C. R. Physique 13 (2012) 359–364

Contents lists available at SciVerse ScienceDirect

Comptes Rendus Physique

www.sciencedirect.com

Science of nuclear safety post-Fukushima

Complementary safety assessments of the French nuclear facilities

Evaluations complémentaires de sûreté du parc nucléaire français

Xavier Pouget-Abadie

Délégué Relations Internationales avec les Autorités de Sûreté, EDF – DIN, Cap Ampère, 1 place Pleyel, 93282 Saint Denis cedex, France

ARTICLE INFO

Article history:
Available online 24 April 2012

Keywords:
Nuclear safety
Fukushima
External natural hazards
Severe accident
EDF
ASN

Mots-clés :
Nuclèaire sûreté
Fukushima
Agressions naturelles
Accident grave
EDF
ASN

ABSTRACT

EDF has conducted, after the Fukushima event, complementary safety assessments of its nuclear facilities. The aim of this in-depth review was to assess the resilience of each plant to extreme external hazards, situations that could lead to severe accident conditions. These analyses demonstrate a good level of safety for all of EDF's nuclear facilities. Supplementary measures post-Fukushima have been put forward to the ASN with the aim of continuing to improve the level of safety at the plants.

Once the ASN position is issued, EDF will develop an action plan over several years, covering both supplementary studies and modifications that have been identified.

RÉSUMÉ

Suite à l'accident de Fukushima, EDF a procédé à des évaluations complémentaires de sûreté pour l'ensemble de son parc de production. Ce réexamen approfondi a consisté à vérifier les marges de sûreté des installations face à des situations d'agressions externes extrêmes pouvant conduire à un accident grave. Ces analyses ont permis de confirmer le bon niveau de sûreté de l'ensemble du parc nucléaire d'EDF. Des mesures complémentaires post-Fukushima ont été proposées à l'ASN pour concourir à élever encore le niveau de sûreté des centrales.

Après l'avis de l'ASN, EDF élaborera un plan d'action sur plusieurs années, comprenant à la fois les études complémentaires et les modifications décidées.

1. Introduction and context

The French nuclear park is made up of standardised reactors using pressurised water technology. This technology, which is widely used internationally, has an intrinsically robust design. Since their commissioning, the plants which make up EDF's nuclear facilities have also been subject to numerous upgrades and modifications designed to improve their level of safety. These upgrades have been carried out in accordance with the principle of continuous safety improvement which has been applied in France since nuclear power plants were first constructed, and is now enshrined in the law of 13 June 2006 in relation to Transparency and Nuclear Safety (TSN), particularly through 10-yearly safety reviews. This continuous improvement of installations' safety level partly relies on feedback from informative national and global events, as well as progress in scientific and technical knowledge generally.

E-mail address: xavier.pouget-abadie@edf.fr.

1631-0705/$ – see front matter
http://dx.doi.org/10.1016/j.crhy.2012.03.003

This continuous improvement in safety requires complete control by the operator, which is directly responsible for safety of plants' design throughout their life cycle. In France, this control is reinforced by the integration within EDF of Research & Development, Engineering and Generation divisions.

The accidents at Three Mile Island in the USA in 1979 and Chernobyl in the Soviet Union in 1986 – the biggest events prior to the Fukushima events in Japan in March 2011 – led operators around the world, and particularly EDF, to carry out major reactor safety improvement programmes. The lessons to be learnt from the Fukushima events will be examined just as closely and will also have a significant industrial impact. The programme of post-Fukushima actions for EDF's nuclear park will include several stages. One of the first stages is defined by the ASN decision of 5 May 2011 which stipulates that EDF should carry out a "complementary safety assessments of its nuclear installations in light of the events which occurred on 11 March 2011 at the Fukushima-Daiichi nuclear plant."

Following this accident and in application of article 8 of the TSN law, on 23 March the ASN was ordered by the Prime Minister to conduct a safety audit of its French nuclear installations in light of events at Fukushima. Almost simultaneously, on 25 March the European Council asked the Commission and all members of ENSREG[1] to define the scope and procedure for stress tests on all nuclear power plants in European Union countries.

