

---

# IRSN Activities in physical Protection in Support of the IAEA : The Insider Threats Approach

C. Brousse  
J. Aurelle  
R. Venot  
J. Jalouneix

*Institut de radioprotection et de sûreté nucléaire (IRSN)  
France*

---

**ABSTRACT** : The objective of this paper is to present an approach to deal with internal threats which allows : (1) to identify specific potential internal threat for nuclear facility or transport based on the Design Basis Threat, (2) to specify the list of potential theft and sabotage targets, (3) how to protect these targets, (4) and how to evaluate the protection level of these targets to avoid unacceptable consequences in full compliance with IAEA standards and recommendations. The implementation of this approach leads to identify, if need be, ways of improvement or strengthening of the protection against the internal threat and to take adequate decisions of implementation of corrective measures.

## 0 FOREWORD

This paper stem from a draft document jointly drawn up by SANDIA NATIONAL LABORATORY (SNL) and IRSN with the aim to precise and clarify the insider threats and to propose a methodology to cope with such events.

## 1 INTRODUCTION

The term of “insiders” will be used to describe individuals with knowledge and/or authorized access to sensitive areas.

The internal threat is particularly difficult to resolve because nuclear facilities typically employ large number of people, and certain employees must have access to sensitive areas in order to perform their work. Thus, insiders could take advantage of that access and of their knowledge of the facility to perform acts of sabotage or theft. However, there are many steps that can be taken to reduce the chance of having an insider attack be successful.

Each type of insiders needs to be identified to understand their motivation, to determine their possible intentions, their capabilities of actions and targets he could aim at.

Facilities and locations handling nuclear material or which could lead to the release of radiological substances into the environment must be inventoried and taken into consideration according to the potential consequences (Sensitivity level). Next, technical and administrative measures to prevent internal threat must be clearly identified, implemented

and described in specific documents. Every document dealing with the security of a facility or material should be written under quality insurance and classified at the relevant level.

Effectiveness and relevance of the security measures, including control, accountancy and physical protection systems, if need be in connection with safety provisions can only be evaluated by a formal, systematic and exhaustive vulnerability assessment based on scenarios linked to each kind of insiders previously identified. A level of vulnerability and a specific response in order to thwart insiders must be associated to each scenario. Finally, mitigation measures to cope with the potential consequences of a malevolent act and emergency plans must be prepared.

According to the level of radiological consequences or potential proliferation, and other criteria such as cost or potential impact on safety, radiation protection or operating requirements every necessary improvement must be implemented.

The security concerns addressed in this document relate primarily to nuclear facilities and nuclear material in use, storage and transport.

## **2 SCOPE**

The scope of this paper deals with unauthorized removal of nuclear material and sabotage of nuclear material and nuclear facilities in full compliance with the field covered by INFCIRC/225 rev. 4.

Theft of sensitive nuclear material can lead to the fabrication of an explosive nuclear device. Sabotage can lead to the release of radioactive substances into the environment or people exposure to radiation. Malevolent actions which could raise consequences in terms of operating loss, industrial tool loss, media impact, brand image weakening etc, are not included in the scope of this guide.

The administrative and technical measures to deal with protection against the unauthorized removal of nuclear material and against sabotage of nuclear material and facilities by insiders may differ. Indeed theft of nuclear material can be prevented by delaying access to the material or by containing the adversaries before they remove the nuclear material from the facility. Sabotage, however, must only be prevented by denying the insiders access to the target or by interrupting and stopping the adversary action prior to the sabotage act.

The methodology applies to any type of nuclear facility notably the nuclear power reactors, the research reactors and all facilities of the nuclear fuel cycle (enrichment plants, reprocessing plants, fuel fabrication plants, storage facilities,...). It also applies to national and international transport of nuclear material.

## **3 INSIDER THREATS IDENTIFICATION**

This chapter presents a methodology for insider threat identification at the facility level based upon the use of the Design Basis Threat (§ 3.1 et 3.2), which gives the global attributes and characteristics of an insider, coupled with a search and rigorous utilization of information gathered on the ground (§3.3).

