DEFENCE IN DEPTH AND PRACTICAL ELIMINATION OF EARLY AND LARGE RELEASES – CONCEPTS AND PRACTICE.

S. MICHAEL MODRO
Nuclear and Industrial Engineering S.r.l, Via della Chiesa XXXII, 759 -55100 Lucca, Italy
TOMISLAV BAJS
ENCONET d.o.o., Miramarska 20, 10000 Zagreb, Croatia
ARTUR LYUBARSKI
Atomenergoprojekt, Moscow, Podolskich Kursantov 1 st , Russian Federation

ABSTRACT

One of the most important requirements of the International Atomic Energy Agency Safety Standard on design (SSR-2/1) is the requirement for practical elimination of accident sequences that would lead to large or early radioactive releases. This requirement is accompanied by requirements for extension of the plant design basis to include conditions considered earlier as “beyond design basis” which may include plant conditions with multiple failures of systems, including safety systems, without and with severe core damage. In this paper we are discussing the concept of practical elimination of large or early radioactive releases in the context of defence in depth and we are addressing some challenges for demonstration of this concept. The demonstration of the “practical elimination” is a complex process for which no specific guidance and criteria are available and not sufficient experience is so far generated. The “practical elimination” shall be considered as integral part of the defence in depth.

1. Introduction

In 2012 the International Atomic Energy Agency (IAEA) has published a Safety Standard on design safety [1] that replaced the previous version published in 2000 [2]. One of the most important requirements in the new standard, that distinguished it from the older version, was requirement for practical elimination by means of the plant design of accident sequences that would lead to early or large radioactive releases. This requirement was accompanied by requirements for extension of the plant design basis to include conditions considered earlier as “beyond design basis” which may include plant conditions with multiple failures of systems, including safety systems, without and with severe core damage. A revision of the SSR-2/1 standard published in 2016 [3] basically does not introduce any new requirements but mainly emphasizes certain aspects of some requirements, especially of those related to defence in depth, design basis and resistance to external natural hazards. These requirements, developed in an international consensus, are designed to enhance the safety of nuclear power plants considering also lessons learned from the Fukushima Daichi accident.

In May 2016 the IAEA has published a report [4] that provides interpretation of the some of the most important design safety requirements of SSR-2/1. The report focuses on the categories of plant states, the concept of defence in depth, the concept of independence of the safety provisions at different levels of defence in depth, the concept of practical elimination, cliff edge effects and safety margins, the design for external hazards, use of non-permanent equipment for accident management, and the reliability of the ultimate heat sink. The goal of this report is to harmonize the understanding of

these important safety concepts and could be used for establishment of high level of safety in new designs or for safety analyses including design or periodic safety reviews of existing NPPs.

In following sections we are discussing the concept of practical elimination of early and large radioactive releases in the context of defence in depth and we are examining some challenges for safety analyses as consequences of the SSR-2/1 requirements. It is evident that these requirements call for a holistic representation of defence in depth using probabilistic and deterministic methods that consider all levels of defence and require suitable deterministic and probabilistic goals and criteria.

2. The concept of „practical elimination“

It is expected that power reactors have high resistance to equipment and human failures and to natural or human made external hazards and that accident sequences that can lead to early or large radioactive releases are practically eliminated. It is understood that practical elimination means that the certain conditions (phenomena) associated with these sequences will be physically impossible or the probability of these conditions to occur will be extremely low with high level of confidence. These conditions could be eliminated by design, for example by developing inherently safe systems, or providing systems which mitigate accidents at various stages and protect the barriers against broad range of challenges, ultimately assuring the integrity of the containment even during accidents with significant core damage.

In general the concept of practical elimination is not new. In 1999 the IAEA International Nuclear Safety Advisory Group (INSAG) published Basic Safety Principles for Nuclear Power Plants – INSAG-12 [5] introducing the concept of “practical elimination”. In 2004 the IAEA issued a guide on design of containment systems for nuclear power plants [6] in which, for new plants, following phenomena of severe accident conditions that challenge the integrity of the containment were identified that should be practically eliminated:

- Direct containment heating,
- Steam explosions and hydrogen detonations in early phases of the accident,
- Basemat melt-through or containment overpressurization in late phases of the accident.

Also, the design should assure elimination of:

- Severe accidents in conditions with open containment, and
- Accidents with containment bypass.

For accident sequences which could not be practically eliminated the containment design should be such that any necessary off-site emergency measures needed would be minimal.

