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.

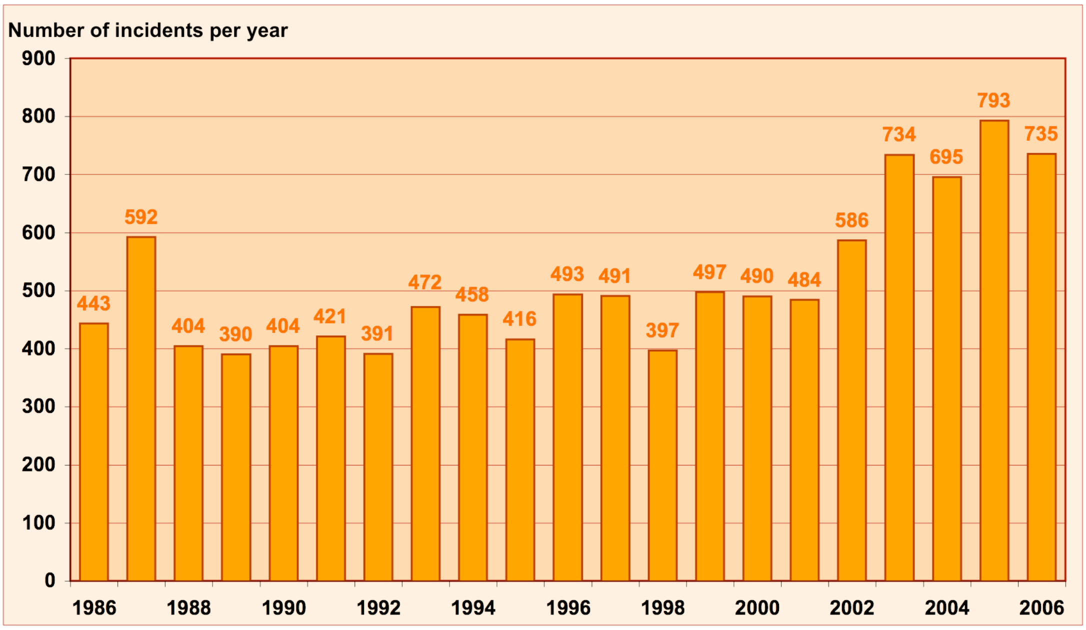
52 D. Quéniart, Director for safety of IPSN, "La sûreté dans les années 1990", *Revue Générale Nucléaire*, n°5, Sept-Oct 1991.

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.

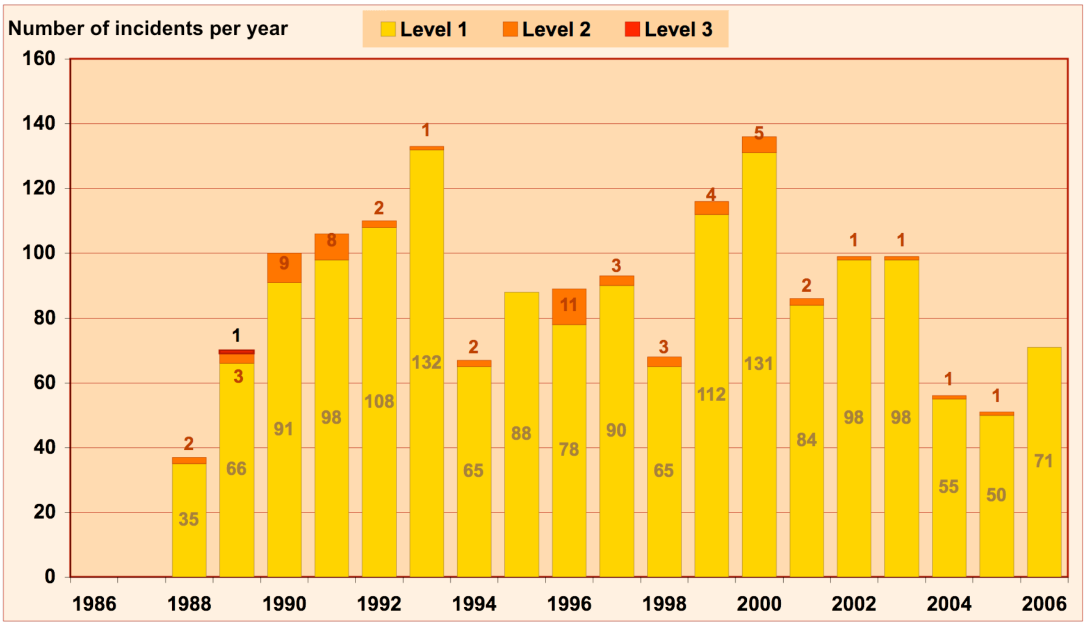
[54] Although a large majority of them are related to safety, it must be noted that these include safety, radiation protection and environmental protection events (respectively 73.7%, 22.2% and 4.1% for the year 2005).