### **3.1 Design Basis Threat (DBT)**

- The Design Basis Threat (DBT) is a regulatory tool used by the State, through the Competent Authority, for planning, designing, and evaluating physical protection

systems. It is a process that needs to be repeated to ensure the continuing relevance of the DBT and the effectiveness of the physical protection system (PPS).

- DBT may refer to both unauthorized removal of nuclear material and sabotage or there may be a DBT for sabotage and another one for the unauthorized removal of nuclear material. The DBT deals with both insiders and outsiders.
- More specifically, the DBT describes the attributes and characteristics of potential insiders and outsiders who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system is designed and evaluated.

### 3.2 Possible insiders

According to the States, DBT may be detailed or not. If DBT is not very detailed, consideration could be given to the following :

- An insider can be in any position in a facility organization, including workers, experimenter, PPS designer, security guard, clerical staff, custodian, maintenance person, all the way up to upper management personnel. Additionally others not employed by the operator such as vendors, emergency personnel, contractors, inspectors who have authorized access should also be considered. Some cultures have a hard time accepting that someone in upper management (even the plant manager) could be the adversary.
- Insider motivations include ideological, personal, economic, psychotic, or other. For instance, real and imagined grievances, personality traits and mental illness, idealism, desire for monetary gain, coercion by outsiders that lead to betrayal, revenge, abnormal behavior.
- Insider intentions may be theft or sabotage either as an end in themselves or as a mean to achieving a secondary aim.
- An Insider may be passive or active; may be violent or non violent; act alone or in collusion with other insiders or outsiders; he may be malevolent by opportunity or his action can be premeditated and well prepared.
- An insider has the opportunity to act during normal operation, maintenance, emergency situation and their knowledge, possible access at different places in the facility, and authority may affect their ability to be detected. He has also the opportunity to act at the most favorable occasion.
- As types of resources or capabilities, insiders may have - knowledge of the layout, processes, physical protection and safety systems and mitigation devices of the nuclear facility, route of the transport - technical skills and experience - tools and equipment which could be available or introduced - weapons - explosives, etc. The State has to precise the attributes and characteristics of the potential insiders and the operator has to refine them in accordance with the characteristics of its facility or transport.

### 3.3 Insiders identification at the operator level

- Insider threat identification at the facility or transport level is up to the operator.
- Insider threat identification at the facility or transport level is *a priori* target independent because targets are defined by their potential consequence and not by their potential threat.
- The methodology for insider threat identification at the facility level consists of three basic sequential parts.

### **Search informations which are necessary to characterize the potential threat**

Before time is spent collecting information, it is important to decide and list what kind of information is needed to complete a definition of threat for a facility or a transport. In so doing, the operator will use the general characteristics of insider described in the State specific DBT and mentioned in § 3.2, will estimate their relevancy with regard to its facility and if be needed will refine them. In so doing, the types of equipment detained in the facility and their utility in the unauthorized removal of nuclear material or the sabotage of nuclear material and the facility have to be taken into account.

### **Gather on the ground information upon the potential threat**

The local environment provides information about the threat to a specific facility or transport. One needs to seek the following local information to define the threat.

i. The conditions inside the facility, including work force, labor issues, industrial relation policies, security awareness and human reliability programs, past workers, etc.

ii. The conditions outside the facility, including the general attitude of the community; whether the surrounding area is urban or rural; the presence of organized groups, etc. In so doing, a review and characterization of the local population can be useful in determining a potential threat to a nuclear facility.

iii. Facility features affecting the threat may include: personnel flow and access control, facility state (normal functioning, shutdown, maintenance duty, etc.) operational processes, authority structure, general job categories, physical protection features, information characterization, safety and/or radiation protection requirements, accountancy and follow up systems for nuclear material.

