
Complementarity between Safety and Physical Protection in the Protection against Acts of Sabotage of Nuclear Facilities

Robert Venot

Institut de Radioprotection et de Sûreté Nucléaire
77-83, avenue du Général-de-Gaulle
92140 Clamart (France)

Abstract: For the objectives of nuclear safety, various sets of accidental sequences are set up and taken into account in safety studies of a facility. The aim of these studies is to give confidence that its operation presents a sufficiently low-level risk, deemed acceptable for personnel, the public and the environment. Accidental sequences could come from failure of a piece of equipment, internal hazards (missiles from inside the containment area, results of piping breaks, turbogenerator bursting, load dropping, fire, internal flooding etc...) or external hazards (earthquake, aircraft crashes, industrial environment, floods etc). Another set of accidental sequences could occur when considering the State's Design Basis Threat and it has to be checked if these sequences are already covered by the nuclear safety case or if the operator has to take additional provisions to protect the facility. Many of the provisions taken to cope with accidental sequences coming from the failures and hazards above could be useful to cope with accidental sequences coming from sabotage. Some of the sequences coming from these other sets of accidental sequences, which are not studied as safety concerns, have to be analysed. Potential conflicting requirements, resulting from nuclear safety and physical protection considerations, should be carefully analysed to ensure that they do not jeopardize nuclear safety or nuclear security, including emergency conditions. More generally it is shown that there are fundamental principles, most of them must be present in the safety field and the physical protection field namely the defence in depth concept. This paper shows, with various examples how the nuclear safety provisions contribute significantly to the protection against sabotage of nuclear facilities.

1. INTRODUCTION

Nuclear facilities present a specific risk in that they all contain, by definition, more or less substantial quantities of radioactive products. These can endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances.

Nuclear safety results from a set of technical and organizational measures taken at all stages in the life of a facility to ensure that its operation and, more generally speaking, its very existence, present a sufficiently low-level risk as to be deemed acceptable for personnel, the public and the environment.

It has to be shown that all types of accidents considered credible have been taken into account and are covered by the accident studies performed and that the systems provided to prevent their development or mitigate their consequences effectively enable the nuclear safety objectives to be achieved.

An act of sabotage involving nuclear material or against a nuclear facility could create a radiological hazard to the personnel, and a potential radioactive release to the public and the environment. If needed, physical protection provisions have to supplement effectively the safety system to cope with sabotage.

Accidental sequences could come from dysfunction or failure of a piece of equipment, internal hazards (missiles from inside the containment, results of piping breaks, turbogenerator bursting, load dropping, fire, internal flooding etc...) or external hazards (earthquake, aircraft crashes, industrial environment, floods etc). Another set of accidental sequences could occur when considering sabotage coming from the

State's Design Basis Threat and it has to be checked if these sequences are already covered by the safety case or if the operator has to take additional provisions to protect the facility.

2. SYNERGIES BETWEEN SAFETY PROVISIONS AND PHYSICAL PROTECTION PROVISIONS

The provisions taken for nuclear safety purposes may also serve in the field of physical protection.

2.1 Fundamental principles

Several fundamental principles are applicable to both nuclear safety and physical protection. They deal with the general organisation. One of them relates to the regulatory framework which affirms the prime responsibility of the operators both in nuclear safety and in physical protection. The safety culture as well as the security culture could be mentioned. The defence in depth is a general approach applicable both in nuclear safety and in physical protection. This concept is based on the precautions taken at the design stage to prevent an undesirable event, the management of the event if it occurs, and finally the limitation of the consequences if, despite everything, such an event occurs. The same goes for quality assurance and contingency plans. A table is provided in the appendix showing these principles.

2.2 Characteristics of components and layout

The provisions included under nuclear safety purposes help to impose the protection of the nuclear facility against sabotage. Because of the single failure criterion, the perpetrators have to act on several components of the facility. Their task is made more difficult when the components are diversified, physically separated, or geographically separated.

