Safety

An evolution laden with risks

"Even a minor accident could be a disaster, because it could question the acceptability of nuclear energy in France, and perhaps in the world."

Bruno Lescœur, Executive Vice President, EDF, biennial general meeting of the World Association of Nuclear Operators (WANO), Berlin, 13-14 October 2003

The nuclear accidents at Three Mile Island (1979) and Chernobyl (1986) have demonstrated the potential for catastrophic events at nuclear power plants. While they had a significant impact in preventing the development of nuclear programmes in a large number of countries, they did not affect the French nuclear industry much. The pioneers of the French nuclear programme had so confidently promised that a major accident could never happen in France that it developed a sense of immunity which partly remains. French nuclear facilities are painted as some of the safest in the world, and the industry carefully sustains the idea that "a Chernobyl-like accident is not possible in France."

What could actually happen is not easy to predict. It is important, first, to note that the technology, organisation and systems of control used in the French nuclear facilities are not really different, taking into account some national specifics, from those in place at least in other western countries. Like anywhere in the world, nuclear accidents are not "impossible" in France, say safety experts, but might rather be "improbable". This fundamental difference opens a whole field of discussion over the likeliness of events, from how they could be assessed to what level of risk is acceptable.

From impossible accidents to acceptable risks and consequences

There has been no catastrophe in the world leading to a large radioactive release with consequences like massive evacuations and land contamination since Chernobyl. There has been no major accident, in the sense of an accidental event in a nuclear facility with immediate, large and serious consequences for workers or populations and the environment, in France. Does that mean that safety has improved worldwide and that it is even better in France?

While any accident proves a safety failure, the contrary is not true. A lack of accidents only indicates that, though potential failures in the safety of nuclear facilities could exist, allowing a tree of events to develop into a major accident, they have not yet occurred in real life. The demonstration of safety relies on a double objective: reaching "acceptable risks" and "tolerable consequences". This is increasingly based on probabilistic safety analysis (PSA), which consists of calculating possible trees of events and their consequences in a given range of probability. This approach provides the reassuring appearance of a very comprehensive and systematic assessment, but is bound to the inherent uncertainty of models as compared to real life.

In short, it is not possible to take into account every single event or combination of events within a certain range of probability (e.g. one chance out of one million per year) so as to exclude any other situation. It seems overconfident to consider a priori the full scope of factors, such as design errors, construction and manufacturing problems, material defects, internal and external events, deficiencies of documentation and voluntary or involuntary violations of rules and procedures. This is particularly true when thinking over the plants' lifetime of tens of years, which brings changes in the internal organisation and external conditions that might not be foreseen, and is also affecting the behaviour of components through ageing in a way that can't be fully predicted.

Moreover, the calculation of consequences relies on assumptions about the response of some components to certain situations that can only be theoretical until the event really happens. This is especially an issue for safety components reserved for the most severe events, such as the melting core management system proposed for the EPR ('corium catcher').

It is therefore important to learn as much as possible from existing events. The numerous incidents that occur in nuclear plants throughout the years without triggering a major accident tend to promote a complacent feeling in the industry that the lessons learnt from Three Mile Island and Chernobyl have improved the level of safety up to really acceptable levels. One can note, however, that the Three Mile Island warning did not prevent the Chernobyl catastrophe from happening. Also, the improvements that actually took place after Chernobyl could not change the design of existing plants, but only involved back-fitting and upgrading of some equipment and the strengthening of procedures and training.

New safety standards and old reactor designs

This is particularly true for the French nuclear power plants, which were decided, designed and constructed in a very standardised way over a very short period of time (see Table 11.) The 42 first units of the LWR programme (36 reactors of 900 MWe and eight reactors of 1,300 MWe), or three-quarters of the currently operating reactors, have been ordered in one decade (between 1970 and 1980) and put in service over the same time (between 1977 and 1987). It took only three more years to order and seven more years to build 12 units of the 1,300 MWe type. Finally, only the realisation of the last four units of 1,450 MWe was stretched out, with orders placed between 1984 and 1993 and start-ups in 2001.

