**Context of Single Failure Criterion (SCF) Application for Small Modular Reactor (SMR)**

I. BASIC

APoSS d.o.o.

Zabok, Croatia

Email: basic.ivica@kr.t-com.hr

I.VRBANIC

APoSS d.o.o.

Zabok, Croatia

Email: ivan.vrbanic@zg.t-com.hr

**Abstract**

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 paper provides an updated overview (previously evaluated by authors in [12],[13] and [26]) of the regulatory design requirements for new reactors including highlights on Small Modular Reactors (SMR) addressing the SFC at international level. It considers the SCF in relation to in-service testing, maintenance, repair, inspection and monitoring of systems, structures and components important to safety, as well as to severe challenges not included in the design envelope. A comparison is provided of the current SFC requirements and guidelines published by the IAEA, WENRA, EUR, USA and Canada. Also, the paper addresses some specific issues concerning the application of SFC. Based on the comparative evaluation, the conclusions are provided concerning that the harmonization at the international level is still needed.

## 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.

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.

In practice, as authors discussed in [12],[13] and [26], the SFC exists in two major contexts: (1) system design requirements, largely associated with the general design criteria which require designing safety-related systems to perform safety functions to mitigate design-basis initiating events, assuming a single failure (and calling for the principles of redundancy, independency, separation, and those associated), and, (2) guidance on design-basis-accident (DBA) analysis, directed towards demonstrating adequate design safety margins based upon defined acceptance criteria.

## Overview of International Requirements Concerning SFC

The IAEA, in the major document related to the design of the nuclear power plants, SSR-2/1 (rev.1) [1], provides under section 5 (General Plant Design) the requirement concerning the single failure criterion (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 single failure criterion17 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.”*

It is, furthermore, explained:

*“A 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.”*

Generally, based on the SSR-2/1 (rev.1) [1], IAEA requires the application of the single failure criterion (SFC) for all safety systems, which is further covered by the IAEA SSG guidelines, e.g. SSG-56, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, [2] or SSG-53 Design of Reactor Containment System for Nuclear Power Plants, [3]. For example, SSG-53 states:

*“3.72. The engineering design rules applicable to an entire system (e.g. single failure criterion, physical and electrical separation, functional independence, emergency power supply, periodic tests) should be derived from the safety class assigned to the system, assuming the function performed by the system is not accomplished.”*

Generally, in applicable IAEA SSG publications it is discussed that 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 bounding all possible conditions. The assumption of a single failure in a safety group should be part of the conservative approach, as indicated in SSR-2/1 (rev.1) [1], (5.26, DBA definition). On the other hand, care should be taken when introducing adequate 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.

.

Screening concerning the application of the SFC was performed and documented in [26], additionally to the IAEA’s requirements, of the Western European Nuclear Regulators’ Association (WENRA) safety reference levels, [9], European Utility Requirements (EUR), [11], and of regulatory requirements in selected countries. The comparative discussion of the requirements and positions is given in [12] and [13].

Obviously, SFC as a design principle does not have a definitive alternative. However, the experience with application of SFC which was gained over the period of time stretching over half of a century points out to some weaknesses and/or insufficiency in rigid SFC rule which may need to be reconsidered in the context of new small modular reactors (SMR) designs. A number of particular considerations may be summarized via the following two main points regarding traditional SFC application, which can be very frequently encountered in the discussions:

* The first point is that traditional application of the SFC has, apparently, sometimes led to redundant system components, which contribute to adequate and acceptable safety margins, but may have only minimal impact on risk, based on conventional risk assessment studies. While maintaining adequate safety margins is a major safety objective, the application of the worst single-failure assumption for all DBAs may, in some cases, result in unnecessary constraints on licensees.
* The second point is that the traditional implementation of the SFC does not consider potentially risk-significant sequences involving multiple (rather than single) failures as part of the DBA analysis. Common-cause failures, some support system failures, multiple independent failures, and multiple failures caused by spatial dependencies and multiple human errors, are phenomena that impact system reliability, which may not be mitigated by redundant system design alone. Some risk-informed alternatives might consider such failures in DBA analyses if they were more likely than postulated single-failure events.