2.2.1 Single failure criterion

In view of their importance, systems operating in normal conditions or actuated during incidents or accidents must have a very high level of reliability. But a reliability study is extremely difficult to carry out at the design stage of a facility, thus a deterministic approach, which is perhaps more approximate but easier to use at this stage is preferred. This is the "single failure criterion" which can be summarized as follows: systems involved in nuclear safety must be able to fulfil their duty in an adequate manner even in the case of failure of any of their components.

The application of this criterion is simple: it is postulated when a system is required, one component of this system is defective. The supposedly defective component will be the one with the most serious consequences. There are several ways of applying this criterion. One of them consists of doubling the functions and the components. Some countries have opted for the installation of triple or quadruple systems, each of them with the capacity to ensure two-thirds or half of the required functions. These are known as 3 or 4 "train", "line" or "channel" systems.

The layout and installation rules are very strict in order to prevent a single event from affecting components on both lines. Redundant system lines have to be installed on different, completely separate premises. This is what is known as geographic separation. In the vicinity of an installation which is unique, notably the control room, to which redundant components must be connected, geographical separation is no longer possible. Physical separation by means of suitable walls is then required.

Internal failures concerning several components are much more difficult to identify and prevent. These failures concern errors in design, manufacturing or maintenance, which are liable to affect several components when their operation is required. They therefore concern the general quality of the plant or its operation. One way of combating these failures is diversification.

2.2.2 Redundancy

The principle of redundancy is used as a basis to guarantee that a function will be assured under all circumstances, notably in the case of a technical failure. This, in fact, relates to a technical facility based on the setting up of two identical pieces of equipment where only one would be sufficient. One of these pieces alone guarantees the performance of the function concerned, whilst the other one is held in reserve. This piece of equipment will be activated as soon as a failure appears on the piece of equipment in operation.

For instance two pumps are sometimes set up side by side. One of these pumps is in operation, whilst the other one is stopped and held in reserve. The pump in operation is itself capable of guaranteeing the circulation of the fluid. In the case where there is a technical failure on the pump in operation, the pump held in reserve is then activated.

This technical provision is adopted as a nuclear safety measure to account for a possible technical failure in a piece of equipment. Even if this failure is not caused by a technical failure, for example due to a sabotage, the piece of equipment held in reserve will itself guarantee continuous operation of the function concerned. As a result, a perpetrator must first identify the redundant components, secondly, take action on each of these in order to stop the function.

This technical provision reduces the relative sensitivity of each component and the possible impact of sabotage perpetrated by persons who are not sufficiently prepared for their action, or by persons with limited time and with limited resources.

2.2.3 Diversification

To reinforce the effectiveness of the principle of redundancy, the designers have, in certain cases, required that certain components be created based on diversified technology. Thus the operation of one of the cooling system pumps is put into motion using an electric motor whilst the associated redundant pump is put into motion using a steam turbine.

This provision of diversification improves protection against sabotage, because it demands the planning of the means of destruction adapted to this diversification.

2.2.4 Physical separation

With regard to nuclear safety, the designers consider that the neighbouring components could be damaged by the failure of one of them. For example, the debris which results from the explosion of a component might damage its surrounding components. Thus, a function designed on the basis of the principle of redundancy mentioned above, could be compromised if the constituent redundant components are located near to each other. The principle of redundancy will then be ineffective. In the same way, other functions could be compromised if the damaged components belong to different functions.

The fitting of physical separation screens between each of these components protects them from each other with regard to any debris that they might produce as well as with regard to any debris they might receive. A slight improvement in the effectiveness of these screens consists of placing the redundant components in distinct locations. The walls of these areas themselves form physical separation screens.

These protective screens contribute towards physical protection. In fact, to succeed in an aggression, their presence must be noted by the use of additional means either to circumvent or to destroy them. The implementation of these means may require better preparation and increase the duration and the resources necessary to accomplish the sabotage. Most of the time, these screens are made up of the walls of the areas in which the components are located. The effectiveness of the physical protection could easily be reinforced by reducing the communication passages between these areas to a strict minimum. Some of them could be usefully equipped with doors fitted as a part of the physical protection system.

