Chapter 3
Safety Principles for Pressurised Water Reactors in the French Nuclear Power Plant Fleet

3.1. Introduction

The goal of this chapter is not to provide an exhaustive explanation of nuclear safety principles and practices at facilities in France (for a discussion on this topic, see the work of J. Libmann [1]), but to illustrate the two complementary safety approaches, deterministic and probabilistic, by introducing a key concept of the first, defence-in-depth, and a general description of probabilistic safety assessments (PSAs), which are part of the second.

Nuclear facilities, in particular those for producing electricity, present specific risks related to the presence of often significant quantities of radioactive substances that can cause individuals, population groups and the environment to be exposed to ionising radiation.

Nuclear safety is composed of a set of technical and organisational measures taken during all phases in the life of a facility (design, construction and commissioning, operation, decommissioning and dismantling) to protect workers, the general public and the environment from the effects of radioactive substances. It involves:

– ensuring normal operation of facilities without excessive exposure for workers and excessive releases of radioactivity in radioactive effluents;

- preventing incidents and accidents;
- limiting the consequences of incidents and accidents that occur despite prevention measures that have been implemented.

Containment of radioactive substances is achieved by placing "barriers" between the substances and people. In diagrammatic terms, for pressurised water reactors (PWRs) of the type operated in France, there are three successive barriers between radioactive substances and the environment: the fuel rod cladding, the reactor coolant system and the containment building. Optimal leak tightness of these barriers in the various situations of normal and emergency operation shall be sought in the design phase. However, in normal operation, the barriers are not generally perfectly leaktight: cladding ruptures and leaks in the reactor coolant system and the containment building of limited significance may occur[1].

It is important to mention in this context the particular case of PWR steam generator tubes, which are part of the second and third barriers, since the rupture of a tube may cause the safety valves of the steam generator to open, thus creating a containment bypass.

The goal of defence-in-depth, introduced in the following section, is to ensure basic safety functions, i.e., controlling reactivity, cooling irradiated fuel and containing radioactive substances; these safety functions are necessary to ensure all barriers remain effective.

3.2. Concept of defence-in-depth

The defence-in-depth concept was introduced in the nuclear safety field in the early 1970s. In nuclear facilities, it is achieved by implementing levels of defence based on the intrinsic characteristics of the facility, equipment measures and procedures put in place to prevent accidents, and if prevention fails, limit accident consequences. Defence-in-depth is a concept that applies to all stages in the life of a facility, from design to dismantling.

How the concept of defence-in-depth is implemented has evolved over time to take into account operational experience from facilities, including incidents and accidents that have occurred, in order to build an ever more effective defence.

For reactors currently in operation, defence-in-depth is based on five levels (see INSAG-10 [2] and Table 3.1) intended to prevent the occurrence and limit the consequences of technical, human and organisational failures. The various levels of defence-in-depth apply in the various states of the facility, from normal operation to core melt accidents. At each level of defence-in-depth, except for level 5, there are measures designed to prevent the occurrence of more severe situations.

The design of current reactors included only three levels of defence-in-depth.

1. Leaks during normal operation will nevertheless meet operating technical specifications.

Level 1: prevention of operating anomalies and system failures

Prevention of operating anomalies and failures in components, equipment and systems assumes prudent design (with adequate safety margins) and components, equipment and systems that have been manufactured and operated to the highest quality standards. This level corresponds to the normal domain of operation for the facility with general rules and operating procedures designed to maintain the plant unit within its normal operating domain.

Level 2: failure detection and comprehensive management of operating malfunctions

This level includes resources and systems designed to control operating malfunctions, which assumes monitoring that will ensure failures are detected. This includes automatic functions and control systems that can return the facility to its normal operating mode. These systems are designed to correct an abnormal change in facility parameters.

