IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

A comparative approach to nuclear safety and nuclear security

Published on April 21, 2009

doc reference

A comparative approach to nuclear safety and nuclear security

First published on April 21, 2009

IRSN Report 2009/117
ISRN/IRSN-2009/117 FR+EN

doc référence

A comparative approach to nuclear safety and nuclear security
04/2009
•IRSN 2009/117

3/23

IRSN

// in brief

The French Institute for Radiological Protection and Nuclear Safety (IRSN) was founded by Act No.2001-398 of May 9, 2001. Its tasks and organization were defined by Decree No.2002-254 of February 22, 2002. The IRSN is a public establishment that carries out both industrial and commercial activities. It is jointly supervised by the Ministers for Defence, Environment, Industry, Research and Health.

IRSN employs over 1,700 specialists, including engineers, researchers, doctors, agronomists, veterinarians and technicians, experts in nuclear safety and radiological protection and in the control of nuclear and sensitive materials.

The Institute performs expert assessments and conducts research in the following fields:

- nuclear safety;
- safety relative to the transportation of radioactive and fissile materials;
- protection of human health and the environment from ionizing radiation;
- protection and control of nuclear materials;
- protection of facilities and transports dealing with radioactive and fissile materials against malicious acts.

Documents de référence

Editions Property of IRSN
31, avenue de la Division Leclerc
92260 Fontenay aux Roses
Tel.:+33(0)1-58-35-88-88

Website: *www.irsn.org*

IRSN
Odile Lefèvre
BP 17
92262 Fontenay aux Roses cedex
Fax: +33(0)1 58 35 79 62

doc.syn@irsn.fr

A comparative approach to nuclear safety and nuclear security
04/2009
•IRSN 2009/117

Foreword

The Institute for Radiological Protection and Nuclear Safety develops research programs and conducts studies on nuclear and radiological risks. It is responsible for public service initiatives aimed at prevention and provides technical support to the public authorities in charge of ensuring nuclear safety and security, together with radiological protection. In fulfilling these various duties, the Institute is called upon to define its position on certain scientific and technical issues.

In line with its policy of transparency and its desire to make quality information available to all partners and stakeholders for use in developing their own views, the IRSN publishes "Doctrine and Summary" documents, which present the Institute's position on specific subjects.

These documents are drafted by IRSN specialists, with the help of outside experts if necessary. They then undergo a quality assurance validation process.

These texts reflect the Institute's position at the time of publication on its website. It may revise its position in light of scientific progress, regulatory changes or the need for more in-depth discussion to satisfy internal requirements or external requests.

This document may be used and quoted freely on condition that the source and publication date are mentioned.

We welcome your comments. These may be sent to the address given in the margin above and should include the reference to the relevant document.

Jacques Repussard

Director General

www.irsn.org

Documents de référence

IRSN
B.P.17
92262 Fontenay-aux-Roses cedex
Fax:+33 (0)1 58 35 79 62

doc.syn@irsn.fr

doc référence

A comparative approach to nuclear safety and nuclear security
04/2009
•IRSN 2009/117

5/23

//Members of the

Working group

Jean Jalouneix — (Submitter) Nuclear Defense Expertise Division

Patrick Cousinou — Safety of Plants, Laboratories, Transport and Waste Division

Jean Couturier — Reactor Safety Division

Denis Winter — Nuclear Defense Expertise Division

A comparative approach to nuclear safety and nuclear security
04/2009
•IRSN 2009/117

Introduction

The operators in charge of nuclear facilities or activities have to deal with nuclear and radiological risks, which implies implementing two complementary approaches - safety and security - each of which entails specific methods. Targeting the same ultimate purpose, these two approaches must interact to mutually reinforce each other, without compromising one another.

In this report, IRSN presents its reflections on the subject, drawing on its expertise in assessing risks on behalf of the French safety and security authorities, together with the lessons learned from sharing experience at international level.

Contents

1/
Purpose and context

1/1
Definitions

The international community uses the following definitions for nuclear safety and security (taken from the IAEA safety glossary):

- nuclear safety: "The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards." This definition of safety includes radiological protection.
- nuclear security: "The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities."

