
SHORT AND MEDIUM TERM CONSEQUENCES OF THE 11TH SEPTEMBER ATTACKS ON PHYSICAL PROTECTION ACTIVITIES IN FRANCE

Jacques AURELLE, Pascal CORNU, Jean JALOUNEIX

Institut de Radioprotection et de Sûreté Nucléaire
77-83, avenue du Général-de-Gaulle
92140 Clamart (France)

ABSTRACT

Last year was presented at the EUROSAFE forum the French approach for studying and assessing the sensitivity and the vulnerability of nuclear facilities regarding sabotage acts. At this time, few weeks after the September 11, 2001, security of industrial facilities had come to the forefront of the News. Many questions emerged about the protection of nuclear facilities against new types of threats and new risks. Today, at the light of the fruitful debates which have been established in France on the relevancy of the various approaches for assessing risks and threats in order to achieve an acceptable level of protection, we comeback on these questions with the aim to present an overview of activities and provisions taken, in the field of nuclear industry security, after September 11, 2001.

This overview which covers particularly:

- Assessment by the State of the protection of nuclear sites and facilities,*
- Specific inspections of all nuclear sites,*
- Implementation of measures to strengthen the physical protection,*
- Revision of the design basis threat,*
- Review of nuclear facilities safety regarding new threats,*
- Evolution of the regulation.*

Allows us to conclude, in the field of the physical protection of nuclear facilities, on a necessary cooperation between the numerous actors involved and on the strong link to preserve between safety and security.

1. INTRODUCTION

Last year was presented at the EUROSAFE forum the French approach for studying and assessing the sensitivity and the vulnerability of nuclear facilities regarding sabotage acts. At this time, few weeks after the September 11, 2001, security of industrial facilities had come to the forefront of the News. Many questions were asked about the vulnerabilities of nuclear sites and security measures in place against new threats and new risks.

Today, at the light of the fruitful debates which have been established in France on the relevancy of the various approaches for assessing risks and threats in order to achieve an acceptable level of protection, we comeback on these questions with the aim to

present an overview of activities and provisions taken, in the field of nuclear industry security, after September 11, 2001.

2. BACKGROUND

The protection of nuclear facilities against malicious acts, and the assessment of this protection, had been a matter of concern for competent authorities, their technical support body and the industry for decades.

The approach adopted for considering malicious actions affecting design and operation of nuclear facilities is aimed at determining the extent to which the facilities are protected.

The approach to be followed can be summed up as follows:

- 1) The sensitivity of each area of the facility is determined ; this can be characterised by the level of the consequences (radiological or chemical) resulting from a malicious action. Sensitivity is determined by taking into account :
 - the radioactive product inventory and/or the toxicity of chemicals if any,
 - possible accident situations,
 - an estimate of the consequences of these accidents.
- 2) The vulnerability of the various areas to each type of aggression is estimated, in other words, an estimate is made of the extent to which it is difficult to carry out a malicious action in the area in question.
- 3) If need be, counter-measures are taken to protect areas for which the consequences would be unacceptable compared to the force of the aggression. Counter-measures are intended both to minimise sensitivity and make it more difficult to carry out the aggression envisaged.

2.1. Determining sensitivity

Analysis of the sensitivity of a facility involves using safety analyses to identify potential accident sequences, which, if they occurred, would have significant consequences for workers, the public or the environment.

An accident sequence is taken to mean a series of events resulting from one or more initiating events (the failure of one or more components or functions, or human error) and which put the facility into a degraded situation with the possibility of radiological consequences, despite the engineered safety systems and mitigation devices installed in it. Safety analyses are performed to study these sequences and the counter-measures to be taken, mainly by using a standard incident or accident list taken into consideration at the facility design stage.

Facility sensitivity analysis deals firstly with components, systems or functions which are important for the safety of the facility and identifies those which would lead to a degraded situation if they were lost or caused to fail by a malicious action. It is however important to note that this first step is not sufficient and that specific initiating events leading to degraded situations caused by malicious actions also have to be considered. To this end, a study is made of the particular cases of failure resulting from malicious

actions with possible losses of functions or equipment not taken into account in the safety case.

Thus the method put forward allows to identify the most sensitive elements in the facility (components, systems or functions) and therefore the areas in which they are located ; there are three types of area depending on the gravity of the consequences of a malicious action in the area:

- areas or systems at risk, when an action is not serious enough to lead to radiological consequences; to cause a significant accident, at least two areas or systems at risk have to be affected,
- critical areas or systems, when an action leads to radiological consequences deemed acceptable from a safety point of view.
- vital areas or systems, when an action leads to more serious radiological consequences than those taken into account in the safety case.

2.2. Assessing vulnerability

The vulnerability assessment of the areas and systems identified previously can be broken down into two parts:

- an estimate of the resources required to destroy or sufficiently damage a system or function (for example, the quantity of explosives necessary),
- qualification of the paths leading to areas or systems deemed sensitive.