The core of the French reactors programme was thus planned more than 25 years ago, too early for any feedback from the reference accidents of 1979 and 1986 to be deeply integrated in plant design. The Three Mile Island accident, because it happened in a nuclear reactor of the same technology that France used to develop its own power plants, was taken very seriously in France. A group of experts appointed by the Ministry of Industry proposed some reinforcements in the operators' theoretical and practical training, some equipment was reinforced and the rules and procedures were strengthened. The accident is recalled as a shock to the French nuclear industry. As stated by one of the most prominent safety experts of the time, Pierre Tanguy, "weaknesses of the earlier safety approach were revealed" and it "blew the idea" of most people in the nuclear community that a major accident was nearly impossible.[51]

However, it was too late to change the basic design of reactors, as 46 of them were already in operation or at least under construction when the French safety experts drew lessons from Three Mile Island in 1981. Accordingly, the major change introduced instead was the reexamination of emergency planning through the Plans d'urgence internes (PUI) and the Plans particuliers d'intervention (PPI) to include the event of a core meltdown with radioactive release outside of the plant. Similarly, the accident triggered the development of new methods to assess the risk in accidental situations, taking better account of multiple defects and human errors.

[51] P. Tanguy, Director of IPSN, "L'impact de Three Mile Island", in *Les réalités de la sécurité nucléaire après Three Mile Island*, Proceeding of an information meeting, Paris 9-10 June 1981, SFEN, 1981.

Table 11 The French programme of Light Water Reactors (LWR)

Type	Number of units	Power plants (nb units)	Order	Grid connexion	Industrial start-up
REP 900 / CP0	6	Bugey (4) Fessenheim (2)	1970 – 1974	April 1977 to July 1979	Dec 1977 to Jan 1980
REP 900 / CP1	18	Blayais (4) Dampierre (4) Gravelines (6) Tricastin (4)	1974 – 1980	March 1980 to Aug 1985	Sept 1980 to Oct 1985
REP 900 / CP2	10	Chinon (4) Cruas (4) Saint-Laurent (2)	1975 – 1980	Jan. 1981 to Nov 1987	Aug 1983 to April 1988
REP 1,300 / P4	8	Flamanville (2) Paluel (4) Saint-Alban (2)	1975 – 1980	June 1984 to July 1986	Dec 1985 to March 1987
REP 1,300 / P'4	12	Belleville (2) Cattenom (4) Golfech (2) Nogent (2) Penly (2)	1980 – 1983	Nov 1986 to June 1993	April 1987 to March 1994
REP 1,450 / N4	4	Chooz (2) Civaux (2)	1984 – 1993	Aug 1996 to Dec 1999	Jan 2001 to Dec 2001
EPR (1,600)	1	Flamanville (1)	2007	—	—

Source: based on CEA, *Elecnuc*

Having worked heavily on learning the lessons from Three Mile Island, the worldwide nuclear industry responded very defensively to the Chernobyl disaster, by pointing out that it was a "Soviet accident" waiting to happen due to specific defects in technology and organisation, and outrageously downplaying the human and environmental consequences. The French authorities were the most defensive, up to the point of denying any impact from the large radioactive cloud that flew over Europe on French territory (thus refusing to take any measures regarding the consumption of food or water, etc.), an attitude remembered in the collective consciousness as the false statement that "the cloud had not passed the French border."

Yet the accident weighted the evolution of safety requirements to be imposed on new reactors, at French as well as international level. As soon as the early 1990s, only two orders of the last series of French reactors – the N4 type of 1,450 MWe – had been completed when official safety experts already saw them as outdated. A director of IPSN (now IRSN) noted that "the conception of the N4 units […] dates back to the first half of the 1980s […]. Today, it appears to all concerned players that a significant improvement in the safety of future units is needed, as compared to those currently in operation."[52] As recalled in parliamentary hearings in the early 2000s, the French nuclear safety authority (now ASN) stated as early as 1995 that it would not be acceptable any more to build N4 reactors, as the reference safety requirements had evolved, in the sense of higher exigencies, since their conception in the early 1980s.[53] The need for a higher standard of safety was the reason for developing a new design, leading to the EPR project developed with Germany.