Level 3: comprehensive accident management (including design-basis accidents)

The first two levels of defence-in-depth reduce the risks of failure at the facility. It is nevertheless assumed that accidents can occur during reactor operation. Accidents considered at this level result from a single initiating event (e.g., the failure of a component essential for a basic safety function – comprehensive management of reactivity, cooling of nuclear fuel or containment of radioactive substances). Resources that limit the consequences of such accidents and ensure basic safety functions are implemented: at this level defence-in-depth consists of implementing safeguards that ensure the integrity of the core structure and limit releases into the environment in the event of an accident (considered for the design-basis of the facility). This level also includes defining emergency operating procedures.

After the accident at Three Mile Island Unit 2 (TMI-2) in the United States in 1979, the concept of defence-in-depth was enlarged to include accidents that had not been explicitly considered during facility design. In particular, lessons from the initial probabilistic safety assessments (Section 3.3) and the TMI-2 accident (Section 7.1) demonstrated the need to take into account accidents resulting from multiple failures and those leading to core melt. These developments led to defining an additional level of defence-in-depth.

Level 4: comprehensive management of severe accidents

This level of defence-in-depth includes procedures and equipment used to handle situations that are not covered by the first three levels of defence-in-depth; these are accidents that could result in reactor core melt. At level 4, the objective is to prevent accidents from resulting in core melt and to limit releases outside the site by ensuring containment of radioactive substances in the event core melt nevertheless does occur.

This level of defence-in-depth includes emergency procedures and associated equipment resources (Section 2.5.2), specific equipment (e.g., hydrogen recombiners), the severe accident operating guidelines and the facility's on-site emergency plan. The licensee prepares and implements the on-site emergency plan. When the plan is implemented, the facility's emergency response teams are mobilised in order to contain the accident and avoid the release of radioactive substances. The purpose of the on-site emergency plan is to protect staff working at the site in the event of an incident or accident and to limit off-site consequences of an accident.

Level 5: limiting consequences of radiation in the event of radioactive releases

Despite all the measures described above, radioactive releases may occur. Additional measures, taken by public authorities, are then implemented to protect the public, on-site staff and property from the consequences of these releases.

Measures for protecting the public from radioactive releases include evacuation, shelter in hardwall accommodation, taking of potassium iodide tablets and restrictions on the consumption of foodstuffs. This level includes off-site emergency plans prepared for each site. Public authorities implement the off-site emergency plan, which organises emergency operations to limit public exposure to radiation in the event of releases.

Table 3.1. The various levels of defence-in-depth.

Level	Objective	Main measures	Corresponding facility condition
1	Preventing operating malfunctions and system failures	Prudent design (including safety margin) and well-designed and well-run facility	Normal operation
2	Detecting failures and comprehensive management of operating malfunctions	Systems for control, protection and review (for maintaining the facility within its normal operating domain) and monitoring (preventing failures)	Operating malfunctions or failures
3	Comprehensive accident management (including design-basis accidents)	Safeguard systems and accident procedures	Accidents including "design-basis accidents" (single initiating event)
4	Comprehensive management of severe accidents, prevention of accident progression and mitigation of consequences	Additional measures and accident management (emergency procedures and associated equipment resources, severe accident operating guidelines, on-site emergency plan)	Multiple failures Core melt accidents
5	Limiting radiological consequences in the event of a release of radioactive substances	Off-site emergency plan	Accidents with radioactive releases

For third-generation reactors, multiple failure and core melt accidents are considered in the initial design of the reactors, which signifies a major step in the range of accident situations for which measures are taken to prevent accidents and limit the consequences must be planned from the design stage. Even if the measures taken for these reactors cannot all be applied in practice to second-generation reactors, they can help identify safety improvements for reactors that are currently in operation and improve defence-in-depth for the reactors.

3.3. Role of the probabilistic approach

Probabilistic safety assessments (PSAs) were first developed in the 1960s for nuclear power plants. The Rasmussen report [3], published in the United States in 1975, which sought to compare risks for the public from nuclear reactors with other industrial and natural risks, demonstrated the value of a probabilistic analysis for assessing nuclear reactor risks. Since then, all nuclear power plants in commercial operation worldwide have been subject to PSAs.