[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.

Focus 06 1986-2006: twenty years of significant incidents in France

Although not much publicised because of their low rate on the INES scale – based on immediate radiological risk rather than intrinsic safety criteria – many significant events occur in nuclear reactors and fuel-chain facilities that show serious flaws of design, quality, procedures and systems, with the potential to trigger a dramatic event. France is no exception to that rule. The 2007 *Residual Risk* report, by an international team of independent experts, obtained from IRSN a selection of some of the most significant of those near-miss and precursor incidents in France for the period 1986-2006. Below is the summary by the report authors of these 18 selected events, presented in chronological order:

■ **12 January 1987, Chinon-B3** (not rated on INES scale). The particularly cold conditions during the winter 1986-87 led to the freezing of several materials and systems significant for the safety of the unit, in particular at the level of feed water intake from the Loire river.

■ **16 August 1989, Gravelines-1** (INES Level 3). The mounting of an inappropriate type of screws onto pressure relief valves on the primary circuit would have rendered the overpressure protection system inefficient. The valves would have opened and closed significantly later than under design basis conditions. The operators did not agree to the Level 3 rating and initiated, in vain, a procedure to get it downgraded to Level 2.

■ **30 October 1990, Cruas-4** (INES Level 1). The explosion of a 6.6 kV commutator caused a fire that entailed the loss of one of the two electrical safety circuits. The destruction of the commutator was caused by the degradation of elastic washers due to the exposure to heat. Subsequently, the second line was found to be affected in the same way.

■ **23 September 1991, Bugey-3** (INES Level 2). A leak was identified during the decennial primary circuit pressure test on the support of the control rod drive mechanisms that was going through the reactor vessel head.

■ **29 January 1994, Bugey-5** (INES Level 2). The reactor was shut down and the primary coolant level was decreased to working level in order to carry out some maintenance operations. The water flow level at the primary pumps and the motor intensity fluctuated for eight hours without any operator intervention. The technical specifications explicitly require close supervision of these parameters under these operational conditions because fluctuation can indicate the degradation of the primary pumps leading to their potential loss and thus the risk of core degradation. The safety authorities identified "significant malfunctioning": the manual was erroneous, the operators had not received any specific training for this "particularly delicate" operation, the situation has been considered falsely as "normal and safe", the visit of the safety engineer in the control room did not lead to any corrective action.66 The event had originally been given an INES 1 rating.

■ **12 May 1998, Civaux-1** (INES Level 2). While the unit was shut down, a 25 cm diameter pipe cracked open due to thermal fatigue and a large leak (30 m3 per hour) occurred in the primary cooling circuit. It took 10 hours to isolate the leak. An 18 cm long crack was on a weld was identified. The unit, which is one of the four most modern French reactors (N4, 1500 MW), had been operating only for six months.

■ **10 June 1999, Tricastin, then identified on all 58 EDF units** (INES Level 1). Polyamide cages, non-qualified for accidental situations, instead of metal cages have been built onto ball bearings of coolant safety injection pumps. First identified at the Tricastin site, the problem turned out to be spread over all of EDF's nuclear power plants.

■ **11 March 1999, Tricastin-1** (INES Level 1). Following a series of organizational and human errors, a technician has penetrated into a protected, highly radioactive area of the reactor (red zone) and has received a dose of about 340 mSv (17 times the current legal limit for worker exposure).

■ **27 December 1999, Blayais-2** (INES Level 2). The unusual storms at the end of 1999 led to the flooding of the Blayais nuclear power plant site. Certain key safety equipments of the plant were flooded, for example the safety injection pumps and the containment spray system of units 1 and 2. The electrical system was also affected. For the first time, the national level of the internal emergency plan (PUI) was triggered.

■ **2 April 2001, Dampierre-4** (INES Level 2). Following human and organizational errors, the correct core loading scheme has not been implemented. The situation could have led to a criticality risk.