The practical elimination appeared in IAEA Safety Standards as requirement in 2012 design safety requirements [1]. Requirements for practical elimination, as consequence, result in in additional changes to the requirements for the design basis of a plant and accident conditions to be considered in the design and analyses. Dedicated systems, or design characteristics, were now required to deal with severe accidents and other

conditions considered before as "beyond design" basis. These dedicated systems were termed "safety features" to distinguish from "safety systems" dedicated to design basis accidents. The extended design basis was termed "design envelope" and the former beyond design basis conditions became design extension conditions. Figure 1 illustrates the plant conditions to be considered as requirement in the plant design and safety analyses. The design and safety evaluation rules remain the same for the design basis accident conditions but are different for the design extension conditions (DEC). The safety features needed to cope with DEC do not have to follow the requirements such as single failure or redundancy, however that need to be qualified for the environment of severe accidents.

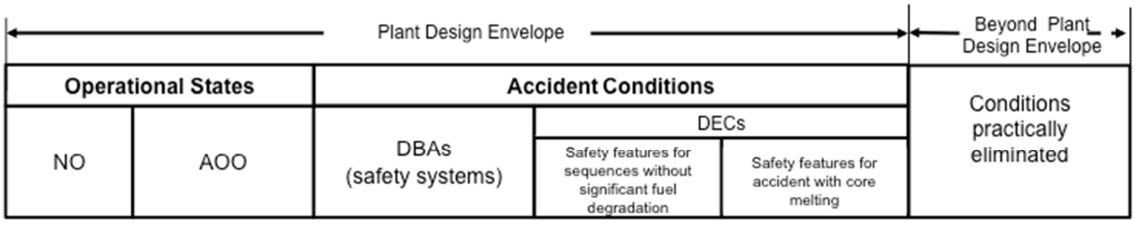

Figure 1. Plant conditions to be considered in the design and safety assessment (SSR-2/1)

To address the practical elimination of the early or large radioactive releases in the design and analyses first the conditions that need to be eliminated must be identified. Then, these conditions need to be addressed by careful design of the plant including possible safety features which would mitigate the accident escalation an/or protect the containment from challenges. Finally, this new design envelope needs then to be evaluated by means of deterministic and probabilistic analyses as well as engineering judgment.

Some insights on conditions to be practically eliminated provide PSA studies. From the deterministic perspective, all conditions that lead to challenges and integrity damage of the physical barriers should be practically eliminated. As discussed above, already NS-G-1.10 [6] provided some guidance on the conditions to be eliminated. The recently published IAEA TECDOC-1791 [4] provides list of similar categories of conditions to be eliminated, however added were events that could lead to prompt reactor core damage such as failure of large coolant system component including the reactor vessel and uncontrolled reactivity accidents. Also severe accidents in a storage pool are considered.

The studies of severe accidents over the last four decades have provided enough understanding of the phenomena and progression of the accidents that the current trend in the NPP designs is to provide for additional safety systems and features with the goal to minimize the potential challenges to the containment integrity and releases of radioactive materials to the environment. These features include designs that provide for in vessel retention of molten cores, core catchers, passive catalytic recombiners, etc.

The final step in the implementation of the concept of “practical elimination” requires demonstration, with high confidence, that sequences, conditions and phenomena leading to early or large releases will not arise due to laws of physics, safety systems and features, or that *the “likelihood of severe accidents with serious radiological consequences is extremely small”*. The demonstration of the physical impossibility of

these conditions requires a through examination of the inherent and engineered systems characteristics and assessment of their ability to eliminate the challenges. Deterministic safety analyses need to provide confirmation of these engineering assessments. The analyses should address all sequences that lead to melting of the core. The special safety features for the design extension conditions need to be modeled. The analyses should be conducted in best estimate fashion, however since quantification of uncertainties can be impractical due to complexity of the phenomena, some conservative assumptions for the operation of the safety features can be used. Extensive sensitivity studies need to be conducted to assure that there are no hidden cliff-edge effects and to assure that there are sufficient margins to account for uncertainties. Currently there are no specific guidelines how to conduct the deterministic analyses in support of the demonstration of "practical elimination".

The "practical elimination" needs to be also addressed through extensive probabilistic analyses. However, if for demonstration of "practical elimination" probabilities or frequencies of occurrence are used probabilistic targets will have to be established and have to be equal or lower than those which regulatory bodies establish for early or large radioactive releases. The TECDOC-1791 [4] identifies release frequency below 10^{-6} per reactor year for early or large radioactive releases can be achieved for designs "which adopt the latest technological solutions" for events of internal origin. Determination of frequency targets for events resulting from external hazards might be more difficult as according to [4] as those might be below the frequency of 10^{-6}/year. Target such as 10^{-6}/year may seem to be too large for "practical elimination", but there is lack of guidance and agreement on such a target, and which would have to be established by regulatory authorities adopting the concept. Additionaly, it is not practical to address quantitatively all PSA Level 2 uncertainties, which may stem from the severe accident analyses. Therefore the dominant sources of uncertainties need to be identified and treated separately in detail.