These definitions show that, while the common aim of safety and security is to protect man and the environment from the effects of ionizing radiation, safety is geared more toward controlling the risks inherent in operating nuclear equipment and facilities or the transportation of radioactive materials, while security is targeted at providing protection against malicious acts that may lead to radiological releases or devastating effects resulting from the use of radioactive or nuclear materials[1].

Every nuclear operator must therefore concern itself as much with the issue of safety as that of security.

[1] Nuclear materials are materials subject to specific regulations within the context of nonproliferation agreements

1/2
Similar risks but different causes

Different events are taken into account depending on each of the two cases. In the case of safety, this involves events that may entail radiological risks as a result of:

- external natural events (earthquakes, serious weather conditions, etc.) or events related to industrial activities;
- or internal events caused by equipment failure (fire, pipe break, loss of electricity supply, etc.) or human error (wrong interpretation of a procedure, incorrectly configured system, etc.).

In the case of security, on the other hand, the feared events are the result of deliberate acts carried out with the intent to cause damage. Such events are therefore based on "intelligent" or "deliberate" actions, carried out for the specific purposes of theft or sabotage, and are likely to involve actions aimed at countering protective measures (by pass of controlled access system or barrier, etc.).

1/3
Transparency and confidentiality

Given the differences in the type of events that must be taken into consideration, the approaches implemented to deal with safety and security differ substantially. The need for transparency was recognized very early on with regard to safety, mainly with a view to sharing experience and ensuring that any incident or accident that might occur in one facility should not be allowed to occur again elsewhere. Transparency in the area of nuclear safety is also explicitly mentioned in France's Nuclear Transparency and Security Act of June 13, 2006. The aim is to inform as wide a public as possible, as well as all the social players involved in nuclear safety and radiological protection. Conversely, and even if the need to share know-how and experience applies also in the case of security, the deliberate and malicious nature of the events taken into account implies a need to develop confidential measures. Protecting information makes it possible to limit the risk of potential saboteurs finding out about the protective measures that they would have to overcome, and also avoids disclosing any possible weakness in a facility's protection system. It is also necessary to prevent knowledge of malicious acts that have actually been perpetrated from leading to similar, copycat, actions.

Security encompasses the concepts of deterrence and confidentiality of protective measures, which do not apply in the case of nuclear safety. In addition, in the case of security and safety alike, constraints related to industrial, commercial or even national defense confidentiality may also have to be dealt with.

1/4
Synergy in dealing with sabotage

The fields covered respectively by safety and security are also distinct to a certain extent. The aim of safety is to protect Man and the environment against radiological risks, whatever the cause (natural events or malicious acts, etc.). The aim of security is to prevent the theft or hijacking of nuclear materials, and to prevent any risk of sabotage targeting nuclear or radioactive materials in facilities or transit. With regard to the risk of theft or hijacking of nuclear materials, security and the related physical protection measures are based on physical monitoring and accountancy of the nuclear materials developed, either at national level or within the framework of international controls. Thus, it is mainly in protecting against the risk of sabotage that the measures implemented in the areas of safety and security complement and reinforce each other.

1/5
A common purpose: protecting Man and the environment

With regard to protection against sabotage, i.e. malicious acts that may result in radiological releases, safety and security share the same common aim to protect human health and the environment. The measures adopted are exactly the same and involve preventive measures and mitigation measures, which are associated with a certain number of fundamental principles (defence-in-depth, graded approach, safety and security culture, etc.), relative to which there is a considerable amount of similarity between safety and security. In both cases, priority is given to the definition of preventive measures.

It should be noted that the principles on which the assessment of a facility's design and its operating procedures is based are the same in the case of both safety and security (robust design, reducing the risks, etc.). Also, the way in which the consequences of an initiating event resulting in a given radiological release are dealt with is the same regardless of whether it is due to a natural event, equipment failure, human error, or a malicious act. Of course, measures implemented to protect against malicious acts are specifically related to physical protection[2], but are also based on the safety measures adopted.

[2] All the physical and organizational measures deployed to prevent malicious acts targeting nuclear materials or facilities.

