SAFETY ASSESSMENT OF ADVANCED REACTOR DESIGNS

Mrs. LAJNEF DORRA  
Tunisian company of electricity and gas  
Rades/Tunis, Tunisia  
Email:lajnef.dorra@gmail.com

Abstract

The safety of the nuclear power plant is an important issue. The role of the safety systems is to ensure the three fundamental safety functions: control of reactivity, removal of heat from the core, confinement of radioactive materials and limitation of accidental releases. The safety has been evolved in the 50-years of nuclear energy history. Regardless the NPP’s size, the efficiency of any safety system depends on the accident against which it is designed to protect. Therefore, to cover a wide range of postulated design-basis-accident, the suppliers have incorporated innovative safety systems that do not depend on the availability of electric power, called passive safety system. In fact, this innovation has marked the generation III reactors because it would be a genuine solution under many accident scenarios. However, passive safety systems are not infallible because it cannot withstand all accidents, eventually, the beyond-design-accidents. In the other hand, the use of advanced models, codes and standards ensure an accurate validation of these safety systems. In light of the introduction of the new concept of small modular reactors, we notice that safety is more and more enhanced due to the design characteristics allowing more efficient control of the radioactive materials and improving the capacity of the NPP to withstand the most severe accident without exceeding certain radiological release limits.

1. INTRODUCTION

The safety of the nuclear power plant is an important issue. The role of the safety systems is to ensure the three fundamental safety functions:
- Control of reactivity.
- Removal of heat from the core.
- Confinement of radioactive materials and limitation of accidental release.

This applies to the three radioactive sources in the NPP which are the core, the fuel storage pool and the radioactive waste treatment systems.

The approach is based on multi-barrier and defence-in-depth concept. It contains several levels of protection, including successive barriers preventing the release of radioactive material to the environment.

2. SAFETY ASSESSMENT OF ADVANCED REACTOR DESIGNS

According to the IAEA the safety function is "The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazard" [1].

2.1. Defence-in-depth and barriers

2.1.1. Defence-in-depth

According to INSAG-12, “the defence in depth concept is a fundamental safety principle that provides an overall strategy for safety measures and features of nuclear power plants. It helps to implement the three fundamental safety functions” [2]. The failure of one or more of these safety functions can lead to an unacceptable risk for the facility, the environment, and a risk of an excessive or unacceptable exposure of workers or populations to radiation. Consequently, two levels of risk are to be considered:
- The potential risks, consisting of the risks incurred in the absence of any protective measures.
- The residual risks that remains in spite of the implementation of the protective measures.
The table below presents the five levels of defence-in-depth-concept.

**TABLE 1. LEVELS OF DEFENCE-IN-DEPTH [3]**

<table>
<thead>
<tr>
<th>Level of defence in depth</th>
<th>Objective</th>
<th>Essential means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Prevention of abnormal operation and failures</td>
<td>Conservative design and high quality in construction and operation</td>
</tr>
<tr>
<td>Level 2</td>
<td>Control of abnormal operation and detection of failures</td>
<td>Conservative design and high quality in construction and operation</td>
</tr>
<tr>
<td>Level 3</td>
<td>Control of accident within the design basis</td>
<td>Engineered safety features and accident procedures</td>
</tr>
<tr>
<td>Level 4</td>
<td>Control of severe of plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents</td>
<td>Complementary measures and accident management.</td>
</tr>
<tr>
<td>Level 5</td>
<td>Control of severe of plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents</td>
<td>Complementary measures and accident management.</td>
</tr>
</tbody>
</table>

2.1.2. *Barriers*

In order to prevent the release of radioactive materials to the environment, designers include many physical barriers. For the pressurized water reactors (PWR), there are three physical barriers as we can see below FIG.1:

- The fuel cladding.
- The primary reactor coolant system used to transfer the heat from the fuel to the steam generator.
- The containment building that plays an important role in the nuclear power plant. It is designed to palliate the radioactive release when both the primary and secondary barriers are lost. It ensures the
protection of the nuclear power plant in the case of the most severe accident. Finally, it ensures the radiation shielding.

The role of the physical barriers is to contain the radioactive materials and protect workers, the population and the environment. The number of the barriers varies from design to design (heavy water reactors or boiled water reactors) depending on designing philosophy.

2.1.3. Redundancy and diversity

First of all, safety isn’t a target, it is a condition. The role of safety systems is to ensure the safe operation of a nuclear power plant. If a design-basis accident occurs (level 3 of defence-in-depth), safety systems are required to ensure the core cooling and to prevent the release of radioactive materials.

Three important concepts should be taken into account in the design of the nuclear power plant:

- Redundancy that means to duplicate safety systems and equipment, as practical as possible, to cope with the single failure criterion and to promote one safety function.
- Diversification that aims to prevent common mode failure. Such failures can be due to a design error, a faulty operating maneuver or an external hazard (fire, flood, etc.). So using diverse systems and mechanisms can help to overcome such events.
- Physical separation of systems fulfilling the same function, in order to reduce the occurrence frequency of simultaneous failure due to an external hazard.