In general, the assessment and the demonstration of "practical elimination" should be not based purely on PSA methods. Both deterministic and probabilistic approaches are necessary and considerations in assessment of the effectiveness of defence in depth discussed in the next section.

2. Defence in depth

The strategy for defence in depth (DiD) is, above all, about preventing accidents. However, if prevention fails, the strategy is to limit potential consequences of the accident and to prevent escalation of the accident into more serious conditions including those which would result in significant or early radioactive releases to the environment. The defence in depth should compensate for human errors and component failures maintaining effectiveness of barriers and providing for mitigation capabilities. The defence in depth as key and universal safety concept is addressed extensively in the IAEA design safety requirements [1]. The defence in depth is structured in levels of equipment and procedures in order to maintain the effectiveness of physical barriers, placed between radioactive material and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accident at the plant. Defence in depth – ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure and human errors. Also, the IAEA standard requires that, to the extent possible, provisions at different levels of defence should be independent. The following table identifies the defence in depth levels and the means by which the defence levels are achieved [4].

Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/ emergency operating procedures	Level 2
3a	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems)	Emergency operating procedures	Level 3
Level 3 3b	Control of design extension conditions to prevent core melt	Safety features for design extension conditions without core melt	Emergency operating procedures	4a
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melt. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	Level 4 4b
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	Level 5

Table 1. Defence in depth levels

The importance of the Level 1 of DiD for practical elimination of early or large radioactive releases is evident as all levels of DiD are determined at the first level when the design is established. This level must assure a robust design that includes the design features and the strategy for prevention and mitigation of accidents escallation with the ultimate goal of practical elimination of all accidents, even those of very low probability, that would lead to radiological consequences. References [3] and [4] provide requirements and detailed discussion of the levels of defence.

The levels of defence in depth can be correlated with the plant conditions shown in Fig. 1, see figure below.

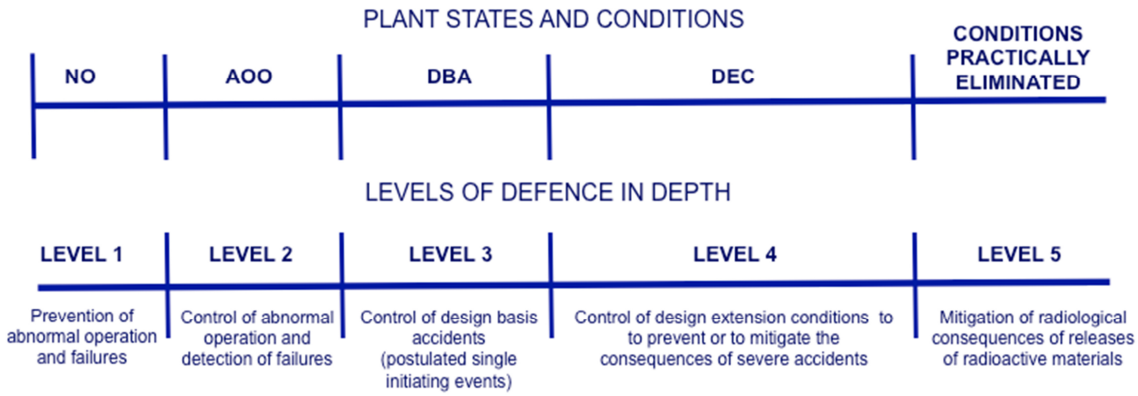

Figure 2. Plant conditions and DiD levels

A question can arise whether the Level 5 of DiD is needed when the “practical elimination” is achieved. At present state of knowledge, limited capabilities to demonstrate “practical elimination”, and lack of specific guidelines and criteria (particularly probabilistic) there is no justification for not implementing this final level of defence.

The demonstration of “practical elimination” could be conducted in the context of the assessment of effectiveness of defence in depth. The IAEA provides guidance on performance of such assessment [7]. The proposed method is a complex process requiring significant effort and specific plant design data, and there is not much experience in the world in application of this assessment process. A different method for assessing the DiD was proposed in [8] is based on probabilistic concept.

The defence in depth can be represented using the event tree techniques as illustrated in Figure 3. Events within one level of DiD are events of certain frequencies that arise independently or propagate from previous level due to failures of protective systems and challenge the next level of DID if additional failures occur. The success of DiD levels can be measured by frequencies that can be associated to the frequencies identified for plant states and conditions identified for example in [4] as shown in Figure 3.

