
The fundamental principles of the physical protection

The Group of Six point of view

Belgium

Claeys, M. *Federal Agency for Nuclear Control*
Carnas, L. *Federal Agency for Nuclear Control*
Robeyns, G. *Designate expert*

France

Rommevaux, G. *CMN - Contrôle des matières nucléaires*
Venot, R. *IPSN - Institut de protection et de sûreté nucléaire*

Germany

Fechner, J.B. *Federal Ministry for the Environment, Nature Conservation and Nuclear Safety*
Hagemann, A. *GRS - Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) mbH*

Spain

Fontaneda González, A. *Nuclear Energy Division, Directorate General of Energy, Policy and Mines Ministry of Economy*
Giménez González, S. *CNS - Nuclear Safety Council*

Sweden

Isaksson, S.G. *SKI - Swedish Nuclear Power Inspectorate*

United Kingdom

Wager, K. *DTI - Department of trade and Industry*
Price, C. *OCNS - Office for Civil Nuclear Security*

Abstract: This paper presents the joint experience of the Group of Six in the field of physical protection against the theft or unauthorised removal of nuclear material and against the sabotage of nuclear material and nuclear facilities, which emerged from the joint discussion. Several fundamental principles stem from this experience. Of course the particular terms and conditions of the implementation of these principles are specific to each country.

1. INTRODUCTION

Following an approach by the US calling for a revision to the Convention on Physical Protection of Nuclear Material and the calling by the IAEA of a meeting of experts, several European countries wished to meet in an informal way to exchange view on the physical protection of nuclear material and nuclear facilities. Thus France and the U.K. met in September 1999. Then they were joined by Germany, Belgium, Sweden and Spain. These European countries form the so-called "Group of Six".

This paper presents the joint experience of the Group of Six in the field of physical protection against the theft or unauthorised removal of nuclear material and against the sabotage of nuclear material and nuclear facilities, which emerged from the joint discussion. Several fundamental principles stem from this experience. Of course the particular terms and conditions of the implementation of these principles are specific to each country.

Physical protection against the theft or unauthorised removal of nuclear material and against the sabotage of nuclear material and nuclear facilities by criminal or terrorist groups or individuals has long been a matter of national and international concern. Although

responsibility for establishing and operating a comprehensive physical protection system for nuclear material and nuclear facilities within a State rests entirely with the Government of

that State, the need for international co-operation becomes particularly evident in situations where the effectiveness of physical protection in one State depends on the actions taken by other States, as appropriate. In addition, a deficient physical protection system in one country may lead to negative consequences for other countries.

A key point equally shared by the six countries is the reference to a “security culture”. Security culture includes characteristics and attitudes in organisations and individuals which ensure that physical protection issues receive the attention warranted by their importance. In this field, practices and knowledge emerge from the experience and cultural context specific to each country. Fundamental joint views are however noted. The Group of Six associates itself with these joint views which deal with philosophical, legal, organisational and technical aspects leading to the implementation of a national system of physical protection.

2. THE FUNDAMENTAL SECURITY PRINCIPLE RELATED TO THE DESIGN OF THE PHYSICAL PROTECTION SYSTEM

2.1. Legislative and regulatory framework

The regulatory system underpinning a physical protection regime would normally be based on various official documents dealing with establishment, implementation and maintenance of physical protection. This system would be oriented towards two main objectives. The first one concerns the prevention and detection of theft or unauthorised removal of nuclear material usable for the fabrication of a nuclear weapons. The second one pertains to the prevention of sabotage against nuclear facilities or nuclear material which could result in a release of significant quantities of radioactive material.

The basic text could be one or more laws, dealing principally with physical protection, passed in Parliament. These laws have usually to be supplemented by a set of decrees, orders, ministerial instructions, regulations and authority guidelines which go into detailed requirements for nuclear material holders, transporters or operators of nuclear facilities. Various regimes might be possible, depending on the quantities of nuclear material involved or the potential for environmental damage. The holders, carriers or operators concerned are required to take appropriate measures to ensure that the objectives of protection are met. The Competent Authority, if necessary assisted by its technical support or expert body, has to inspect the holders, carriers or operators concerned to assess compliance with the law. In some cases, this may include evaluation of technical files and/or licensing documents and inspection of the physical protection system.

2.2. Implementation of the Competent Authority

The State needs to identify clearly the authority specially designated to implement the legislation and the regulations adopted for the purposes of physical protection. This authority is called the Competent Authority.

The Competent Authority must be vested with adequate legal powers, possess the appropriate competence and the human and financial resources to meet the responsibilities which it has been given and, finally, have the necessary independence from any organisation responsible for the promotion or the use of nuclear energy. This independence is considered as a key requirement for the effectiveness of the national physical protection system.