The second part can be dealt with by identifying all the paths leading to sensitive areas or systems and estimating for each one the difficulties involved or, more generally, the time taken to overcome obstacles and the potential for detecting adversaries.

The previous approach, which has to be linked to response forces interventions, must make it possible to estimate, at least qualitatively, the vulnerability of areas and systems and the need, if any, to take additional steps (design modifications, additional physical protection devices etc.). This analysis has to strike a balance between the need for adequate physical protection measures and the problems associated with facility operating conditions, safety measures....

The resources in the possession of the adversaries depend on the threats being considered. A distinction is made between internal and external threats. In the case of external threats, adversaries are armed or equipped with explosives, whereas in the case of internal threats, adversaries only have access to everyday tools or perhaps more sophisticated ones if they are usually on hand in the facility. It is therefore clear that inside adversaries have more limited resources than external ones; on the other hand, insiders are assumed to be familiar with the facility and they are operational immediately since they have authorised access. What is more, it may be more difficult to detect an aggression by an insider than one by an outsider. Thus it is that vulnerability assessments vary enormously depending on whether internal or external threats are being considered.

The steps to be taken to reduce the vulnerability of components, systems or functions also vary depending on the kind of threat (internal and external). Although physical

protection devices installed between the area outside the facility and the identified targets effectively counter external aggressions, they are of no use in the case of internal threats and other steps have to be taken. For example, poor operation of an item of equipment has to be detected as far as possible by adding sensors for sending alarms to the control room or by making certain items of equipment less accessible.

2.3. Criteria

Acceptable consequences are taken as being those leading to levels of radioactive releases less than, or equal to, those taken into account in the facility safety case. This implies that vital area vulnerability be reduced to a minimum so that an excellent level of protection can be provided for these areas. In the case of critical areas, the level of protection is considered on a case-by-case basis, depending on the consequences of malicious actions.

2.4. Types of aggression to be taken into account

Several types of threats have been identified for the purposes of these studies :

- Internal threats involving actions taken by insiders acting alone or not.
- External threats involving actions by small group of attackers. Two assumptions are made when testing the ability of protection systems to counter aggressions of this type. The first one involves a small team of attackers with limited resources, and the second one takes into account a larger team with more sophisticated resources. Assumptions are also made as to the types of action which could be taken by malicious workers in sensitive areas and the aggravating factors to be considered. As an example the loss of the offsite power supply could be taken into account.

These assumptions are included into the Design Basis Threat considered today in France which is the threat against which the licensee must be able to protect its facility.

3. IMMEDIATE ACTIONS

In the aftermath of the terrorist attacks on September 11 in the United States, the French Government launched a comprehensive review of the security of the main industrial facilities in the light shed by the recent events. For the nuclear industry, this work covers the assessment of the state of the protection of nuclear sites and installations, specific inspections of all nuclear sites, the implementation of new measures to strengthen the physical protection and a review of the Design Basis Threat. IRSN got immediately in touch with relevant agencies to identify relevant new elements of threats to be taken into account and to assess the relevance of the existing regime and measures of physical protection of nuclear facilities against malicious acts to these new elements.

3.1. Assessment by the State of the protection of nuclear sites and installations

The new kinds of threats, revealed by September 11 attacks, were not directly taken into account for the design of the facilities : neither on the safety side where the very little likelihood allows to turn down this risk, nor on the security side where the threats

assessment never points out nuclear plants as target to be protected by on-site measures, due to no concrete threats to nuclear installations in France.

The two competent authorities respectively in charge of safety and in charge of physical protection simultaneously requested assessments of the protection of the nuclear sites and nuclear installations.

In the field of Safety, the identification, by specialists in safety, of targets which could be sensitive in case of the crash of a large commercial airplane has been carried out. After the definition of commercial aircrafts and characteristic parameters to be considered (mass distribution, stiffness, weights, impact areas, speed, angles ...) calculation of mechanical impact and thermal consequences were performed. The evaluation of the potential consequences is under way. Aggravating factors like large scale fire due to the kerosene are taken into account.

In the field of Security, the identification, by physical protection experts, of types of plausible aggressions and of the vulnerability of targets identified by the safety analysis have been achieved. Various scenarios of attacks have been considered such as :

- Intentional aircraft crash (small plane loaded with explosives, commercial airliner),
- Suicidal attack by aggressors carrying on explosives,
- Attack by terrorist groups (commando),
- Suicidal attack by truck or car loaded with explosives (kamikaze bomb truck),
- Explosives introduced surreptitiously by the means of delivery.

For carrying out these studies meetings were organised with representatives from the whole spectrum of nuclear activity (operators, authorities and their support body) and from State specialized agencies , police, Gendarmerie etc..

3.2. Implementation of measures to strengthen the physical protection

The strengthening of access controls led to improve the checks for personnel and for vehicles. To improve the efficiency of checks and reduce the risk of introduction of dangerous devices on the sites significant cuts in vehicle number authorized to enter on the site have been performed.

Moreover, the organization for transshipment and checks of parcels and packages was reviewed and search measures of material delivered to plant were intensified.

