Security

An industry incapable of adapting to the post-9/11 world

"Security measures offer no real guarantee against the kind of kamikaze actors."

French Ministry of Defence internal memo, cited by *Libération*, 12 September 2001

For the nuclear industry, security, or protection against malicious acts, is a preoccupation that runs parallel to safety, or protection against accidents. In both cases, the objective is to prevent nuclear installations from being exposed to the situations foreseen, and to limit by design the possible consequences to these installations if these situations occur in spite of everything. While the logic of prevention is necessarily different with respect to chance events and deliberate actions, the two areas overlap at the level of installation design.

Unlike accident scenarios, malicious acts are by definition intended to produce the desired level of damage. A key issue in the field of security is therefore to identify threats judged to be "credible", by evaluating (in particular through intelligence) the interest of groups or individuals in targeting a nuclear installation and the means that they could employ.

The impractical challenge of evolving threats

Here the nuclear industry runs up against a fundamental difficulty inherent in the fact that threats evolve over time, whereas the degree of protection that installations have is essentially fixed for their whole lifespan when they are designed. If threats develop which exceed the load level built into the design, protection must henceforth rely on prevention alone.

In France, the authorities have chosen not to make any information available on "design basis threats", in other words the types and levels of credible threat of a malicious act against which nuclear installations should be protected. These details are covered by the secrecy rules protecting national security – "defence secrecy". As a result, we do not know whether these threats have been re-evaluated, and if so in what way, since the attacks of 11 September 2001 in the USA.

Nonetheless, it is incontestable that this date marked a major turning point. Previously, it appears that the threats taken into account were limited by a principle extending nuclear deterrence to any action against nuclear installations carried out with clearly identified foreign support. In the context of the time, only small-scale attacks had to be allowed for in the design under these conditions.

Since then, the design basis of installations has been essentially, if not totally, determined by external attacks or internal situations of accidental origin, liable to cause mechanical or thermal stresses greater than those caused by limited malicious acts.

During the 1980s and 1990s, France witnessed several attacks on its electrical industry. Most aimed to destroy pylons of high-tension transmission lines. The most notable, however, hit the Superphénix reactor on 19 January 1982. Activists opposed to the breeder reactor project attempted to destroy the

reactor, then under construction, by attacking it with heavy weaponry. They failed to hit their precise target, but out of five rockets fired, four hit the reactor – three hitting the containment building and one a lifting system. The damage was estimated at around 100,000 francs at 1982 prices (€15,000). The perpetrators, who had obtained the necessary equipment from actual terrorist groups, were never found until one of them confessed of his own accord 22 years later.[64]

Weapons of the type used, while rare and hard to obtain at that time, have become commoner and more accessible in the last twenty years, as is shown by their being used increasingly often in heavily armed attacks on armoured money convoys. Thirty years after the first French reactors entered service, the threats that need to be taken into account today bear no resemblance to those of that time.

After the World Trade Center attacks, any scenario involving twenty or so people prepared to sacrifice their lives has to be considered as plausible. Obviously this includes the use of hijacked airliners to hit installations – which, whether reactors or fuel manufacturing or processing plants, have not been designed to withstand such an impact.

This fact clearly shows the limitations of the essentially probability-based approach to the design basis of installations. Faced with the risk of malicious acts, a different approach is required. Security thus depends upon an evaluation of the potential dangers. This, as the IPSN (now IRSN) explained after 11 September 2001, involves an estimation of risk based on the identification of the system's sensitivity (ie the potential for a release of radioactivity) combined with its vulnerability (how difficult it is to cause such a release).[65]

Blackout on evaluation and mitigation

No public evaluation exists of the potential consequences of an airliner crashing into one of EDF's 58 reactors. Following an independent assesment published by WISE-Paris in the context of the debate aroused by 9/11 on the potential consequences of such a crash on the fuel ponds at La Hague, an official evaluation by IRSN concluded that if such a scenario occurred it could bring about the release of up to 10% of the radioactive inventory of the fuel in one pond. The release of around 1.5% of the caesium contained in one pond would correspond to the caesium released by the Chernobyl accident.[66]

However, this scenario is not the only one to be taken into account – intruders must also be considered. According to what little information is available on this subject, exercises carried out by the French special security forces have highlighted the poor extent to which nuclear installations are protected against an attack. At another level, Greenpeace anti-nuclear activists have on several occasions been able to carry out protests actually inside power stations, evading security for several hours and reaching sensitive areas of the installations.

