

---

# Protection of nuclear facilities and nuclear materials against malevolent actions

P. Cornu, J. Aurelle, J. Jalouneix

*Institute for Nuclear Safety and Protection (IPSN)  
Radioactive Materials Security Department  
France*

---

**Abstract:** The french approach for considering malevolent actions affecting the design and operation of nuclear facilities is aimed at determining the extent to which the facilities are protected. When carrying out these studies, operating organizations have to demonstrate that their are complying with the objectives set by the Competent Authority for reducing the risk of internal or external malevolent actions. The approach to be followed consist to determine the sensivity of each zone and to estimate the vulnerability of the most critical zones to each type of aggression. The sensitivity can be defined by the level of the radiological consequences resulting from a malevolent action. The estimation of the vulnerability is made of the extent to which it is difficult to carry out a malevolent action. If need be, counter-measures are taken to protect zones 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. 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 the vulnerability of the most sensitive zones should be reduced to a minimum so that an acceptable level of protection can be provided for these areas. Emphasis will be paid on the defence in depth approach organized around prevention, management and mitigation measures.

## 1. INTRODUCTION

In France the basic document in the field of the protection of industrial installations against sabotage is the Ordinance 58.1371 published on 29 December 1958. This text deals with the protection of high sensitive installations. This text concerns different aspects of the protection such as fundamental interests of the Nation (commercial or military), the non-proliferation of nuclear material and the security of the public. Specific ministerial instructions detail the arrangements defined for nuclear installations.

How to protect nuclear material and installations against such actions ?

The French approach as regards malevolent actions is aimed at protecting nuclear material and nuclear from the following two events :

- actions which could lead to the release of radioactive substances into the environment,
- the theft of nuclear material which could lead to the construction of a nuclear explosive device.

The aim of this paper is to present the process used, in France, to cope with sabotage against nuclear material or nuclear facilities.

## 2. DESIGN BASIS THREATS

What are the appropriate threats to protect against ?

Concerning malevolent action, threats have been defined concerning internal and external threats.

To this term 'threats' are associated the **risk** of aggression and the **means used** by malevolent people. These means are considered as basic assumption in the studies performed to assess the foreseen or the already existent protection measures.

The approach adopted for considering sabotage affecting the design and operation of nuclear facilities is aimed at determining the extent to which the facilities are protected. When carrying on these studies, the operators have to demonstrate that they are complying with the objectives set by the Competent Authority for reducing the risk of internal or external malevolent actions. The method to be followed is developed in section 4.

Several types of threats are taken into account for the purposes of these studies :

- Demonstration of a hostile crowd,
- Internal threats involving actions taken by insiders acting alone or not,
- External threats involving actions by small groups 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 type of actions which could be taken by malevolent workers in sensitive zones and the aggravating factors to be considered. As an example the loss of the offsite power supply could be taken into account.

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.

But, taking into account malevolent actions against nuclear facilities requires being able to define precisely the characteristics of the corresponding threats. In order to well appreciate the reasons for and the means used by an adversary, it has been decided to collect information in relation to these kinds of actions (successful or not) and try to improve our knowledge of these actions.

A specific list is made from the compilation of events related by medias, by French intelligence agencies or reported by the staff facilities. In 1990, the competent authorities asked the operators of nuclear facilities to declare, without delay, the malevolent actions which may happen in their facilities and to make a report when there is reason to suspect that any malevolent activity has occurred. The criteria selected to characterize the malevolent actions to be declared were specified in 1995. These criteria which are similar to those used by the US NRC are :

1) Bomb related criterion, this category covers all actions involving use of real or hypothetical explosives and incendiary devices.

- 2) Security criterion related to incidents of attempted or actual penetration of an installation's security system.
- 3) Demonstration involving several people (crowd) taking place in the vicinity of the plant.
- 4) Aircraft or vessel considered to be in an exclusion area.
- 5) Installation or security system operation harm criterion related to operation of the installation itself and its security system.
- 6) Nuclear material criterion related to the nuclear materials that may be lost, allegedly lost, considered missing, or unexpectedly discovered in an unauthorised place.
- 7) Weapons criterion related to incidents which take place inside an installation or in its immediate vicinity, and involving firearms.
- 8) Radioactive material criterion. This criterion regards the use of radioactive material to create a real or potential threat or to aggravate an existing threat.

