants are operated in accordance with design assumptions and intentions as documented in the Safety Analysis Report (SAR). Among others, reference level H defines the unavailability of limits as:

H6.1 Limits and conditions for normal operation shall include limits on operating parame-ters, stipulation for minimum amount of operable equipment, actions to be taken by the operating staff in the event of deviations from the OLCs and time allowed to com-plete these actions.

H6.2 Where operability requirements cannot be met, the actions to bring the plant to a safer state shall be specified, and the time allowed to complete the action shall be stated.

H6.3 Operability requirements shall state for the various modes of normal operation the number of systems or components important to safety that should be in operating condition or standby condition.

Also, per H9.1 the licensee shall ensure that an appropriate surveillance program (*The objectives of the surveillance programme are: to maintain and improve equipment availability, to confirm compliance with operational limits and conditions, and to detect and correct any abnormal condition before it can give rise to significant consequences for safety. The abnormal conditions which are of relevance to the sur-veillance programme include not only deficiencies in SSCs and software performance, procedural errors and human errors, but*

also trends within the accepted limits, an analysis of which may indicate that the plant is deviating from the design intent. (NS-G-2.6 Para 2.11)) is established and implemented to ensure compliance with OLCs and shall ensure that results are evaluated and retained.

In H10 non-compliances with defined OLCs requires the reports of non-compliance and corrective action shall be implemented in order to help prevent such non-compliance (taking into account that if the actions taken to correct a deviation from OLCs are not as prescribed, including those times when they have not been completed successfully in the allowable outage time, plant shall be deemed to have operated in non-compliance with OLCs.) in future.

Furthermore, the WENRA RHWG report on safety of new NPP designs [29] discusses some considerations based on the major lessons from the Fukushima Daiichi accident, especially concerning the design of new nuclear power plants, and how they are covered in the new reactor safety objectives and the common positions. The WENRA Objectives O1-O7 cover the following areas:

O1. Normal operation, abnormal events and prevention of accidents

O2. Accidents without core melt

O3. Accidents with core melt

O4. Independence between all levels of Defence-in-Depth

O5. Safety and security interfaces

O6. Radiation protection and waste management

O7. Leadership and management for safety

Within the WENRA Safety Objectives for New Nuclear Power Plants the words “reasonably practicable” or “reasonably achievable” are used. In this report the words Reasonably Practicable are used in terms of reducing risk as low as reasonably practicable or improving safety as far as reasonably practicable. The concept of reasonable practicability is directly analogous to the ALARA principle applied in radiological protection, but it is broader in that it applies to all aspects of nuclear safety. In many cases adopting practices recognized as good practices in the nuclear field will be sufficient to show achievement of what is “reasonably practicable”.

The major change is refined structure of the levels of DiD (Defense in Depth) presented in [29]. The WENRA RHWG safety objectives for new NPP designs[29] does not change the definition and usage of SFC according to WENRA RHWG safety reference levels for existing reactors [28] but discusses the some design expectations related to SFC. For example: while the postulated single initiating events analyses in combination with the single failure criteria usually gives credit on redundancy in design provisions of safety systems and of their support functions, addressing multiple failure events emphasizes diversity in the design provi-sions of the third level of DiD. Based on the [29], for DiD level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on probabilistic insights. Best estimate methodology and less stringent rules than for level 3.a may be applied if appropriately justified. However the maximum tolerable radiological consequences for multiple fail-ure events (level 3.b) and for postulated single failure events (level 3.a) are bounded by WENRA Objective O2 (accident without core melt).

Table 1 The refined structure of the levels of DiD proposed by RHWG

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 [1] 3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions [2]	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact [4]	Postulated single initiating events
3.b		Additional safety features[3], accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features[3] to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures[5]	-

[1] Even though no new safety level of defence is suggested, a clear distinction between means and conditions for sub-levels 3.a and 3.b is lined out. The postulated multiple failure events are consid-ered as a part of the Design Extension Conditions in IAEA SSR-2/1.

[2] Associated plant conditions being now considered at DiD level 3 are broader than those for existing reactors as they now include some of the accidents that were previously considered as "beyond de-sign" (level 3.b). For level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on probabilistic in-sights. Best estimate methodology and less stringent rules than for level 3.a may be applied if ap-propriately justified. However the maximum tolerable radiological consequences for multiple failure events (level 3.b) and for postulated single failure events (level 3.a) are bounded by WENRA Objective O2.

[3] The task and scope of the additional safety features of level 3.b are to control postulated common cause failure events as outlined in Section 3.3 on "Multiple failure events". An example for an additional safety feature is the additional emergency AC power supply equipment needed for the postulated common cause failure of the primary (non-diverse) emergency AC power sources. The task and scope of the complementary safety features of level 4 are outlined in Section 3.4 on "Provisions to mitigate core melt and radiological consequences". An example for a complementary safety feature is the equipment needed to prevent the damage of the containment due to combustion of hydrogen released during the core melt accident.

[4] It should be noted that the tolerated consequences of Level 3.b differ from the requirements con-cerning Design Extension Conditions in IAEA SSR-2/1 that gives a common requirement for DEC: "for design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary".

[5] Level 5 of DiD is used for emergency preparedness planning purposes.

The WENRA RHWG safety objectives for new NPP designs[29] does not deal with safety demonstration of the SFC. However, it points that the demonstration of physical impossibility, based on engineered provisions, can be difficult. Care must be taken to recognize that some claims for practical elimination may be based on as-sumptions (e.g. non-destructive testing, inspection) and those assumptions need to be acknowledged and addressed. For engineered provisions this can be done by excluding the certain feature from the design making further development of accident scenario impossible (accident sequence cut-off).

It should be noted that the level of defence are varying according different international guidelines as a basis to develop an evaluation basis for SFC criteria. See Table 2 bellow.

Exception during testing and maintenance - Allowable Outage Time (AOT)

However, WENRA RHWG safety objectives do not discuss application of the SFC in the context of determination of the allowable outage times (AOT) for redundant components. There is no recommendation how to treat the the reduction of redundancy during in-service maintenance and repair actions in operating nuclear power plants.

Table 2 Level of DiD according different guidelines as a basis to develop an evaluation basis for licensing

Level of Defence	Initiating Event Frequency / yr	IAEA, SSG-2 [1], NOTE 2	EUR[30]	WENRA Note 1	STUK[38], [40]	US-NRC[14]	ASME Service Levels
1	f=1	Normal Operation	DBC 1, Normal Operation	Normal Operation	DBC 1, Normal Operation	Normal Operation	A
2	$f>10^{-1}$	Anticipated Operational Occurances	DBC 2 Incidents	Anticipated Operational Occurances	DBC 2, Anticipated Operational Occurances	Anticipated Oper-ational Occurances (AOO)	B
3	$10^{-1}<f<10^{-2}$		DBC 3, Accidents of low Frequency	Design Basis Accidents 3.a Postulated Single Initiating Events	DBC 3, Class 1 postulated accidents $10^{-2}<f<10^{-3}$	Design Basis Accidents (DBA) (Limiting Faults)	C
	$10^{-2}<f<10^{-4}$	Design Basis Accidents			DBC 4, Class 2 postulated accidents $f<10^{-3}$		
	$10^{-4}<f<10^{-6}$	Beyond Design Basis Accidents	DBC 4, Accidents of very low Frequency	Design Basis Accidents 3.b Postulated Multiple Initiating events	DEC A		D
4a	$10^{-6}>f$	Severe Accidents	Complex Sequences	DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved;	DEC B	Beyond Design Basis Accidents	N/A
4b			Severe Accidents	DEC B with postulated severe fuel damage.	DEC C	Severe Accidents	
5			Severe Accidents	Accident with significant release of radioactivity to the			

Level of Defence	Initiating Event Frequency / yr	IAEA, SSG-2 [1], NOTE 2	EUR[30]	WENRA Note 1	STUK[38], [40]	US-NRC[14]	ASME Service Levels
				environment			

Note 1: It should be noted that DiD for associated regulation was not assessed toward the initiating event frequency. The presented categorisation was made based on analogy with IAEA SSR-2/1. It was generally required that a list of PIEs shall be established to cover all events that could affect the safety of the plant. From this list, a set of anticipated operational occurrences and design basis accidents shall be selected using deterministic or probabilistic methods or a combina-tion of both, as well as engineering judgement. The resulting design basis events shall be used to set the boundary conditions according to which the structures, sys-tems and components important to safety shall be designed, in order to demonstrate that the necessary safety functions are accomplished and the safety objectives met.

Note 2 Regarding the IAEA SSG-2, please note that it is meant to apply for all the operating reactors in the world and that IAEA tends to come with guidelines which are acceptable for all reactor types and and all member states. In comparison to EUR, for example: EUR is meant for new reactors to be built in EU member countries. Furthermore: the limit / target of 1E-05 /yr from Canadian REGDOC 2.4.1 (section 8.2.3) is not necessarily directly comparable to the target of 1E-04 /yr in the IAEA's SSG-2 (Table 2). Canadian limit relates to "design basis accidents" (DBA). IAEA's target relates to "postulated initiating events" (PIE).
The "DBA" involves the "PIE" and allows / tolerates a single failure (provided that SFC is applied in the design, which should normally be the case). (For example: design basis LOCA followed by a failure of one ECCS train is still a design basis accident, if ECCS was designed according to the SFC.) The probability of a single failure (train level) by the "rule of thumb" can be taken as 1E-02 for a train with motor-driven pump, or 1E-01 for a train with a turbine-driven pump. Thus, when the IAEA SSG-2 says that PIE with freq. > 1E-04 /yr shall be enveloped by the design basis, it means that any accident sequence with frequency in the range 1E-06 - 1E-05 per year or higher (1E-04 /yr x (0.01 to 0.1)) shall produce no consequences larger than design basis consequences (concerning, for example, dose limits).

Table 2 was created by combining few sources which are not fully comparable but certain analogy was done. For illustration, please see bellow the original tables from SSG-2[4] and EUR rev D [30]:

SSG-2 Deterministic Safety Analyses for Nuclear Power Plants (2009), Table 2

Occurrence (1/reactor year)	Characteristics	Plant state	Terminology	Acceptance criteria
10^{-2}–1 (expected over the lifetime of the plant)	Expected	Anticipated operational occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions	No additional fuel damage
10^{-4}–10^{-2} (chance greater than 1% over the lifetime of the plant)	Possible	Design basis accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions	No radiological impact at all, or no radiological impact outside the exclusion area
10^{-6}–10^{-4} (chance less than 1% over the lifetime of the plant)	Unlikely	Beyond design basis accidents	Faulted conditions	Radiological consequences outside the exclusion area within limits
$<10^{-6}$ (very unlikely to occur)	Remote	Severe accidents	Faulted conditions	Emergency response needed

EUR Reference: Rev. D Section 2.1.8.2 Table 2

Design Basis Category	Definition	Frequency of initiating event (per year)	Acceptance Criteria	
			Plant parameters	Radio-active releases
1	Normal Operation*		• Process parameters within Normal Operation* range of Technical Specifications*	Table 1
2	Incidents*	$f > 10^{-2}$	• Process parameters within applicable acceptance criteria	Table 1
3	Accidents (low frequency)	$10^{-2} > f > 10^{-4}$	• Acceptance criteria for Category 3 (1) • Limited Fuel Damage* (3) • Shutdown for Inspection* may be necessary	Appendix B
4	Accidents (very low frequency)	$10^{-4} > f > 10^{-6}$	• Acceptance criteria for Category 4 (1) • Core coolable geometry retained • Plant restart may be impossible • Peak clad temperature: 1204 °C (4, 5) • Local clad oxidation: 17% (4, 5) • Radial average peak fuel enthalpy at hot spot: 837 kJ/kg (4, 6, 7)	Appendix B

2.3 European Utility Requirements (EUR) for LWR NPP related to Single Failure Critera

In general, the last 15 years EU countries (including Finland) are focused on the armonization of new nuclear power plant installation requirements in two ways:

– Through the WENRA (West European Nuclear Regulators Association, including 17 EU countries + Swiss + observers: Armenia, Austria, Denmark, Ireland, Luxemburg, Norway, Poland, Russian Federation, Ukraine). WENRA approach to SFC is described in section 2.2 above

– Through the European utility Requirements (EUR) including the biggest European + Russian utilities (CEZ, EDF, EDF Energy, ENDESA, Enel, ENERGOATOM, Fortum, GDF SUEZ/Tractebel Engineering, GEN energija, IBERDROLA, MVM, NRG – ROSENERGOATOM, Swissnuclear, TVO, Vattenfall and VGB Power Tech).

The European electricity producers involved in the making of the EUR document aim at harmonization and stabilization of the conditions in which the standardized LWR nuclear power plants to be built in Europe in the first decades of the century will be designed and developed. This is expected to improve both nuclear energy competitiveness and public acceptance in an electricity market unified at European level. Beyond Europe, the EUR utilities also promote world-wide harmonization of the design bases of the next nuclear power plants. However, EUR was changed since 2001 (revision C, [31]), 2012 (revision D, [30]) and the new revision E which is expected to be published in 2016. It was very important to mention that the "Feedback from TVO BIS experience for FIN5" was included in EUR rev. D because this document cover Finnish national EUR rev. C prepared especially for EPR Olkiluoto 3 Terms of Reference. In another word, Finnish licensing practices (based on their Regulatory Guides, YVL) are included partially in EUR rev. D.