At least two types of entity are likely to be involved, namely the Competent Authority and the various holders, carriers or operators. In addition, other State organisations such as Police which could supplement the on-site response forces may be involved. Other bodies involved may include a Technical Support Body or contracted experts to advise the Competent Authority on the physical protection matters.

2.3. Responsibilities of the entities involved

Depending on the specific circumstances, regulations that stem from different authorities, notably safety and/or radiological protection authorities could lead to the adoption of provisions which may run counter to the objectives of physical protection. Conversely, the provisions adopted for the purposes of physical protection could be contradictory to the objectives of regulations from other authorities. In order to prevent conflicts a sufficient exchange of information should be provided between the different authorities concerned. The procedures for resolving conflicts, should they arise, must be clearly specified.

The basis for this arrangement depends on the State ensuring that the responsibilities for implementing the various elements of physical protection be clearly identified. Accordingly, the State must take the appropriate steps to ensure that each licensee or holder of authorisation meets his responsibility. In this context, the State lays down the objectives to be achieved in the field of physical protection and the licensee or holder of authorisation takes responsibility for the means and resources required to achieve these objectives.

The Competent Authority, assisted by its technical experts as necessary, is responsible for :

- definition and implementation of the regulations,
- definition of the objectives to be met by the licensees or holders of authorisation,
- decisions concerning licensing or sanctions if need be,
- control of the correct implementation of the regulations, or licensing documents which may require it to check that the licensees or holders of authorisation have taken the right measures to satisfy the specified objectives and that these measures are operational,
- promotion of a security culture,
- assessment of the files and studies produced by the licensees or holders of authorisation,
- assessing compliance with the regulations through mandatory inspections,
- proposal of regulatory updates arising from its experience, feedback or the changing international context.

On his site or during his transportation, the licensee or holder of authorisation must take all the necessary measures to guarantee the physical protection of his nuclear material or his nuclear facilities. In other words, he must define the principles of his protection systems and then put them into practice. He must also devise the procedures necessary to ensure the satisfactory functioning of the various components of the systems. In particular, he is responsible for the maintenance of the equipment, periodic tests for checking its satisfactory functioning and performance, the definition of operating procedures, the training of personnel, the execution of periodic exercises, etc... Moreover, the licensee or holder of authorisation has to prove that his arrangements satisfy the objectives specified by the authority.

2.4. Compliance-based approach or performance-based approach

During the first steps of the implementation of a national control system, it is convenient to impose precise requirements upon the licensee in the field of physical protection.

In this context, it seems easy to impose detailed requirements about physical protection. As an example the design of various devices such as the barriers, fences and security doors or the check of the people accessing to the most sensible areas could be detailed. Moreover it seems also easy to control the execution of the required provisions because inspection could be limited to check whether the physical protection provisions exist or not. This compliance-based approach, however, does not leave much flexibility for the licensee to tailor his physical protection measures to the specific characteristics of his nuclear facility and to other local conditions.

A dispensation regime may be possible to accommodate the oldest facilities designed according to different rules. However, this approach may not be flexible enough to cover the characteristics and the particularities of each kind of installation nor to take into account technological development relating to physical protection equipment.

The performance-based approach facilitates the possibility of better allocation of responsibilities between the authorities and the licensees or holders of authorisation. The latter are responsible for the physical protection and its implementation and the Competent Authority is responsible for ensuring that they comply with the stated objectives. It gives the licensees or holders of authorisation more flexibility in choosing the means and measures which have to be taken. It gives also more independence to the authorities which are not then bound to judge the efficiency of the various arrangements that they had more or less imposed through the regulations. This approach allows a better adaptation to the risks which could occur in each type of facility and allows, at any time, the possibility of improving the physical protection techniques to take advantage of the emergence of new concepts and new devices. It may be more difficult to apply a performance-based approach than a compliance-based approach, but overall it is a more powerful and more flexible approach.

It is noted that the performance-based approach requires that the competent authority or its technical support body be comprised of qualified, experienced and well-trained staff on the one hand to assess the effectiveness of the adopted provisions and on the other hand to judge the way in which they are applied. For the same reasons it is vital that the licensees or authorised entity have staff with a good engineering background.

3. THE FUNDAMENTAL SECURITY PRINCIPLES IN THE IMPLEMENTATION OF THE PHYSICAL PROTECTION SYSTEM

3.1. Design Basis Threat

The foundation of a physical protection system must, in the end, rest on an evaluation of the threat with which each State finds itself confronted. The definition of the threat against which protection has to be provided is developed from this evaluation and known by the name of "Design Basis Threat". The design Basis Threat can – and almost certainly will - vary from one State to another one, since the assessment takes into account both the international context and the specific situation within the State in question at a given moment. A regular revision of these threats must also be undertaken based notably on lessons learnt from an analysis of the changing situation.