■ **21 January 2002, Flamanville-2** (INES Level 2). The installation of inappropriate condensers due to an inappropriate procedure led to the simultaneous loss of several control-command boards and systems while the unit was operating as well as to the destruction of two safety significant pumps during the shut down sequence.

■ **24 December 2003, all 900 MW reactors** (INES Level 2). The misconception of the reactor sump filters induced the potential risk of debris blocking the cooling function in case of the need for recirculation under post-accident conditions. The problem has been subsequently identified not only in all of the French 900 MW reactors but also in many other plants around the world.

■ **24 January 2004, Fessenheim-1** (INES Level 1). Following the erroneous operation of an auxiliary circuit valve, ion exchange resins68 have been introduced into the primary cooling circuit. Their presence could have threatened the integrity of the primary pump joints as well as the proper functioning of the control rods. Both elements are essential to control and shut down the reactor.

■ **22 March 2004, all 58 EDF reactors** (INES Level 2). An insulation default at an electrical switchboard, experienced on unit 2 of the Penly nuclear power plant, was triggered by a steam leak close to electrical equipment that was to be qualified to resist accidental conditions. The non-conformity of the cabling has been subsequently identified on all of the French nuclear power plants and led to large-scale verification and remediation operations.

■ **16 May 2005, Cattenom-2** (INES Level 1). The sub-standard of the secondary coolant pump power supply cabling led to a fire in the electricity funnel. As a consequence one of the two safety circuits had to be disconnected. The operator EDF triggered its local (Level 1) internal emergency plan (PUI) The technical emergency center (CTC) has been activated for a few hours. The nuclear safety authorities issued a nine-line press release. Details of the event have never been published.

■ **7 April 2005, Gravelines-3** (INES Level 1). During the year 2006 the operator has noticed the presence of provisional pieces of equipment on both of the reactor protection control command lines. These pieces were applied during the previous reactor outage and had been left there by mistake. Under accidental conditions certain automatic sequences would not have taken place in a normal way.

■ **30 September 2005, Nogent-1** (INES Level 1). A certain number of material failures added to a human error during the restart of the reactor led to the hot water and steam penetrating the four rooms containing the control command boards of the reactor protection system. Under normal conditions these rooms are independent from each other and should never be put in danger simultaneously. In the case of an accident, this incident could have made it difficult for the operator to bring back the reactor into safe state. EDF has activated its internal emergency plan and the nuclear safety authority ASN activated its national emergency organisation for a few hours. ASN issued a 10-line press release.

■ **21 December 2005, Chinon-B, four units** (INES Level 1). An ill-conceived surveillance of the tertiary cooling water intake canal led to its significant silting up. The collapse of the sand hill could have led to the heat sink loss of all four reactors.

Focus 07 The EPR, supposed improvements versus new vulnerabilities

"The design of EPR ensures the high level of safety that is required worldwide for the future nuclear power plants."

Areva, *EPR, un choix stratégique*, brochure,February 2004

Lessons from Three Mile Island and Chernobyl came too late to bring in-depth modification of the design of the 58 reactors currently operated by EDF. Although they consider them as safe as was required at the time of their conception, the operator as well as the authority have recognised for more than ten years that these reactors would fail to meet current safety standards applied to new reactors.

From the mid-1990s, the French nuclear industry developed, together with the German and then alone, the EPR design as a response. This reactor builds upon the designs of the latest French and German concepts, respectively N4 and Konvoi, and seeks to reinforce their safety by adding supplementary and redundant features instead of deeply reviewing the designs. This approach has been qualified as "evolutionary", as opposed to more "revolutionary" reactor concepts developed in other countries – and the EPR might be the less innovative amongst new "evolutionary" designs like the US reactor AP-1000, which has developed more passive safety features.

The reinforcements of the EPR design, as compared to its predecessor N4, mostly consist of an increased thickness of containment, a multiplication and improvement of the backup system, or the adding of water in the primary circuit, as well as improvements in the operational procedures and automation of control and command. All of these tend to reduce the probability of a scenario leading to a core fusion. The overall goal is to reduce such probability by a factor of ten, from a "guaranteed" level of one chance out of one million per reactor per year for existing plants to one chance out of ten million. Nevertheless, as if to acknowledge that even this reduction of the probability remains hazardous, the main innovation of the EPR is a "core catcher" designed to receive and let cool down the melted corium in case of a major accident, with the aim of preventing any large radioactive release outside the plant in such a scenario.