PSAs supplement traditional deterministic analyses and enable a systematic investigation of the numerous possibilities of event combinations and sequences that constitute accident scenarios. They consist of a set of technical analyses for assessing the risks at a facility in terms of accident frequency, e.g., core melt, and their consequences. They provide an overall view of reactor safety, including both equipment resistance and operator behaviour. They can show topics for which changes both in design and operation can be studied and even judged necessary.

There are three major types of PSAs based on consequences under examination:

- level 1 PSA: used to identify sequences leading to core melt and quantifying their frequency;
- level 2 PSA: used to assess the nature, significance and frequency of releases of radioactive substances outside the containment building;
- level 3 PSA: used to assess the probabilities of consequences on the public in terms of dosimetry and contamination (even in terms of frequency of cancers or other effects on health).

The Rasmussen report [3] is the first example of a level 3 PSA. As will be seen in Section 4.3.2 later, this report remains a reference for an approach to managing core melt accidents. PSAs carried out until now in France for 900, 1300 and 1450 MW plant units and the EPR have been level 1 and 2 [4–9] (see also Sections 4.2 and 4.4). They are prepared by EDF and IRSN with the studies by EDF considered as the reference cases. They are updated by EDF and IRSN, particularly during safety reviews, to take into account changes in knowledge and operating experience and are used for safety assessments of PWRs according to the conditions stated in basic safety rule 2002-01 [10]. The results of level 1 PSAs and the method and applications of level 2 PSAs prepared by IRSN are described in Section 4.4.

Compared with assessments of the same type performed abroad, level 1 and 2 PSAs in France benefit from the standardisation of plant units in France, which helps assess the

reliability of equipment and the probability of certain initiating events on broader statistical bases. In addition, French assessments consider all reactor states: operation at full and intermediate power and maintenance outage. Taking into account the specific operating configurations in these states, including the lesser degree of automatic safeguard actions, French PSAs have demonstrated that these reactor states play a significant role in the probability of core melt. The results brought about improvements in operation (technical specifications and procedures) and design (implementation of alarms and controllers).

The same PSAs also provided a more quantitative assessment of the value of measures taken to improve accident management. Level 2 PSAs are also used to evaluate measures given in severe accident operating guidelines that operators on-site should implement in such situations, particularly to ensure maximum containment of radioactive substances [11–13].

The PSAs however have certain limitations due to uncertainties associated with them that require using caution when interpreting results and using them for making decisions. The existing French PSAs are thus not exhaustive in terms of coverage, since they only partially take into account internal and external hazards. In addition, uncertainties stem from quantitative input data and simplifications and assumptions adopted for the design study [14]. A non-exhaustive list would include uncertainties associated with the choices in combining initiating events, supporting scenarios for thermal-hydraulic and neutronic calculations, modelling of physical phenomena and human actions, estimating the reliability of software and equipment, the choice of event trees (events and chronological order) and probabilistic quantification software (see Section 4.4 for further details).

Global safety PSAs are thus used to support or supplement traditional deterministic safety analyses both for a more quantitative assessment of the level of safety at plant units in France and to constitute analytical tools for these plant units. Insofar as comparison of the results of PSAs to standard criteria must be done with caution given the uncertainties mentioned above, the probabilistic approach is useful for determining weaknesses related to plant units under consideration and to assess, for example, the relative benefit of changes in design or operation.

3.4. Conclusion

The deterministic and probabilistic approaches to safety constitute an ensemble that contributes to preventing and limiting the consequences of accidents, especially severe core melt accidents and thus ensure a heightened level of safety at nuclear facilities. The approaches continue to evolve and it is important not to overlook the permanent interaction between the level of safety at facilities and the current state of knowledge available from research on core melt accidents, which is presented here in Chapter 5; more detailed studies (such as PSAs), given in Section 4.4; operating experience; and incident and accident analysis.

