Compatibility of Safety and Security

J. Repussard
General Director of IRSN, Fontenay-aux-Roses, France
jacques.repussard@irsn.fr

1. Purpose and context

1.1 Definitions

The international community uses the following definitions for nuclear safety and security (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.*"
- (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 safety essentially targets at protecting the health of man and the environment from the effects of ionizing radiation, and security essentially targets at providing protection against malicious actions that may entail radiological releases or the devastating effects resulting from the use of nuclear materials with also the final aim to protect the man and the environment.

1.2 Different approaches

The events taken into account differ depending on the two cases. With regard to safety, the feared failures that may entail radiological risks are from either natural type events (such as earthquakes, major climatic phenomena, etc...), or hardware failures or installation internal type events (fire, pipe breakage, loss of electric power supply, etc...), or human failures (wrong interpretation of procedure, wrong alignment of circuits, etc...). With regard to security, the feared events result from malicious acts carried out with the intent to cause damage. These events are therefore based on "intelligent" or "deliberate" actions carried out purposefully for theft or sabotage and liable to counter protective measures.

1.3 Transparency and confidentiality.

The result from this difference in the nature of events taken into account to approach this problem differs noticeably between safety and security. The need for transparency is revealed in the very early stages with regard to safety, in particular to share experience feedback and to prevent incidents or accidents that occurred in one installation from occuring in another. Conversely, and even if the need to share know how and experience from the previous events exist also for security, the voluntary and malicious nature of the event to take into account incites the setting up of confidential measures. Information protection in fact makes it possible to prevent potentially malicious minded people finding out the protective measures they would have to deal with or even avoid disclosing a possible weakness in a facility. It is also necessary to avoid that the knowledge of perpetrated malevolent actions could lead to similar events.

1.4 A synergy in the field of sabotage

The field covered respectively by safety and security are also partially distinct. Safety is targeted at protecting man and the environment with regard to radiological risk and naturally covers all aspects related to radiation protection. Security covers prevention with regard to theft and hijacking of nuclear material, and prevention of any risk of sabotage that may target nuclear installations or radioactive material. With regard to the risk of theft or hijacking of nuclear materials, security is based on follow up and accountability of nuclear material developed either at national level or within the framework of international controls. Therefore, it is essentially in the protection with regard to the risk of sabotage that safety and security are found in a common field and are mutually complementary.

1.5 A common aim: the protection of man and environment

With regard to protection against sabotage, i.e. malicious acts that may entail radiological releases, safety and security share the same common aim to protect the health of man and the environment. The method is also identical and includes measures of prevention of risks and limitation of the consequences. In both cases, priority is given to prevention. A certain number of fundamental principles are associated to the above, in which there is a considerable amount of similarity between safety and security.

Moreover, it is essential to note that the acceptable risk is the same whether the initiating event of a given radiological release is following a natural event, equipment failure or a malicious act. The steps taken to provide protection against a malicious act naturally incorporate specific features related to physical protection, but are also based on intrinsic provisions concerning safety.

2. Organizational principles

2.1 A legislative and regulatory framework in safety as well as in security

In this field, the principles are the same in terms of safety and security. The State must set up appropriate legislative and regulatory frameworks to ensure control of installations and activities that, on the one hand, generate a radiological risk and, on the other hand, require security provisions. These regulatory frameworks for both safety and security make it possible to:

- implement an authorization system to carry out the above-mentioned activities,
- assess provisions implemented by nuclear operators,
- implement an inspection system,
- observe international commitments,
- designate a competent authority.

These provisions may depend upon the same legal vector or, which is more frequent, be the subject of laws and regulations specific to each of the safety and security fields.

2.2 One or two competent authorities

The State must designate competent authorities both in the safety and security fields. These authorities are responsible for the implementation of the regulatory provisions and must be accredited with the authority, competence and the financial and human resources required to accomplish their tasks. Moreover, they must be independent from nuclear operators and other government entities responsible for promoting nuclear power or the use of radioactive material.

The competent authority must define, for both safety and security, the goals to attain and perform a nuclear operator activity control and assessment mission.

A single authority may be responsible for safety and security, but these authorities may depend on different government entities due to the different fields covered by safety and security. In the latter case, they could have specific structures and means of control of a different type. A consultation and coordination mechanism is required between the two authorities to ensure efficient protection with regard to the risk of sabotage and to prevent conflicts between regulatory requirements that may be contradictory.

2.3 A difference in the distribution of responsibilities between the operators and the state

2.3.1 Prime responsibility of operators

Nuclear operators are the prime accountables for the safety and security of their installations and in no case whatsoever can this responsibility be delegated. This prime responsibility is based on the same safety and security principle, i.e. the operator is the person in the best position to identify the risks associated with his activities and to detect any deviations in relation to safety or security requirements. In this context, the operators:

- design, implement and maintain technical solutions making it possible to satisfy regulatory requirements ,
- ensure first level control,
- verify the skills and appropriate training of personnel,
- inform the competent authority of any event likely to affect the safety or security of their installations,
- implement a quality system in the safety and security fields.