The EPR design is therefore based on the same principle that accidental events can be fully projected in probabilistic trees, an assumption even more problematic given the planned lifetime of 60 years for new-built EPRs.[56] Also, the complexity of the safety systems involved makes their assessment subject to high uncertainty, as they cannot be fully tested except in the unfortunate case of a real accident.[57] Some key elements of the EPR safety case, like the efficiency of the core catcher, the prevention of hydrogen explosions in case of a core fusion, or the behaviour of the automated system of control-command, remain prone to controversy. Also, the level of performance intended for the reactor raises some new safety issues. In particular, the behaviour of fuel elements that would reach the very high burn-ups targeted could not be fully guaranteed with existing technologies.

Finally, it should be noted that the safety of a reactor is also that of the whole fuel-chain that it needs, the overall level of safety being that of the weakest part of the system. The EPR brings no improvement as it will rely on the same front-end and back-end technologies as existing reactors. On the contrary, the higher fuel performances that it aims for will induce new safety and radiation protection problems at all stages of fuel management.

Altogether, the ten-fold reduction in probability of a major accident in the reactor appears neither sufficiently assessed given the uncertainty regarding key features, nor sufficiently comprehensive in view of the limits of the probabilistic approach on one hand, and the need to consider the safety of the full system on the other hand. As compared to the potential field of innovative safety systems, one can doubt that the EPR design fits the evolution of safety requirements in a century – the time scale that would separate the shutdown of an EPR started-up in 2020 from the 1980s conception of the N4 reactor which it is based upon.

[56] The probabilistic approach also fails to cover the scope of malevolent acts that could reasonably, after 9/11, lead to thermal and/or mechanical loads superior to those arising from accidental situations.

[57] For instance, the resistance of the containment to the high pressure of an accident could be tested, but not coupled with the high temperature that would go with such pressure.

Focus 08 Is France prepared for a major accident?

France has chosen nuclear weapons and nuclear electricity generation, and has maintained that choice. As a result, France's territory contains over 35 nuclear sites[58] and is criss-crossed all year long by numerous consignments of radioactive material being transported by rail or road.

Safety and security systems invariably have limitations. So one question remains, which we could put like this: "What if there was an accident?" Though the authorities have long considered this question at best preposterous, at worst seditious, nonetheless we believe that it is worthy of attention. Indeed, one is entitled to believe that a country that opts for nuclear has a duty to adopt appropriate emergency and public security measures. Since the chance of a major accident occurring is not zero, one must be prepared for it. So, what do the authorities have to say on the subject?

The official plan is explained on the website of the Autorité de Sûreté Nucléaire (the French Nuclear Safety Authority) – www.asn.fr. Unfortunately, this does not appear very up-to-date, as the institutional changes which gave rise to the ASN in 2006 are not taken into account. The key measures and above all the 'doctrine' for the management of a crisis have barely evolved at all.

According to the plan, if a major event occurs, the operator is to alert the prefect of the *département* concerned and the ASN. The ASN will evaluate the situation and "advise" the prefect, who will take the decisions. He or she is the keystone of the plan.

The population, once alerted by a special siren, is supposed to follow these rules: take shelter (there is no longer any mention of containment), listen to the radio, do not use the telephone too much, leave the children at school and await instructions. The prefect, meanwhile, activates the Plan Particulier d'Intervention (PPI, specific intervention plan) for the nuclear site concerned. Of course, this PPI is supposed to have been prepared in advance and updated at least every five years. Simulations are sometimes carried out in order to test the arrangements.

From theory to practice…

The management of a nuclear crisis thus relies essentially on advance preparation, flagging up of the actions to be undertaken by the various actors, and prior information. However, the doctrine has many intrinsic weaknesses; in particular it is a long way from reality.

The 10km rule. PPIs are drawn up on the basis of a zone within a 10km radius of the nuclear installation. The ASN explains that this limit was set on the basis of a range of accident scenarios, and that beyond the 10km limit the authorities would be able to organise a second line of response when needed. However, the few accident scenarios published by independent experts call this rule into question. Weather conditions are a major factor in the speed of dispersal of radioactivity. The least that should be done is probably to take account of the geographical locality and observed weather patterns.