The additional issue is that SMRs, taking into account design requirements for big power reactors, should apply and satisfy design extension conditions and the concept of practical elimination as described in SSG-88 [4], [10] or/and [17]. IAEA SSR-2/1(rev.1) [1] specifies that “*the levels of defense in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems*”. EUR [11] requires that the *SFC shall be applied to any system designated to perform 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.* Specifically, EUR [11], in section 2.1.5.1.5 (Requirements on SSCs according to Safety Class) defines that *SFC is not applied to systems identified to support DEC scenarios and designed as a backup of a safety class 1 system which provides an alternative means to accomplish the same safety function as that performed by the safety class 1 system. The reliability of such system should be adequate to meet the total Core Damage Frequency (CDF) target.* However, I&C systems designed as a backup to safety class 1 I&C systems may require the redundancy to be applied to prevent spurious actuation (e.g. for the diverse actuation system).

## SINGLE FAILURE CRITERION APPLICATION IN NEW SMALL REACTOR DESIGNS

In the last decade there was a lot of discussion related to the implementation of so called “small reactors” (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, the Russian Federation, South Africa, USA, and several other IAEA Member States. By definition, SRs and SMRs should have many advantages like as fitness for smaller electricity grids, options to match demand growth by incremental capacity increase, tolerance to grid instabilities, site flexibility, 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 and other.

IAEA developed the safety report, SRS-123 [5], for preparing user requirements documents for small and medium reactors and their application, presenting a high level review of the applicability of IAEA safety standards to EIDs (including SMRs) — in particular, to consider whether the current requirements and recommendations are applicable to these technologies and to identify any gaps, that is, new safety issues on which the standards appear to be silent or not fully address. 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. SRS-123[5], identifying gaps and areas for additional consideration through SSR-2-1 [1], concludes that for SMRs, additional explanatory guidance might help with the interpretation and application also on a module level, considering the complementarity of module, plant and site level views. For example, it is considered that SSR-2/1(rev.1) [1], further consideration for passive systems regarding the applicability of the single failure criterion and CCFs may be useful in Requirement 24 and 25.

From 2016 to 2023 IAEA issues 6 different TECDOCs (2040 [18], 2031 [19], 2003 [20], 1936 [21], 1972 [22], 1915 [23] and 1785 [24]) discusses innovative small and medium sized reactors including, very briefly, design features, safety approaches and R&D trends. The mentioned documents provide brief information regarding SMRs design requirements and lessons learned in regulating small modular reactors.

IAEA report NP-T-2.2 [7] 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. This IAEA report NP-T-2.2 [7], discussing the advances in small modular reactor technology developments, mentions, for the few applications, that the defense 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. However, a newer Safety report on DID, SRS-46 [6], mentions directly that the described methods could also be adapted for other types of reactors, such as small modular reactors.

In the U.S., the current regulations, e.g., the 10 CFR Part 52 combined license (COL) or early site permit (ESP) processes, were developed on the basis of experience gained over the past 40-50 years from the design and operation of large light-water reactor (LWR) facilities. In order to facilitate the licensing of new reactor designs that differ from the current generation of large LWR facilities, the NRC staff has been considering ways to resolve key safety and licensing issues and to 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. Those included a possible need to re-evaluate the role of SFC.

In parallel, 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 [32] which 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 design certificates. Thus, it was recommended to initiate 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. Among other issues, discussed was the application of SFC. Report mentioned 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, given the rigorous application of risk analysis in a plant design.

Actually, re-evaluation of SFC by the U.S. NRC in the context of non-LWR technologies, relying on inherent / passive safety features rather than redundancy, has a history of several decades by now. For example, SECY-03-0047, [27], dated 2003, addresses, among others, the question to what extent can a probabilistic approach be used to establish the licensing basis for: selection of events to be considered in the design and for emergency planning; safety classification of systems, structures, and components; and *replacement of the SFC*. It provides a recommendation to replace the SFC with a probabilistic (reliability) criterion, which would lead to a technology neutral, systematic and consistent approach for establishing key aspects of the licensing basis for non-LWRs, while accommodating their unique aspects. With SFC replaced with a reliability criterion, the event scenarios identified in the PRA would be examined against this criterion. This could lead to having to consider multiple failures in AOO, DBE, and Emergency Planning accident scenarios. This would, of course, however, require that PRA becomes part of the licensing basis for the plant with appropriate controls on PRA completeness, quality and documentation.