The characteristics of adversaries and the means at the disposal of these adversaries, in particular the likelihood of being assisted by one or more individuals who have authorised access to the facilities, the tactics employed by these groups, their technical competence, size and the equipment available to them for use in any attack constitute the threat. These definitions of the characteristics and means stem from an evaluation of the intentions and capabilities of individuals or groups of individuals believed to pose a threat to national security or a serious threat to law and order in the State, in particular to nuclear undertakings. From this evaluation the Design Basis Threat determines the level of protection measures required to protect against theft or unauthorised removal of nuclear material and sabotage at nuclear facilities.

Since the objectives of the protection against theft or unauthorised removal or against sabotage may be different for different nuclear facilities and transport, because of e.g. the attractiveness of the material concerned, the vulnerability of a facility and the possible consequences are different, there are different sets of threats. Both internal and external threats have to be taken into account in each set.

As an example, the Design Basis Threat dealing with the theft of nuclear material could be :

- theft of small quantities of nuclear material without being discovered by an employee who usually has access to the nuclear material;
- theft of a significant quantity of nuclear material all at once by an employee who may or may not have access to the nuclear material;
- theft of a significant quantity of nuclear material by outsiders. Several assumptions could be considered according to the size of the team of attackers and their resources.

Likewise, different types of threats could be taken into account to cope with the sabotage of nuclear facilities such as :

- demonstration by a hostile crowd;
- internal threats involving actions taken by insiders acting alone or with others;
- external threats involving actions by small groups of adversaries. Several assumptions could be made when testing the ability of protection systems to counter adversaries of this type. Assistance by an insider may also be considered.

Assumptions could also be 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 might be taken into account.

3.2. Defence in depth

The physical protection system should be mainly based on the principle of defence in depth. INFCIRC/225/Rev.4 defines this as a concept used to design physical protection systems that require an adversary to overcome or circumvent multiples obstacles, either similar or diverse, in order to achieve his objective. More generally and based on the experience gained in the field of safety analysis, this concept could be organised around prevention, management of the event and mitigation (to cope with the radiological consequences of sabotage or to locate and recover missing or stolen nuclear material). For this purpose the system could be designed with several lines of defence including both administrative aspects and technical aspects. The administrative aspects deal with procedures, instructions, sanctions, access control rules, confidentiality rules... The technical aspects are based on multiple barriers fitted with detectors and delaying devices and so on.

The defence in depth concept has to be 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 area generally accessible. These areas have to be included one within another and attention has to be paid that 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 have to provide uniform and uninterrupted protection. In particular, they are designed and built to prevent specified penetration attempts. They are usually 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 have to be equipped with the appropriate intruder detection devices. The Design Basis Threat is a helpful tool for the design and the assessment of physical protection measures and concepts.

The conditions for access must 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 authorisation to the different areas. Access authorisation must also depend on the outcome of individual trustworthiness checks made by the Competent Authority as well as the need to enter areas for work purposes.

The physical protection arrangements should be supported by on-site and off-site response forces. These may be under the responsibility of the licensees or holders of authorisation, and/or the State authorities. In each case the duties and the allocation of responsibility of these response forces must be clearly defined and written down.

A standard example is that the operator has on-site response forces which essentially perform the functions of control and surveillance of the facility and form part of the deterrence. Guards belonging to the on-site response forces 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 response, supplemented by State response forces when needed. Exercises are carried out periodically in order to check the effectiveness of the response force. If possible, exercises to enhance the co-operation between on-site and off-site response forces should take place. Furthermore it is desirable to involve personnel from both management and operating levels in security exercises.

3.3. Quality assurance

The physical protection of nuclear material and nuclear facilities have to be governed by a quality policy and a quality assurance system which conforms to current international standards. Issue of the various documents have to be covered by quality assurance. These quality assurance programmes enable all the activities which affect the physical protection to be carried out in a disciplined manner, notably the confirmation that each task has been completed satisfactorily and that any necessary corrective measures have been taken. All the activities comprising the design, manufacture, implementation, operation and maintenance of the protection and control systems should be covered. As an example the documents to issue under quality assurance system should include documents to grant a licence, licensee's security plan, licensee's contingency plan etc...

3.4. Confidentiality

The physical protection system also has to include appropriate rules of confidentiality. A number of measures need to be taken to ensure appropriate protection of nuclear material and facilities. Sanctions against persons violating confidentiality, including criminalising breaches, should be part of the State's legislative or regulatory system. Consequently, confidentiality serves as a deterrent. Confidentiality also serves as an advanced warning and detecting system in the concept of defence in depth described above. Clearance rules have to be introduced to limit access to sensitive information. In particular, information concerning the complete physical protection concept itself and possible weaknesses in the physical protection system must be highly protected, in order not to indicate the way for potential adversaries.