Preparing the inhabitants. People living within the aforementioned 10km limit should normally all have received a leaflet telling them what to do in case of an alert: shelter indoors, do not flee, do not go to pick up one's children, listen to the radio in order to hear instructions. Depending on the *département*, leaflets are distributed more or less regularly and new arrivals are thus not necessarily informed. In the case of tourists, visitors etc, it is up to their hosts to convey the information – which does not generally take place. The PPI is a public document, theoretically available at the prefecture to citizens who want it. Those who have tried to obtain a copy can bear witness to the difficulties encountered.

Warning sirens. Each nuclear site is equipped with sirens to warn of accidents. The inhabitants are supposed to recognise the signal and act accordingly. However, during simulations organised by the

[58] Counting only the principal sites. In particular, France has 58 pressurised water reactors on 19 sites, several nuclear research centres comprising numerous industrial and research installations, plants such as La Hague, and waste storage centres. The total count runs to over 200 installations.

authorities, it is regularly noted that the sirens are not audible far enough away and do not really cause any reaction.

The Flamanville PPI

The 1998 Flamanville PPI (which was the one available to the public in 2007 – it should normally be revised every five years) offers a good illustration of the difference between doctrine and operational reality. A PPI describes the area, the number of inhabitants, the factories, schools etc, and lists the available means for potential evacuations, the roads to be used or to be blocked, the assistance that can be mobilised, the reception centres and so on.

Quite apart from the generally outdated nature of this PPI, however, the bizarre approximations that it contains are astonishing. For example, the tourist coach companies are duly listed along with the number of vehicles they possess – all assumed to be available. But at any normal time, of course, the coaches are not in the garage awaiting the alert with a driver alongside. Moreover, a few discussions with the employees concerned make it clear that they do not consider themselves to be 'requisitionable' and that their first instinct would be to go to fetch their families.

Again, people seriously contaminated as a result of an accident are supposed to be transported to Cherbourg hospital, which has a specialist unit – with only a few beds. For a *département* which includes a nuclear power station and the plant at La Hague, this is clearly inadequate. Moreover, the PPI does not mention which personnel will be sent on site like the 'liquidators' at Chernobyl. Would it be the fire service? The army?

What about iodine tablets?

Everybody has heard of the need to take iodine tablets in the event of a nuclear accident where radioactivity has been dispersed. The taking of stable iodine, to saturate the thyroid gland and prevent it from fixing the highly volatile radioactive iodine (iodine 131) released during an accident, is one of the measures used to protect populations. But this policy has some limitations:

- Firstly, only residents of the 10km zone around sites are supposed to keep iodine at home.
- Stocks of iodine tablets are obtainable from pharmacies but will only be distributed on the order of the authorities. It is easy to imagine the resultant panic and the queues at dispensaries. We can only hope that an accident will not be so ill-mannered as to happen in August.
- People will probably have difficulty taking the pills at the right time, and in the correct dosage, although these are important parameters and an overdose can be harmful.
- Finally, and above all, iodine merely protects the thyroid from iodine 131 – and if there is an accident many other radioactive elements will be released into the environment.

Post-accident management

After a major accident, and the implementation of the first emergency measures, comes the post-accident period, with the need for radiation protection and public health measures, bans on food or water consumption, evacuations, decontamination and so on. On this topic, the special dossier in the ASN journal *Contrôle*, published July 2008 (issue 180), makes interesting reading.

The editorial by the Director-General of the ASN is crystal clear: "In order to carry out the mission entrusted to it on the instructions of the Prime Minister in June 2005, the ASN has established the steering committee (CODIRPA) to manage the post-accident phase of a nuclear or radiological accident. […] This committee has the mission of developing a national doctrine on this subject – a doctrine which is still lacking not only in France, but also in most countries with nuclear energy."

One could go on adding examples and illustrations showing that in France today too little account is taken of the possibility of a major accident to enable serious preparation. It is of course a complex and costly undertaking to be permanently ready for a situation considered to be very unlikely. But the discussion about our country's level of preparation must take place, because 'improbable' is not synonymous with 'impossible'.

Focus 09 Growing safety concerns in the fuel chain

The incidents at Tricastin and Romans-sur-Isère in July 2008, involving uranium spilling into the environment at nuclear facilities related to uranium conversion and enrichment and fuel fabrication, showed that nuclear safety is not only about nuclear power plants.