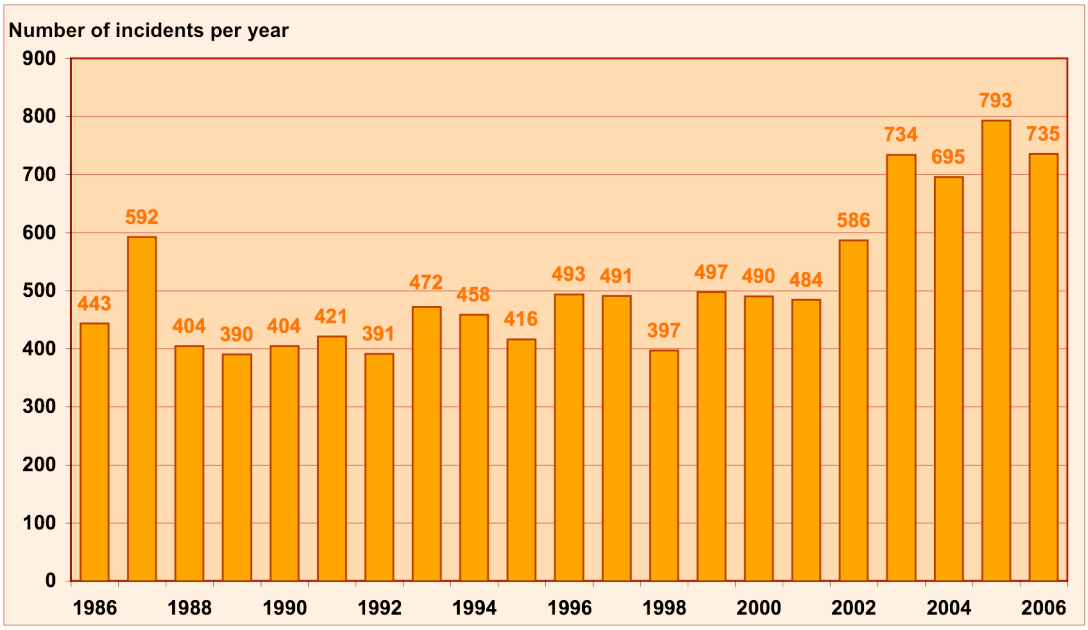
[52] D. Quéniart, Director for safety of IPSN, "La sûreté dans les années 1990", *Revue Générale Nucléaire*, n°5, Sept-Oct 1991.

[53] Ch. Bataille, C. Birraux, *La durée de vie des centrales nucléaires et les nouveaux types de réacteurs*, May 2003, OPECST, from the hearing of B. Dupraz, Director of the Energy division, EDF, on19 December 2002.

Distorsion in the public account of safety events

Yet the same reactors that would not be constructed now because they are seen as insufficiently safe are said to operate with an acceptable level of safety. This view is largely based on the statistics of events that are considered relevant for safety by operators and the authorities. The operators of 200 nuclear facilities in France declare a very large number of events every year, with EDF alone declaring between 10,000 to 12,000 of them,[54] of which 700 to 800 are considered "incidents" or "significant events" (see Figure 12.) These are regularly analysed by IRSN and then discussed in internal meetings with EDF and ASN to prepare their classification and draw lessons for the prevention of operational risks.

Figure 12 Significant incidents in French nuclear power reactors, 1986-2006



Source: *Residual Risk*, 2007, based on IRSN

The database of these events and their analysis is not publicly available. According to a report citing the director of the nuclear safety department of IRSN,[55] approximately 200 events are considered "outstanding" every year (244 in 2006), and 100 are retained in the framework of national feedback. On average, around 20 events each year are seen as precursors, in the sense that they put into jeopardy several lines of defense and could have led under other circumstances to a serious accident. Finally, between two and three events usually undergo a detailed in-depth analysis by IRSN.

Unfortunately, there is no indication given about the existing link between this statistical analysis and the classification of events using the International Nuclear Events Scale (INES) regularly published by the ASN (see Figure 13.) The number of events recorded on the INES scale in France through the years shows very important variations which found no technical explanation. It is difficult to find trends in these statistics. According to an analysis presented in the ASN annual report for 2005, a remarkable one is that the more recent plants (by technology and by operational age) encounter more incidents than the older ones, with an average of 10 incidents per 900 MWe per year, increasing to 12 per 1,300 MWe per year and 13 per 1,450 MWe per year.