Per EUR rev. D, SFC is defined as An occurrence which results in the loss of capability of a component to perform its intended Safety Functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming Passive Equipment* functions properly) nor (2) a single failure of a Passive Equipment (assuming Active Equipment functions properly) results in a loss of capability of the system to perform its Safety Functions. Safety Functions ensure achievement and maintenance of the safety objectives in Design Basis Conditions and Design Extension Conditions. The Safety Functions are plant specific and will be defined by the Plant Designer during design process of safety and automation systems. The plant specific Safety Functions are classified either in Level F1A, F1B, or F2.

EUR Volume 2 Chapter 1, under section 2.1.3.2 defines that the requirements for dealing combinations of DBC (Design Bases Conditions) events are given in EUR sections focused on the Single Failure Criterion and the approach to Hazards and that usage of a number of deterministic conventions, in particular application of the Single-Failure Criterion to systems that perform specific Safety Functions, should ensure appropriate Redundancy provisions. In section 2.1.3.3 is required that each initiating event shall be analysed to demonstrate compliance with the acceptance criteria summarised in a detailed list provided by the Designer, taking into account any consequential failures resulting directly from the initiating

event, and applying the Single-Failure Criterion (SFC), to the systems that perform level F1 Safety Functions. The initiating event and the unavailability according to the SFC shall be combined with Loss Of Off-site Power (LOOP) where this is unfavourable. However, the acceptance criteria for Design Basis Category 2 and 3 Conditions combined with the unavailability according to the SFC and LOOP may be relaxed to those for Design Basis Category 4 Conditions* where this can be justified on probabilistic grounds. The initiating event shall be assumed to precede the LOOP.

EUR Volume 2 Chapter 1, under section 2.1.3.4 defines that An Assembly of Equipment[A] satisfies the Single Failure Criterion (SFC) if it can perform its Safety Function despite a single random failure assumed to occur in any part of the assembly during any plant design condition in which the assembly is required to operate. This includes unrevealed pre-existing failures. Consequential failures resulting from the assumed single failure shall be considered to be an integral part of the single failure. The SFC shall be applied to each Assembly of Equipment which performs all actions required to fulfil a level F1 function for a given initiating event in order that the limits specified in the design basis for that event are not exceeded. The need to apply SFC to level F2 functions should be determined on a case by case basis. The need and safety benefits to apply SFC to systems and equipment not taking part in performing the level F1 or F2 functions shall be assessed by Designer. If, for a particular Safety Function, it is necessary to operate various systems simultaneously or successively, a single failure shall be postulated in any one of the systems in turn but not simultaneously in more than one of them. In the single failure analysis (A leak of a fluid system is not considered credible during the first 24 h after the initiating event), the failure of a passive component may not need to be assumed if this component is designed, manufactured, installed, inspected and maintained in service to a high quality level. However, when it is assumed that a passive component does not fail, such an approach shall be justified, taking into account the total period of time that the component is required after the initiating event. The treatment of certain components sometimes considered passive, such as check valves, should be based on a realistic assessment, rather than on prescriptive Rules*. Thus, single failures should be assumed for check valves that have to change state unless sufficient evidence exists to show, in relation to their implicit reliability, that this is unduly conservative.
In certain cases it may not be necessary to consider the combination of an event or Hazard with a single failure when the probability of the combination is very low e.g. aircraft crash. The Designer shall implement specific design provisions to avoid and inhibit spurious actuations of plant automation unless probabilistic arguments can be deployed to show it to be unreasonable. The Designer shall provide an assessment of such design provisions (permissives, interlocks, priority Rules among signals, voting logic principles, etc.) implemented in Instrumentation and Control (I&C) and Human-Machine Interface (System) (HMI) design. Single Operator* errors shall not be considered as a single failure.

[A] An Assembly of Equipment is defined as the combination of systems and components that perform a specific function. Therefore, the required Redundancy may not be applied to a single system if another system is available to perform the same Safety Function with performances compatible with the safety objectives. The functional safety class corresponding the Safety Category of any individual system or equipment inside Assembly of Equipment shall be equal or higher than the safety class of the highest Safety Functions they perform.

While failure of active components is included in the application of the Single Failure Criterion as in the current practice, this requirement includes also passive pre-existing failures, such as minor leaks, that may be existing unrevealed, during plant operation.
In this context, where the Assembly of Equipment is a system with Redundancy, the term is to be understood to mean the whole redundant system.

SFC is strictly connected to the Redundancy through 2.1.6.2.1 where it is required that Redundancy, the use of more than the minimum number of sets of equipment to accomplish a given Safety Function, shall be employed for improving the reliability and to meet the Single-Failure Criterion in systems performing F1 functions and certain F2 functions. Redundancy enables failure or unavailability of one set of equipment to be tolerated without loss of the function. For the purposes of Redundancy, identical or diverse components may be used. The assessment of the degree of Redundancy required should take account of the requirements of the SFC, and of the requirements resulting from the PSA results.

Exception during testing and maintenance - Allowable Outage Time (AOT)
Allowable Outage Time (AOT) is not defined in EUR Volume 2 Chapter 1, under section 2.1.3.4 but it is stated that components may be withdrawn from service for repair, periodic maintenance or testing. During this limited period, the combined frequency of Postulated Initiating Event and loss of Safety Function or the effect on the system's capability to perform its Safety Function shall be demonstrated to be low enough in order not to consider SFC. Under the section comment is written that in some countries, the N+2 criterion is required (single failure together with unavailability due to maintenance or testing) for Safety Systems and systems important for the overall plant availability.

2.4 US NRC's application of Single Failure Criteria (SFC) and allowable outage time (AOT)

US NRC Regulations, Title 10 [1], Code of Federal Regulations under its Appendix A (General Design criteria (GDC) for Nuclear Power Plants) defines the Single Failure:

"*A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions.*" With note 2: "*Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development*."

US NRC RG-1.53 [19] requires that the safety systems for plants with construction permits issued after May 13, 1999, must meet the requirements of IEEE Std. 603-1991. EEE Std. 603-1991 uses the term "safety systems" rather than "protection systems" to define its scope. A "safety system" is defined in IEEE Std. 603-1991 as "a system that is relied upon to remain functional during and following design basis events to ensure: (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (iii) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10 CFR Part 100 guidelines." A"safety function" is defined in IEEE Std. 603-1991 as "one of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event." IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,"1 was prepared by Working Group SC 6.3 of IEEE Nuclear Power Engineering Committee and was approved by the IEEE Standards Board on September 21, 2000. The standard provides guidance on the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. The systems include the actuation and protection systems, as well as the sense, command, and execute features of the power system. The guidance in this standard has been developed for electrical systems. However, where the interface with mechanical systems is unavoidable (e.g., sensing lines), the mechanical portions are considered to be a part of the electrical system with which they interface. The NRC recognizes that "protection systems" are a subset of "safety systems." Safety system is a broad-based and all-encompassing term, embracing the protection system in addition to other electrical systems. This regulatory guide is not intended to change the scope of the systems covered in the final safety analysis report for the currently operating nuclear power plants. Therefore, the regulatory guidance in this revision applies only to plant protection systems for currently operating nuclear power plants; and any application to a broader scope, namely safety system modifications, is voluntary. The staff continues to encourage, but not require, operating nuclear power plants to comply with IEEE Std. 603-1991 and IEEE Std. 379- 2000 for future system-level modifications.

Also, the risk-informed and performance-based alternatives to the single-failure criterion was studied [22] to identify potential alternative risk-informed approaches to the SFC. Example

applications of each alternative were carried out; the findings are discussed in this report. Additional examples or pilot activities would give a better understanding of the potential usefulness of such alternatives, including approaches to implementation, and the implications on resources required for their further development and implementation. For few alternatives, the approaches are based on low assessed event probabilities. Work would be needed to both create a basis for assessing the requirements for implementation implied by the approach, and establish protocols for making licensing decisions. A new regulation would require an acceptable rationale to reasonably assure that certain event probabilities are low, and that they would remain so, and that if the probabilities change, what licensing actions need to result. Additionally, some relationships between the safety analyses and plant equipment classification cut across regulations. Rather than working with assessed probabilities directly in licensing decisions, one alternative employs reliability targets defined relative to top-level safety objectives. The development of regulatory protocols and rationale apply to an even greater extent to this alternative. In summary, it was concluded that care will be needed to make sure that the ramifications of these changes are considered. A detailed deliberation of these alternatives would need to be informed by practical trial applications, including a consideration of implementation methods.

Exception during testing and maintenance - Allowable Outage Time (AOT)

10CFR50.36 requires that each operating license (OL) issued by the Commission contain technical specifications (TS) that set forth the limits, operating conditions, and other requirements imposed upon facility operation for the protection of public health and safety. As part of the regulatory standardization effort, the staff has prepared standard technical specifications (STS) for each of the light–water reactor nuclear steam supply systems (NSSSs) and associated balance–of–plant equipment systems (e.g. NUREG-1431[15]). These STS are subject to revision, and the latest versions are available from the U.S. Nuclear Regulatory Commission (NRC) website at http://www.nrc.gov

Since the mid-1980s, the NRC has been reviewing and granting improvements to technical specifications that are based, at least in part, on probabilistic risk assessment (PRA). The Commission reiterated that it expects licensees to use any plant-specific PRA or risk survey in preparing technical specifications for NRC approval when it issued the revision to 10 CFR 50.36[21] , "Technical Specifications," in July 1995. In August 1995, the NRC adopted a final policy statement on the use of PRA methods in nuclear regulatory activities that encourages greater use of PRA to improve safety decisionmaking and regulatory efficiency. Since that time, the industry and the NRC have been pursuing increased use of PRA in developing improvements to technical specifications. Consistent with the Commission's policy statement on technical specifications and the use of PRA, the NRC and the industry continue to develop more fundamental risk-informed improvements to the current system of technical specifications. We use the term "risk management technical specifications" to emphasize the goal of constructing technical specifications that reinforce the pro-active management of the total risk presented by the plant configuration and actions that may be needed to respond to emergent conditions. These improvements are intended to maintain or improve safety while reducing unnecessary burden and to bring technical specification requirements into congruence with the Commission's other risk-informed regulatory requirements, in particular, the maintenance rule. The use of risk information and technology has long been a fundamental ingredient in improving technical specifications. In the 1983 publication "Technical Specifications - Enhancing the Safety Impact" (NUREG-1024), the NRC Task Group on Technical Specifications commented on the technical specifications of the era:

"The Task Group recognizes that the times associated with surveillance frequencies, allowable outage times, etc., have been established on a deterministic basis using engineering

judgment. The Task group also believes that engineering judgment must be the primary basis for any changes to the Technical Specifications. However, the Task Group believes that the use of insights from probabilistic risk assessments could be a significant aid in arriving at these judgments."

Technical Specifications have taken advantage of risk technology as experience and capability have increased.

Guidance documents have been prepared to assist in requesting risk-informed completion time (also called allowed outage time) and surveillance test interval extensions (Regulatory Guide 1.177 [17] and Standard Review Plan Chapter 16.1 [14]. Use of this guidance (categorized as "Option 1" in the framework of the Risk-Informed Regulatory Improvement Program) has resulted in risk-informed amendments at numerous plants and in owners groups continuing to submit topical reports to support additional applications for Standard Technical Specification (STS) changes.

Before issuance of the maintenance rule, 10 CFR 50.65[20], in July 1991, technical specifications primarily governed plant operations. They dictated what equipment must normally be in service, how long equipment can be out of service, compensatory actions, and surveillance testing to demonstrate equipment readiness. The maintenance rule marked the advent of a regulation with significant implications for the evolution for technical specifications. The goal of these technical specifications is to provide adequate assurance of the availability and reliability of equipment needed to prevent and, if necessary, mitigate accidents and transients. The maintenance rule shares this same goal but operates at a more fundamental level with a dynamic and more comprehensive process.

In addition to specifying a process for monitoring the effectiveness of maintenance, including performance and condition monitoring, and for balancing maintenance unavailability and equipment reliability, the maintenance rule requires licensees to assess and manage plant configuration risk that results from maintenance. The maintenance rule has put in place many of the mechanisms, measures, and processes envisioned by staff as needed to enhance the safety impact of technical specifications. Thus, achieving synergy between the static technical specifications and the dynamic maintenance rule is a major aim of the effort to create risk management technical specifications.

US NRC RG-1.174 [14] describes an acceptable approach for assessing the nature and impact of proposed licensing basis changes by considering engineering issues and applying risk insights. The changes that make up a combine change request should be related to one another, for example, by affecting the same single system or activity, by affecting the same safety function or accident sequence or group of sequences, or by being of the same type (e.g., changes in outage time allowed by technical specifications). However, this does not preclude acceptance of unrelated changes. Assessments should consider relevant safety margins and defense-in-depth attributes, including consideration of success criteria as well as equipment functionality, reliability, and availability. The analyses should reflect the actual design, construction, and operational practices of the plant. Acceptance guidelines for evaluating the results of such assessments are provided. This guide also addresses implementation strategies and performance monitoring plans associated with licensing basis changes that will help ensure that assumptions and analyses supporting the change are verified. Consideration of the Commission's Safety Goal Policy Statement [18] is an important element in regulatory decisionmaking. Consequently, this regulatory guide provides acceptance guidelines consistent with this policy statement. In theory, one could construct a more generous regulatory framework for consideration of those risk-informed changes that may have the effect of increasing risk to the public. Such a framework would include, of course, assurance

of continued adequate protection (that level of protection of the public health and safety that must be reasonably assured regardless of economic cost). But it could also include provision for possible elimination of all measures not needed for adequate protection, which either do not effect a substantial reduction in overall risk or result in continuing costs that are not justified by the safety benefits. Instead, in this regulatory guide, the NRC has chosen a more restrictive policy that would permit only small increases in risk, and then only when it is reasonably assured, among other things, that sufficient defense in depth and sufficient margins are maintained. This policy is adopted because of uncertainties and to account for the fact that safety issues continue to emerge regarding design, construction, and operational matters notwithstanding the maturity of the nuclear power industry. These factors suggest that nuclear power reactors should operate routinely only at a prudent margin above adequate protection. The safety goal subsidiary objectives are used as an example of such a prudent margin. Finally, this regulatory guide indicates an acceptable level of documentation that will enable the staff to reach a finding that the licensee has performed a sufficiently complete and scrutable analysis and that the results of the engineering evaluations support the licensee's request for a regulatory change.