The coherency of the two initiatives is ensured by their joint reference to the specifications proposed by WENRA[2] as well as the subsequent organisation of "peer reviews" by ENSREG.

In France, the ASN decision of 5 May 2011 stipulates that, for each site concerned, complementary safety assessments (ECS – Evaluations Complémentaires de Sûreté) should initially be carried out, in accordance with WENRA specifications validated by ENSREG, resulting in a report by the operator presenting the results of the safety assessments of its installations and their resilience to extreme events such as those at Fukushima-Daiichi.

In order to meet the requirements of ECS specifications, EDF very quickly set up a 300-strong full-time project team, representing Generation and Engineering, in order to carry out the assessments within a very short period of time (three months).

On 15 September 2011, following these assessments at 19 EDF nuclear sites, the 19 EDF reports relating to the plants in operation, as well as the PWR under construction at the Flamanville site, were submitted to ASN.

The purpose of this article is to present, firstly, the general approach and methodology followed to produce the complementary safety assessments in light of the Fukushima events and, secondly, the results of these assessments and the actions proposed by EDF at the end of this exercise.

2. Complementary safety assessments: a two-stage approach

The incident which occurred at the Fukushima-Daiichi plant on 11 March 2011 was caused by a violent earthquake (magnitude 9) to the north-east of Japan, followed by a massive tsunami. This triggered a series of events which led to critical situations (core meltdown) on three operational production (units 1 to 3) and finally to significant releases of radioactivity into the environment. It should be remembered, in relation to EDF's complementary safety assessments and based on information available to date, that:

- during the earthquake the plants shut down automatically, but the earthquake caused a total loss of external power supply. The residual heat removal systems started up, since their power was supplied by emergency diesel generators which started successfully;
- the tsunami then caused the loss of the emergency diesel generators and destroyed the pumping stations, depriving the reactors and their spent fuel pool, located in the same building, of its cooling source. Both the causes and the consequences of the Fukushima-Daiichi nuclear accident therefore went far beyond the reactor design basis considered, both in terms of their means of protection against accidental conditions and the management of resulting emergency situations.

So the principle adopted for complementary safety assessments was therefore to examine the robustness of installations beyond the existing dimensioning for protection against these types of unforeseen situations, as well as procedures for managing potential disaster situations under these circumstances.

The audit areas considered are those highlighted by feedback from events at Fukushima-Daiichi, i.e. earthquake, flooding, total loss of power supply and cooling systems and management of severe accidents.

This approach is innovative and ambitious compared with those of the periodic safety reviews carried out during 10-yearly reviews, since in addition to a review of existing dimensioning principles, the review covers installations' robustness well beyond their dimensioning and looks for installations' limitations in relation to threat scenarios such as core meltdown and significant environmental discharge. The complementary safety assessments also examined the previously unexplored hypothesis that the events and situations under consideration affect all reactors at a single site and take place over a long period of time.

[1] European Nuclear Safety Regulators' Group.
[2] Western European Nuclear Regulators' Association.