The risk of major accident in case of core fusion is specific to nuclear reactors. This scenario is seen as the most extreme, in terms of potential damage, that could happen on nuclear facilities. As such, it focuses most of the attention paid to safety in terms of R&D programmes, regulations, safety studies, etc. In France, after nuclear facilities had been operating for more than ten years, the plan to develop nuclear reactors to produce electricity led to the first regulations specific to nuclear activities, a 1963 decree that defined the status of "nuclear basic installation" (installation nucléaire de base, INB) and introduced a framework centred on the control of the risk of criticality.[59] The basic safety requirements, defined by orders called "fundamental safety rules" (règles fondamentales de sûreté, RFS) dealing with various issues, were introduced much later for other nuclear facilities than nuclear reactors. The RFS relating to the approach for considering the risk of plane crashing, for instance, was introduced in 1980 for reactors, and only in 1992 for other facilities. The same delay applied to other issues such as seismic risk. The MOX fuel fabrication unit ATPu, which was eventually shut down in Cadarache due to unsufficient seismic design, is only one of many facilities that were built up to the mid-1980s without sufficient regulation on that point.

In addition, the high level of variety of nuclear facilities other than power plants, as opposed to the standardisation of EDF reactors, makes it even more complicated to develop a thorough assessment and control of all relevant risks in all facilities.

When WISE-Paris published, in the aftermath of 9/11, estimates on the risk of radioactive releases "up to 67 times the equivalent of Chernobyl"[60] at La Hague reprocessing plants in the case of a plane crashing on one spent fuel storage pond, it seemed like this was a brand new issue. One of the immediate answers from Areva was that this was absurd, as "there is no risk of chain reaction in such a facility, unlike in reactors"… The assessment was based on US safety authority NRC's calculations that 50 to 100% of fuel rods could catch fire from their own thermal output if the pool was emptied, as could happen in the case of a plane crash or other events (explosion, seism, etc.). Commissioned by the Ministry of Industry to analyse the issue, the IRSN concluded that "only" 10% of the fuel inventory might burn, which still meant a release six times larger than the Chernobyl accident! The inventory of radioactive materials at La Hague, where all spent fuel from EDF reactors, and high and intermediated level waste arising from their reprocessing is stored, is such that the potential for radioactive release in case of an accident might exceed that of a single reactor in the worst case.

Any facility involving the storage of radioactive materials presents a risk which is a combination of the potential danger linked to the radioactive inventory and the vulnerability of the plant to scenarios leading to the release of some fraction of this inventory – taking into account that containment systems are generally not as large in those facilities as they are for reactors. The same applies to the transport of nuclear materials and waste.

The historical development of the French nuclear industry around various sites, and the extension of the services it provides to every step from front-end to back-end of the fuel chain, creates a whole range of hazards that have long been dealt with as secondary while the prime focus was on reactors. Moreover, the decision to develop industrial reprocessing and plutonium re-use leads to a qualitative and quantitative increase of risks, as it implies more manipulation, transport and storage of more dangerous materials.

---

59 This decree remained for more than 40 years the main regulatory framework for nuclear activities, until it was eventually included in a comprehensive nuclear law untitled "law on nuclear transparency and security" passed in June 2006.

60 This "equivalence" was based on the content of Caesium-137 to be released, as this radionuclide represents around 75 percent of the long-term collective dose from the Chernobyl accident.

Focus 10 Pressure on performance and safety

> *"The drop of the availability factor is an alarm signal for safety and is a wake-up call: are we paying sufficient attention to staff competence as well as to maintenance quality and material ageing?"*
>
> **Pierre Wiroth, Inspector General for Nuclear Safety and Radiation Protection, EDF, January 2008**

The economic performance of nuclear facilities relies on such factors as their level of availability or the cost of maintenance. The need for profitability might therefore reduce the safety of the plants, for instance by delaying refurbishment or shortening technical controls. This particularly applies to French nuclear power plants, which already see their economics limited due to their huge overcapacity – and are subject to generic problems due to their high level of standardisation. For instance, in an internal note of 2001, EDF's financial department directorate estimated the loss of profitability at €76 million per percent point of productivity.[61]