2/ Organizational principles

2/1 A legislative and regulatory framework relative to safety as well as security

Insofar as regards legislation and regulation, the principles applied are the same in terms of safety and security: the State establishes, in each country, the legislative and regulatory frameworks setting out the prime responsibility of the operators and providing for a control system to ensure compliance with the regulations regarding nuclear facilities and related activities (including transportation). These regulatory frameworks, for both safety and security, cover the following points:

- designation of a competent authority;
- implementation of a licensing system;
- assessment of the provisions implemented by nuclear operators;
- implementation of an inspection system;

and serve to demonstrate compliance with international agreements.

These provisions may depend upon the same legal vector or, as is more often the case, be the subject of laws and regulations specific to the separate fields of safety or security.

2/2 The competent nuclear safety and security authorities

The State designates the authorities with competence in the fields of nuclear safety and nuclear security; a single authority may also

be responsible for both safety and security. Regarding both safety and security, within the framework of a strict liability to perform, the competent authority defines the objectives that must be achieved and, in particular, assesses and controls the activities of nuclear operators, while the State is responsible for certain decisions. In general, they must have the authority, competence and the financial and human resources required to carry out their duties. Moreover, they must be independent of the nuclear operators and other government bodies responsible for promoting nuclear power or the use of radioactive material.

The authorities responsible for safety and security may come under different government bodies (ministries, etc.) in view of the specific nature of the various fields covered by safety and security. Where this is the case, they may have specific organizational structures and may implement different control procedures. Consultation and coordination between the two authorities is essential to avoid any conflict between requirements that may be contradictory. Lastly, the authorities may draw on the support of an independent organization specializing in the fields of security and safety.

2/3
A difference in the distribution of responsibilities between the operators and the State

2/3/1
Prime responsibility of operators

Nuclear operators have prime responsibility for the safety and security of their facilities and under no circumstances whatsoever can this responsibility be delegated. This prime responsibility is based on the same principle in the area of safety and security alike, i.e. the operator is best placed to identify the risks associated with its activities and to detect any deviation in relation to safety or security requirements and take appropriate corrective action. In this context, the operators:

- design, implement and maintain technical solutions designed to achieve satisfactory standards of safety and security and, in particular, to comply with the regulatory requirements;
- implement a quality system in the fields of safety and security and, in particular, ensure first level of control;

– ensure that their personnel have the required skill, mainly by providing the appropriate training;

– inform the competent authority of any event likely to compromise the safety or security of their facilities;

if necessary, implement compensatory measures in order to attain satisfactory safety and security standards.

2/3/2
A different involvement of the State

The State sees to it that the responsibilities of each party (operators, authorities, etc.) are clearly defined insofar as concerns safety and security. Protection against malicious acts, however, requires a different approach as well as broader and more direct involvement of the State in security than in safety.

An operator cannot protect a site or a facility against every form of malicious action on its own, and the State plays a decisive role in security matters:

- Firstly, the State is directly involved in gathering intelligence and assessing the risk of malicious action that may impact on nuclear facilities and radioactive materials. Since such risk changes all the time, the State must check that the security measures are constantly adapted to the current situation;
- The State defines the design basis threats that must be used to design and assess the physical protection systems;
- The State also plays a determining role in the response to be given to counteract certain malicious acts by means of intervention by the law enforcement agencies (police or the Gendarmerie);
- Managing a crisis resulting from a malicious act also requires input from a greater number of State bodies than managing a crisis related purely to safety issues. For example, law enforcement agencies, the judicial authorities (even though the latter may be involved to a lesser extent in the event of a safety crisis) and mine-clearing services, may all be involved;
- Lastly, the State defines the rules relative to confidentiality and the protection of information and sets up a screening system for everyone requiring access to sensitive activities or information.

As regards the safe transportation of radioactive materials, the requirements set out in international treaties and EU directives

necessitate compliance with harmonized objectives (without which international and multimodal transportation would be problematical), together, where appropriate, with specific provisions at national level. International Conventions relative to nuclear safety and security, aiming to develop common principles, take a similar approach.

2/4 Safety culture and security culture

Every nuclear operator develops a safety culture and a security culture within the company. Safety culture and security culture are based on very similar principles (an explicit commitment made by Management of every operator to promote these cultures, provide training and raise awareness, etc.). Both are evident in three key areas. The first concerns the policy that the State wants to implement. The second involves the organization set up by the different operators. The third concerns the attitude of the personnel.