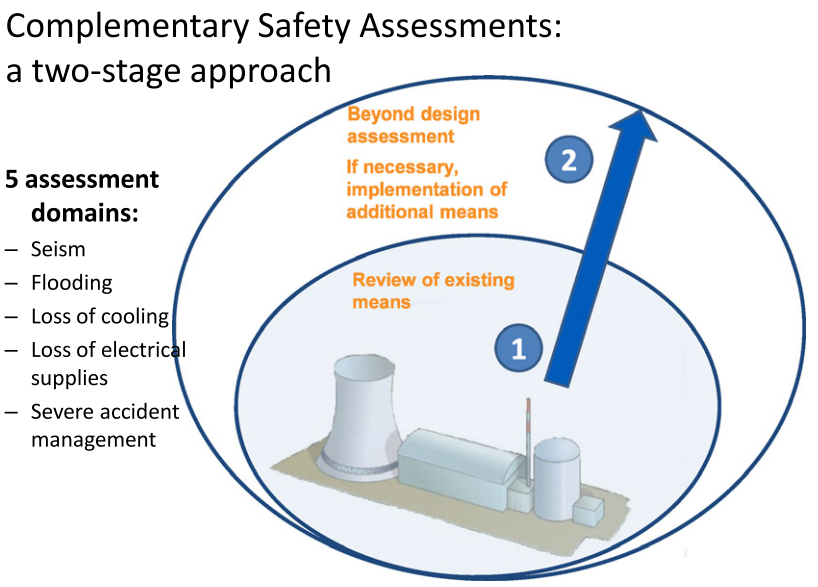

Fig. 1. A two-stage process – see text for further details.

The two stages in the approach selected for complementary safety assessments (see Fig. 1) are:

1. An in-depth re-examination of existing lines of defence, with respect to safety reference baseline and existing regulations, through a re-examination of the protection measures in place and their dimensioning principles, as well as measures for controlling incidents taken into account at the design stage.
   - From this perspective, the most important aspect of an installation's robustness is the validity of its design principles, selected at the outset and re-examined during periodic safety reviews. In the case of the Fukushima-Daiichi, certain analyses carried out by the international community following the 11 March incident raise questions regarding the adequacy of the installations' design and dimensioning principles to withstand stresses which should have been taken into account in light of particular historical events (earthquakes and tsunamis), leading to the first stage of the robustness review which requires verification of the validity of the installations' dimensioning principles.
2. An analysis going beyond the design basis for very implausible situations in order to assess installations' resilience in terms of effectiveness of protection measures beyond their dimensioning and capacity to control extreme situations.
   - In relation to situations beyond this dimensioning, the ASN's specifications require "assuming the successive loss of lines of defence, applying a deterministic approach, independent of the probability of this loss." This approach is unbounded, since it must be independent of the probabilities of occurrence, i.e. independent of the plausibility of both the unforeseen circumstances considered and their consequences on the lines of defence. This apparently leads unavoidably to consideration of events and situations irrespective of how plausible they may be.

The approach's originality lies in the second stage which aims to identify threshold effects[3] in the installation's response as well as possible situations leading to threat scenarios. In general, the threat scenario to prevent in relation to the core is core meltdown (start of severe accident), following the uncovering of fuel assemblies in the spent fuel pool after failure of the core cooling system. If, despite the numerous measures taken, it is still subject to a severe accident, the threat scenario to prevent will be a significant discharge of radioactivity into the environment. The threat scenario to prevent for spent fuel pools is the exposure of fuel assemblies stored in the pool following total failure of the pool cooling system. This is because this type of exposure would not guarantee both functions carried out by the pool water, i.e. radiological protection against radiation from spent assemblies and their cooling.

Application of this approach to external hazards involved increasing the level of the external hazards considered in the reference system by set amounts and analysing installations' response. For example:

- For the earthquake, the acceleration level considered for complementary safety assessments is 1.5 times the level of the Safe Shutdown Earthquake considered for the dimensioning of structures and components;
- For flooding at a riverside site, the water level considered is 1.3 times that of the Augmented Millennial Flood[4] used when dimensioning protection structures.

[3] Sudden change in the installation's behaviour. In the event of flooding, the water level will gradually rise and a tipping point will be reached when the level reaches the top of the sea wall and floods the whole site.

[4] The existing reference system requires a millennial flood augmented by 15% to be taken into account.

Given the timescale available for completing the complementary safety assessments, it was agreed with the ASN that the analyses should be based on existing studies and expert judgements throughout the process involving national reviews theme by theme as well as reviews site by site.