2.3.2 A different involvement of the State

The State must verify that the responsibilities of each and everyone are clearly identified and accepted, both in the safety and in the security domains. Protection with regard to malicious acts requires, however, a different positioning and larger and more direct involvement of the State in security than in safety.

The operator alone cannot ensure protection of a site or an installation, and the State plays a more determining role in numerous aspects in relation to security. First of all, the State is directly involved in the assessment of malicious action risk that may affect nuclear installations and radioactive material. This risk is moving with the time and the State has to check that the security measures are continuously suited to the situation. Consequently, the State defines the design basis threats to take into account to design and assess 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 gendarmerie). Management of a crisis linked with malicious acts also demands the contribution of a greater number of State bodies than managing a crisis purely dependent on safety. In additions to the services already concerned by the safety crisis, the following services are also concerned, for example: law enforcement agencies, mine removal services, judicial authorities (even if the latter may intervene to a lesser degree during a safety crisis). Finally, the State has also to define rules for confidentiality and information protection.

2.4 Safety culture and security culture

Safety culture and security culture are based on very similar principles. Both are involved in three main fields. The first field concerns the policy the State wants to implement. The second is the organization set up in each organization involved. The third concerns the attitude of individuals. Whether safety or security is concerned, the same types of organizations are involved and the same types of requirements are found in the setting up of either the safety or the security culture.

However, the security culture must integrate deterrence and confidentiality notions that do not exist in the safety culture. Furthermore, with regard to the sharing of responsibility and the confidentiality of information, the development of a security culture cannot be conceived without the major participation of the State. The involvement of a great number of State entities in security matters imposes a certain number of structures and communication, information and exchange systems so that the organizations involved understand and complete each other.

With regard to individuals involved in safety culture, sharing of information in the general concern for transparency and dialogue is demanded. The security culture requires that individuals only communicate information to other authorized people. Furthermore, security may involve all people, but only some are more especially in charge of applying security requirements and some information must be protected. The two cultures require a prudent and interrogative attitude, and, if needed, a very fast reaction in relation to some events. However, these measures, similar in their expression cover in practice differences in their application.

The two cultures must not oppose each other and one of them must not take more importance than the other. However, it cannot be envisaged to melt the two cultures into one. They must however co-exist, back each other up and mutually enhance each other. All the synergy between safety and security and between the cultures supporting them must be developed and encouraged.

3. Application principles of safety and security approaches

When considering the different design and operating situations of nuclear installations, similarities and differences appear in the application of the safety and security approaches.

Generally speaking, the sizing of a new installation is governed to a great extent by safety requirements: thus, it is first of all necessary to take into account all provisions related to safety once the design of the installation is defined, to complete it, amend it or modify it. In this early phase, the security approach is not necessarily implemented as the associated requirements have less impact on the general installation of structures, circuits or equipment. The same applies during the definition of civil engineering work or the layout plan. Thus, the safety approach is of a more structuring nature during design than that of security.

3.1 A similarity in design provisions

Certain design principles apply identically.

3.1.1 The graded approach

One of the fundamental principles retained during design of an installation, both for safety and security, is the graded approach. This consists of analyzing the risk and its potential consequences with a view to defining measures appropriate and proportional to the estimated risk. To this end, the safety approach uses probabilistic or deterministic methods and defines the accident study rules. In the security domain, the approach is essentially deterministic as it is very difficult to quantify in a probabilistic manner the malicious type human actions, and the design basis threats constitute the equivalent of accident study rules.

3.1.2 The defense in depth

The defense in depth is also a general safety and security principle used at design level. However, the methods of application of this fundamental principle slightly differ in the two cases. Consecutive barriers, whether physical or organizational are set up to prevent the risk of aggression and the risk of an accident. The physical safety defense lines are very often directly involved in the process, whereas those implemented for security apply to the entire site.

Emphasis could be put on the fact that security is based on a first line of defense, consisting of deterrence provisions. Deterrence means all that can be implemented with a view to discouraging aggressors from carrying out a malicious act. For example, this concerns making access difficult to information required for the aggression, highlighting the penalties applicable to a potential aggressor, setting up of monitoring and collection systems for intelligence. The safety approach is not based on this concept.

3.1.3 A safety and security synergy

In addition, certain design principles relative to safety considerably reinforce the efficiency of the protection of an installation with regard to a malicious act. Thus, the safety approach imposes to respect the single failure criterion. This criterion allows that the installation is designed in order to provide certain functions even if one of the equipment of the system is failing. In particular, through the application of this criterion, aggressors must attain several targets in the installation in order to provoke an accidental situation.

Furthermore, the task of the aggressors is hintered by the implementation of redundancy, diversification, physical or geographical separations, used for safety purposes to design an installation. For example, safety imposes that certain functions are performed by two independent systems in which one can perform the function needed when the other is failed or unavailable. This technical feature reduces the relative sensitivity of each item of equipment and the impact of sabotage perpetrated by people insufficiently prepared or with limited means or time to carry out their action.

3.2 A similarity in operating provisions

The major principles governing operation of the installation are identical with regard to safety and security.