2.5 Finish Regulatory Framework for Single Failure Criteria (SFC) and Allowable Outage Time (AOT)

By virtue of section 55, second paragraph, point 3 of the Nuclear Energy Act (990/87) and section 29 of the Council of State Decision (395/91) on General Regulations for the Safety of Nuclear Power Plants, the Finnish Centre for Radiation and Nuclear Safety (STUK) issues detailed regulations concerning the safety of nuclear power plants. YVL Guides are rules an individual licensee or any other organisation concerned shall comply with, unless STUK has been presented with some other acceptable procedure or solution by which the safety level set forth in the YVL Guides is achieved. To satisfy this requirement, the safety functions of the nuclear power plant shall be highly reliable. Design objectives ensuring the reliability of the most important safety functions are given in Guide YVL B.1[38].

Previous guideline YVL 2.7[46] discussed the general design principles, application of failure criteria to safety functions refering to IAEA 50-P-1 (see section above IAEA above, principles of application, rules of application,special requirements for fire protection), the diversity principle, application of failure criteria in compliance with the diversity principle and the failure. YVL 2.7 defined single failure as random failure plus its consequent effects which are assumed to occur during either a normal operational condition or in addition to an initiating event and its consequent effects. YVL 2.7 is supersseded by YVL B.1[38] in 2013 to be more similar with IAEA SSR-2/1[1] and EUR revision C[31].

YVL B.1[38] defines that single failure shall refer to a failure due to which a system, component or structure fails to deliver the required performance. Single failure criterion (SFC) (N+1) shall mean that it must be possible to perform a safety function even if any single component designed for the function fails. YVL B.1 discusses actually the two failure criteria:

- (N+1) failure criterion shall mean that it must be possible to perform a safety function even if any single component designed for the function fails.
- (N+2) failure criterion shall mean that it must be possible to perform a safety function even if any single component designed for the function fails and any other component or part of a redundant system – or a component of an auxiliary system necessary for its operation – is simultaneously out of operation due to repair or maintenance.

YVL B.1 discusses in bullet 4.3.1 and 4.3.2 independence of the defence in depth levels and strength of individual levels of defence in depth. According to Section 12 of Government Decree 717/2013, the levels of defence required under the defence-in-depth concept shall be as independent of one another as is reasonably achievable. The loss of any single level of defence may not impair the operation of the other levels of defence. From the maintenance point of view it is important (bullet 432) that no single anticipated failure or spurious action of an active component taking place during normal plant operation shall lead to a situation requiring intervention by systems designed to manage postulated accidents. Provisions shall be made for failures by ensuring that systems performing a safety function consist of two or more redundant systems or system parts in parallel, so that the safety function can be performed even if any of them is rendered inoperable. The redundant parts of a system performing safety functions shall be assigned to different safety divisions. 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. The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of internal events (e.g. fire, flood or dynamic effects) or external events. Detailed requirements regarding the separation of safety divisions hosting redundant parts of safety systems are provided in Guide YVL B.7[44]. Just for example of definition different failure criterion for various safety systems YVLB.1 in specific requirements for systems needed for achieving and mainaining a controlled state (4.3.3) defines the acceptance criteria set for events in design basis categories DBC1, DBC2, DBC3, DBC4 and DEC. The acceptance criteria for radiological consequences in each event category are specified in Sections 8, 9 and 10 of Government Decree 717/2013 and in Guide YVL C.3. The acceptance criteria concerning fuel failures are specified in Guide YVL B.4 [41], and those concerning overpressure protection in Guide YVL B.3[40]. The analysis requirements for demonstrating fulfilment of the criteria are given in Guide YVL B.3[40]. Under bullet 446 it is required that In addition to the fast shutdown system based on solid neutron absorbers, the reactor shall have a diverse shutdown system capable of shutting down the reactor into a controlled state and keeping it subcritical for a prolonged period of time following an initiating event of any anticipated operational occurrence or Class 1 postulated accident (with the exception of loss of coolant accidents included in Class 1 postulated accidents) in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design basis category DEC are not exceeded. The shutdown system that complies with the diversity principle shall satisfy the (N+1) failure criterion. Also, under bullet 448 it is written that in the event of anticipated operational occurrences or postulated accidents, it shall be possible to accomplish decay heat removal from the reactor and containment by one or several systems that jointly meet the (N+2) failure criterion and the 72-hour self-sufficiency criterion in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in the respective design basis category DBC2, DBC3 or DBC4 are not exceeded. In addition to the decay heat removal system(s) meeting requirement 448, the nuclear power plant shall have a system that complies with the diversity principle and is capable of removing the decay heat from the reactor and containment following an initiating event of any anticipated operational occurrence or Class 1 postulated accident in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design basis category DEC are not exceeded. The decay heat removal system that complies with the diversity principle shall satisfy the (N+1) failure criterion and the 72-hour self-sufficiency criterion. If the system that complies with the diversity principle is capable of providing decay heat removal in such a way that the limits set forth for fuel integrity, radiological

consequences and overpressure protection in the respective design basis categories DBC2, DBC3 or DBC4 are not exceeded, the system can also be counted among the systems that jointly meet the (N+2) failure criterion given in requirement 448. Section 4.3.4 of YVL B.1 deals with the specific requirements for systems needed for reaching and maintaining a safe state. The chapter 5 of YVL B.1 deals with the design of specific nuclear power plant systems where the application of SFC requirement for various systems are defined.

YVL B.3[40] defines the minimum system performance. Minimum system performance can be determined by making the following assumptions:

- Consider the consequential effects of the initiating event (component failure, for example).
- Furthermore, select the failure combination that is most detrimental to the functionality of the system in accordance with the failure criterion presented in chapter 4.3 of Guide YVL B.1[38]. The single failure with the highest reactivity effect is also assumed to occur in the reactor scram system.
- Determine the performance parameters for each functioning component, which conform to the acceptance limits of components in periodic tests.

Sub YVL guidelines (e.g.YVL B.6 [43], B.5[42], B.2[39] or B.8[45]) based on YVL B.1[38] define the applicability and requirements for SFC for various systems, structures and components. For example, YVL B.6 refers in bullet 105 that section 14(8) of Government Decree 717/2013 states that the plant shall be provided with systems, structures and components for controlling and monitoring severe accidents. These systems shall be independent of the systems designed for normal operational conditions, anticipated operational occurrences and postulated accidents. Systems necessary for ensuring the integrity of the containment in a severe accident shall be capable of performing their safety functions, even in the case of a single failure. Under bulletin 330 and 336 it is required that the containment isolation and containment heat removal shall be possible during accidents even in case of a single failure. YVL B.5 defines in 416 that the components that can increase pressure in the primary circuit (e.g. pressuriser heaters or pumps) shall be equipped with a system that stops the operation of the component to prevent inadvertent pressure increase and is capable of performing the protection function also in the event of a single failure. YVL B.2 discusses under bullet 325 that Safety Class 2 systems, structures and components required to bring the plant to a controlled state during anticipated operational occurrences or Category 1 accidents at least to the extent that the system's earthquake-resistant subsystems accomplish the single-failure criterion. YVL B.8 discuss that in evaluating implementation of the defence in depth approach to fire protection, failures or impairments in the nuclear facility's fire protection shall be assumed. It shall be demonstrated that a single failure or deviation in fire protection does not lead to uncontrolled fire spread and endanger the facility's safety. When a fire in the fire compartment under analysis cannot cause an initiating event at the nuclear power plant but causes the failure of a redundant subsystem important to safety, the failure is then considered a single failure/common cause failure as referred to in Guide YVL B.1. It shall be possible to bring the nuclear power plant into a safe state even if a fire causes consequential failures in safety functions, in addition to the initiating event, and even if safety functions are affected by a single failure that is independent of the fire.

Also, sub YVL guidelines (e.g. YVL C.3[47]) discusses the SSCs which does not need to satisfy SFC. For example YVL C.3[47] in 513 discusses that the releases of radioactive iodine through the vent stack shall also be measured by means of a stationary, continuously-

operating radiation monitoring system based on the measurement of the activity of 131I contained in the sample that is collected in the filter on a continuous basis. However, this system does not need to meet the single failure criterion.

Exception during testing and maintenance - Allowable Outage Time (AOT)

YVL A.6[31] defines under 737 that the Operational Limits and Conditions (OLC) shall specify the requirements established for operating the nuclear power plant unit concerned covering:

- the process parameter limits that are critical in terms of the integrity of barriers, derived from the analyses serving as the design basis;
- the limits for the activation of protection and limitation systems;
- the basic requirements for safety systems to be complied with in different operational states, limit values, allowed deviations, operability requirements, the actions to be taken, and the time allowed to complete these actions;
- the periodic testing, inspection, and surveillance programmes for ensuring the operability of systems, structures, and components subject to operability requirements;
- the testing frequency, staggering, operational state, and the related instructions;
- any preventive maintenance giving rise to inoperability;
- the administrative requirements;
- the justifications for the requirements specified above.

YVL A.7[37] under 317 defines the risk-informed development of the Operational Limits and Conditions (OLC) to assess their coverage and balance. The description of the risk-informed method shall be submitted to STUK for approval during construction and the application for information in connection with the submission of the OLC document. The PRA shall be used to determine the surveillance test intervals and allowed outage times of systems and components important to safety. The Operational Limits and Conditions and allowed outage times applied on structures, systems and components shall be separately analysed for every plant operational state. The PRA shall also be used to analyse failures where the change of the operational state may cause a greater risk than repairing the failure without changing the operational state. Furtehrmore, the following 3 bullets discuss the risk-informed development of the Operational Limits and Conditions (OLC):

318. The PRA shall be used in the risk-informed development of testing procedures for systems and components important to safety. The description of the risk-informed method shall be submitted to STUK for approval during construction and the application for information no later than with the submission of the Operational Limits and Conditions document.

319. The PRA shall be used in the risk-informed development of on-line preventive maintenance programmes carried out during power operation for systems and components important to safety. The description of the risk-informed method shall be submitted to STUK for approval during construction and the application for information no later than with the submission of the Operational Limits and Conditions document.

320. The licensee shall apply the PRA in the risk-informed development of pre-service and in-service inspection programmes for piping and submit the methodology descriptions and applications of the inspection programmes to STUK in accordance with Guide YVL E.5.

Detailed methodology for determination of the surveillance test intervals and allowed outage times of systems and components important to safety are not given in YVL. It appears that Finnish Regulator (STUK) makes regulatory decisions regarding this subject on the case by case basis.

2.6 UK Regulatory Framework for Single Failure Criteria (SFC) and Allowable Outage Time (AOT)

ONR (Office for Nuclear Regulation) has established its Safety Assessment Principles (SAPs) [32] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. SAP EDR.4 defines the Single failure criterion: During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. Bullet 175 defines that the consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure. Bullet 175 refers the further discussion of the single failure criterion is given in IAEA Safety Standard NS-G-1.2 even that it is already superseded by GSR Part 4 and SSG-2. Further more, SAP ESS.24, defines the minimum operational equipment requirements as the minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion. SAP FA.6 (Fault sequnces) defines that each design basis fault sequence should include as appropriate: a) failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause; b) single failures in the safety measures in accordance with the single failure criterion; c) the worst normally permitted configuration of equipment outages for maintenance, test or repair; d) the most onerous permitted operating state within the inherent capacity of the facility.

It should be noted that NS-TAST-GD-044[35] was withdrawn in 2013 based on the redundancy and referring to WENRA Reactor Safety Reference Levels [28] Issues E and F, as well as IAEA standard and guides: IAEA Safety Standards – Safety Assessment for Facilities and Activities, GSR Part 4[6].

NS-TAST-GD-003 [32] technical assessment guide is one of these guides. Safety Systems represent a central pillar of the 'Defence in Depth' safety philosophy that is insisted upon in UK nuclear plants. It should be noted that under bullet 3.4 the explicit linkages between relevant sections of this guide and related WENRA Reactor Reference Levels are tabulated in Appendix 4 of [32]. The main aim of this philosophy is to avoid situations where an initiating fault can lead directly to an accident with nothing able to prevent it. Although faults cannot be prevented, provisions (engineered systems and/or procedures) can be deliberately put in place to recognise and respond to faults to prevent and/or mitigate the accident that would otherwise ensue (i.e. they provide protection against those faults). Such provisions are known as Safety Systems (SSs). Encompassed within the term 'safety system' are i) the protection system - the instrumentation which measures (or monitors) plant parameters (or states) and generates safety actuation signals when these parameters (or states) move beyond pre-set limits; ii) the safety actuation system - the equipment that physically accomplishes the required safety action(s) in response to actuation signal(s) from the protection system; and iii) the safety system support features - the equipment that provides services such as cooling, lubrication and energy supply to the protection and safety actuation systems. Where credit is claimed for redundancy or diversity, appropriate levels of separation should be shown between each SS, between the services to each SS (unless the SS is shown to be fail-safe with respect to service failures), and adequate segregation between the SSs and other equipment. Additionally the system as a whole should either be shown to be invulnerable to single failures, or the components with single-failure potential should be shown to be reliable and robust enough for

their failure contribution not to compromise system unreliability. Where a SS cannot be shown to be independent of the fault sequence that it safeguards (e.g. by being part of the control system whose failure is a fault initiator), then the potential exists for a single failure both to induce the fault sequence and also to render the SS unavailable. In these circumstances no credit should be allowed for the SS. If a licensee wishes to claim credit then it will be necessary to show that the dependencies are not able to prejudice operation of the SS.