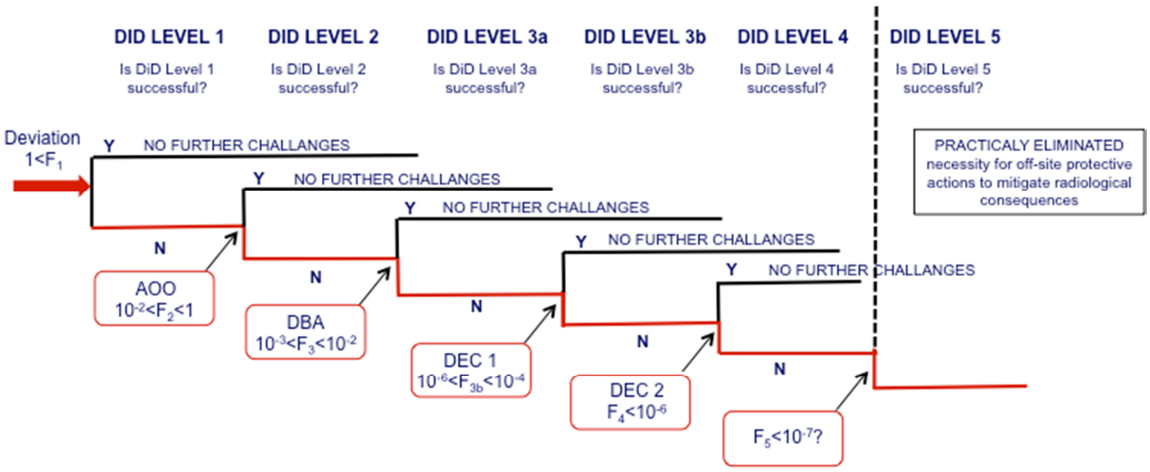

Figure 3. Concept of DiD represented by the event tree technique.

The proposed method needs establishment of the probabilistic criteria, but also deterministic criteria and goals need to be identified and valuated for each level of defence [8].

Using the PSA techniques the independence of level of defence can be evaluated and the proposed approach can also be used for defining reliability criteria for equipment at various levels of defence to achieve the desired practical elimination.

3. Conclusions

The practical elimination of large or early radioactive releases during nuclear power plant accidents is desired. However, the demonstration of the “practical elimination” is a complex process for which no specific guidance and criteria are available and not sufficient experience is so far generated. The “practical elimination” shall be considered as integral part of the defence in depth. The identified probabilistic method can support the decision making process in the design of new power plants and assist evaluation of DiD for existing plants and designs.

4. Acknowledgements

The authors wish to acknowledge the advise and contributions of Irina Kuzmina of IAEA.

3. References

1. SAFETY OF NUCLEAR POWER PLANTS: DESIGN; IAEA SAFETY STANDARDS SERIES No. SSR-2/1, INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA 2012
2. SAFETY OF NUCLEAR POWER PLANTS: DESIGN; SAFETY STANDARDS SERIES No. NS-R-1; INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 2000
3. SAFETY OF NUCLEAR POWER PLANTS: DESIGN; IAEA SAFETY STANDARDS SERIES No. SSR-2/1 (Rev. 1); INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA, 2016
4. CONSIDERATIONS ON THE APPLICATION OF THE IAEA SAFETY REQUIREMENTS FOR THE DESIGN OF NUCLEAR POWER PLANTS, IAEA TECDOC-1791, INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA, 2016
5. BASIC SAFETY PRINCIPLES FOR NUCLEAR POWER PLANTS 75-INSAG-3 REV. 1, INSAG-12, A REPORT BY THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1999
6. DESIGN OF REACTOR CONTAINMENT SYSTEMS FOR NUCLEAR POWER PLANTS, SAFETY GUIDE, IAEA, SAFETY STANDARDS SERIES No. NS-G-1.10, INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 2004
7. ASSESSMENT OF DEFENCE IN DEPTH FOR NUCLEAR POWER PLANTS, IAEA SAFETY REPORTS SERIES No. 46, INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 2005
8. AN APPROACH FOR HOLISTIC CONSIDERATION OF DEFENCE IN DEPTH FOR NUCLEAR INSTALLATION USING PROBABILISTIC TECHNIQUES, I. KUZMINA ET AL., 2011 INTERNATIONAL TOPICAL MEETING ON PROBABILISTIC SAFETY ASSESSMENT AND ANALYSIS, WILMINGTON, NC, MARCH 13-17, 2011