### **Organize threat information to make it usable**

The operator has to organize all this information to outline the characteristics and attributes of credible potential insider groups to be considered for his own operation. These characteristics and attributes include access, knowledge, authority, equipment, objective, sophistication, willingness to violence.

- The outputs of the described methodology are the credible range of insiders considering their position, motivations, intentions, access, capabilities, etc.

## **4 REVIEW OF TARGETS**

Insider Target identification is an evaluation of what to protect *a priori* without consideration of the threat or the difficulty of providing physical protection. Insider Target identification identifies areas, components, systems, functions or actions to be protected.

- The approach consists to analyze the sensitivity of a :
  - Facility or a transport, using safety analysis to identify potential sabotage targets,
  - Nuclear material, using categorization of nuclear material in the field of nuclear weapons proliferations (INFCIRC/225).
- The approach leads to a ranking of targets depending on the gravity of consequences resulting from their attack.
- The objectives of a theft of nuclear material and of a sabotage are of different natures, consequently the protecting goals and targets are also different. Therefore, targets are ranked for theft and/or sabotage. A unique ranking for theft and sabotage is not feasible.
- A target may be more sensitive to sabotage than theft or conversely (i.e. nuclear wastes are more sensitive to sabotage than to a theft for proliferation purpose). At the end, the greater sensitivity has to be first considered.
- Targets which are sensitive for theft are usually less numerous and less dispersed in the facility than sensitive targets for sabotage. Indeed nuclear material are usually located

either in storage or process areas. However nuclear material locations may vary according to the type of facility and specific assessments have to be performed for each type of nuclear facilities.

### ***Specify nuclear material and facility sabotage targets***

- 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. However, sabotage is not taken into account in the safety scenarios. As an example, the simultaneous failure of the redundant equipment 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 mode 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 equipments not taken into account in the safety cases.
- The levels of the radiological consequences have to be established by the State or the Competent Authority mainly from the results of safety analysis studies. These levels may be different from one country to another one. It is desirable that these levels are consistent with those taken from the safety criteria. For example, unacceptable consequences could be those leading to radiological release levels more severe than those taken into account in the facility safety case.
- Thus the method put forward allows to identify the most sensitive elements in the facility (components, systems or functions) and therefore the zones in which they are located .

### ***Specify nuclear material theft targets***

- The characteristics of an insider lead to take into account two potential types of thefts of nuclear material:
  - i) The repeatedly steal of small quantities of nuclear material to get significant quantity of nuclear material (protracted theft),
  - ii) The theft all at once of a significant quantity of nuclear material (abrupt theft).

These two possibilities have to be taken into account when reviewing the targets.

- Targets may be ranged in three categories I, II, III as drawn from the categorization table of nuclear material of INFCIRC/225. One has to remind that this categorization is based on the possibility of the material being used for a nuclear explosive device. In this regard, significant quantities of nuclear material currently in use for manufacturing a nuclear explosive can be drawn from IAEA safeguards glossary 2001. Direct use of nuclear material (plutonium, uranium 233 and enriched uranium at 20% or more in uranium 235) has to be given a special attention as regard non proliferation matter.
- Potential targets are reviewed by identifying for each of them its sensitivity degree evaluated especially from the physicochemical nature of the nuclear material (massive or scrap, metal or oxide, fresh or irradiate material, etc). In this regard, one will find in IAEA

safeguards glossary 2001 an approach to the sensitivity of nuclear material by use of a comparison scale stretching to items for nuclear weapons to miscellaneous impure compounds.

- In conclusion, the method put forward allows to identify the most sensitive nuclear material and its location.