2.2.5 Geographical separation

Physical separation can be further improved by adding a geographical separation. Thus, the redundant components will be separated from each other by several tens of meters, including different floors of the same building, or even in different buildings. For example, the emergency power supplies are installed in distinct buildings located at either ends of the main buildings.

This facility layout is adopted as a nuclear safety measure to take into account external or internal hazards such as aircraft crashes, explosions of neighbouring industrial installations, floods etc.

In relation to physical protection, interest in this facility layout is much more significant than for the provisions of physical separation mentioned above. In fact, to succeed in an attack, it would be necessary to locate the various targets through the facility and to move around, sometimes over wide areas, in order to go from one component to the associated redundant component. In the process of this movement, the physical protection barriers will probably have been crossed. The preparation and execution of the sabotage will then have to take into account these elements.

3. THE SPECIFICS OF PHYSICAL PROTECTION NOT COVERED BY SAFETY

Certain assumptions include under nuclear safety purposes and the provisions which these assumptions impose, are sometimes insufficient to take into account the release of radioactivity resulting from the sabotage of a nuclear facility. For example, the effectiveness of the containment of buildings could be compromised. The same could be true to provisions taken to fight against the fire propagation. Cooling water could be made unusable because of the leakage of a tank. Circuits could be connected to other components than those envisaged in the exploitation rules. Actions initiated from the control room, apart from the normal procedures, could lead to unacceptable situations. Finally, the rate of radioactivity of certain components may be not sufficient enough to dissuade certain perpetrators.

3.1 Leak rate to the outside atmosphere and filtering provisions

In the event of an accident which has occurred in a building, the radioactivity leak rate to the outside atmosphere depends on the overpressure in this building induced by the accident itself, on this building leak rate and on the ventilation and filter systems. In this case to evaluate the released quantities of radioactivity, the assumptions posed for safety studies deal with, on one hand, the risk of direct release coming from the building containment and, on the other hand the reduction of the effectiveness of its filtration system.

It is not excluded that the perpetrators, during their progression into the facility buildings create holes in the walls of these buildings, or more simply, not close the doors considered part of the containment of the buildings, after their passage. The perpetrators then cause the rupture of the containment of the buildings and create direct ways of release in the environment which were probably not taken into account in the safety studies. In addition, the effectiveness of filtration system could be seriously damaged if they use explosives.

Thus new ways of radioactivity release appears which are perhaps not covered by the safety studies. The quantity of radioactivity likely to be spread in the environment would then be much higher than that considered acceptable in the safety studies.

3.2 Fire area

For fire protection, the premises of nuclear facilities are gathered in fire areas so that a fire which has broken out in one of the areas does not spread to another area. "Fire doors" allow the personnel to move from one area to another. These doors are designed to prevent a possible fire spreading and will be permanently closed.

It is not excluded that the perpetrators, during their progression into the facility leave these doors open after their passage, voluntarily or involuntarily. In these conditions, a fire which spreads from one area to another will affect several fire areas. Components known as independent for nuclear safety will then become defective simultaneously.

3.3 Low energy tank or pipe

In relation to nuclear safety, a fluid leakage for which there are provisions to limit and/or isolate is considered as a failure. These provisions are effective for small breaks whose dimension is within a certain size for which it is possible to imagine that these breaks occur during the normal operation of the components concerned. This is the case for tanks and pipes transporting low pressure fluids.

In the case of the sabotage of a component described as being "low energy", it must be considered that all the fluid escaping is lost because the provisions planned to limit and/or isolate this fluid will not be

applied notably if explosives have been used to damage the component. Should this case arise, it is advisable to plan physical protection provisions for these components.

3.4 Alignment error

The operation of facilities requires that operators move in order to control certain components locally to put them either in operating position or in rest position according to operating requirements. Administrative management procedures exist for the control of these components but, most often there is no remote data report indicating the position of these components as the operators in the control room cannot always control the operating or rest positions. These provisions are not sufficiently effective to prevent sabotage, as it is often easy to modify the position of a component beyond the procedures planned for this effect.

Possible improvements consists of locking the valve control wheels or the electric apparatus control buttons in position using locking devices most often based on chains and padlocks. The remote data report, to the control room, indicating the position of such components is an other improvement which helps to detect the alignment errors.