Possible alternatives to SFC were subject of SECY-05-0138, dated 2005 [28]. Three were found: Alternative 1 - Risk-Inform Application of SFC to DBA Analysis; Alternative 2 - Risk-Inform Application of SFC Based on Safety Significance, and Alternative 3 - *Replace SFC* with Risk and Safety Function Reliability Guidelines. Particularly, the Alternative 3 would replace the SFC with a combination of quantitative targets and guidance: 1) top-level risk targets for CDF and LERF; 2) lower-level functional reliability targets commensurate with challenge frequency; and 3) guidance for redundancy, diversity, and CCF. Licensees would determine which plant features to credit to address the targets, and how much credit to take for those features.

Approach of the industry in U.S. toward achieving safe non-LWR design is described in NEI 18-04, [29]. This guideline is stated to present a modern, technology-inclusive, risk-informed, and performance-based process for selection of Licensing Basis Events; safety classification of SSCs and associated risk-informed special treatments; and determination of defense-in-depth (DID) adequacy for non-LWRs. In the task related to selecting deterministic DBAs and design basis external hazard levels, it is stated that, in view of the fact that advanced non-LWRs will employ a diverse combination of inherent, passive, and active design features to perform the required safety functions across layers of defense, and, taking into account the fact that the reactor safety design approach will be subjected to an evaluation of DID adequacy, the application of a *SFC is not deemed to be necessary*.

NEI 18-04 was endorsed by U.S. NRC Regulatory Guide 1.233, [30], in which it is stated that the approach described in NEI 18-04 is consistent with the above mentioned SECY-03-0047, [27], to replace the SFC with a probabilistic (reliability) criterion. It was found that the NEI 18-04 methodology, including assessments of event sequences and DID, “obviates” the need to use the SFC as it is applied to the deterministic evaluations of AOOs and DBAs for LWRs. Also, it was noted that the NEI 18-04 methodology is similar to the mentioned Alternative 3 in SECY-05-0138, [28].

Recently, the NRC staff has provided the draft proposed 10CFR53 rulemaking package, [31], which accommodates all reactor technologies and includes two distinct and self-contained licensing frameworks, Framework A and Framework B. The frameworks offer flexibility for the roles of risk assessment techniques and design approaches in establishing licensing basis information. Framework A represent a PRA-led approach that aligns with the U.S. Department of Energy cost-shared, industry-led Licensing Modernization Project methodology. This framework introduces changes from the traditional or deterministic approaches in 10CFR50 and 10CFR52 in areas such as *replacing the SFC* with a probabilistic reliability criterion (with a reference to the above-mentioned SECY-03-0047, [27]. Framework B represents a traditional, deterministic approach that aligns with international guidance and includes an alternative evaluation for risk insights approach, which would not require a PRA if certain entry conditions are met. designs. This framework would maintain the traditional role of specific design rules, *including use of the SFC* as a tool in the reactor safety analysis process.

Canadian regulatory requirements for design of small reactor facilities [33] (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 [25] (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 [33] 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.

## Concluding Remarks

The most important conclusion which can be made is that nuclear industry and regulation applications either to single failure criterion or defense-in-depth are still not very well harmonized in the international practice not only for high-power reactor but for SMR too. Additional effort is advisable to be made in order to establish more strict and harmonized design requirements with regard to either SFC or DiD to improve safety of nuclear installations in the future.

Past experience with application of SFC which was gained over the period of time stretching over half of a century points out to some weaknesses in rigid application of traditional SFC rules. Those include failing to establish reliability of the functions important to safety which would be commensurate with frequencies of challenges to them.

It has been many times repeated that traditional design basis analyses (DBA) are conservative because they assume failure of a single train. It has been rarely pointed out that the same analyses may be optimistic because they assume that complementary train will succeed for granted.

It seems to be advisable to reconsider and adjust the SFC approach for application to the new water-cooled (or other) reactor designs including SMR. The options for that have been discussed and identified in the references.