## **5 ADMINISTRATIVE AND TECHNICAL MEASURES AGAINST INSIDER THREATS**

### **5.1 General overview**

In a general way, the definition and the implementation of administrative and technical measures to cope with the internal threat have to comply with the physical protection objectives and fundamental principles. More particularly, at the facility or transport level, due consideration has to be taken to the following principles :

- Security culture which includes characteristics and attitudes in organizations and of individuals which establish that physical protection issues receive the attention warranted by their significance.
- Threat, taking into account the process described in chapter 3.
- Graded approach, taking into account the current evaluation of the threat, the relative attractiveness of the targets and the potential consequences of a malevolent action.
- Defense in depth which develop several layers and methods of protection (structural or other technical, personnel and organizational).
- Quality assurance policy and programmes.
- Confidentiality about information and documentation, the disclosure of which could compromise the protection of nuclear material and facilities.

Since insiders have privileged knowledge and authorized access to sensitive areas, internal threat must be approached in a different way than that of the outsiders. Security system must be based not only on technical and administrative provisions but also on specific complementary measures mainly dedicated to the human behaviour. Indeed, the specific point of the internal threat is that the malevolent act will come from a person, a scientist, a manager, or a worker living with and sharing different experiences with the others. Insider is usually someone whose people don't beware of. Therefore, specific procedures, fully integrated in a well-developed security culture are needed.

In particular for insiders, provisions taken in the field of physical protection must be completed by other lines of protection. Each line of protection may be not considered as sufficient by itself. But the sum of these provisions coming from different fields complement each other and form a coherent whole which could considerably reduce the risk of internal threat or even delete it.

The physical protection system itself is organised around prevention, management of the event and mitigation as regards of 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) than the adversary have to overcome or circumvent in order to achieve his objectives.

For safety purposes, design criteria such as redundancy or diversification in technology of important to safety systems or equipment or layout criteria such as physical or geographical separation or segregation of these systems or equipment are introduced at the design phase

of the facility. These provisions improve protection against sabotage by requiring more preparation, more means and more time for a potential insider to commit a malevolent action. Consequently they could be of significant efficiency to deter, to prevent, to delay and even to mitigate sabotage resulting from an insider.

Moreover, radiation protection rules by the implementation of access limitation to specific areas and radiation protection devices could also act as to deter and to prevent attempts of theft of nuclear material or sabotage resulting from an insider.

Measures taken for control and accountancy of nuclear material could be efficient to detect theft or diversion of nuclear material resulting from an insider. They have to be considered as a necessary complement of physical protection measures. Emphasis has to be put on the fact that the control system of nuclear material be more effective than the physical protection system to detect the repeated theft of small quantities of nuclear material in a facility.

It is considered as good practices that risks of theft of nuclear material or sabotage of nuclear material or facilities are taken into account at the design stage of the facilities, not only for the definition of the physical protection system but also as design criteria for all other involved areas (safety, radiation protection, control and accountancy of nuclear material,...).

Each operator must develop and adapt general provisions for its aspects.

## **5.2 PPS primary Functions**

The physical protection system is based on a set of provisions taken at the State level and at the operators level to protect the nuclear facilities against sabotage and to protect nuclear material against theft.

Some elements of the physical protection system participate in all or several functions listed below, such as guards who participate in prevention, detection, delay and response.

The provisions developed hereafter deal with how to take into account the internal threat at the operator level. **The considerations linked to these provisions will not be developed in the frame of this paper.**

### **Preventive measures**

The aim of these measures is to minimize the likelihood that an attack will occur. Preventive Measures are for instance : Confidentiality; Pre-employment and employment checks; Security awareness; Compartmentalization; Escort and surveillance of infrequent workers; Disciplinary actions/prosecution; Nuclear safety.

### **Protective measures**

The protective measures cover detection, delay and response.

#### **Detection**

Detection is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of nuclear material or equipment, systems or devices in a protected area. To be useful, detection needs to be promptly coupled with the determination of the cause of the alarm and the extent of the action at the origin of the alarm. Detection measures are for instance : Supervision; Access control; Searches people, packages and vehicles for contraband; Searches of nuclear material on exit; Two-person rule; Operation monitoring or process control; Operating conditions; Routine testing; maintenance and requalification; Tracking; Material Control and Accountancy.