The fact that a large number of State bodies are involved in security matters implies the need to organize communication, information and exchange systems enabling the bodies concerned to understand and complement each other in dealing with sensitive information.

As regards the individual employees concerned by safety culture, they are mainly required to share information with a view to ensuring dialogue, vigilance and improvement. Security culture also entails information sharing, albeit limited to authorized personnel. Furthermore, although security issues concern everyone, only certain people are in charge of applying security requirements and some information must be protected. The two cultures require a prudent and questioning attitude, and, when needed, an immediate response to deal with certain events. Nonetheless, these measures, although similar in their expression, cover quite different areas of application in practice.

The two cultures must not be pitted against each other and neither one should have ascendancy over the other. However, it is not possible to merge the two cultures into one. They must co-exist, mutually consolidating and enhancing each other. Synergy between safety and security and between the cultures underlying them should be developed and encouraged.

3/ Principles for the application of safety and security approaches

Insofar as regards both the design and the operation of nuclear facilities, a number of similarities and differences appear in the application of safety and security principles.

In general, nuclear safety and security provisions are examined at as early a stage as possible in the design of nuclear facility. Designing nuclear equipment, facilities or transportation packages is, in fact, subject to restrictive safety and security requirements, especially relative to the regulation. A certain number of general safety principles have an especially strong impact on the overall architecture of a system, its level of redundancy or diversification and on system or equipment layout. Similarly the general security principles may impact on the general layout of the site buildings, their design (physical divisions, etc.), and on the building and structural design.

It should be pointed out that the different types of nuclear facility (nuclear power plants, plants used for training and research, fuel cycle processing facilities, fuel or waste storage or disposal facilities) have specific features that must be taken into account at the design stage. For example, in the case of research reactors and, where appropriate, power reactors, the risks related to access to the reactor buildings when they are under operation must be taken into consideration when defining operating procedures with a view to

safety and security. In addition, the risks linked to experimental units must be dealt with in the design and safety analysis for such units (especially by examining the events liable to occur at such units, given their operating rules), as well as in the analysis of measures to prevent malicious acts (for example, damage to the reactor core caused by wrongful use of the facility).

In the case of power reactors, the large amount of energy released when in operation, and even during outage and, depending on the case, the high pressure contained within certain equipment, is one of the features that must be taken into account.

In the case of transportation packages, the robust design required for safety purposes serves to protect against malicious acts, together with special measures if required.

3/1 Similar design principles

Certain design principles apply in exactly the same way insofar as regards safety and security.

3/1/1 The graded approach

One of the fundamental principles retained during design of a facility, both for safety and security, is the graded approach. This approach entails analyzing the risks to Man and the environment in terms of the potential consequences of accidents or malicious acts, with a view to defining appropriate and proportional measures in the fields of prevention and mitigation.

3/1/2 Defence-in-depth

Defence-in-depth is another general safety and security principle used at design level. However, slightly different methods area used to applying this fundamental principle in each of the two cases. A diverse series of measures of different nature, both physical and organizational, are implemented in a balance way to counter the risk of malicious action and the risk of accident. The physical safety defence lines are often directly integrated in the plant itself (systems, circuits, components, etc.), while security measures apply to the entire site, or beyond.

It should nonetheless be noted that security is based on a first line of defence consisting of measures designed to deter potential

attackers. Deterrence means all the measures that can be implemented with a view to discouraging attackers from carrying out a malicious act. For example, this means making it difficult to access information required to mount an attack, highlighting the penalties applicable to potential attackers, and setting up monitoring and intelligence-gathering systems. The safety approach is not based on this concept.

Furthermore, insofar as regards defence-in-depth, the safety approach takes a deterministic approach based on analysis of potential events, generally supplemented by probabilistic assessments. Insofar as regards security, the approach taken is basically deterministic since it is extremely difficult to quantify malicious acts perpetrated by people in probabilistic terms. The design basis threats are the equivalent of the postulated events defined in the safety analysis.