3.2.1 A same need to treat the experience feedback

The availability of safety and security systems is permanently ensured. Maintenance operations are carried out on a regular basis and compensatory measures are taken when a safety or protection provision is unavailable.

Events concerning equipment failure, identified anomalies, human errors, and sabotage attempts are recorded and processed appropriately. However, it may be delicate to identify precisely the malicious origin of an event. In all cases, each incident is analyzed, whether related to safety or security.

The information gained from identified incidents in the installation or in other installations of equivalent design or operation makes it possible to improve its safety or its protection.

3.2.2 A same need to update the basis rules

This experience feedback must also be performed periodically in both domains. In order to maintain an appropriate level of safety and security, it is necessary to periodically re-examine the status of the installation and update devices and rules on a regular basis and, more generally, the baseline of the installation taking into account changes to techniques, gained experiences, knowledge and threats in particular. However, in the security field, there is also a need to update the design basis threat.

3.2.3 An exchange of good practice more constrained in security

However, the daily operation of an installation calls upon good practice rules, of which the conditions of implementations differ for safety and security.

Thus for safety, the operator's personnel are mainly requested to endeavor to share information as far as possible. Exchange is much more limited in the security domain and, outside the circle of people on a need to know basis, the information must be limited to exchanges on methods used.

3.2.4 Need for Managing conflicts between safety and security

In addition, some operating arrangements that depend on safety or security requirements may potentially be contradictory. For example, the access and the intervention of emergency teams (fire fighting, etc…) must be facilitated for safety reasons, but particular access to the installation must be permanently controlled. In addition, certain sensitive zones for security reasons are subject to special protection systems (badge systems, etc...), but it must be possible to evacuate personnel from these areas urgently in case of fire or criticality risks. The respect of safety procedures can result in slowing down a transport whereas the needs for security can require minimizing the duration of the transport.

Consequently, the operating rules and procedures must take into account the respective safety or security requirements and implement provisions satisfying both fields.

3.3 A similarity in emergency management

Preparation for downgraded situation management of the installation concerns both safety and security.

3.3.1 Elaboration of emergency and contingency plans

Both operators as well as public authorities are requested to elaborate plans to be prepared to prevent a risk and limit its consequences. The plans to design for safety reasons must cover both human errors and equipment failure fields, as well as those of malicious acts. On the other hand, the protection plans for the installation are designed to prevent aggressions and secure the location before any mitigation actions. The implementation of contingency plans is upstream emergency plans concerning safety and constitutes a specific line of defense to manage a malevolent act. There is an obligation for these plans to be complementary and coherent. Therefore, it is also necessary to ensure that perfect coordination is organized between the different participants as scheduled in this emergency planning.

3.3.2 Performance of exercises

Therefore, it is essential to carry out regularly exercises. The purpose of these safety or security exercises is similar. The aim is to assess and validate the plans prepared by the operators and the public authorities, as well as to train the different participants on how to react in such a situation.

It is also necessary to test during safety or security exercises:

- the global operation of the entire decision chain of the public authorities and the operator,
- the coordination between the different intervening entities and the general consistency of the provisions,
- the intervention time delays and means,
- the reactivity of decision-making and corresponding actions to be undertaken.

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

- local exercises organized by the operator without any participation of the public authorities. This may concern an alert, mobilization, specific test procedure or work team exercise;
- local exercises, organized by the operator, with the participation of local public authorities, especially to test alerts, mobilization procedures of the latter indicated and related coordination with the operator;
- national exercises.

Obviously, it is necessary to carry out global exercises in order to confirm the coordination of the entire safety and security organization. For example, an exercise scenario may simulate a group of aggressors who enter an installation and who endeavor to trigger an accident. In the first stage, crisis management will be focused on its security effects, but very quickly, it will be necessary to envisage safety problems related to this aggression.

3.4 Activities managed by quality system

Activities related to safety or security of an installation are managed by a quality management system.

This type of system does not differ from the standpoint of principles, depending on safety and security and takes them into account at the same level.

In particular, the management commitment in the implementation of a quality management system applies in an equivalent manner to both safety and security fields.

However, certain activities address more especially one or the other of these fields. For example, the management of classified information only concerns security. On the other hand, the obligation to carry out exchanges of information will be taken into account in the quality management system to improve installation safety.

It may also be found to be necessary to set result indicators, which depend purely on safety or security. In fact, it is necessary that the management of a company be capable of measuring separately the installation global status of safety or security and to define the progress focuses in each of these fields.

4. Conclusions

Nuclear safety and nuclear security present large similarities in their aim as in their methods and are mutually complementary in the field of protection with regard to the risk of sabotage. However they show specific attributes in certain areas which leads to differences in their implementation.

The large diversity of nuclear activities and facilities (power reactors, research reactors, nuclear fuel facilities, transport,…) needs to adapt, on a case by case basis, safety and security provisions to fit with the characteristics and the risks of each one.

In this context, research reactors present the particularity that two types of population cohabit: the operating team and the research team. A well shared safety culture and security culture is consequently, in this area more than in another one, the guarantee of a safe and secure operation of these facilities.