#### **Delay**

Delay is the slowing down of an insider's action. Delay increases the insider's task time. If a detection has occurred, each additional minute required by the insider provides additional time for assessment and for response forces to cope with the malevolent action. Delay measures are for instance : Complexity to perform the task; Equipment under locks and keys; Action of guards.

#### **Response**

Guards and/or the response force need to respond more rapidly to prevent sabotage than to prevent theft. Indeed, to prevent sabotage, the guards and/or the response force need to stop the adversaries before they can access the nuclear material or a vital equipment that could be sabotaged and potentially result in a radiological release.

According to the means associated to insiders, the response can be conducted not only by dedicated person, guards, security personnel, appropriately equipped and trained but also by one or several witnesses of the malevolent action.

### **Mitigation measures**

Mitigation measures and contingency plans may be significantly different in case of theft of nuclear material or in case of sabotage. Usually they need close co-operation between the operator and the State's level organizations.

Contingency plans of action for mitigation are prepared to counter effectively any attempted sabotage or any attempted unauthorized removal of nuclear material. They describe communication and immediate counter-measures which have to be applied in different cases namely in case of sabotage and in case of theft of nuclear material. In addition they have to describe mitigation provisions. These plans may cover both the internal threat and the external threat.

As far as sabotage is concerned, these contingency plans have to mention the provisions taken at the operator's level for coordination with safety authorities to minimize the radiological consequences of a malevolent action.

## **6 EVALUATION OF THE PROTECTION SYSTEM**

### **6.1 Objectives**

The aim of this chapter is to assess if the targets identified by the methodology described in chapter 4 are vulnerable to internal threat (insiders). That leads to assess if all elementary events which lead to an "undesirable event" can be performed by insiders based on the definition of the internal threat as explained in chapter 3.

Evaluation of the scenarios of sabotage or theft of nuclear material is mainly based on a detailed examination of the physical protection system duly complemented, for repeated thefts by an assessment of the material control and accountancy systems and for sabotage by an assessment of the relevant safety provisions.

Many scenarios could be envisaged, but only realistic scenarios have to be considered, having in mind that all the actions and associated means have to be consistent with the insider threat definition.

### **6.2 Development of scenarios**

The development of scenarios consists in identifying for each one all elementary actions and the associated means necessary to perform them. In the field of sabotage, are concerned the actions which must be performed to initiate an accidental sequence leading to unacceptable radiological releases. In the field of theft of nuclear material, are concerned the actions which must be successively performed to reach nuclear material, to remove them from their containment then to get out the facility where they are located.

### **Identify Adversary/Target couples**

The approach developed in chapter 3 leads to identify the potential types of insiders (i.e. adversary). The two kinds of malevolent actions developed in chapter 4 -theft or sabotage- lead to grade the targets according to the potential consequences. Insiders characteristics and the list of targets are the relevant inputs for the development of scenarios.

The principle of this approach consists in identifying couples adversary/target which lead to events with undesirable effects. All adversaries/Targets couples are obtained by crossing adversary and target lists in a table.

### **Identify protection elements**

A schematisation of the facility has to be performed with the aim to identify the protection areas in connection with relevant targets. This schematisation should include the description of their protection provisions (detection or delay), and applicable operational features. The identification and the inventory of the protection elements depend on the state of the facility (design stage or under operation). This step is based both on the review of layouts and documents (including safety and security documentation) and walk-down of the facility (by operator staff and physical protection specialists).

This step consists also in the inventory of the methods or the means, used by the insiders to defeat or to get over each protection element previously identified. The objective is to identify the protection elements which could be defeated by insiders. The method is based on : (i) the review of insiders attributes (access, authority, job privileges, skills or knowledge, other resources) in comparison of protection element performances and efficiency, (ii) the analysis of relevant experience data, (iii) the judgment of experts.