3/1/3
Synergy between safety and security

In addition, certain design principles relative to safety considerably improve the effectiveness of the protection of a facility with regard to malicious acts. Thus, the safety approach largely depends on satisfying the "single failure criterion". This criterion is used to ensure that the facility is designed to perform certain functions even if a system or piece of equipment within a system fails or is unavailable. In particular, thanks to application of this criterion, an attacker would have to damage several targets in the facility in order to cause an accident situation. Furthermore, the attacker's task may be hampered by the implementation of redundancy, diversification, physical or geographical segregations integrated in the facility design for safety purposes. These technical features reduce the relative sensitivity of each item of equipment and mitigate the impact of sabotage perpetrated by people with inadequate means or limited time to carry out their action.

In addition, the designers of new-generation nuclear units use the principle that an aggression in the meaning of the safety analysis, such as fire, explosion or flooding, etc., cannot result in an accident situation (reactivity insertion accidents, break in the residual heat removal system, etc.). The designers are thus expected to integrate provisions which, in certain cases, serve to improve security for these units.

3/2
Similar operating principles

The key principles governing operation of nuclear facilities and associated equipment and transportation systems are identical as regards safety and security.

3/2/1
The same requirement regarding constant monitoring

The operator has to be fully aware at all times of every aspect of the facility, including the systems used both for safety and security purposes, with rigorous monitoring of equipment availability, any modifications to or changes affecting the facility, together with any temporary palliative measures implemented, etc.

Safety and security systems availability have to be checked regularly and preventive maintenance performed. If necessary, compensatory measures have to be taken in the event that any system is found to be unavailable.

These operating provisions, aimed at checking facility compliance and availability, help to reduce the risk of malicious damage caused by surreptitious degradation of the facility's safety level.

3/2/2
The same need to take account of feedback

Events concerning equipment failure, identified anomalies, human error, and sabotage attempts are recorded and processed mainly with a view to prevent them from reoccurring. However, identifying the malicious origin of an event precisely may be a delicate matter. In all cases, the operator must analyze every incident, whether related to safety or security, and include an appropriate analysis of any aspects related to human factors.

The lessons learned from incidents occurring at the facility or at other similar facilities can be used to improve safety and protection against malicious acts.

Feedback on operating must gathered and processed on a regular basis in the areas of both safety and security.

3/2/3
The same need to update the baseline

In order to maintain a suitable level of safety and security, it is vital to periodically review facility compliance and regularly update the

systems and rules and, more generally, the facility's baseline, taking into account feedback and evolutions in scientific and technical knowledge, and in the regulations relative to safety and security. Insofar as regards the latter, in the area of security, it is essential to periodically update the baseline of threats and the related studies.

3/2/4
Sharing good practices is more restricted in the area of security

Notwithstanding, the daily operation of a facility draws on the rules of good practice, entailing different conditions of implementation in the areas of safety and security.

Thus, insofar as regards safety, personnel are expected to share information as widely as possible. This requirement applies equally in the area of security, but with the proviso that the rules regarding confidentiality are not violated. Less restricted sharing may apply solely in the case of the methods used.

It should nonetheless be noted that different population groups (operating personnel and applied scientists, for example) work side by side at facilities set up for training operators or for research purposes (the use of neutrons for fundamental research, R&D on fuel cycle processes, etc.). These population groups generally come from different entities with different cultures (operators, laboratories, universities, etc.), with potential conflicts of interests. Given this, in the areas of safety and security alike, particular care must be taken when sharing information between these different population groups.
Similarly, the fact that operators use external service providers implies a need to establish appropriate measures in the area of safety, where any loss of vigilance can be identified, especially in the event of incident, as well as in the area of security, where the operator in charge is required to control such service providers.

3/2/5
The need to deal with the respective requirements of safety and security

In addition, some operating arrangements related to safety or security requirements may potentially be contradictory. For example, access and operations by emergency teams (fire-fighting, etc.) must be facilitated for safety reasons, but access to certain areas of the facility or to transportation systems must be permanently controlled. Also, certain security-sensitive zones are

subject to special protection systems (ID badges, etc.), but it must be possible to evacuate personnel from these areas in case of fire or criticality emergency. Complying with safety procedures may increase transportation times in order to adhere to a principle of prudence, whereas security requirements may stipulate reducing transportation times to a minimum.