References

1. IAEA Safety Standard Series, SSR-2/1, Safety of Nuclear power Plants: Design, Rev.1, IAEA, Vienna, 2016
2. IAEA Safety Standards Series, SSG-56, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, IAEA, Vienna, 2020
3. IAEA Safety Standards Series, SSG-53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA, Vienna, 2019
4. IAEA Safety Standards Series, SSG-88, Design Extension Conditions and the Concept of Practical Elimination in the Design of Nuclear Power Plants, IAEA, Vienna, 2024
5. IAEA, Safety Report Series No. 123, Applicability of IAEA Safety Standards to Non-Water Cooled Reactors and Small Modular Reactors, IAEA, Vienna, 2023
6. IAEA, Safety Report Series No. 46, Assessment of Defence in Depth for Nuclear Power Plants, IAEA, Vienna, 2005
7. IAEA Nuclear Energy Series, NP-T-2.2, Design Features to Achieve Defence in Depth in Small and Medium Sized reactors, 2009
8. IAEA ARIS, Advances in Small Modular Reactor Technology Developments, 2022
9. Western European Nuclear Regulators’ Association, Safety Reference Levels for Existing Reactors, WENRA, 2020
10. Report Practical Elimination Applied to New NPP Designs - Key Elements and Expectations, WENRA, 2019
11. European Utility Requirements for LWR Nuclear Power Plants, Revision E, December 2016
12. Bašić, I. Vrbanić, Assessing Regulatory Requirements and Guidelines for the Single Failure Criterion (Research Project R557.1), ENCO FR-(15)-12, June 2015
13. Bašić, I. Vrbanić, International Context Regarding Application of Single Failure Criterion (SCF) for New Reactors, Proceedings of the 10th International Conference of the Croatian Nuclear Society, Zadar, Croatia, 5-8 June 2016
14. U.S. NRC SECY-05-0138, Risk-Informed and Performance-Based Alternatives to the Single-Failure Criterion, U.S. NRC, 2005
15. NUREG-1860, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, U.S. NRC, 2007
16. 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]
17. IAEA TECDOC-1791, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA, 2016
18. IAEA TECDOC-2040, Considerations for the Back End of the Fuel Cycle of Small Modular Reactors, IAEA, 2023
19. IAEA TECDOC-2031, Advancing the State of the Practice in Uncertainty and Sensitivity Methodologies for Severe Accident Analysis in Water Cooled Reactors of PWR and SMR Type, IAEA, 2023
20. IAEA TECDOC-2003, Lessons Learned in Regulating Small Modular Reactors Challenges, Resolutions and Insights, IAEA, 2022
21. IAEA TECDOC-1936, Applicability of Design Safety Requirements to Small Modular Reactor Technologies Intended for Near Term Deployment Light Water Reactors High Temperature Gas Cooled Reactors, IAEA, 2020
22. IAEA TECDOC-1972, Benefits and Challenges of Small Modular Fast Reactors Proceedings of a Technical Meeting, IAEA, 2021
23. IAEA TECDOC-1915, Benefits and Challenges of Small Modular Fast Reactors Proceedings of a Technical Meeting Considerations for Environmental Impact Assessment for Small Modular Reactors, IAEA, 2020
24. IAEA TECDOC-1785, Design Safety Considerations for Water Cooled Small Modular Reactors Incorporating Lessons Learned from the Fukushima Daiichi Accident, IAEA, 2016
25. REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, CNSC, rev.2.1, 2023
26. Bašić, I. Vrbanić, Overview and Comparison of International Practices Concerning the Requirements on Single Failure Criterion with Emphasize on New Water-Cooled Reactor Designs, International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water-Cooled Nuclear Power Plants, IAEA Headquarters in Vienna, Austria, June 2017
27. SECY-03-0047, Policy Issues Related to Licensing Non-Light-Water Reactor Designs, U.S. NRC, March 28, 2003
28. SECY-05-0138, Risk-Informed and Performance-Based Alternatives to the Single-Failure Criterion, U.S. NRC, August 2, 2005
29. Nuclear Energy Institute (NEI) 18-04, “Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” Revision 1, August 2019.
30. U.S. NRC Regulatory Guide 1.233, Guidance or a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors, Revision 0, June 2020
31. SECY-23-0021: Proposed Rule: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors, with enclosures; U.S. NRC, March 1, 2023
32. Interim Report of the American Nuclear Society President’s Special Committee on Small and Medium Sized Reactor (SMR) Generic Licensing Issues, US ANS, July 2010
33. RD-367, Design of Small Reactor Facilities, Canadian Nuclear Safety Commission, 2014