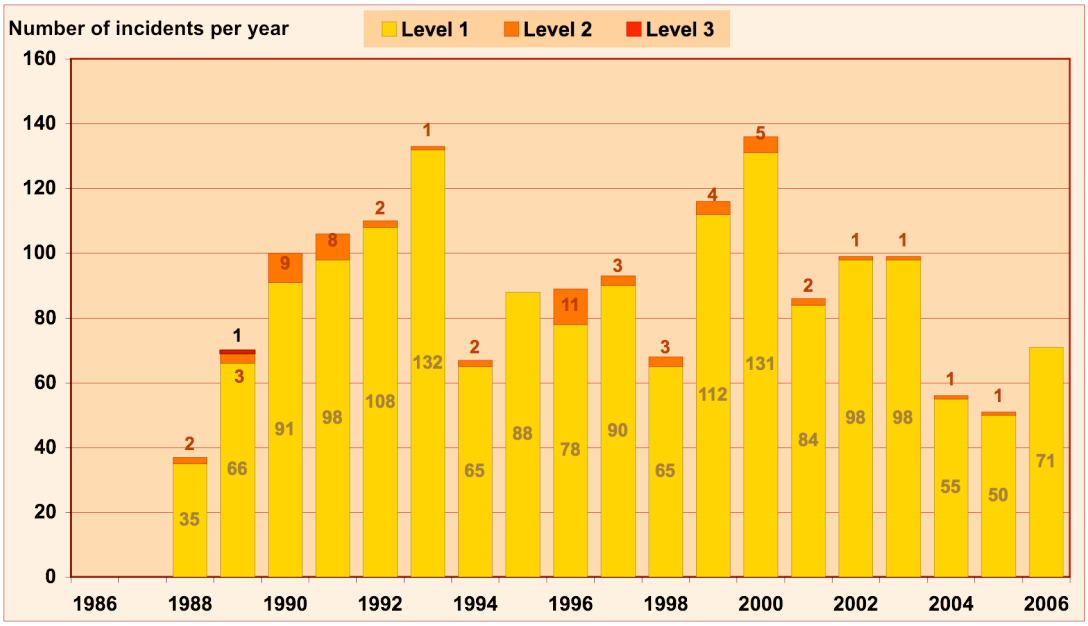
[54] Although a large majority of them are related to safety, it must be noted that these include safety, radiation protection and environmental protection events (respectively 73.7%, 22.2% and 4.1% for the year 2005).

[55] M. Schneider (Dir.), *Residual Risk – An Account of Events in Nuclear Power Plants Since the Chernobyl Accident in 1986*, May 2007.

A cumulative 10,786 significant events have been declared in French nuclear power plants between 1986 and 2006, of which 1,615 were rated INES Level 1 and 59 Level 2. Only one event was rated Level 3. The ASN reported 764 events declared by EDF for 2007, of which 56 were rated at Level 1, and none at higher level. In addition, between 50 and 200 events are reported each year for fuel chain facilities, other nuclear facilities and transports.

The problem with the INES scale is that it tends to distort the reporting and classification of events as compared to their real importance in terms of safety. While the number of reported events almost doubled between 1998 and 2005, the number of events rated 1 or more on the INES scale went down from 136 in 2000 to 51 in 2005… In other words, there is a trend of a steady increase in the number of events (from 7.1 per reactor per year in 2000 to 10.8 in 2007), but the number of those which seem important using INES criteria is decreasing.

Figure 13 INES rated incidents in French nuclear power reactors, 1986-2006



Source: *Residual Risk*, 2007, based on IRSN

The International Atomic Energy Agency (IAEA)'s INES defines events as "deviations" (Level 0), "anomalies" (Level 1), "incidents" (Level 2) "serious incidents" or "near accidents" (Level 3) and "accidents" (Levels 4 to 7). The criteria used to rate safety events on the INES scale are complex but mostly based on the potential for immediate radiological consequences to workers, the public or the environment rather than the measurement of how close the given situation came to very serious damage or the weaknesses in the safety system that could be pointed even by minor events.

As a consequence, some events that were close to developing into serious accidents but did not thanks to one hazardous factor – or some events that might be taken as early warnings or as precursors of serious incidents – are given a low level on the scale compared to other events with minor implications in terms of flaws in the lines of defence but immediate consequences. Accordingly, a negative side-effect of the INES rating might be that operators tend to feel relief when an incident closes without immediate consequences rather than concern about the fact that a 'near-miss' situation could have developed.

The Forsmark incident, which happened in Sweden in July 2006, illustrated the potential significance of such a 'near-miss' scenario, although there were no direct radiological consequences. After a short circuit in an outdoor switching station of the grid near the nuclear power plant had caused the emergency shutdown of the reactor, a complex set of events led to subsequent failures. The incident

clearly revealed a weakness in the plant's design and, according to some experts, the reactor was just a few minutes away from a Chernobyl-scale scenario.

Only one "accident" in the sense of the INES scale was ever registered in France. On 13 March 1980, on the gas-cooled unit of Saint-Laurent-A2, a local defect of the cooling system due to the fatigue of some components inside the reactor vessel led to the total fusion of two fuel elements and the partial fusion of two others. Even incidents rated at Level 3 are very rare. One is the fire in radioactive waste (bituminised sludge from reprocessing) at La Hague storage facilities in 1981.

