Journal of Energy
VOLUME 65 - 2 | 2016
journal homepage: http://journalofenergy.com/

International Context Regarding Application Of Single Failure Criterion (SCF) For New Reactors

Ivica Bašić, Ivan Vrbanić
APOSS d.o.o.
Repovec 23B, 49210 Zabok, Croatia
basic.ivica@kr.t-com.hr, ivan.vrbanic@zg.t-com.hr

ABSTRACT

The paper 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 report [1] discusses the detailed 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. However, this paper presents the summary of work from [1] and 2major examples from IAEA and WENRA and applications for small and modular reactors.

1 INTRODUCTION

The Single Failure Criterion (SFC) ensures reliable performance 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 particular safety system performs its safety functions as designed under the conditions which can include:

- All failures caused by a 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 postulated event.

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 [2]), 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.

I. Bašić, I. Vrbanić, International Context Regarding Application Of Single Failure Criterion (SCF) For New Reactors, Journal of Energy, vol. 65-2 (2016) Special Issue, p. 144-159

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*."

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 [22] 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 [22] 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 should be 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 ([3], 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 requirements from IAEA SSR-2/1 [2], SSR-2/2 [3]((IAEA Safety Standard Series, SSR-2/2, Safety of Nuclear power Plants: Commissioning 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.

IAEA Safety Guide NS-G-2.2 [4] 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.

Previously, IAEA had a document Safety Series document 50-P-1 (Application of the Single Failure Criteria, [8]). This document is outdated but there is still no new IAEA document superseded it. However, [8] 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 [7]). 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[6] 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 [9], [11] and [11].

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) [15] . 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 19 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 Importance), 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 complete 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 [16] 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 covers 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 and 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 Practi-cable 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 WENRA RHWG safety objectives for new NPP designs [16]. This document does not change the definition and usage of SFC according to WENRA RHWG safety reference levels for existing reactors [15] 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 provisions of the third level of DiD. Based on the [16], 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 defense 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 appropriately 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[16] 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-assumptions (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 defense 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

2.3 Level of Depth in Defence (DiD) according different guidelines as a basis to develop an evaluation basis for licensing

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 [5], NOTE 2	EUR[17]	WENRA Note 1	STUK[20],	US-NRC[13]	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 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 combination 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, systems 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 below the original tables from SSG-2[5] and EUR rev D [17]:

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

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

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

2.4 SINGLE FAILURE CRITERION APPLICATION IN NEW SMALL REACTOR DESIGNS

In tha last decade there was a lot of discussion related to 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 [25], 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 [26] 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 [27], as well as TECDOC-1536 [28], discusses advantages of SMRs design only partially and without specific design requirements.

IAEA report NP-T-2.2 [24] 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 documents discussing the advances in small modular reactor technology developments, [29], 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 [23] 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 sections 2.1-2.3 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 [30] (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 [21] (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 [30] 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 [14], in order to identify potential alternative or complementary risk-informed approaches with respect to the SFC, for use in the new requirements for SMRs.

2.5 SFC Summary Table

Table 3 summarizes the approaches discussed in [1] 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 Cooling Water, etc.)	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: • (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			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?
			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 argument covering the allowable outage time			Actually, similar to text for IAEA, WENRA, EUR, US NRC above even that section 7.6.2 of REG-DOC-2.5.2 [21] refers to the old IAEA, Safety Series No. 50-P-1 [8] which was withdrawn without applicable replacement.

3 CONCLUSION

The most important conclusion based on the presented work is that nuclear industry and regulation applications either to single failure criteria (SFC) or Defence in Depth (DiD) are not well harmonized. A bigger additional effort should be done to establish more strict and harmonized design requirements regard either SFC or DiD to improve safety of nuclear installation in future.

.

REFERENCES

[1] I. Bašić, I. Vrbanić, "Assessing Regulatory Requirements and Guidelines for the Single Failure Criterion (Research Project R557.1), ENCO FR-(15)-12, June 2015

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

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

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

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

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

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

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

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

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

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

[12] 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]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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