At the same time, insider collusion may enhance the effectiveness of malicious acts. Several incidents have shown how vulnerable nuclear installations are in this respect. One incident at the Bugey power station in 2003, which went totally unnoticed by the public, illustrates this vulnerability. On 12 June 2003, during a strike at the site, the mere closing of a hatch triggered a sequence of security system activations, culminating in the automatic shutdown of unit 2 as a result of the activation of the turbo-alternator group protection systems. It is easy to see the potential danger of such an action if the perpetrator had intended to cause more serious harm.

Moreover, nuclear installations are not the only elements to be taken into consideration. The very numerous transports of radioactive material – and especially nuclear material (uranium and plutonium) – resulting from the industry's activities can be seen as so many hard-to-protect "mobile installations". There is a risk both of an attack aiming directly to disperse the material being carried by a transport,

[64] The rocket launcher, an RPG-7, and the rockets were obtained from the German RAF (Red Army Faction) group via the Belgian CCC (Communist Combatant Cells) group, according to one of the perpetrators, Chaim Nissim, in a book published in 2004.

[65] IPSN, *La protection des installations nucléaires contre la malveillance* [The protection of nuclear installations against malicious acts], note of 30 October 2001.

[66] In other words around 26kg, which according to international estimates was responsible for three-quarters of the overall long-term collective dose caused by the accident.

and of an attempt to hijack these materials in order to use them subsequently for a "dirty bomb" or, if nuclear material is involved, to make a nuclear weapon. This risk of misappropriation also exists for all installations that have a significant stock of radioactive material.

Faced with these different risks, how well is the French nuclear industry protected? Planned with reference to threats which are now superseded, the industry appears badly adapted in terms of the design of its installations as much as in its general organisation. As we have seen, the reactors and plants have not been designed to resist the sorts of attack that can now be envisaged. Nor has their location: for example, the centralisation of all reprocessing activities at La Hague gives rise to long transport journeys from the reactors. Even more so, the distance between La Hague, which separates plutonium, and the MOX fuel manufacturing plant at Marcoule which uses it, bears witness to the priority given to economy (in terms of minimising the volumes transported)[67] over security.

Would it have been possible to predict better the way in which threats have evolved? This question is a very difficult one to answer. On the other hand, one might ask how capable the nuclear industry is of adapting. While some parameters are fixed – such as the design basis and the general design of the installations, other factors may be developed in such a way as to reduce the system's vulnerability or sensitivity to the risks of attack.

External security measures have undoubtedly been strengthened – both in the short term, such as the temporary deployment of radar and anti-aircraft missiles to protect the installations at La Hague or in the Rhône valley, or more permanently. On the other hand, the authorities have given no indication of any possible adaptations at the level of the industry.

On the contrary, nothing seems to have changed, even in the most at-risk areas. So, in spite of the anxieties aroused by nuclear transports crossing the country, these transports continue, apparently under the same conditions. The industry's chosen path of reprocessing, of separating plutonium and reusing it in twenty or so of EDF's reactors, which increases the number of transports even while exacerbating their intrinsic danger, has not been revised at all in terms of the security factor. These choices, moreover, result in the long-term accumulation of very large amounts of radioactive material in temporary, low-security storage, by comparison for example with underground stores such as could be implemented in the space of a few years. One again, this issue does not appear to trouble the industry.

In reality, it is by choice that protection relies above all upon external arrangements, so as to dismiss any calling into question of the industrial system's design and direction. Detecting preparation for actions by surveillance of the national territory, and preventing those actions from being carried out through the intervention of security forces, are therefore key.

Secrecy, a substitute for security?

One consequence of this doctrine is the enforcement of a maximum level of secrecy. Of course, as the ASN explained as early as the end of 2001, counter-terrorist protection measures "like the studies conducted into the resistance of nuclear installations to a terrorist act, cannot, by their very nature, be publicly communicated".[68] Details of them must not be disseminated. But the doctrine implemented by the nuclear industry and the French authorities implies any security flaw in the design of the industrial system should be accepted, so long as that flaw can be kept secret!