3. Complementary safety assessments results and actions proposed by the operator

3.1. Conformity of installations

The complementary safety assessments do not reveal any significant shortcomings in the definition of external hazards considered (earthquake, flooding, etc.). However, some particular points were identified which should lead to adjustments in the context of the periodic safety reviews in progress. These reviews, particularly taking national and international feedback into account, constitute a comprehensive framework making it possible to permanently assure the safety of reactors with respect to the safety reference system in force. This is particularly the case following revision of earthquake safety requirements following safety reviews and associated modifications to installations (level of earthquake, prevention of damage to earthquake-classified systems by non-classified equipment) or, in relation to flooding, the taking into account of feedback from the storm of 1999 and flooding of the Blayais plant's site.

Each time a point to be re-examined is identified for one or more reactors in the park in respect to the existing safety reference system, in line with EDF's policy in this area, it is characterised and addressed with a certain timeframe depending on its impact on safety. This allows EDF to ensure that each reactor with an issue waiting to be addressed remains under control and with a good level of safety, by implementing provisional compensatory measures where necessary.

The complementary safety assessments reports set out and describe points requiring this type of review for the fleet's various power plants as at 30 June 2011, in relation to the themes of the Fukushima-Daiichi disaster.

In summary, given their initial design, periodic safety reviews carried out on these reactors and measures taken to permanently control points for review in respect of the safety reference system in force, the complementary safety assessments demonstrate that EDF power plants have a robust level of safety in relation to their safety regulations.

3.2. Complementary safety assessments of installations' resilience beyond their dimensioning

The detailed analyses conducted in the complementary safety assessments show that in relation preventive measures to protect installations against the effects of an earthquake and flooding, the current level of robustness also offers a satisfactory margin beyond their dimensioning.

These analyses also demonstrate good robustness of emergency resources in place in the event of total, cumulative loss of power sources and cooling, particularly given the number of lines of defence planned during design and considered to have been lost in a deterministic way in the additional safety audits' worst-case scenarios.

Finally, for extreme serious incidents, these analyses confirm the benefits, in terms structural integrity and therefore protection of the population from radioactive leaks, of the measures taken following the Three Mile Island and Chernobyl accidents.

To be more precise, in the event of extreme situations the safety objective is to remove residual power and confine radioactive material. Possible methods for removing this power include:

- Cooling of the core using the secondary circuit via the steam generators;
- Cooling of the core through evaporation of the water in the primary circuit;
- Control of pressure in the containment (reactor building) through aspersion of water and cooling or, if this method is not available and if the maximum withstand pressure is reached, by opening a depressurisation vent to the outside;
- Cooling of the pools: by cooling the water and, if this method fails, boiling and evaporation of the water.

These kinds of removal means require pumps (either electric pumps or turbopumps powered by steam from the steam generators[5]), water reserves and a means of command and control. All these methods are organised into successive multilayered and redundant lines of defence based on the concept of defence in depth.

In accordance with the specifications, the complementary safety assessments evaluate installations' autonomy in response to the successive and cumulated failure of all these measures, whatever the cause (plausible or not), until total loss of all normal and emergency measures. In the most extreme cases:

- If only one pump remains to supply the steam generators, the timescale before an incident involving core meltdown occurs would be at least a day, approximately, if there was still no means of replenishing the water reserves. In the event of loss of all normal and emergency power supplies,[6] this pump could be the turbopump powered by the steam generators. If no pumps remain to feed the steam generators,[7] in the hypothetical event of simultaneous total loss of

[5] One turbopump per 900 MW reactor, two turbopumps per 1300 MW reactor.

[6] Two main emergency diesel generators per unit, plus one generator (diesel or combustion turbine) per site to power one site unit.