SAP Target 9 gives a 'broadly acceptable' risk for large release accidents (>=100 fatalities) of 1E-7/yr. Hence for such accidents, again applying the 10% principle in SAP para 618, the limiting frequency for a single class of accident should be 1E-8/yr. For faults within the Design Basis, or where the SSs require a combined fpd between 1E-2 and 1E-4, there should be at least two redundant means (of comparable reliability) of achieving the safety function. The single failure criterion should be complied with; vulnerability to potential common-cause failures (ccfs) shown to be small in relation to the claimed fpd; services and connections free of common dependencies; adequate segregation from non SSs; and adequate separation between these and other SSs.

Exception during testing and maintenance - Allowable Outage Time (AOT)

Safety Assessment Principles (SAPs) [32] discuss also the operating limits and conditions (OLC). In SAP SC.6 it is defined that the safety case for a facility or site should identify the important aspects of operation and management required for maintaining safety. The important aspects of operation and management required to maintain safety should emerge from the safety case. All such aspects should be clearly set out and easy to understand and implement. Bullet 97 defines that the safety case for each life-cycle stage should include: a) the required maintenance, inspection and testing regimes that have been assumed for the case to remain valid; b) the operating limits and conditions required to ensure that the facility is kept in a safe condition; and c) inputs to emergency planning. SAP FA.9 defines that DBA (Design Basis Accident) should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions. Per bullet 526, DBA should provide the basis for: a) safety limits, ie the actuator trip settings and performance requirements for safety systems and safety-related equipment; b) conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment; c) the safe operating envelope defined as operating limits and conditions in the operating rules for the facility; and d) the preparation of the facility operating instructions for implementing the safe operating envelope, and other operating instructions needed to implement the safety measures.

NS-TAST-GD-003 [32] defines features of individual SSs including the means provided to maintain, calibrate, test (under operational conditions where possible) and inspect each component (including sensors and actuators); the intervals proposed; and the method of reinstatement after maintenance /calibration /testing /inspection. [SSs should be designed and installed so as to facilitate maintenance and testing etc without excessive dose uptake to operators and without introducing new or increased risks.] Proof tests should be shown to be fully effective for all parts of the system involved in delivering the relevant safety function, including any automatic testing or diagnostic test equipment used as part of testing, either during service or during proof test. Capability aspects define the evidence of performance adequacy including range, accuracy, response time, calibration, and margins to the fault study claims.

The old IAEA TECDOC [8] refer the development of technical specification surveillance requirements for Sizewell "B" power station (Westinghouse NPP) to the adaptation of Standard Technical Specifications (NUREG-1431) to the licensing requirements in the UK for the first Westinghouse PWR. The application of probabilistic methods in the design and safety analysis is described, and the decisions to be taken on the scope, structure and interdependence of the technical specifications for Sizewell "B" Power Station are assessed. Provisions have been made in the Station Instrumentation system to structure the on-line data base to be available for input to a system to monitor compliance with Technical Specifications. The detail of the computerized aid to the operating staff have yet to be decided, but the use of PSA in the development of Technical Specifications has been agreed. Refered paper describe the Specific guidance is given in Nuclear Electric Design Safety Guidelines on the treatment of maintenance and testing in reliability analyses. Nevertheless, when plant is out on maintenance or is undergoing testing it is desirable that the actual system unreliability at that particular point in time is sensibly limited. It would be undesirable for the cooling system unreliability at any point in time to be worsened by more than one decade when the permitted unreliability lies between 10^{-4} and 10^{-5} ,, or by two decades when the permitted unreliability is 10^{-6} or less. For cases where the permitted unreliability lies between 10^{-3} and 10^{-4} the point unreliability should never be increased above 10^{-3}.
Taking into account the above discussion, it can be reasonably concluded that UK regulator also accepts the USA NRC practice related to the definition of Operational Limits and Conditions (OLC), Surveillance Requirements (SR) and Allowable Outage Time (AOT) following USA NRC SRP 0800 chapter 16 (Technical Specification) and 16.1 (Risk-informed Decision Making: Technical Specifications).

2.7 Japan Nuclear Regulation Authority(NRA) application of Single Failure Criteria (SFC) and allowable outage time (AOT)

Japan Nuclear Safety Commision (NCS) documentation written in English is limted to publicly available resources on internet (http://www.nsr.go.jp/archive/nsc/NSCenglish/guides/index.htm). L-DS-I.0 [48] presents the Japan Nuclear Safety Commision (NSC) Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities. Per L-DS-I.0, the "Single failure" refers to the loss of intended safety functions of a component by a single cause. Multiple failures due to secondary causes are included in this category.
Guideline 9 (design consideration for reliability) defines:

1) SSCs with safety functions shall be so designed that their adequately high reliability will be ensured and maintained as required according to the importance of their safety functions.
2) Systems with safety functions of especially high importance shall be designed with redundancy or diversity and independence considering their physical make-up, working principles, and assigned safety functions, etc.
3) The systems referred to in item (2) above shall be designed to be capable of fulfilling their safety functions even in case of unavailability of off-site power in addition to an assumption of a single failure of any of the components that comprise the systems.

Context of "... adequately high reliability... as required according to the importance of their safety functions" and "systems with safety functions of especially high importance" are specified separately in "Importance Classification Guide".
"Single failure" is categorized into two kinds, i.e., single failure of active component and single failure of passive component. Systems with safety functions of especially high importance shall be designed so that they can fulfill their expected safety functions even with an assumption of a single failure of any active component during a short term and with an assumption of either a single failure of any active component or a postulated single failure of any passive component during a long term. In evaluating the long-term safety functions for which either a single failure of any active component or a postulated single failure of any passive component is to be assumed, the assumption of a single failure in particular components can be exempted if it is assured that such a single failure can be removed or remedied within a period of time not being detrimental to safety.

Guideline 9 is than applied for requirements of all other safety systems. E.g.guideline 24 discuss the systems for removing the residual heat: (1) The systems for removing residual heat shall be designed to be capable of removing fission product decay heat and other residual heat from the core during reactor shutdown, thereby preventing the acceptable fuel design limits and design conditions for the reactor coolant pressure boundary from being exceeded.
(2) The systems for removing residual heat shall be properly provided with redundancy or diversity and independence so that they can fulfill their safety functions even in case of unavailability of off-site power in addition to an assumption of a single failure of any of the components that comprise the systems. They shall also be designed to allow testing with respect to their functional capability.

Similar approach to the one from guideline 9 is applicable to the following systems:

- Guideline 25. Emergency Core Cooling System

- Guideline 26. Systems for Transporting Heat to Ultimate Heat Sink
- Guideline 32. Reactor Containment Heat Removal System
- Guideline 33. Systems for Controlling Containment Facility Atmosphere
- Guideline 34. Redundancy of Safety Protection System
- Guideline 48. Electrical Systems (The emergency on-site power system shall incorporate redundancy or diversity and independence and have enough capacity and capability to accomplish the following properly even with an assumption of a single failure of its components.)

Furthermore, in context of the guideline 30 "... in general be designed to be automatically and properly closed" refers to the capability of containment isolation valves to automatically close in response to the containment isolation signals from the safety protection system, for example, and minimize the leakage of radioactive materials from the reactor containment in conjunction with isolation barriers other than containment isolation valves even in case of unavailability of off-site power in addition to an assumption of a single failure.
In the context of guideline 38 (Function of Safety Protection System in Case of Failure) the "driving power loss, system cut-off or any other unfavorable situation" refers to the loss of electric power or instrumentation air or a situation in which the safety protection system has its logic circuit cut off for some reason. The factors to be considered as the "unfavorable situation" shall be determined depending on the respective design, including environmental conditions. "Settled in a state of safety eventually" means that even in case of a failure in the safety protection system, the nuclear reactor facility will be settled into a state on the safe side or can be maintained in a safe state despite the failure in the safety protection system being not repaired.
Also, in the context of guideline 39 (Separation of Safety Protection System from Instrumentation and Control Systems) "... the system does not lose its safety functions" means that, even if any of the components or channels comprising the instrumentation and control systems which are connected to the safety protection system may be subjected to a single failure, mis-operation or removal from service, the safety protection system with its functions not being impaired can fulfill the requirements in paragraphs 34 through 38.

<u>Exception during testing and maintenance - Allowable Outage Time (AOT)</u>
L-DS-I.0 defines in guideline 10 (design considerations for testability) that SSCs with safety functions shall be designed to be capable of being tested or inspected to verify their integrity and capability by adequate methods consistent with the importance of their safety functions during reactor operation or shutdown. In the context of guideline 10 the"adequate methods" include the use of testing bypass systems in case test or inspection using systems in actual service is inadequate.
The similar approach from guideline 10 (“systems should be designed to to allow testing with respect to their functional capability”) are specified for the following guidelines:

- Guideline 15. Independence and Testability of Reactor Shutdown System
- Guideline 24. Systems for Removing Residual Heat
- Guideline 25. Emergency Core Cooling System
- Guideline 26. Systems for Transporting Heat to Ultimate Heat Sink
- Guideline 32. Reactor Containment Heat Removal System

- Guideline 33. Systems for Controlling Containment Facility Atmosphere
- Guideline 35. Independence of Safety Protection System
- Guideline 40. Testability of Safety Protection System (The safety protection system shall be designed to be capable of being tested in general during reactor operation on a periodical basis and allow testing of each constituent channel independently so that the integrity and redundancy of the system can be verified.)

Taking into account that Japanese NPPs design are based on USA NRC design bases it is reasonable to conclude that Japan follow the USA NRC practice related to the definition of Operational Limits and Conditions (OLC), Surveillance Requirements (SR) and Allowable Outage Time (AOT) following USA NRC SRP 0800 chapter 16 (Technical Specification). In one older IAEA-TECDOC [8] it was disscused that in Japanese safety regulations, operational limits and limiting conditions for operations are specified, however, they are only basic requirements and based on the deterministic methods. Each utility applies detailed procedures voluntarily. The probabilistic approach is not officially adopted in Japan to determine Technical Specifications requirements. Probabilistic methods are, however, used supplementarily to evaluate the validity of Technical Specifications. The trend in Japan is to increase the use of the probabilistic methods in the future. Some studies are being made on the applicability of probabilistic methods to the establishment of Technical Specifications.

2.8 Korean Regulatory Framework for Single Failure Criteria (SFC) and Allowable Outage Time (AOT)

Korean Regulatory Framework is defined by the 5 nuclear acts, from [23] to [27]. The regulatory framework document "Regulations on Technical Standards for Nuclear Reactor Facilities No. 4" [23] discuss the nuclear power plant design bases. Among other requirements, the Single Failure relevant regulatory requirements are listed bellow:

Article 2 (Definitions)

11. The term "single failure" means a failure which results in the loss of capability of a component to perform its intended safety functions, and multiple failures resulting from such failure are considered to be a single failure.

Article 24 (Electric Power System)

(1) Onsite and offsite electric power systems necessary for the performance of the functions of the structures, systems, and components important to safety shall be provided to nuclear reactor facility to meet the following requirements:

1. In the event of a loss of either onsite or offsite electric power systems, the remaining available system shall have sufficient capacity and capability to prevent the specified acceptable fuel design limits and the design conditions of reactor coolant pressure boundary from being exceeded in anticipated operational occurrences and to maintain the safety; and
2. The systems shall have sufficient capacity and capability to maintain reactor core cooling, containment structural integrity, and other essential functions in the design basis accidents.

(2) The onsite electric power system, including the batteries, and onsite electric distributions system shall have sufficient independency, redundancy, and testability necessary to maintain their safety functions assuming a single failure.

(3) Electric power from power transmission network to the onsite electric distribution system shall be supplied by two physically and electrically independent circuits to minimize the likelihood of their simultaneous failure under normal operation conditions, design basis accidents, and all environmental conditions. And it shall be designed to meet each of the following requirements:

1. Each circuit shall be available immediately following a loss of all the onsite alternating current power supply and the other offsite electric power circuit; and
2. One of the two independent circuits shall be available within a few seconds following loss of coolant accidents.

(4) The stability analysis of the electric grid shall assure that the probability of losing any of the remaining power sources as a result of the loss of at least one among the electric power sources by the nuclear power unit, from the transmission network, or from the onsite electric power sources including emergency power sources is extremely low.

(5) Safety-related electric power systems shall be designed to allow periodic tests and inspections in order to check the continuity of such systems and the states of their components.

(6) An alternative alternating current power source with necessary capacity and reliability shall be provided to prepare for the cases of total loss of alternating current power and no

capability to cope with the such loss. The performance of the alternative alternating current power source shall be demonstrated through tests.