3.5 Actions in the control room

A nuclear facility control room requires special attention because, on one hand, it is unique and, on the other hand, it enables all the facility's components to be controlled.

If the control room is destroyed, it remains possible to bring the reactor to a safe condition provided that the transfer switches to the emergency shutdown panels have been switched by the operators just before they leave the control room to go to the auxiliary control room. If at the moment of destruction it was not possible to operate these switches it is to be feared that the situation will develop unpredictably because unwanted commands may be sent to the components in random sequences.

Another equally worrying situation may result from the take-over of the control room by an armed group determined to cause an accident. As a result, from the control room, this armed group could generate incorrect commands aiming, for example, to trigger an irreversible reactor defect.

3.6 Self-protection of certain equipment related to radioactivity or to the dose rate

Components which are in contact with radioactive products and the radioactive products themselves generally involve a large dose rate. For this reason, they are usually fitted behind biological protection screens. This dose flow usually constitutes a physical protection which is a sufficient deterrent with respect to perpetrators looking, for example, to penetrate beneath the reactor vessel, or wishing to seize irradiated fuel.

However the action of perpetrators who are not afraid of losing their own lives, or even the action of perpetrators insufficiently informed of the risks they are running relating to radioactivity cannot be completely disregarded.

3.7 Superpipes

The interposition of three independent barriers between radioactive products derived from fuel fissions and the environment includes a highly significant special case. The steam generator tubes are clearly part of the reactor coolant pressure boundary since the core cooling water circulates within them. The steam generator tubes with a considerable surface area and with very thin walls therefore comprise the second and third barriers altogether. But according to this specific situation, special attention is laid on the enclosures protecting the secondary system limited to the section between the containment and the main steam stop valves. This section is known as super pipe.

In the event of rupture of a main steam line between the containment and the corresponding stop valve there would be rapid drainage of the steam generator. The corresponding cold surge on the core would induce a power excursion. Consequently the rupture of several main steam lines is not acceptable in the safety demonstration.

The safety demonstration requires careful design, layout rules and particular controls in order to aim at a probability of rupture sufficiently low and no common failure mode are allowed on these pipes.

However an attacker could cause the rupture of one or more of these pipings for example by using explosive devices. Another possibility of malevolent action could be to tamper the correct regulation of the safety valves by diverting them of their safety purpose to create a rapid drainage of the steam generators.

4. DETERMINATION OF TARGETS

The failure of some components could initiate an accidental sequence causing significant consequences for persons or the environment. We have seen above that measures have been taken, for safety purposes, to prevent component failures. We have also seen that measures have been taken to limit the consequences of events which would result from these failures. These measures are mainly taken in terms of redundancy, diversification, physical separation and geographical separation of equipment.

The accidental sequences considered for nuclear safety come from a conventional list including equipment failures, human error, aggressions of internal hazards or of external hazards. Hazards may be of natural origin, such as earthquake but also wind, storm, floods, etc., or of human origin, such as aircraft crashes, explosions, fire outside the facility or the spreading of toxic gases. The internal hazards are hazards generated by the facility itself, such as missiles from inside the containment (flywheel bursting, for example), the results of pipe breaks, load dropping, fires or internal flooding.

The failures caused by sabotage should be added to this conventional list of events. The study consists of checking, for each component, system or equipment, that the provisions taken for safety purposes are sufficient to suitably limit the consequences that may result from the sabotage. In other words, it is advisable to make sure there are no accidental sequences resulting from a sabotage affecting a component, system or equipment that would not be examined in a safety demonstration, taking into account the assumptions selected in this area.

This results in a list of components, systems or equipment for which the total or partial failure may, by nature, cause unacceptable consequences. On one hand, this list results from safety studies, on the other hand, from studies specifically carried out for sabotage.