Having become the first line of defence, secrecy must be protected at all costs – or at least the appearance of secrecy. By this logic, no explanation is possible; nor even any serious expression of doubt. No internal analysis is disseminated outside the circle of those privy to the secret, and any criticism from outside is immediately denounced as playing into the hands of potential terrorists.

Soon after 11 September 2001, several members of Global Chance involved in a working group on France's energy security inside the Commissariat Général au Plan (French planning commission)

[67] Marcoule is near the enrichment plants that produce the depleted uranium which makes up over 90% of the MOX fuel, as against 10% of plutonium.

[68] DGSNR, Annual Report 2001.

proposed that it should include a consideration of the relative resistance of different energy systems to malicious acts (particularly in terms of their degree of centralisation and of the networks on which they depend). The representatives of Cogema (now Areva) and EDF in particular refused point blank to discuss the resistance of different installations to different kinds of attack, bringing the group's work to an end.

This logic can tip over into absurdity when it attempts to keep secret elements that are under the eyes of the public, such as the timetables and itineraries of nuclear material transports, which regularly take the biggest public roads in an easily identifiable form. Again, the lack of any guarantee as to the resistance of present-day reactors to a crashing airliner can hardly be considered a secret.

Deadlock on updating security standards

The same policy now extends to the new EPR reactor project. In 2005-06 the dedicated commission organising a national public debate (Commission Particulière du Débat Public, CPDP) on the Flamanville project censured a paragraph of the contribution by the Sortir du Nucléaire network which cited a note from EDF in support of its doubts as to the reactor's ability to withstand an airliner crash. The problem was the Network's proposal to circulate this note – seen as a "compromise" of defence secrecy, even though the note, classified as "confidential" by EDF, had already been leaked into the public domain.

The dossier submitted to the national public debate thus included contradictory statements, discussion of which was forbidden by defence secrecy. In the context of a democracy, however, it seems vital to assess the EPR in these terms and so to determine what progress it represents in comparison with present-day reactors. The crisis which this incident instigated notably led, in the context of the public debate, to the creation of a working group on freedom of information in the nuclear field.[69] This group acknowledged that, while defence secrecy is an indispensable element of nuclear security, its exact role in the protective arrangements, and thus its limits, remain subjects for debate.

The progress of the debate on the EPR reactor exemplifies the doctrine which gives more importance to secrecy about the EPR's degree of resistance to new terrorist threats not anticipated by its design basis, than to consideration of how to address these threats better at the design stage of a new reactor. Security still ranks low down the list of both short- and long-term priorities, as the industry's preferred vision of the reactors of the future shows.

This vision is in line with international work on the 'fourth generation', a catch-all term which encompasses all reactor concepts, whether new or resurrected, that make a break with the models which currently dominate the industry worldwide.[70] This work is carried on in particular in the context of the Generation IV International Forum, which brought together the "world's top nuclear experts" to define the objectives to be reached and select the most suitable concepts to achieve them.

The objectives, set in April 2001, prioritise safety and above all the management of uranium and waste. Moreover, five of the six design concepts chosen in 2002 rely on a 'closed cycle', not only of plutonium but also of the minor actinides. This choice of designs which require more complex management involving the separation of the most dangerous materials reflects the lack of concern about the terrorist threat.

France's participation in the Forum gives priority to the liquid sodium-cooled fast breeder reactor family. The nuclear industry's objective in this context is to have a prototype put into service in 2020 that would dispel the sense of failure produced by the 1998 closure of the Superphénix breeder reactor, which belonged to this family. This choice, synonymous with a potential worsening of the nuclear system's vulnerability and sensitivity to terrorist threats, shows the French nuclear industry's profound inability to carry out the increasingly urgent updating of its security doctrine.

---

[69] Commission Particulière du Débat Public on the project of a first EPR at Flamanville, *Rapport de restitution du groupe de travail dit "Accès à l'information"*, February 2006.

[70] Known as 'second-generation' reactors, while the reactors developed from these designs, such as the EPR, are referred to as 'third-generation'.