Article 26 (Protection System)

(1) Protection system that meet each of the following requirements shall be installed at reactor facilities:

1. The protection system shall be designed to initiate automatically the operation of appropriate systems including the reactivity control systems in order to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences such as noticeable increase in reactor power or a significant reduction in core cooling capability.
2. The protection system shall be designed to sense accident conditions and to initiate the operation of systems important to safety.

(2) The protection system shall be designed in accordance with each of the following requirements in order to assure the performance of its safety functions:

1. The protection system shall meet each of the following requirements to ensure the reliability of the safety functions and to check any failure, etc. during operation:
    a. The design features of redundancy and independency shall be considered to ensure that no single failure results in loss of protection function, and that removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated; and
    b. The protection systems shall be designed to permit periodic testing of its functioning, including the capability to test channels independently, in order to check failures and loss of redundancy during reactor operation.
2. The effects of normal operation conditions including natural phenomena, checking, maintenance, and testing, anticipated operational occurrences, and accident conditions on multiple channels shall not result in lose of the protection functions.
3. The protection system shall remain in a safe state under a component failure, loss of energy sources such as electric power and instrument air, or the worst postulated environment conditions, by adoption of the design feature of fail-safe behavior.
4. The protection system shall be separated from the control systems to ensure that the protection system satisfies all the reliability, diversity, and independence requirements in the following states:
    a. Failure of a single component or channel of control systems;
    b. Failure of a common component or channel of control and protection
    c. Removal from service of a single channel.
5. The protection system shall be designed to assure that the specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems such as accidental withdrawal of control rods.
6. The protection system shall be able to accomplish the safety functions required in anticipated operational occurrences.

7. The protection system shall have the capability to adjust trip or operation set-points according to the operation conditions.
8. In the case of adoption of software-based digital equipment, the design concepts of defence-in-depth and diversity including manual functions shall be applied to the design of the protection system in order to assure the implementation of protection functions required at a common mode failure of software.

Article 28 (Reactivity Control System)

(1) Reactivity control systems (meaning systems to control reactivity using control rods and using liquid absorber material by its injection or changes in its concentration) shall be installed to meet each of the following requirements:

1. Reactivity control systems shall be capable of reliably controlling anticipated reactivity changes under normal operations and anticipated operational occurrences, and capable of maintaining operating states without exceeding specified acceptable fuel design limits.
2. Two independent reactivity control systems of different design principles shall be provided and one of the systems shall use control rods.
3. One of the systems as provided in the foregoing Subparagraph 2 shall be capable of rendering the reactor subcritical from normal operation and maintaining the core subcritical under cold condition.

(2) The control rods system shall be capable of immediately performing its functions and reliably controlling reactivity changes to assure that specified acceptable fuel design limits are not exceeded with appropriate margin under the condition of any single stuck rod.

(3) The second reactivity control system using liquid absorber material or etc. shall be capable of reliably controlling the rate of reactivity changes due to planned normal power changes to assure that specified acceptable fuel design limits are not exceeded.

(4) The reactivity control materials shall have necessary physical and chemical properties under the severe conditions caused by pressure, temperature, and radiation during normal operations.

Article 29 (Residual Heat Removal System)

(1) System capable of removing heat due to fission product decay heat and other residual heat from the core shall be installed to assure that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

(2) The system for residual heat removal shall have the design features of redundancy, leak detection, and suitable isolation capabilities to maintain the safety under the assumption of loss of offsite or onsite power-single failure.

Article 30 (Emergency Core Cooling System)

(1) A system for emergency core cooling with sufficient capability necessary to maintain the safety shall be installed to meet each of the following requirements following loss of residual heat removal capability or loss of reactor coolant accidents, and such system shall meet the

requirements determined and publicly notified by the Nuclear Safety and Security Commission:

1. Cladding temperature shall not exceed an acceptable design value;
2. Oxidization and hydrogen generation in cladding shall be limited to an allowable level;
3. Deformation of fuel and internal structures shall not reduce the effective core cooling; and
4. Core cooling shall be ensured for a time necessary for the removal of decay heat.

(2) The system for emergency core cooling shall have the design feature of redundancy, leak detection, isolation, and containment capabilities to maintain the safety functions with sufficient reliability under the assumption of loss of offsite or onsite power-single failure.

Article 31 (Ultimate Heat Sink)

(1) A system to transfer the combined heat load of structures, systems, and components important to safety to an ultimate heat sink during normal operations and design basis accident conditions shall be provided.

(2) The system shall have the design feature of redundancy, suitable interconnection and isolation capabilities, and etc. to maintain the safety under the assumption of loss of offsite or onsite.

Article 44 (Reliability) Structures, systems, and components that perform safety functions shall meet each of the following requirements to assure and maintain sufficiently high reliability commensurate with the importance of the safety functions.

1. The principles of redundancy, diversity, functional independence, and physical separation shall be adopted in the design, considering their structure, operational principles, and safety functions to be performed; and power-single failure.
2. The safety functions shall be accomplished in case of loss of offsite or onsite power-single failure.

Article 66 (Radioactive Waste Management Program)

(1) In accordance with Article 41 (1) 10 of the Decree, the operator of a nuclear power reactor shall establish a radioactive waste management program, minimize the amount of radioactive wastes and effluents, and reduce the environmental impact of radioactive effluents.

(2) The radioactive waste management program as provided in the foregoing Paragraph (1) shall include procedures to monitor, measure, store, transport and process radioactive wastes in an appropriate manner, and include each of the following items for the assessment of the environmental impact of discharging radioactive effluents:

1. Offsite dose assessment;
2. Operation of radioactive effluents monitoring system;
3. Sampling and analysis program regarding liquid and gaseous effluents; and
4. Radioactive waste solidification process program, etc.

(3) The annual dose at the exclusion area boundary due to gaseous effluents, which are discharged from the operation of a single nuclear power reactor or multiple nuclear power reactors within the same site, shall not exceed the limit prescribed by the Nuclear Safety and Security Commission in order to prevent the environmental hazard.

(4) Processing, discharge and storage of radioactive wastes shall be in accordance with Article 10 of the Radiation Safety Regulations.

Exception during testing and maintenance - Allowable Outage Time (AOT)

The regulatory framework document "Regulations on Technical Standards for Nuclear Reactor Facilities No. 4" [23] defines in the Article 41 (Testability, Monitorability, Inspectability, and Maintainability) that:

(1) The structures, systems, and components important to safety shall be designed to be tested, monitored, inspected, and maintained in accordance with the importance of safety functions to be performed to ensure that their structural integrity, leak tightness, functional capability, and operability are maintained during the lifetime of the nuclear power plant.

(2) For cases where periodic testing, monitoring, inspection and maintenance are limited or not possible to detect the possible faults of components, safety measures shall be made in the design to cope with expected failures.

(3) Pressure vessels (excluding auxiliary boilers), pipings, major pumps and major valves shall meet the acceptance criteria of pressure retaining test determined and publicly notified by the Nuclear Safety and Security Commission.

Also, [23] in Article 97 (Surveillance and Checking of Nuclear Fuel Cycle Facilities) discuss that the pursuant to Article 68 (1) 3 of the Decree, a nuclear fuel cycle enterpriser shall conduct surveillance and checking of nuclear fuel cycle facilities atleast once a day. Furthermore, Article 98 (Self-check of Nuclear Fuel Cycle Facilities) defines that the pursuant to Article 68 (1) 5 of the Decree, a nuclear fuel cycle enterpriser shall take each of the following measures:

– With respect to any equipment that requires special control to achieve safety as provided in the safety control regulations, such equipment shall be inspected on an annual basis to ensure that the performance of the equipment has been maintained;

– As regards alarm system, emergency electrical power system and other Regulations on Technical Standards for Nuclear Reactor Facilities, etc. emergency apparatus, performance inspection for the operation thereof shall be performed on a monthly basis concerning each part of such apparatus, and a general inspection for the operation of the whole apparatus be conducted on an annual basis; and

– As regards measuring instruments and radiation measuring apparatus directly related with the safety control of nuclear fuel cycle facilities, calibrations shall be performed on an annual basis.

Detailed methodology for determination the surveillance test intervals and allowed outage times (AOT) of systems and components important to safety are not given in [23].

Taking into account that Korean PWR NPPs designs are based on USA NRC PWR design bases it is considered reasonable to conclude that Korea follows the USA NRC practice related to the definition of Operational Limits and Conditions (OLC), Surveillance Requirements (SR) and Allowable Outage Time (AOT) following USA NRC SRP 0800

chapter 16 (Technical Specification) and 16.1 (Risk-informed Decision Making: Technical Specifications). This can be concluded from the Safety Evaluation Report of an application for a license to new Barakah units 1 and 2 (Korean PWR APR-1400) where it is clearly stated that the Korean PSAR (Preliminary Safety Analysis Report) follows the US NRC Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants" and US NRC Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants".

2.9 Russian FederationRegulatory Framework for Single Failure Criteria (SFC) and Allowable Outage Time (AOT)

NP-001-97 (General Regulations On Ensuring Safety Of Nuclear Power Plants) [51] defines Single Failure Principle - principle in accordance with which the system shall perform the predetermined functions during any initiating event requiring its operation and failure of anyone of active or passive elements moving mechanical parts independent of the initiating event. Furthermore, under 2.5 (Safety Classes) it is required that to Safety Class 2 the following elements of NPP are assigned:

- elements whose failures are initiating events leading to damage of fuel elements within limits
- established for design basis accidents on proper functioning of safety systems with allowance for specified number of failures in them for design basis accidents;
- safety systems elements , single failures of which lead to non-performance of functions by the relevant systems.

Nuclear Safety Rules For Reactor Installations Of Nuclear Power Plants (NP-082-07, [49]) establish requirements for nuclear safety ensurance of reactor installations of nuclear power plants during design, engineering, construction and operation. These federal standards and rules are issued to substitute the old Nuclear Safety Rules for Reactor Installations of Nuclear Power Plants PBYa RU AS-89 with Alteration №1 and Section 4 of Nuclear Safety Rules for Nuclear Power Plants PBYa-04-74.
Based on article 1.5, the Nuclear safety of RI (Reactor Installation) and NPP is ensured by a system of technical and organizational measures envisaged by the defense-in-depth concept, including:

- implementation and further development of inherent safety features;
- use of safety systems built on the basis of the principles of independence, diversity and redundancy, and single failure criterion;
- use of reliable, field-proven technical solutions and justified methodologies, calculation analyses and experimental studies;
- following the RI and NPP safety norms, rules and standards, and design requirements; stability of processes;
- implementation of quality assurance systems at all stages of creation and operation of
- NPP;
- building and implementing safety culture at all stages of creation and operation of NPP.

Article 2.3.1.4 defines that the RI design shall provide for, at least, two reactor shutdown systems, each one being capable, independently from the other, of rendering the reactor subcritical and maintaining it in this state considering single failure criterion or human error. These systems shall be designed in accordance with the diversity, independence and redundancy principles. Article 2.3.2.9 requires that Emergency Protection structure shall be selected so as to provide compliance with the mandatory criteria (single failure, common cause failure) and meet reliability indicators.
NP-006-98 (Requirements To Contents Of Safety Analysis Report Of NPP With VVER Reactors, [50]) lists under section 8.6 (Emergency Power) among other US standards as the official publications, the IEEE Standard Application of Single Failure Criteria for Class 1E Systems of Nuclear Power Generating Stations (379-1977), Chapter 12 (Safety systems) list the single failure principle under design bases (12.1.1.1) requiring the proof that the system has been designed taking into account the single failure principle shall be presented. Similar is

inside section 12.3 (supporting safety systems). NP-006-98 [50] under General Requirementt discuss that in section related the analysis of design shall be a description of how the system functions in normal operation conditions, operational events including pre-accident situations and design basis accidents; its interaction with other systems taking into account their possible failures, and measures to protect the system from consequences of these failures. For the intended operational modes there shall be operating limits and conditions, safety limits, safety system actuation settings and indicators of reliability of the system and its components. The information shall be presented in the following sequence:

- system reliability indicators;
- normal operation;
- system performance in case of failures;
- system performance in design basis accidents;
- system performance in case of external impacts;
- safety analysis of the design;
- comparison with similar designs.

Each subsection shall end up with an analysis of how the relevant safety requirements, principles and criteria are met.

Exception during testing and maintenance - Allowable Outage Time (AOT)

Nuclear Safety Rules For Reactor Installations Of Nuclear Power Plants (NP-082-07, [49]) defines under 1.4 that Nuclear safety of a RI and NPP is determined by technical perfection of designs; required quality of manufacturing, assembling, aligning and testing of safety important systems and components; their operational reliability; diagnostics of technical conditions of the equipment; quality and timeliness of maintenance and repair of the equipment; monitoring and control over processes during operation; organization of work; and qualifications and discipline of the personnel. Furtehmore, 2.1.6. To maintain and verify design characteristics the safety important RI and NPP systems (components) shall be subjected to inspections and tests during their manufacturing, assembling, aligning, as well as to periodic in-service inspections. The RI and NPP designs shall provide for tooling, devices, methodologies and frequencies of safety important systems checks against their design characteristics, including comprehensive testing (signal sequence and transmission time including those of Emergency Protection) response, switching over to emergency power supply sources, performance of safety functions, etc.). The RI and NPP designs shall contain lists of systems and components which performance and characteristics are to be verified at the operating or shutdown reactor, along with a description of RI and safety important RI and NPP systems' conditions. Devices and methodologies for inspection of safety important systems and their components shall not affect NPP safety.