The physical separation of redundant systems and their diversification should be planned at the design stage. Definitely, the redundancy and the diversification enhance the safety of the nuclear power plant. But we cannot duplicate the safety systems indefinitely, because it would have an impact on the cost of the nuclear power plant. Optimally, safety should be ensured by several and different systems without compromising the cost of the facility.

2.2. Safety approach

The safety assessment isn’t an obvious task. In fact, the efficiency of any safety system depends on the accident against which it is designed to protect. And we cannot imagine all the accident scenarios. But, we are aware of the most hazardous event: the radioactivity release in case of core melt accident. There are two different approaches to deal with the safety assessment:

- Deterministic approach which consists on proving that a design is tolerant to a limited number of hazards defined as design-basis accidents, taking into account the most pessimistic scenarios. The analysis is based on credible accidents or not that can lead to the workers exposure to radiation or to environmental contamination. The deterministic approach is based on the defence-in-depth concept. First of all, it is about ensuring the normal operation of the power plant and predict failure mode. Then,
if a fault condition occurs, immediate measures may be taken to avoid severe accident. Finally, it is about considering the worst case scenario and how to limit the radiological risk to population and radioactive release.

- **Probabilistic approach** which is a risk assessment methodology based on a systematic survey of accident scenarios, used to assess the risks associated with nuclear facilities in terms of frequency of dreaded events and their consequences. The probabilistic analysis techniques were emphasized just after three miles accident to supplement conventional safety assessment procedures for nuclear power plants, and to facilitate the determination of acceptable safety levels for nuclear facilities. In the probabilistic approach, a dreaded situation is defined (the core damage, large radioactive release), and an event-tree is established using a list of initiating events (with Annual frequencies) as complete as possible.

Both approaches are intended to maintain the risks associated with nuclear facilities at acceptable levels. The difference between them is methodological. Each approach has its limitations so optimally, the design should be based on the deterministic approach, using the concept of defence-in-depth, and it must be supplemented by the probabilistic approach to analyze external events.

### 2.3. Safety systems

The three major accidents in the history of civil nuclear power (three miles island, Chernobyl, Fukushima) highlighted the importance of nuclear safety.

Active safety systems that rely on operator commands can operate reliably in normal circumstances and in the case of postulates accidents (design basis accidents). But, Fukushima accident emphasize the importance of considering the beyond design basis accident and calls into question the active safety systems limitation.

Passive safety systems, which do not depend on the availability of electric power, would be a genius solution under many accident scenarios, but not all. No safety system is one hundred percent infallible even if it is passive.

As a result, a reliable design should include both active and passive safety systems. This would add to cost but enhance the global safety of the design. The best compromise will probably be an optimal combination of the two types of safety systems.

### 2. SMALL MODULAR REACTORS

Safety is more and more enhanced in light of the introduction of Small Modular Reactors (SMR). This new design presents many characteristics allowing more efficient control of the radioactive materials and improving the capacity of the NPP to withstand the most severe accident without exceeding certain radiological release limits.

According to the IAEA, Small Modular Reactors refer to reactors with an electrical power less than 300 MWe. Lowering the reactor power leads to the reduction of the source term. And this can make the control of the radioactive inventory in the reactor easier.

In the other hand, the small size of these reactors enables the natural convection cooling and then keeping the core at safe temperature in the case of serious accident.

Some vendors propose the underground design that has some safety advantages, for example the optimization of the nuclear site. In fact, in some situation such as earthquake, underground reactor can be a genius solution. However, the design can increase the risk in other situations such as flooding. And the emergency intervention can be more difficult.

Other vendors present integral pressurized water reactor (iPWR). This innovative design is original because it is compact. In fact the reactor pressure vessel contains the main components, notably the steam generators, the control drive mechanisms and the pressurizer.

The fact to incorporate the main structures into one space requires novel layout and this can be a double-edged-sword. Indeed, the potential safety benefit is that the design eliminates the possibility of loss of coolant accident by eliminating the large diameter piping outside the reactor vessel. However, the steam generator is subject to intense radioactivity. As a consequence, some issues, such as corrosion, are affected. This innovative design is like a black box which can make inspection and maintenance more difficult.

Finally, the challenge for the Small Modular Reactor is to reduce size and cost without compromising safety and security.
REFERENCES


BIBLIOGRAPHY

REPORTED BY A GROUP OF EXPERTS, OECD, Paris, Probabilistic safety assessment: an analytical tool for assessing nuclear safety (8, January 1992),
https://www.oecd-nea.org/brief/brief-08.html

ARGONNE NATIONAL LABORATORY, Defence-in-depth (April 2011).
http://www.ne.anl.gov/pdfs/nuclear/defense_in_depth_fanning.pdf

WORLD NUCLEAR ASSOCIATION, Small nuclear power reactors (16 January 2017).


EDWIN LYMAN, Small isn’t always beautiful (September 2013).