[7] So for the fleet, failure of one or both turbopumps in addition to the loss of all normal and emergency power supplies.

power making it impossible to inject any water into the primary circuit, an accident involving core meltdown would occur within a few hours.
- In this second extreme situation, the containment provided by the reactor building offers between one and three days' autonomy, depending on the disaster scenarios, before significant discharge into the environment. Even after this period of autonomy, the discharges would remain far below those recorded at Fukushima-Daiichi, particularly with very low long-term contamination around the plant. This is because pressure would gradually increase inside the building, which is of a considerable volume. Once maximum pressure is reached in the containment, opening the containment's depressurisation vent would avoid any serious irreversible damage while reducing discharges, since the vent filters out the radioactive discharges which have the longest lifetime.[8] Continuing with the hypothesis that no emergency measures have been put in place, the basemat melt through will occur after several days.
- Meanwhile, recombiners in the containment would prevent any hydrogen deflagration.
- In relation to the fuel building pool, spent fuel assemblies would begin to become uncovered after more than a day if the reactor is at the start of unit shutdown after unloading of the core into this pool, and after several days in other situations.

3.3. Proposed actions to improve installations' resilience beyond their dimensioning

Given their implausibility and the improvements already made to learn lessons from the Three Mile Island and Chernobyl accidents, no attempt has previously been made to identify precautionary measures for situations as extreme as those studied in the complementary safety assessments robustness analyses, which go well beyond the scope of current safety regulations. However, since the complementary safety assessments specifications require their plausibility to be set aside, it is proposed that the following main additional precautionary measures, which are compatible with the levels of autonomy described above, should be studied to address these situations:

- Establishment of new means for replenishing water reserves for feeding the steam generators, the primary circuit or the fuel building pool through the use of autonomous motopumps drawing water from the water table;
- Strengthening of the robustness of turbopumps supplying the steam generators and their command and control, in relation to earthquakes and flooding;
- Establishment of an additional, earthquake- and flood-resistant emergency generator per unit to power a motopump to inject into the steam generator, the primary circuit or the storage pool;
- Establishment at a national level of a national nuclear action force (FARN – Force d'Action Rapide Nucléaire) capable of sending teams to the affected site which are competent in operation, maintenance and logistics, with the primary objective of supporting or even replacing the site operations team in order to re-establish reactor cooling or ensure its long-term reliability, then implement logistical measures applicable to the management of any nuclear crisis of this scale. After 24 hours the team will make it possible to reinject water into the steam generators, the primary circuit or the storage pools using mechanical or electrical "plug and play" connections;
- In relation to control of severe accidents, a study of how to improve the earthquake-robustness of the systems used to filter discharges during containment depressurisation.

Structures, systems and components not covered by the existing reference requirements and which robustness analysis requires to be used in the extreme situations studied, should be subject to requirements to guarantee their availability.

The complementary safety assessments also take into account the conditions under which personnel operate in crisis situations. In particular, concerning short-, medium- and long-term crisis management of the extreme situations considered, the analysis reviews:

- radiological control and protection of operatives;
- operative's living conditions, the physical resources required to manage such crises, particularly the features of security buildings and ancillary buildings;
- information and communication systems and resources.

The resources to associate with these principles still need to be precisely defined after submission of the reports on 15 September 2011. Three aspects will be investigated:

- assuring operability of the site's existing security building in the event of an earthquake. However, even after this action, this existing building would not be suitable for long-term management of a crisis on the scale considered in the additional safety audits;
- studying a nearby crisis management building (advanced command post, as close as possible to units and sufficiently vast and well equipped for long-term management of a site-wide crisis);

[8] Caesium, whose period is 34 years.

– studying a rear base (a few kilometres from the site) to give the national nuclear action force a calm environment for organising the logistics of its intervention (crisis management support base).

4. Conclusions

EDF carried out complementary safety assessments of its installations following the events in Fukushima-Daiichi and in accordance with the ASN decision.

These complementary safety assessments confirmed the current good safety level of these installations.

The new analyses involved analysing, going beyond all previous hypotheses, even for implausible events, the consequences of failure on a scale never previously considered, taking full advantage of available information from Fukushima-Daiichi. The results of these analyses led EDF, as a responsible operator, to propose additional measures.

These additional measures will contribute to even further improving the level of safety of EDF's nuclear power plants. They will be the subject of ASN instructions by the end of 2011, which in particular will set out the timetable for studies and implementation of the changes.