Since 1996, the competent authorities have asked the operators to use a specific form to make their declaration. This form contains the following items : description and chronology of the event, kind of threat, evaluation of the consequences, action undertaken to avoid such an event happens again, preliminary analysis and lessons learned.

Today, this list contains around 600 events which have occurred in France and concern nuclear facilities. First listed events go back to 1975. 40 to 80 events appear each year.

Concerning the breakdown of these events in relation to the relevant criteria, it should be noted that a significant part (about 1/3) of those events are related to the operation of the facility or the physical protection of the facility, then events in relation to aircrafts or vessels, explosive devices, demonstrations and intrusion. Few actions concern radioactive material. The actions concerning nuclear material or involving firearms are rare.

### **3. LEGISLATIVE AND REGULATORY FRAMEWORK**

The French regulatory system regarding physical protection is based on two different sets of texts.

The first set is oriented towards the detection and prevention of loss, theft or diversion of nuclear material usable for the fabrication of a nuclear explosive device. The basic text is a law passed in the parliament on 25 July 1980. This law is supplemented by a set of decrees, orders and ministerial instructions which go into detailed requirements for nuclear material holders. The concerned operators are required to take appropriate measures to ensure that these objectives are met. The Competent Authority with its technical support body, makes checks on the operators concerned. Depending on the case, this may include assessment of technical files and inspection.

The second set is oriented towards malevolent actions on nuclear facilities. The basic document in this field is the Ordinance 58.1371 published on 29 December 1958 dealing with the protection of high sensitive installations. Specific ministerial instructions detail the arrangements defined for nuclear facilities. The latest is the ministerial instruction HFD 50 of 16 May 2000 upgrading older documents. In this frame, two standing advisory groups of

experts (one for reactor and one for other facilities) have been created in 1983 to examine how malevolent actions have been taken into account in the conception and operation of nuclear facilities.

### **3.1. Implementation of the competent authorities**

The function of the Competent Authority has been devoted in France to the ministry in charge of industry, and more precisely to the High Civil Servant for defence and a specialised division : the Division for protection and control of nuclear and sensitive material. As concerns the protection of nuclear facilities against sabotage, the link with safety issues is materialised via a two-headed authority, shared with the safety authority.

### **3.2. Responsibilities of the entities involved**

Three different entities are involved in the French national control system : the Competent Authority mentioned previously, its technical support body (namely the Nuclear Protection and Safety Institute-Radioactive Material Security Department) and the Operators. The organization clearly defines the roles and responsibilities between these entities.

It is important to note that such an organization closely involves together the authorities and the operators and allows a profitable dialogue between them.

### **3.3. Regulatory steps**

For the design and the operation of a nuclear facility the competent authorities consult the relevant restricted standing advisory group of experts (experts' group), for reactor or for other facilities according to the case, and ask to examine how malevolent actions have been taken into account in the design or operation of this facility.

The group is composed of experts in the field of safety and experts in the field of security and physical protection.

Operating organizations have to perform studies aimed at demonstrating that they are complying with the objectives set by the Competent Authorities for reducing the risk of internal or external malevolent actions.

The technical support body of the Authorities has to assess the operating organization studies and to produce a report which is presented to the experts' group. On the basis of this report, the group issues advice and any specific recommendations that may be necessary to the Competent Authorities.

Then, the Authorities notify the operators by letter, if need be with requirements to upgrade the foreseen or existing arrangements. Requirements are aimed at improving the physical protection measures or decreasing the consequences to the environment in case of malevolent action.

## 3.4. Principles

### 3.4.1. Performance-Based Approach

The French regulatory bodies have adopted a performance-based approach which gives flexibility to the operators to choose the means and measures which have to be taken and independence to the authorities who are not obliged to judge arrangements more or less imposed through the regulations. Moreover, this approach permits a better adaptation to the risks which might occur in each type of facility and allows us to improve physical protection techniques on a continual basis.