EDF reactors have always shown a relative load factor. This combines the availability factor (the time when the plant is ready to produce) and the use factor (the actual production when available). EDF reactors have historically experienced a low use factor because of their excess capacity at large periods of insufficient demand. This, for instance, led to a worldwide unique pattern of reactor management where some units were shut down at weekends, particularly in summer. The constraints induced on the fuel assemblies were one of the potential causes of the unexpected failure of a highly unusual number of fuel rods at Cattenom in 1999-2000, which remains largely unexplained.[62]

Weekend shutdowns have supposedly ceased. However, over 40 units are still operated on load following mode, which could have unforeseen consequences on the fatigue of some components of the plants. Meanwhile, some problems have appeared that affect the technical availability of EDF reactors. Although it remains low, with 77.3 percent cumulated over the reactors' lifetime, the availability has been in constant progress during the last few years, with an increase from 80.4 percent in 2000 to 83.6 percent now, bridging some of the gap with the 90 percent availability or so that the reactor fleet achieves in some countries. But it dropped to 80.2 percent in 2007, clearly on technical grounds.

The main cause is a generic problem of plugging of the tube sheet penetrations of steam generators, that reduces the power output through cuts in the heat-exchange capacity, and could lead to tube cracking in huge numbers. EDF estimates that it will take until 2010 to solve this problem, which needs chemical cleaning. Only five to six units can be industrially treated each year, and 15 of the 900 MWe and 1,300 MWe have already been identified as affected, while some still wait for inspection. This would cost, according to EDF, another 2 percent of availability at least in 2008 and 2009. Yet another problem could further weight availability, as ASN ruled in February 2008 that an "anti-vibratory support default" has to be corrected in all affected reactors, the number of which has not been made public.

These are only the latest examples in a long series of generic problems that have affected the operation of EDF reactors. The negative side of standardisation is that it multiplies problems in large parts of the reactor fleet – and has associated high costs. An example of this link between safety and economy is the series of reinforcements of seismic withstanding after the ASN reassessed in 2003 the level of seismic hazard that had to be taken into account. This involved heavy refurbishments being required at specific points on some reactors, including anchoring points and metallic structures. EDF's reluctance led to the commissioning of a working group between the operator, ASN and IRSN to discuss in detail the exact level of reinforcements on each reactor involved.

---

61 The figure must be higher now, following the increase of electricity prices in recent years.

62 The problem had affected a total of 92 fuel rods in 28 different fuel assemblies (out of 193 assemblies with 264 rods each). This compares to an usual figure of a few rods failures at most in all French reactors in one year.

Another issue where economic pressure and safety can diverge is the search for fuel performance. The goal there is to improve the quantity of energy delivered by each fuel assembly, to allow a reduction in the number and intervals of outages for reloading of the core. EDF reactors were designed for nominal fuel burn-ups of 33 GW.d/t (gigawatt day per ton) which could be reached after a few years, then regularly improved up to 55 GW.d/t currently for uranium oxide fuel (UOX) – although not as quickly as EDF had wanted to. The operator plans to reach even higher burn-ups, both in currently operated reactors and in the future EPR reactor, for which the economic case is based on the hypothesis of a 70 GW.d/t burn-up.

The problem, on the safety side, is to keep control of the behaviour of fuel rods with increased burn-up. The concern with plutonium-uranium fuel (MOX) has for many years prevented ASN authorising a burn-up increase for that specific fuel from 42 to 47 GW.d/t. Fuel rod failures, among other problems, might be the start-up for some accidents. The zircalloy currently used for cladding is not resistant enough to reach the high burn-ups aimed for UOX fuel. The industry developed a new alloy, named M5. The first ever cycle of a full reactor reload cladded with the new M5, in 2002 in Nogent-2, had to be stopped because of primary fluid contamination following a record 39 rod failures on 23 assemblies. Although it remains unclear whether M5 cladding was a root or secondary cause, ASN suspended any extension of its use until full investigations.

Finally, cost-cutting impacts in many ways on operational safety. One recurring concern is the ever-growing use of external, underqualified and untrained workers for various maintenance tasks on nuclear power plants. The management of stocks recently arose as a new concern. EDF's inspector general for nuclear safety and radiation protection insisted in its report on the year 2007 on the problems raised by the massive reduction of costly replacement pieces.[63] He explained that it had become hard for sites to get those pieces when needed, reporting astounding cases where pieces had been unmounted to be replaced and were eventually put back in place due to the lack of spare parts.

[63] *Rapport de l'Inspecteur Général pour la Sûreté Nucléaire et la Radioprotection 2007*, EDF, January 2008.