NP-006-98 (Requirements To Contents Of Safety Analysis Report Of NPP With VVER Reactors, [50]) in Chapter 16 (similar to USA NRC SRP-0800) define the Safe Operation Limits And Conditions and Operational Limits. The NPP PSAR Chapter 16 shall contain the information on safe operation limits and conditions and operational limits specified in the design for safety systems (elements) and safety important systems as well as NPP in general. Subsection 16.3.4 (Conditions for SIS maintenance, testing and repair) defines that it is required to specify conditions for testing, inspection, maintenance and repair of safety important system. It is required to present the information on timing, scope, methods and means to carry out these works and operation restrictions if necessary.

Based on the above discussion it can be reasonably concluded that detailed methodology for determination of the surveillance test intervals and allowed outage times (AOT) of systems and components important to safety are not given in available Russian Regulatory Framework ([49] to [51]). It is interesting that in old IAEA TECDOC-599 [8] it was written that the regulatory body in the USSR (SCSSINP) recognizes in principle the use of probabilistic methodology as a supplementary tool to the deterministic approach for NPP safety assessment and for evaluation of technical specifications. Probabilistic indicator goals in the USSR regulations are based on large radioactivity releases, severe core damage, and take into account the destruction of the pressure vessel as a design basis initiating event. At present investigations are under way on establishing similar indicators on functional-system level. The problem is to develop a consistent and sufficient system of indicators and procedures for the reliable assessment of such indicators. In order to streamline and adjust the whole PSA system and to promote nuclear safety, SCSSINP recognized a necessity to develop a series of guidelines for conducting PSA. This work is now in progress. The Soviet Union regulatory body (at the time) considered all attempts to implement methods of reliability and risk analysis and improvement of technical specifications of NPPs to be useful and promotes these activities in the research and design organizations and by NPP personnel. But, as in the past, the regulatory body will assume regulatory decisions in the near future mainly on a deterministic basis.

2.10 PR China Regulatory Framework for Single Failure Criteria (SFC) and Allowable Outage Time (AOT)

Section 5.3.2 in HAF-102 [55] defines requirements for SFC application. The text is similar to IAEA NS-R-1[11] (revision 2000, already superseeded by IAEA SSR-2/1[1], discussed in section 2.1 above). It was mentioned that the single failure criterion shall be applied to each safety group incorporated in the plant design. Section 5.3.2.2 discusses that o test compliance of the plant with the single failure criterion, the pertinent safety group shall be analysed in the following way. A single failure (and all its consequential failures) shall be assumed in turn to occur for each element of the safety group until all possible failures have been analysed. The analyses of each pertinent safety group shall then be conducted in turn until all safety groups and all failures have been considered. (safety functions, or systems contributing to performing those safety functions, for which redundancy is necessary to achieve the necessary reliability have been identified by the statement 'on the assumption of a single failure'.) The assumption of a single failure in that system is part of the process described. At no point in the single failure analysis is more than one random failure assumed to occur. Section 5.3.2.3 discusses the spurious action which shall be considered as one mode of failure when applying the concept to a safety group or system. Also, under section 5.3.2.4 it is repeated IAEA NS-R-1 requirement 5.37 related to the compliance with the criterion which shall be considered to have been achieved when each safety group has been shown to perform its safety function when the above analyses are applied, under the following conditions:

(1) any potentially harmful consequences of the PIE for the safety group are assumed to occur; and

(2) the worst permissible configuration of safety systems performing the necessary safety function is assumed, with account taken of maintenance, testing, inspection and repair, and allowable equipment outage times.

Section 5.3.2.6 discusses that in SFC analysis, it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality, provided that it remains unaffected by the PIE. However, when it is assumed that a passive component does not fail, such an analytical approach shall be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary.

Finally, it is mentioned that the non-compliance with the single failure criterion shall be exceptional, and shall be clearly justified in the safety analysis.

HAF-102 [55] defines application of SFC for various safety systems: 6.2.5 Core Residual Heat Removal, 6.2.6 Emergency Core Cooling, 6.3.9 Containment Heat Removal, 6.3.10 Containment gas cleanup and control systems, 6.4.7 Reactor Protection System and finally 6.6 Emergency Power. Similarly to IAEA NS-R-1, under Appendix II, meeting of SFC is discussed in II.7 (Redundancy) taking the credit of failure or unavailability of at least one set of equipment to be tolerated without loss of the function. For example, three or four pumps might be provided for a particular function when any two would be capable of carrying it out. For the purposes of redundancy, identical or diverse components may be used.

Exception during testing and maintenance - Allowable Outage Time (AOT)

Allowable Outage Time (AOT) is not defined in HAF-102. The section 5.3.5 under Equipment Outages discuss that the design shall be such as to ensure, by the application of measures such as increased redundancy, that reasonable on-line maintenance and testing of systems important to safety can be conducted without the necessity to shut down the plant.

Equipment outages, including unavailability of systems or components due to failure, shall be taken into account, and the impact of the anticipated maintenance, test and repair work on the reliability of each individual safety system shall be included in this consideration in order to ensure that the safety function can still be achieved with the necessary reliability. The time allowed for equipment outages and the actions to be taken shall be analysed and defined for each case before the start of plant operation and included in the plant operating instructions. There is no details related to accepted methodology.

It could be reasonable to conclude that Chinese NPPs developed their internal AOT optimization methods taking into account an old IAEA technical report [12] (related to development of methodologies for optimization of surveillance testing and maintenance of safety related equipment at NPPs) refering Chinese plans in this area. Taking into account that Chinese NPPs adopt vendor country licensing rules (among other NUREG-0452 and NUREG-1431 as standard format of NPP Technical Specification) it is reasonable to conclude that Chinese regulator accepts also the USA NRC practice related to the definition of Operational Limits and Conditions (OLC), Surveillance Requirements (SR) and Allowable Outage Time (AOT) following USA NRC SRP 0800 chapter 16 (Technical Specification) and 16.1 (Risk-informed Decision Making: Technical Specifications).

2.11 Canadian Context

Canadian Regulatory Guides ([52] and [54]) define the SFC as criterion used to determine whether a system is capable of performing its function in the presence of a single failure where single failure is A failure that results in the loss of capability of a component to perform its intended safety function(s), and any resulting consequential failure(s).

Similar to WENRA DiD (section 2.2) Canadian REGDOC-2.4.1[52] mainly addresses analysis methods and assumptions for the deterministic safety analysis (DSA) of AOOs and DBAs for Level 3 defence in depth. Similar analysis methods and assumptions can be applied for Levels 2 and 4 defence in depth (with appropriate levels of conservatism). Certain conservative rules, such as the single-failure criterion, are not applied in Level 2 and Level 4 analyses. Comprehensive calculations are conducted to assess the plant performance against each applicable acceptance criterion. Sensitivity studies are undertaken to assess the impact on analysis results of key assumptions – for example, in identifying the worst single failures in various systems, or to assess the impact of using simplified models instead of more accurate and sophisticated approaches (requiring significant effort in the calculations). Section 4.4.4.1 provides guidance for single-failure criterion in safety group. The single-failure criterion stipulates that the safety group consisting of a safety system and its support systems should be able to perform its specified functions even if a failure of single component occurs within this group. Expectations related to the application of the single-failure criterion in design are refered to REGDOC-2.5.2[54], Design of Reactor Facilities: Nuclear Power Plants. REGDOC-2.4.1 refer the newes IAEA standards SSG-2 and GSR Part 4.

REGDOC-2.5.2[54] defines the SFC in section 7.6 (Design and reliability) under bullet 7.6.2 In accordance with 7.6.2 , all safety groups shall function in the presence of a single failure. The single-failure criterion requires that each safety group can perform all safety functions required for a PIE in the presence of any single component failure, as well as:

1. all failures caused by that single failure

2. all identifiable but non-detectable failures, including those in the non-tested components

3. all failures and spurious system actions that cause (or are caused by) the PIE

Each safety group shall be able to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage. Analysis of all possible single failures, and all associated consequential failures, shall be conducted for each component of each safety group until all safety groups have been considered. Unintended actions and failure of passive components shall be considered as two of the modes of failure of a safety group.

The single failure shall be assumed to occur prior to the PIE, or at any time during the mission time for which the safety group is required to function following the PIE. Passive components may be exempt from this requirement. Exceptions to the single-failure criterion shall be infrequent, and clearly justified. Exemptions for passive components may be applied only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation shall include justification of such exemptions, by analysis, testing or a combination of analysis and testing. The justification shall take loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary. REGDOC-2.5.2[54] finally defines applicability of SFC in design of plant safety systems(e.g. 7.9.3 Accident monitoring instrumentation,

8.2.4 Removal of residual heat from reactor core, 8.3.3 Turbine generators, 8.4 Means of shutdown, 8.9 Electrical power systems inside8.9.1 Standby and emergency power systems).

Exception during testing and maintenance - Allowable Outage Time (AOT)

Section 7.6.2 of REGDOC-2.5.2[54] provides detailed guidance for application of SFC including consideration for an exception to the SFC during testing and maintenance should fall into one of the following permissible categories:

- the safety function is provided by two redundant, independent systems (e.g., two redundant, fully effective, independent cooling means)
- the expected duration of testing and maintenance is shorter than the time available before the function is required following an initiating event (e.g., spent fuel storage pool cooling)
- the loss of safety function is partial and unlikely to lead to significant increase in risk even in the event of failure (e.g., small area containment isolation)
- the loss of system redundancy has minor safety significance (e.g., control room air filtering)
- the loss of system redundancy may slightly increase PIE frequency, but does not impact accident progression (e.g., leak detection)

A request for an exception during testing and maintenance should also be supported by a satisfactory reliability argument covering the allowable outage time. The OLCs should clearly state the allowable testing and maintenance time, along with any additional operational restrictions, such as suspension of additional testing or maintenance on a backup system for the duration of the exception. However, section 7.6.2 refer to the old IAEA, Safety Series No. 50-P-1 [7] (Application of the Single Failure Criterion) which was withdrawn without applicable replacement.

There is no corresponding PSA numerical targets for minimal risk increase due to exception during testing and maintenance in the context of the requirement “should also be supported by a satisfactory reliability argument covering the allowable outage time”. Also, in REGDOC-2.4.2 [53] which deals with PSA analysis, there is no PSA numerical targets for minimal risk increase due to exception during testing and maintenance which can be used for optimization of Technical Specification AOT. It is recommended to develop a new guidance document to assist in applications for the risk-informed completion times (also called allowed outage times) and surveillance test interval extensions. More discussion on this matter is provided in section 4. As an example of such guiding document, the USA NRC Regulatory Guide 1.177 [17] and Standard Review Plan Chapter 16.1 [14] can be pointed.

2.12 Summary Table

Table 3 summarizes the approaches described in sections 2.1 to 2.11 in a limited scope due to the fact that all regulatory requirements related to the AOT and associated SFC are not written and defined in the same manner. Nuclear industries (utilities, NPPs, etc.) have developed procedures how to response to regulatory requirements and , typically, national regulators accept or refuse proposed application for relaxing the AOTs or SFC.

Table 3 Summary Table

Regulatory Position	**SFC applied to safety group or individual system**	**What systems have to meet SFC?**	**Is SFC applied during planned maintenance?**	**Is SFC applied during a repair within AOT?**	**Is SFC applied to passive components?**	**Is SFC applied in addition to assuming failure of a non-tested component?**
IAEA	Safety system	General approach: systems which prevent radioactive releases in environment. Because of different designs, system names and description it can be related to: • Reactor Protection System • Engineering Safety Feature Actuation System • Core Decay Heat Removal System • Emergency Core Cooling System • Containment decay heat removal system • Containment Isolation System • MCR Habitability System • Emergency AC/DC power • Safety System Support System (Component	Not discussed directly in regulations. The allowable periods of safety systems inoperability and the cumulative effects of these periods should be assessed in order to ensure that any increase in risk is kept to acceptable levels.		General approach is that the fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming Passive Equipment functions properly) nor (2) a single failure of a Passive Equipment (assuming Active Equipment functions properly) results in a loss of capability of the system to perform its Safety Functions. Exemption for passive components exists if justification of high standard and quality design and maintenance is possible.	Not discussed directly in regulations. See 4th column on left side. In other words it means that if assessment of potential failure of any single component designed for the function in stand-by (non-tested) system shows the increase in risks above acceptable levels such test/maintenance should be excluded.
WENRA	Safety system					
EUR	Assembly of Equipment (combination of systems and components that perform a specific function)					
US NRC	Safety system					
Finish (STUK)	Safety system		Not discussed directly in regulations. The PRA shall be used to determine the surveillance test intervals and allowed outage times of systems and components important to safety. Actually, it is similar with above.			YVL B.1 discusses actually the two failure criteria as described in 4th column on the left side for Finish (STUK).