Following the Fukushima Daiichi accident, French nuclear facilities underwent complementary safety assessments (CSAs) which focused on five key points regarding power reactors: risks of flooding, earthquakes, loss of power, loss of heat sink, and operational

management of accident situations. These assessments are aimed at determining the robustness of French reactors in response to extreme external events and adding to existing safety provisions to enhance this robustness.

In particular, efforts are under way at IRSN to expand the scope of PSAs by including recent knowledge from research, handling hazards such as flooding and earthquakes and taking into account operational feedback from facility operation: the goal of these efforts is improved assessment of power reactor risks and measures taken for emergency operation.

References

[1] J. Libmann, *Éléments de sûreté nucléaire*, Collection IPSN, EDP Sciences, 1996.

[2] International Nuclear Safety Advisory Group Report, INSAG-10, IAEA Report, Vienna, 1996.

[3] N. Rasmussen *et al*., Reactor safety study, WASH-1400, Washington D.C., US NRC, 1975.

[4] A. Ellia-Hervy, F. Corenwinder, J.-M. Lanore, V. Sorel, Les Études Probabilistes de Sûreté de niveau 1: les méthodes, les connaissances utilisées, les résultats», *Revue Générale Nucléaire* **1**, 12-16, 2003.

[5] E. Kalalo, D. Brenot, "Rôle et limites des EPS", *Revue Contrôle* **155**, 39-42, 2003.

[6] A. Dubreuil-Chambardel, G. Body, V. Sorel, Qu'est-ce qu'une étude probabiliste de sûreté de niveau 2? Exemple de la troisième visite décennale des REP 900 MWe, *Revue Générale Nucléaire* **1**, 88-92, 2010.

[7] E. Raimond, Apport des études probabilistes de sûreté de niveau 2 dans l'analyse de sûreté – Point de vue de l'IRSN, *Revue Générale Nucléaire* **1**, 99-105, 2010.

[8] E. Raimond, N. Rahni, K. Chevalier-Jabet, T. Durin, L'EPS de niveau 2 pour les REP 900: du développement aux enseignements de l'étude, IRSN, Rapport scientifique et technique, 2008.

[9] E. Raimond, C. Caroli, B. Chaumont, Status of IRSN level 2 PSA, CSNI/WG Risk Workshop, Cologne, Germany, 2004.

[10] Règle fondamentale de sûreté n° 2002-01 – Développement et utilisation des études probabilistes de sûreté pour les réacteurs nucléaires à eau sous pression, document ASN (2002); http://www.asn.fr/index.php/Les-actions-de-l-ASN/La-reglementation/Regles-fondamentales-de-surete-et-guides-de-l-ASN/Guides-de-l-ASN-et-RFS-relatives-aux-REP/RFS-2002-1-du-26-12-2002.

[11] E. Raimond, B. Laurent, N. Rahni, K. Chevalier-Jabet, T. Durin, Application des EPS de niveau 2 et des techniques de fiabilité dynamique à la validation des guides d'intervention en cas d'accident grave, IRSN, Rapport scientifique et technique, 2007.

[12] E. Raimond, T. Durin, B. Laurent, K. Chevalier-Jabet, Level 2 PSA: a dynamic event tree approach to validate PWR severe accident management guidelines, *Conference PSA2008*, Knoxville, USA, 2008.

[13] E. Raimond, K. Chevalier-Jabet, F. Pichereau, Link between level 2 PSA and off-site emergency preparedness, *Conference PSAM8*, New Orleans, USA, 2006.

[14] E. Raimond, N. Rahni, M. Villermain, Method implemented by the IRSN for the evaluation of uncertainties in level 2 PSA, *Workshop on the evaluation of uncertainties in relation to severe accidents and level 2 PSA*, Cadarache, France, 2005.