The components, systems or equipment on this list are the potential targets to be protected against sabotage. Two solutions are then possible to reduce the identified risks. The first one consists of reducing the sensitivity of the considered equipment, that means reducing the failure consequences. It is a matter of measures rather relevant to the nuclear safety area. For example some components have been added to improve the redundancy factor and thus reduce the sensitivity of certain cooling circuits. In other cases, wastes have to be well-conditioned immediately after they have been produced. The second one consists of reducing the vulnerability of the considered equipment, that means reducing the aggression possibilities of the equipment. It is a matter of measures relevant to the physical protection. Thus certain premises are locked and under surveillance done by the physical protection system.

5. MANAGEMENT OF CONFLICTS OR POTENTIAL CONTRADICTIONS

Potential conflicting requirements, resulting from safety and physical protection considerations, should be carefully analyzed to ensure that they do not jeopardize nuclear safety, including during emergency conditions. In certain situations nuclear safety provisions may be contrary to the physical protection provisions.

5.1 Criticality accident

Numerous exits for the evacuation of personnel are planned within the buildings of nuclear facilities involving a risk of a criticality accident. These exits make it difficult to set up barriers around the physical protection areas and complicate the control of persons entering and leaving these areas. The control of persons leaving via these exits is particularly crucial in the case of a criticality accident. Personnel retention areas created at the evacuation exits of the protected areas facilitate the control of

persons, especially when these persons are required to use the evacuation exits to rapidly leave a protected area in which a criticality accident has occurred.

5.2 Evacuation or fire fighting action

In the case of a fire occurring in a nuclear facility, on one hand, it is necessary to evacuate persons as quickly as possible and, on the other hand, it is also necessary to enable the rapid arrival of emergency responders and fire fighting teams. The physical protection barriers must therefore be crossed quickly by each of these. In addition, the control of persons entering is then particularly crucial, notably when it concerns off-site response, persons, or means. Here again, the retention areas around the protected areas may be set up to allow satisfactory control of the persons leaving.

Appendix

Comparison between fundamental principles in the field of physical protection and in the field of nuclear safety

<p>Physical protection - Objectives and fundamental principles IAEA WP13</p>	<p>Convention on Nuclear Safety (INFCIRC/449)</p>
<p>FUNDAMENTAL PRINCIPLE E: <i>Responsibility of the License Holders</i></p> <p><i>The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorizing documents (e.g., operators or shippers).</i></p>	<p>ARTICLE 9. RESPONSIBILITY OF THE LICENCE HOLDER</p> <p>Each Contracting Party shall ensure that prime responsibility for the safety of a nuclear installation rests with the holder of the relevant licence and shall take the appropriate steps to ensure that each such licence holder meets its responsibility.</p>
<p>FUNDAMENTAL PRINCIPLE F: <i>Security Culture</i></p> <p><i>All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.</i></p>	<p>PREAMBLE - THE CONTRACTING PARTIES</p> <p>.....</p> <p>(iv) Desiring to promote an effective nuclear safety culture;</p>
<p>FUNDAMENTAL PRINCIPLE I: <i>Defence in depth</i></p> <p><i>The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives.</i></p>	<p>ARTICLE 18. DESIGN AND CONSTRUCTION</p> <p>Each Contracting Party shall take the appropriate steps to ensure that:</p> <p>(i) the design and construction of a nuclear installation provides for several reliable levels and methods of protection (defence in depth) against the release of radioactive materials, with a view to preventing the occurrence of accidents and to mitigating their radiological consequences should they occur;</p>
<p>FUNDAMENTAL PRINCIPLE J: <i>Quality Assurance</i></p> <p><i>A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.</i></p>	<p>ARTICLE 13. QUALITY ASSURANCE</p> <p>Each Contracting Party shall take the appropriate steps to ensure that quality assurance programmes are established and implemented with a view to providing confidence that specified requirements for all activities important to nuclear safety are satisfied throughout the life of a nuclear installation.</p>
<p>FUNDAMENTAL PRINCIPLE K: <i>Contingency plans</i></p> <p><i>Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned.</i></p>	<p>ARTICLE 16. EMERGENCY PREPAREDNESS</p> <p>Each Contracting Party shall take the appropriate steps to ensure that there are on-site and off-site emergency plans that are routinely tested for nuclear installations and cover the activities to be carried out in the event of an emergency.</p>