Regulatory Position	SFC applied to safety group or individual system	What systems have to meet SFC?	Is SFC applied during planned maintenance?	Is SFC applied during a repair within AOT?	Is SFC applied to passive components?	Is SFC applied in addition to assuming failure of a non-tested component?
		Cooling Water, etc.)	YVL B.1 discusses actually the two failure criteria: • (N+1) failure criterion shall mean that it must be possible to perform a safety function even if any single component designed for the function fails. • (N+2) failure criterion shall mean that it must be possible to perform a safety function even if any single component designed for the function fails and any other component or part of a redundant system – or a component of an auxiliary system necessary for its operation – is simultaneously out of operation due to repair or maintenance. Some systems need to satisfy criteria (N+1) and some (N+2)			
UK	Safety system		See IAEA, WENRA, EUR, US NRC above.			See IAEA, WENRA, EUR, US NRC above.
Japan	Structure, System and Components (SSCs)					
Korean	Safety system					
Russian	Safety features (safety systems elements)					
China	Safety system					
Canadian	Safety group/Safety system		A request for an exception during testing and maintenance should be supported by a satisfactory reliability			Actually, similar to text for IAEA, WENRA, EUR, US NRC above even that section

Regulatory Position	SFC applied to safety group or individual system	What systems have to meet SFC?	Is SFC applied during planned maintenance?	Is SFC applied during a repair within AOT?	Is SFC applied to passive components?	Is SFC applied in addition to assuming failure of a non-tested component?
			argument covering the allowable outage time			7.6.2 of REG-DOC-2.5.2 [54] refers to the old IAEA, Safety Series No. 50-P-1 [7] which was withdrawn without applicable replacement.

3. SINGLE FAILURE CRITERION APPLICATION IN NEW SMALL REACTOR DESIGNS

In tha last decadethere was a lot of discussion relatedto the implementation of so called “small rectors” (SR) and “small modular reactors” (SMRs). To establish some context, it may be pointed that IAEA provides the following definitions concerning the “sizes” of the reactors:

- Small-sized reactors: < 300 MW(e)
- Medium-sized reactors: < 700 MW(e)
    - Upper power limit may change as the current Large-sized reactors are being designed for up to 1700 MW(e).

Until recently, several dozens of Design Concepts of SRs and SMRs have been developed in Argentina, China, India, Japan, the Republic of Korea, Russian Federation, South Africa, USA, and several other IAEA Member States.

According to the definition of its role in the on-going SRs and SMR process, IAEA:

- Coordinates efforts of Member States to facilitate the development of SRs and SMRs by taking a systematic approach to identify key enabling technologies to achieve competitiveness and reliable performance of SRs and SMRs, and by addressing common issues to facilitate deployment;
- Establishes and maintains international network with international organizations involved on SRs and SMRs activities;
- Ensures overall coordination of Member States experts by planning and implementing training and by facilitating the sharing of information/experience, transfer of knowledge ;
- Develops international recommendations and guidance on SMRs, focusing on addressing specific needs of developing countries.

By definition, SRs and SMRs should have the following advantages:

- Fitness for smaller electricity grids;
- Options to match demand growth by incremental capacity increase;
- Tolerance to grid instabilities;
- Site flexibility;
- Other possible advantages;
- Lower capital cost but perhaps higher capital cost per MWe;
- Shorter and more reliable construction;
- Easier financing scheme;
- Enhanced safety;
- Reduced complexity in design and human factors;
- Suitability for process heat application.

IAEA developed the guidance for preparing user requirements documents for small and medium rectors and their application [59], although without clear design requirements. It is mentioned that the technical requirements should indicate that the design of a given new facility has to be in conformance with applicable rules, regulations, codes and technical standards. IAEA-TECDOC-1451 [60] discusses innovative small and medium sized reactors including, very briefly, design features, safety approaches and R&D trends. However, the

mentioned document does not provide clear information regarding SMRs design requirements and, consequentially, does not mention SFC at all. Similarly to IAEA-TECDOC-1451, the IAEA-TECDOC-1485 [61], as well as TECDOC-1536 [62], discusses advantagees of SMRs design only partially and without specific design requirements.

IAEA report NP-T-2.2 [58] discusses the design features for achieving defence in depth in 10 different designs of small and medium sized reactors where the part devoted to the application of SFC was very limited. In this document there is no mention of SFC as a specific design requirement from the IAEA. The latest IAEA doscuments discussing the advances in small modular reactor technology developments, [63], mentions, for the few applications, that the defence in depth (DID) concept is based on Western European Nuclear Regulators Association (WENRA) proposal and includes a clarification on multiple failure events, severe accidents, independence between levels, the use of the SCRAM system in some DID Level #2 events and the containment in all the Protection Levels. The safety systems are duplicated to fulfil the redundancy criteria, and the shutdown system is diversified to fulfil regulatory requirements. Application of SFC is not discussed at all.

In USA some utilities are considering licensing small modular reactor designs using the 10 CFR Part 52 combined license (COL) or early site permit (ESP) processes. The U.S. Nuclear Regulatory Commission (NRC) expects to receive applications for staff review and approval of small modular reactor (SMR)-related 10 CFR Part 52 applications as early as by the end of 2015. The NRC has developed its current regulations on the basis of experience gained over the past 40 years from the design and operation of large light-water reactor (LWR) facilities. Now, to facilitate the licensing of new reactor designs that differ from the current generation of large LWR facilities, the NRC staff seeks to resolve key safety and licensing issues and develop a regulatory infrastructure to support licensing review of these unique reactor designs. Toward that end, the NRC staff has identified several potential policy and technical issues associated with licensing of small LWR and non-LWR designs. The current status of these issues may be found in the series of related Commission documents (http://www.nrc.gov/reactors/advanced.html). The NRC staff has also assembled a list of stakeholder position papers identifying stakeholder documents that communicate opinions to the staff on technical or policy issues. Additionally, the NRC's Office of Nuclear Regulatory Research has engaged in an extensive program focusing on nine key areas of anticipatory and confirmatory research in support of licensing reviews for advanced reactors. The NRC also interacts with its international regulatory counterparts to share information. In August 2012, the NRC provided to Congress a requested report (Advanced Reactor Licensing) addressing advanced reactor licensing. The report addresses the NRC's overall strategy for, and approach to, preparing for the licensing of advanced non-LWR reactors. The report addresses licensing applications anticipated over the next two decades, as well as potential licensing activity beyond that time. It focuses on the licensing of nuclear reactor facilities for commercial use and illustrates regulatory challenges that may occur if various advanced reactor initiatives evolve into licensing applications. During 2012, DOE (Department of Energy) instituted an Advanced Reactor Concepts Technical Review Panel (TRP) process to evaluate viable reactor concepts from industry and to identify R&D needs. TRP members and reactor designers noted the need for a regulatory framework for non-light water advanced reactors. The TRP convened in spring 2014 reiterated the need for a licensing framework for advanced reactors:

- 10 CFR 50 requires applicants to establish principal design criteria derived from the General Design Criteria (GDC) of Appendix A.

- Since the GDC in Appendix A are specific to light water reactors (LWRs), this requirement is especially challenging for potential future licensing applicants pursuing advanced (non-light water) reactor technologies and designs.
- NE and NRC representatives agreed in June 2013 to pursue a joint licensing initiative for advanced reactors.

Overall purpose of this initiative is to establish clear guidance for the development of the principal design criteria (PDC) that advanced non-LWR developers will be required to include in their NRC license applications.

In the meantime, while USA NRC was still defining the position related to the licensing review of SMRs, the American Nuclear Society (ANS) issued in 2010 the Interim Report of the American Nuclear Society President's Special Committee on Small And Medium Sized Reactor (SMR) Generic Licensing Issues [57] which, among other issues, discusses the application of single failure criterion (SFC). Report mentions that the current SFC may not be appropriate to risk-informed safety assessments since it defeats the fundamental purpose of a risk analysis, given that all components, regardless of safety classification, have the opportunity to fail in a probabilistic assessment. SFC can be used to assess the importance of components and structures for design improvement, should the consequence be significant, but should not be mandatory. This SFC discussion is based on the the rigorous application of risk analysis in a plant design where the important design-basis events can be deduced from the event and fault trees. In addition, safety classification of systems, structures, and components can be directly determined from the analysis, as can reliability requirements for component performance and the need for inspection, test, and surveillance based on component importance. The risk-informed assessment also allows for explicit treatment of uncertainties, which conventional deterministic analysis largely ignores by applying "margins" and "conservatisms" intended to bound these unknowns. The risk assessment methodology allows for a more transparent understanding of the safety basis of reactors.

Finally, ANS concluded that a key element to development and implementation of innovative reactors is the use of a risk-informed framework, coupled with a demonstration test program upon which to issue DCs. Thus, the American Nuclear Society President's Special Committee on SMR Generic Licensing Issues (SMR Special Committee) recommends immediate development of a rulemaking to establish a new risk-informed, technology-neutral licensing process with a license-by-test element, to allow innovative designs to be developed and deployed more efficiently in the longer term.

None of other regulatory frameworks related to the SFC application discussed in section 2 deals with the application of SFC specifically for the SMRs, from which it can be reasonably concluded that current regulations for large commercial NPPs (including the SFC application) will be in place until new regulations become available.

Canadian regulatory requirements for design of small reactor facilities [64] (RD-367, Design of Small Reactor Facilities) defines the "small reactor facility" as a reactor facility containing a reactor with a power level of less than approximately 200 megawatts thermal (MWt) that is used for research, isotope production, steam generation, electricity production or other applications. For reactors with power level above 200MWt Canadian regulatory requirements from REGDOC 2.5.2 [54] (Design of Reactor Facilities Nuclear Power Plants)are applicable. Differing to the all other regulatory approaches discussed above, Canadian regulatory requirements for design of small reactor facilities [64] in section 7.8.2 clearly defines that all

safety groups shall be designed to function in the presence of a single failure. Each safety group shall perform all safety functions required for a PIE in the presence of any single component failure, as well as:

- all failures caused by that single failure;
- all identifiable but non-detectable failures, including those in the non-tested components;
- all failures and spurious system actions that cause (or are caused by) the PIE.

Each safety group shall be able to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage. Analysis of all possible single failures and associated consequential failures shall be conducted for each element of each safety group until all safety groups have been considered. Such requirement is similar for the current large commercial nuclear power plant.

With above overview and discussion in mind, it is considered recommendable for the CNSC to investigate the risk-informed and performance-based alternatives to the single-failure criterion, such as those studied and described in [22], in order to identify potential alternative or complementary risk-informed approaches with respect to the SFC, for use in the new requirements for SMRs. Some of the complementary risk-informed approaches are further discussed in section 4 below.

4. RECOMMENDATIONS

As it can be seen from the overview presented in this report, the single failure criterion is in international practices addressed in terms of two complementary aspects:

a) Postulation of SFC requirements for safety functions.

The SFC requirements are, typically, established through a set of deterministic principles which consider postulated initiating events, plant conditions and safety systems / functions involved in their prevention and / or mitigation. Application of these requirements results in identification of systems and functions which must satisfy the SFC.

b) Considerations of allowability of any exemptions of SFC.

From the provided overview of international practice, the instances of potential allowability of exemptions can, generally, be divided into two broad categories:

- Potentially allowable exemptions in *plant design*;
- Potentially allowable exemptions in *plant operation*.

They are briefly discussed below.

b.1) Potentially allowable exemptions in *plant design*.

Any exemption to SFC from this category (i.e. exemption from SFC in the plant design) is potentially allowable only if at least one of the following two conditions is met:

- Plant condition relevant for the considered function is of demonstrably very low likelihood (e.g. certain hazard categories), or
- Considered function is of demonstrably very high reliability.

Regarding the second condition, based on the reviewed international practices it can be said that this kind of argument would only be considered (but not necessarily allowed!) for passive functions and structures (or functions involving at least one passive line of defense).

In other words, any exemption to SFC in plant design would be considered for allowability only if:

- All requirements under a) above have been satisfied, *and*
- Risk impact associated with exemption can be demonstrated to be very low (to the extent that it can be considered "practically eliminated").

b.2) Potentially allowable exemptions in *plant operation*.

Typically, the exemptions to SFC during plant operation phase are associated with in-service testing, inspections or maintenance activities, which can be scheduled or unscheduled. The exemptions to SFC which may result from such activities or conditions are usually controlled by Operational Limits and Conditions (OLCs) which are provided in the form of Technical Specifications (TSs) or similar, depending on a national practice or terminology. Usually, OLCs/TSs include two two types of requirements:

- Requirements regarding systems operability (e.g. minimum numbers and combinations of equipment available) and allowable outage times for equipment;
- Surveillance requirements (e.g. periodicity of testing).

Both of these two requirements are related to the risk impact of potential exemptions to the SFC during plant operation: the first requirement limits the time spent in the condition with non-satisified SFC; the second requirement ensures monitoring of the equipment reliability, including the reliability of remaining "available" equipment during the allowed outage time. Here it needs to be pointed that the meaning of the second requirement is broader: it is meant to ensure the reliability as a complement to the SFC requirement. This is important to comprehend because the SFC requirement in plant design and operation makes sense only as long as it can be ensured that remaining part of the system (not affected by a single failure) will perform intended function. (Deterministic design basis analyses are "pesimistic" in postulating a single failure. However, it needs to be understood that they are, in a way, "optimistic" by assuming that the remaining part of the affected system will be successful.)

It can be said that any exemption to SFC during plant operation can be considered as potentially allowable only if associated risk impact is demonstrably very low. More specifically: risk impact associated with specified allowable outage time should be demonstrably very low and so should be risk impact associated with specified surveillance requirement (e.g. test interval). For the generation of operating plants these OLC requirements were initially postulated deterministically (for example, the allowed outage time such as 72 hours or surveillance test requirements such as monthly or quarterly). However, even then the underlying reasoning was associated with low risk impact. On the other hand, it can be said that current state-of-the-art practice is to support the OLC/TS requirements related to SFC exemptions by risk-informed principles on the basis of plant-specific PSA. This can be seen from the overview of international practices. For example, earlier mentioned IAEA safety standard SSG-3, [5], contains the statement in the section on Risk Informed Technical Specifications: "10.31. A risk informed approach should be used to provide a basis for the technical specifications. The aim should be to provide a consistent basis that is related to the risk significance of the affected plant features."