### **Identify scenarios**

The strategy of insiders is to complete successfully a scenario which leads to a theft of nuclear material or to a sabotage. The full range of scenarios going from the strategy that minimizes probability of detection to the one that reduce time required to perform the malevolent act, has to be studied.

Three main families of scenarios should be taken into account according to the targets identified in the facility : (i) sabotage, (ii) theft of a significant amount of nuclear material all at once (in a unique or multiple locations), (iii) repeated theft of small quantities of nuclear material to make up a significant amount.

The research of potential scenarios must cover all the stages of the facility life (normal operation, maintenance, emergency situation,...).

This step needs to precisely describe, for each adversary/target couple, how undesirable event may occur. That means, to describe for each adversary/target couple, the detailed paths in the facility to reach the target and the actions performed by insiders. The different barriers (technological and organizational) and detection devices met during the insiders advance have to be carefully identified and detailed.

The identification of all potential paths and actions is based on the review of layouts and documents (including safety and security documentation) and walk-down of facility by operator staff and physical protection specialists.

## **6.3 Evaluation of the effectiveness of the implemented measures against scenarios**

This step consists in the evaluation of the effectiveness of the implemented measures and consequently the difficulty to carry out scenarios leading to undesirable consequences. At this stage the vulnerability of the targets is evaluated. The outputs of this step consist in judgment based as far as possible on detailed analyses and precise data on the success of the scenarios.

The target vulnerability assessment can be broken down into several parts (generally two parts in case of sabotage and three in case of theft):

- (i) an exhaustive inventory of the paths leading to zones or systems deemed sensitive,
- (ii) a detailed analysis of the resources to destroy or sufficiently damage a system or function, or steal nuclear material,
- (iii) a detailed analysis of the possible sequences to bring the stolen nuclear material out of the facility.

The first part can be dealt with by an evaluation for each path leading to sensitive zone or equipment of the difficulties involved or, more generally, the time taken and the means involved by the insider to reach the target and the potential (or probability) to detect him and to thwart his attempt by an adequate response.

The second part involves an assessment (if possible with quantitative data) of the insider means, time required and capabilities to effectively achieve the theft or the sabotage on the spot of the target.

The third part, specific for stolen material, detailed the possible ways for the insider to complete his theft. He can, for example, leave directly the facility with the stolen nuclear material or hide these material on the site of the facility to bring them out later on in a more favourable occasion.

The specific planned response, in order to thwart insiders, must be associated to each scenario in the evaluation process.

The unacceptability of scenarios is based on the potential consequences of the malevolent action. However emphasis has to be put on other criteria such as :

- The relative easiness to perform a malevolent action. A scenario with limited consequences but rather easy to perform may be deemed as not acceptable and require corrective actions (for example : unauthorized alteration of a threshold in the process, unauthorized alignment of a circuit).
- The case of a situation deemed acceptable but not far from threshold beyond which consequences are no more acceptable. Such a case may be not disregarded and prudent management practices may require protective measures.
- The outputs of this step is a list of scenarios which can success realistically. For these scenarios upgrades in the protection against insiders are of course necessary. The operator will deal first with the scenarios with the worst potential consequences.

## 6.4 Upgrades

The last step of the process is to upgrade, when necessary, the protection against insiders. For the scenarios which could succeed and are unacceptable, corrective measures must be taken to reduce the risk to an acceptable level.

Weaknesses of the protection system are identified, then quantified in order to examine possibility of upgrades.

It is the responsibility of the operator to define and implement all necessary corrective measures.

The efficiency of the overall protection system thus modified needs to be carefully examined. Correctives measures may concern prevention, protection or mitigation. Measures allocated to prevention and to a certain extend to protection are usually more effective than measures allocated to mitigation. Consequently, where feasible, due priority has to be put on improvement of prevention.

Potential conflicting requirements resulting from safety and physical protection considerations, should be analysed to ensure that they do not jeopardize nuclear safety.

Finally, the relevant upgrades are properly implemented and their actual benefit, in term of protection, evaluated by the method, here-above developed.