Another serious incident took place in Bugey on 14 April 1984 that would probably be rated Level 3 today, but was not at the time. A defect in the design of electric cables linked to the control-command system led to their failure, causing a complete blackout of unit 4 of the plant. The safe shutdown of the plant absolutely required the use of alternate electricity sources provided by two diesel engines, of which the first one could not be started when needed – leaving the second backup engine as the last and only safety line before a fusion of the core. On 16 August 1989, another incident was rated at Level 3 in Gravelines-1, when it was found that the reactor had been operated for about one year with inappropriate screws, causing a severe degradation of the protection system against overpressure of the primary circuit.

Worrying lessons from a whole range of incidents

The authors of the *Residual Risk* report obtained in 2007 from IRSN a commented selection of the most significant incidents for safety on French nuclear reactors between 1986 and 2006 which shows how much this criteria might differ from the INES scale: eight of the 18 incidents selected by IRSN were only rated Level 1 on the INES scale, and one was not even rated.

The selection shows how various factors can affect the safety of French nuclear facilities, as the 18 incidents cover the whole range of root causes: from design errors and defective components to inappropriate procedures and human errors.

Some incidents illustrate the potential weakness of the probabilistic approach, as in the case of the Blayais-2 incident of 1999. The unexpected strength of the storm that struck France on 27 December 1999 was such that it led to a combination of two critical conditions: a centennial flooding of the plant and the loss of the external electric grid. This led to an emergency shutdown while some key safety equipments (injection pumps, containment spray systems…) were unable to work, and any human intervention was perilous because of storm conditions. Each of the events had been separately considered to fall within the range of probabilities to take into account, but not their simultaneous realisation. Also, the incident led to a reassessment of flood protection provision at all sites, which concluded there was a need for higher maximum flood design levels and better protection at the Belleville, Bugey and Chooz nuclear power plant sites.

This highlights the difficulty of predicting at the time of conception of a reactor the whole range of probability of internal and external events that could happen throughout its entire life. The probability of severe climatic events, in particular, must be reassessed, taking into account the local impact of ongoing climate change. An improvement in methods of assessing seismic hazard has also led to some reassessment of the major seismic events to be considered at some sites, which in turn has triggered a reassessment of how key equipment withstands stress. This applies to EDF reactors that undergo a large programme of back-fitting, and also to other facilities, particularly the oldest ones, built under very lax anti-seismic requirements. The MOX fuel fabrication plant of ATPu, in Cadarache – on the seismic fault of Durance – was eventually closed in 2003 following years of pressure by ASN because of its insufficient anti-seismic design.

These selected incidents also illustrate how the high level of standardisation of EDF reactors can lead to generic failures, some of the events affecting all 58 reactors in operation. The most serious was probably the problem of sump clogging, a phenomenon that could strongly affect the recirculation of primary cooling water needed in the case of a large loss of coolant accident. The problem, already known on foreign reactors with similar designs as early as the beginning of the 1990s, was acknowledged to affect all 34 units of the 900 MWe series as of December 2003.

Generic faults were still found on EDF reactors in 2007. On 26 February 2007, the ASN issued a note concerning all 58 reactors, after it was found that error margins had not been taken into account during periodic tests of key safety devices – while with the margin of error some tests might have been counted as having failed. This incident received a Level 1 INES rating.

Also in 2007, a very serious problem appeared with an extensive plugging of tube sheet penetrations, affecting a large number of reactors. The phenomenon could affect up to 80 percent of the tubes of concerned reactors and is estimated to increase by five percent per year. The problem will have serious economic consequences as it reduces the power output of the generator, and it raises safety concerns because it increases the sensitivity of the tubes to vibratory fatigue and can lead to tube cracking, as already happened at the Cruas power plant. In addition, in February 2008, following a problem of tube leak in Fessenheim-2, the ASN requested EDF to proceed before September 2008 with the plugging of all steam generator tubes in all reactors affected by a generic fabrication defect of anti-vibratory supports – the number of reactors and tubes has not been made public.

Although the French nuclear facilities enjoy a good record of a very low number of accidents or serious incidents as rated on the INES scale, an analysis of the increasing number of events seen as significant for safety, some of them close to really severe situations, points to an increasing risk of catastrophe. The time is long gone when French official safety experts could pretend that the risk of a major accident was so low that it could be ignored. The rising number of issues with key equipment in the 58 reactors, and the increase in potential events needing to be considered sheds a worrying light on the real level of safety in the French nuclear industry.