If the Canadian regulatory framework related to the SFC (and discussed in chapter 2.11) is compared against the above discussion, it can be seen that current CNSC SFC-related requirements are based on the same general philosophy and basically contain all the elements discussed. What can be considered as recommendable is to consolidate some risk and reliability aspects of SFC. Specifically:

- In the light of the above discussion, it is considered recommendable for CNSC to develop a guiding document for risk-informed principles of OLC development or its optimization. This document would provide guidance on quantitative risk targets or criteria associated with exemptions to SFC, such as risk impacts of allowable outage times and surveillance schemes (e.g. test intervals). The risk impacts / targets would be defined in terms of risk metrics calculated by the Canadian PSAs (in accordance with corresponding CNSC regulatory document). As an example of this kind of guiding document from the international practice, U.S. NRC's Regulatory Guide 1.177, [17], can be pointed out. The mentioned guiding document would, also, provide

interpretations, clarifications or illustrations, from the quantitative perspective (quantitative risk impact), for certain statements or requirements from the REGDOC-2.5.2, relevant for the exemptions to SFC. For example (section 7.6.2 Single-failure criterion):

- Statement: "*the loss of safety function is partial and unlikely to lead to significant increase in risk even in the event of failure*"
  - What does it mean, in terms of quantitative risk metrics, "…unlikely to lead to significant increase in risk…"?
- Statement: "the loss of system redundancy has minor safety significance"
  - What does it mean, in terms of quantitative risk metrics, "…minor safety significance…"?

Also, in the same section of REGDOC-2.5.2 there is a statement: "*A request for an exception during testing and maintenance should also be supported by a satisfactory reliability argument covering the allowable outage time.*" Here it can be pointed that reliability by itself may not be a sufficient argument for a request for exception to SFC as the required level or reliability may considerably depend on the risk significance of considered system or equipment. Recommended guiding document for risk-informing the OLC may provide further explanations related to this subject. The reliability requirements are further discussed in the next bullet.

- As a companion to the guiding document on risk-informing the OLC, it is considered recommendable to establish a guidance or requirements for demonstrating the effectiveness of maintenance in the NPPs (or to make an interface or link to the existing CNSC regulatory documents covering this subject). The purpose of demonstrating the effectiveness of maintenance is to demonstrate the adequacy of the reliability and availability of equipment. As already mentioned above, REGDOC-2.5.2 required that an exception (to SFC) during testing and maintenance is supported by a reliability argument. Reliability is, together with availability, input into the PSA model and, therefore has a major influence on the calculations of risk impacts (and therefore on any risk-informed application or decision, including the development / optimization of OLC / TS). Both reliability and availability are, at the basic level, controlled by OLC requirements, as already pointed. However, they are opposing requirements: increasing the scope of maintenance or inspections (in order to increase the reliability) would in many cases reduce the availability; on the other hand, decreasing the the scope of maintenance or inspections (which may increase the availability) can reduce the reliability. One of the main goals of demonstrating the effectiveness of maintenance is, therefore, to find a proper balance (an optimum) between the reliability and availability. As an example, the U.S. NRC "Maintenance Rule", 10CFR50.65, [20], with associated Regulatory Guides (and other background documents, including the Mitigating Systems Performance Indices, MSPIs) can be pointed. It is noted that CNSC already has some regulatory documents which can be used as a basis for monitoring the effectiveness of maintenance, e.g. RD/GD-98, Reliability Programs for Nuclear Power Plants. It is considered recommendable to make a connection (or, at least, to provide some related guidance / interpretation) between the reliability program and requirements concerning the reliability in relation to the exceptions to the SFC and OLC in general, from REGDOC-2.5.2. As an example:

- In the introduction to section 7.6 there is a statement: "*The safety systems and their support systems shall be designed to ensure that the probability of a safety system failure on demand from all causes is lower than 10-3*."
    - How does this reliability target relate to the reliability argument for exception to the SFC from 7.6.2: "*A request for an exception during testing and maintenance should also be supported by a satisfactory reliability argument covering the allowable outage time"*?.

The above recommendations are aimed at establishing (or, rather, improving) the risk-informed context which would serve as a complement to the SFC requirements (rather than used to replace it, as it might have been implied by the use of the term "alternatives" in the reference [22]). This complementary approach would, for example, refine and improve the requirements (based on the risk and reliability) regarding possible exemptions to the SFC or would provide more specific guidance, on risk-informed principles, for demonstration of acceptability of exemption to the SFC, where and if applicable.

The above recommendations apply to the regulatory framework for the operating plants, for the new plants based on the existing designs, as well as for the new designs, including the small modular reactors discussed in section 3.

5. CONCLUSIONS

Under this task, a review of the current SFC reactor design requirements and guidelines published by the IAEA, WENRA, EUR and nuclear regulators in the United States, United Kingdom, Russia, Korea, Japan, Finland and PR China was performed. France was not specifically addressed, based on the fact that French Regulatory Body plays an important role under WENRA harmonization project and EDF plays the leading role under the EUR revision. Specifically, SFC requirements and guidelines for new reactor design were compared against Canadian requirements, with specific consideration to testing, maintenance, repair, inspection, monitoring, and allowable equipment outage times. The probabilistic approaches to grant SFC exceptions (both permanent and temporary) were listed in the cases where they identified. The approach was analysed of each selected country as SFC applies to two-, three- and four-train systems.

The general observation is that the single failure criterion applications vary from country to country taking into account terminology, methodology of assessment etc. Treatment of exceptions during testing and maintenance, including the term Allowable Outage Time (AOT), variess even more, including the fact that even the term is not common for different nuclear industries or national regulatory bodies.

It is recommendable to use more common SFC terminology from IAEA SSR-2/1[1] (new revision will be issued in 2016) and to refer to WENRA DiD documents [28] and [29] in Canadian Regulatory Guides. Also, it was observed that in either REGDOC-2.5.2 [54] or REGDOC-2.4.2[53], which deals with PSA analysis, there is no corresponding PSA numerical targets for acceptable minimal risk increase due to exception during testing and maintenance in the context of the requirement “should also be supported by a satisfactory reliability argument covering the allowable outage time”. The established PSA acceptable numerical targets for minimal risk increase due to exception during testing and maintenance can be used for optimization of Technical Specification AOT. It is recommended to prepare additional guidance document to assist in applications for the risk-informed completion times (also called allowed outage time) and surveillance test interval extensions. Also, it is considered recommendable to establish, as a companion, a guidance for demonstration of maintenance effectiveness in order to demonstrate adequate reliability and availability of equipment, especially those from the “SFC systems”.

6. REFERENCES

[1] IAEA Safety Standard Series, SSR-2/1, Safety of Nuclear power Plants: Design, Rev.1 in preparation Step 13, rev.1, 6.11.2014

[2] IAEA Safety Standard Series, SSR-2/2, Safety of Nuclear power Plants: Commisioning and Operations, Rev. 1 in preparation, 2014

[3] IAEA Safety Guide NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, 2000

[4] IAEA Safety Standard Series, SSG-2, Deterministic Safety Analysis for Nuclear Power Plantsfor, 2010

[5] IAEA Safety Standard Series, SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, 2010

[6] IAEA General Safety Requirements Part 4, GSR Part 4, 2009

[7] IAEA Safety Series No. 50-P-1, Application of the Single Failure Criterion, 1990

[8] IAEA-TECDOC-599, Use of probabilistic safety assessment to evaluate nuclear poer plant technical specification, 1990

[9] IAEA-TECDOC-729, Risk based optimization of technical specifications for operation of nuclear power plants, 1993

[10] IAEA-TECDOC1200, Applications of probabilistic safety assessment (PSA) for nuclear power plants, 2001

[11] IAEA Safety Standard Series, NS-R-1, Safety of Nuclear power Plants: Design, Rev.0, rev.0, September 200

[12] IAEA-J4-RC-654, Development of Methodologies for Optimization of Surveillance Testing and Maintenance of Safety Related Equipment at NPPs, 1996

[13] US NRC 10CFR50, [36 FR 3256, Feb. 20, 1971, as amended at 36 FR 12733, July 7, 1971; 41 FR 6258, Feb. 12, 1976; 43 FR 50163, Oct. 27, 1978; 51 FR 12505, Apr. 11, 1986; 52 FR 41294, Oct. 27, 1987; 64 FR 72002, Dec. 23, 1999; 72 FR 49505, Aug. 28, 2007]

[14] US NRC SRP, NUREG-0800, July 2014

[15] US NRC, NUREG-1431, rev. 4, 2012

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

[17] US NRC RG-1.177, An Approach for plant-specific, risk informed decisionmaking: technical specifications, August 1999

[18] USNRC, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," Federal Register, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986.

[19] USA NRC RG-1.53, Application Of The Single-Failure Criterion To Safety Systems, November 2003

[20] USA 10CFR50.65, Requirements for monitoring the effectiveness of maintenance at nuclear power plants, 72 FR 49501, Aug. 28, 2007

[21] USA 10CFR50.36, Technical Specifications, 73 FR 54932, Sep. 24, 2008

[22] USA NRC SECY-05-0138, Risk-Informed And Performance-Based Alternatives To The Single-Failure Criterion, 2005

[23] Nuclear Laws of the Republic of Korea No.1, Nuclear Safety Act, March 2013

[24] Nuclear Laws of the Republic of Korea No.2, Enforcement Decree of the Nuclear Safety Act, August 2013

[25] Nuclear Laws of the Republic of Korea No. 3, Enforcement Regulation of the Nuclear Safety Act, August 2013

[26] Nuclear Laws of the Republic of Korea No. 4, Regulations on Technical Standards for Nuclear Rector Facilities, Nov. 2011

[27] Nuclear Laws of the Republic of Korea No. 5, Regulations on Technical Standards for Radiation Safety Control, Nov. 2011

[28] WENRA RHWG, WENRA Safety Reference Levels for Existing Reactors, 24.09.2014

[29] WENRA RHWG, Report Safety of new NPP designs, March 2013

[30] European Utility Requirements for LWR Nuclear Power Plants, Revision D, October 2012

[31] European Utility Requirements for LWR Nuclear Power Plants, Revision C, April 2001

[32] Safety Assessment Principles (SAP) for Nuclear Facilities, Revision 1, 2006

[33] NS-TAST-GD-003, Safety Systems, Revision 7, 2014

[34] NS-TAST-GD-011, The single Failure Critera, Revision 1, May 2013

[35] NS-TAST-GD-044, Fault Analysis, Withdrawn 2013

[36] YVL A.6, Conduct of operations at a nuclear power plant, 15 Nov 2013

[37] YVL A.7, Probabilistic risk assessment and risk management of a nuclear power plant, 15 Nov 2013

[38] YVL B.1, Safety design of a nuclear power plant, 15 Nov 2013

[39] YVL B.2, Classification of systems, structures and components of a nuclear facility, 15 Nov 2013

[40] YVL B.3, Deterministic safety analyses for a nuclear power plant , 15 Nov 2013

[41] YVL B.4, Nuclear fuel and reactor, 15 Nov 2013

[42] YVL B.5, Reactor coolant circuit of a nuclear power plant, 15 Nov 2013

[43] YVL B.6, Containment of a nuclear power plant, 15 Nov 2013

[44] YVL B.7, Provisions for internal and external hazards at a nuclear facility, 15 Nov 2013

[45] YVL B.8, Fire protection at a nuclear facility, 15 Nov 2013

[46] YVL 2.7, Ensuring a nuclear power plant's safety functions in provision for failures, 20 May 1996

[47] YVL C.3, Limitation and monitoring of radioactive releases from a nuclear facility, 15 Nov 2013

[48] NSCRG, L-DS-I.0, Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities, August 1990

[49] NP-082-07, Nuclear Safety Rules For Reactor Installations Of Nuclear Power Plants, June 2008

[50] NP-006-98, Requirements To Contents Of Safety Analysis Report Of NPP With VVER Reactors, 2003

[51] NP-001-97 (PNAE G- 01 011-97), General Regulations On Ensuring Safety Of Nuclear Power Plants, 1997

[52] REGDOC-2.4.1, Deterministic Safety Analysis, May 2014

[53] REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, May 2014

[54] REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, May 2014

[55] HAF-102, Nuclear power plant design and safety requirements (National Nuclear Security Administration, April 18, 2004 revision)

[56] IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition

Small Modular Reactors (SMRs)

[57] Interim Report Of The American Nuclear Society President's Special Committee On Small And Medium Sized Reactor (SMR) Generic Licensing Issues, July 2010

[58] IAEA Nuclear Energy Series, NP-T-2.2, Design Features to Achieve Defence in Depth in Small and Mendium Sized rectors, 2009

[59] IAEA-TECDOC-1167, Guidance for preparing user requirements documents for small and medium rectors and their application, 2000

[60] IAEA-TECDOC-1451, Innovative small and medium sized reactors: Design features, safety approaches and R&D trends, 2005

[61] IAEA-TECDOC-1485, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, 2006

[62] IAEA-TECDOC-1536, Status of Small Reactor Designs without On-site Refuelling, 2005

[63] IAEA-SMR-Booklet 2014: Advances in Small Modular Reactor Technology Developments, A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2014

[64] RD-367, Design of Small Reactor Facilities, June 2011