The security re-screening for trustworthiness of all operating personnel by relevant authority was performed. This vetting was extended to off-site personnel like subcontractors workers.

Operators suppressed public visitor tours in facilities and information from web sites. On large sites like nuclear power plants, specific exhibition halls were closed.

The protection against "kamikaze" vehicles was strengthened by implementation of obstacles on access roads and the impossibility to park near sensitive areas.

Interfaces between inside and outside response forces were improved, and security measures like strengthening of patrols inside and outside the sites and in the vicinity of all nuclear sites were decided.

The contingency plans involving the intervention of national special forces have been reviewed.

In addition to that, studies to improve detection of aerial aggressions on nuclear sites are in progress.

3.3. Specific inspections of all nuclear sites

Unexpected inspections, simultaneously, on 26 nuclear sites, was achieved on the 28th of September 2001 with the aim to control the application of the so called "Vigipirate" reinforced plan on the French nuclear facilities. 20 nuclear power plant sites, 3 nuclear research centres and 3 fuel cycle facilities were concerned by these inspections. The operators involved were EDF, CEA and COGEMA.

It was the first time that an unexpected inspection was undertaken in the field of physical protection.

For this operation organized on 4 days, it was necessary to write a guidelines for the 34 inspectors involved, in order to have an homogeneous framework for each of these inspections. The operation was well coordinated and kept secret. Finally, all the inspectors arrive at each site at 7 am the 28th of September.

The main topics examined by the inspectors were:

- access control for personnel and vehicles,
- organisation of delivery of materials or parcels,
- communication means (internal and external) to be used in case of sabotage or a malicious action performed on the site,
- procedures applied by guards or on site response forces ,
- application of the authority requests.

All inspection's reports were forwarded to the Competent Authority the 2nd of October. In parallel a global assessment of the protection of the French nuclear industry against sabotage was provided to the authority.

In the aftermath of this inspection, the most significant recommendations produced to the operators by the authority were focused on vehicle searches and packages delivery organisation.

Moreover, the number and the frequency of inspections dealing with sabotage on nuclear sites were increased in 2002.

4. ASSESSMENT OF THE THREAT AND REVISION OF THE DBT

The threat assessment is the responsibility of State specialized entities who have to estimate the motives, intentions and capabilities of potential adversaries. In other words these services estimate at each moment the actual threat. The level of this threat can vary significantly according to time.

In fact the question is : What are the threats to be protected against ?

First at all, a necessary allocation of responsibilities has to be performed by the State who decides which part of the threat must be supported by operators, and which part he will directly address.

That fraction of the threat to be dealt with directly by operators depends on the type of threat to be considered: for example the State cannot be expected to provide significant protection against a disgruntled employee, while the operator will expect a strong involvement of public forces against a violent external attack.

The approach needs the definition of a Design Basis Threat (DBT), on the basis of the experience feedback of the threat assessment. The DBT is the threat against which the operator must be able to protect its facility. In France two sets of threats have been defined, the first one dealing with theft of nuclear material, and the second one dealing with malevolent acts or sabotage. These two sets of threats consider internal and external threats.

In the period following September 11 attacks, the review of the DBT dealing with malevolent acts or sabotage was performed. As a consequence of this new context, a revision of the DBT was decided by the authority and it was agreed that the external threat has to be hardened. The threat to be countered could affect national security and may require support from State local law enforcement agencies and national special forces. It could be noted that new factors are considered, for example attackers could be prepared to commit suicide...

As a result of this revision of the DBT the operators will have to check, in the light of the new DBT, the adequacy of the physical protection measures in force on all nuclear sites or installations.

5. EVOLUTION OF THE REGULATION.

Another consequence of the September 11 attacks was the decision to improve the regulatory and legislative framework in the field of protection of nuclear industry against terrorism. It was clearly identified that ministerial instructions dealing with this subject are not the correct type of documents and upper rank documents such as Orders or Decrees are necessary. Moreover, updating of the technical content of these documents has been decided notably to introduce an harmonization of the approaches coming under local and national authorities in the security areas.

Consequently an improved regulation is under way. This (or these) new text(s) will be more precise in the allocation of responsibilities of the actors involved in the protection of nuclear sites and facilities against malicious actions and sabotage (authorities, licensees, technical support body of the authority, other State entities). Particularly, the commitments of the licensee will be better precised.

6. CONCLUSION

An intensive work has been performed, in the aftermath of the September 11 attacks, to respond promptly and effectively in strengthening, where necessary, protection arrangements of nuclear sites and facilities.

An adequate security on physical protection of nuclear facilities needs strong cooperation and coordination between numerous actors, from different background, to clearly define roles, responsibilities and complementarities between all the involved entities.

Emphasis has also to be laid on the necessary common work between safety and security specialists to assess the sensitivity of the facilities. but the However the methodology applied, for decades in France, to determine the extent to which the facilities are protected against malicious actions affecting design and operation of nuclear facilities seems always relevant and has not been impacted.