### 3.4.2. Defence in depth principle

The French physical protection system is mainly based on the principle of defence in depth. This concept of defence in depth is organised around prevention, management of the event and mitigation as regards the theft of nuclear material or the sabotage of nuclear facilities. It takes the form of several lines of defence including both administrative aspects (such as procedures, instructions, sanctions, access control rules, confidentiality rules, ...) and technical aspects (multiple barriers fitted with detectors and delaying devices). This concept of defence in depth is applied to the design and operation of the physical protection system and takes the concrete form of successive barriers, delimiting security areas placed between the sensitive elements of a facility (nuclear material or equipment whose failure would lead to radiological consequences for the environment) and the public area. These areas have to be included one within another and the barriers are designed to be functionally independent.

The physical barriers generally consist of fences for the outside areas and building walls for the areas inside the buildings. These barriers contribute to deterrence and delay for potential intruders and provide uniform and uninterrupted protection. In particular, they are built in order to prevent them from penetration without the need of auxiliary means. They are equipped with devices that detect any intrusion or attempted intrusion and, for the majority, with surveillance and/or alarm assessment systems, as well as lighting devices where necessary. The access points in these barriers (gates and doors) are kept to a strict minimum and are equipped with the appropriate detection devices.

The conditions for access become increasingly stringent as the areas become more sensitive. The conditions for checking individuals become increasingly strict the further they progress inside the facility. In addition, the management of the facility is responsible for establishing, with the adequate procedures, the grounds for granting access authorization to the different areas, but authorization also depends on the results of individual trustworthiness checks made by the Competent Authority as well as work purposes.

Moreover, the operator has on-site response forces which essentially performs the function of control and surveillance of the facility and participate in the deterrence. They are responsible for assessing the alarms, transmitting the alert to the State authorities and, generally speaking, taking countermeasures in the event of any malevolent action in order to mitigate the consequences of these actions. They act as the first level of intervention.

In connection with the on-site response forces placed under the responsibility of the operators, the off-site response forces are, in France, under the responsibility of the State authorities represented by the National Gendarmes forces or the National Police. Exercises are carried out periodically in order to check the effectiveness of the response forces organization.

## 4. METHOD

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

1) The sensitivity of each zone is determined; this can be characterised by the level of the radiological consequences resulting from a malevolent action. Sensitivity is determined by taking into account :

- the radioactive product inventory,
- possible accident situations,
- an estimate of the consequences of these accidents.

2) The vulnerability of the various zones 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 malevolent action in the zone in question.

3) If need be, counter-measures are taken to protect zones 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.

### 4.1. 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 and accident list taken into consideration at the facility design stage.

In fact, sabotage is not taken into account in the safety demonstration, as an example : the simultaneous failure of the redundant equipments of a safety related system as the pumps of an emergency cooling system cannot be considered as probable in the safety analysis if there is no common failure risks. And yet, this failure caused by an action of sabotage can lead to an incident or an accident with radiological consequences.

Facility sensitivity analysis deals firstly with components, systems or functions which are important for the safety of the facility and identifies those that would lead to a degraded situation if they were lost or caused to fail by a malevolent action.

Specific initiating events leading to degraded situations caused by malevolent actions also have to be considered. To this end, a study is made of the particular cases of failure resulting from malevolent actions with possible losses of functions or equipment not taken into account in the safety case.

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

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

The study of measures permitting to decrease the sensitivity of vital or critical zone must be performed. When it is feasible these measures have to be implemented, as an example by limiting the quantity of radioactive materials contained in a capacity,

For the zones which sensitivity cannot be reduced, the vulnerability is examined either in any case for vital zones or as the case may be for critical zones.

## **4.2. Assessing vulnerability**

The vulnerability assessment of the zones 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 zones or systems deemed sensitive.

The second part can be dealt with by identifying all the paths leading to sensitive zones 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 zones and systems and the need, if any, to take additional steps to strengthen the system (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, facility safety and the mitigation of accident situations.

The resources in the possession of the adversaries depend on the threats being considered, in accordance with the relevant DBT. 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 (public area) 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 items of equipment less accessible (under lock and key if necessary) according to their sensitivity.

### **4.3. 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 zone vulnerability be reduced to a minimum so that an excellent level of protection can be provided for these areas. In the case of critical zones, the level of protection is considered on a case-by-case basis, depending on the consequences of malevolent actions.