Another example relates to nuclear materials monitoring. In the case of safety and security, it is necessary to know the quantities of the materials held as precisely as possible, but the safety rules require maintaining a conservative margin, mainly to guard against criticality risks, whereas the security approach is concerned to account as precisely as possible for the actual quantity of nuclear materials held in order to guard against the risk of diversion.

The operating procedures and rules must, therefore, take account of the respective safety and security requirements and implement measures that are satisfactory in terms of safety and security.

It should be noted that physical protection must take account of safety requirements such as accessibility to equipment for the purposes of in-service monitoring and maintenance, together with requirements relative to safety in the workplace or to the effectiveness of an operation, aimed at facilitating the evacuation of or access to premises in the event of an incident or accident.

3/3 Similar emergency management

Preparation for managing a downgraded situation at the facility concerns both safety and security.

3/3/1 Developing emergency and contingency plans

The operators and the public authorities draw up emergency response plans to limit, in a downgraded situation, any releases and their impact. These plans must cover equipment failure and human error, as well as malicious acts. Facility protection plans are designed, in terms of security, to stop malicious attack and secure the premises so that the operators can initiate mitigation operations. Protection plans are thus implemented prior to emergency response plans related to safety and are a line of defence specifically aimed at preventing malicious acts. It is especially important for the people in charge of safety and those in charge of security to liaise in drawing up these plans (protection and emergency plans) and that they are complementary and

consistent. There is also a need that arrangements be made to coordinate emergency response operations. This approach applies to facilities and also to transportation.

3/3/2
Carrying out exercises

It is essential to carry out exercises at regular intervals. Safety and security exercises have similar aims; they both involve ascertaining that the plans developed by the operators and public authorities are adequate and are necessary to train various emergency response services specialized in ensuring safety or security.

During safety or security exercises, the following points must, in particular, be tested:

- the overall functioning of the entire decision-making chain involving the public authorities and the operator;
- coordination between the different entities involved, to ensure coherent action;
- the response times and the means deployed for emergency action;
- the responsiveness of the people involved in decision-making and implementation.

In the two fields, different levels of exercises are organized to achieve this:

- local exercises, organized by the operator, and not involving the public authorities. This includes alert or mobilization exercises, specific procedures tests or emergency response team exercises;
- local exercises, organized by the operator, with the participation of local public authorities, especially to test the latter's alert and mobilization procedures and how well they can coordinate with the operator;
- national exercises involving all the stakeholders (operators and the various public authority services, at local and national level for each).

It is also essential to carry out general exercises combining safety and security aspects so that coordination between all those involved in the two areas can be tested (case of a group of attackers entering a facility and causing an accident).

3/4

Activities subject to quality requirements

Activities related to the safety or security of a facility or transportation system are subject to quality requirements. Consequently, operators set up organizations which make no distinction between safety principles and security principles, and in which the management of the involved entities are implicated in a similar manner. These organizations serve to assess the overall situation concerning safety and that concerning security in a distinct manner, for example, based on monitoring appropriate performance indicators, in such as way as to define possibilities for improvement in each area.

Deploying a quality management system relies on information sharing, by means of feedback, for example. Nonetheless, information sharing implies specific measures insofar as security is concerned, especially for managing classified information.

4/ Conclusion

Nuclear safety and nuclear security have many similarities in terms of aims and approach, and are mutually complementary in the field of protection against the risk of sabotage. Nonetheless, each has specific characteristics which imply different operational requirements:

- greater and more direct involvement of the State in the area of security than in safety;
- a certain confidentiality regarding security issues.

A coordinated approach serves to promote synergy between safety and security, ensuring protection against the risk of sabotage and, if necessary, managing contradictory requirements.

In addition, safety and security requirements must be taken into account as far upstream in the design of nuclear facilities and related activities.

Nonetheless, it should be emphasized that, given the wide diversity of nuclear activities and facilities (power reactors, reactors built for training or research, fuel cycle facilities, etc.), all the players involved (public authorities, designers and operators, etc.) must adapt the safety and security measures to each individual case according to the specific characteristics and risks inherent in each.