Transactions of the 17th International Conference on Structural Mechanics in Reactor Technology (SMiRT 17)
Prague, Czech Republic, August 17 –22, 2003
Paper # WHJKP01-1

Engineering Safety Aspects of the Physical Protection of Nuclear Installations against Sabotage

Aybars Gürpinar [1)]

[1)] Head, Engineering Safety Section, IAEA

Introduction

After the attacks of 11 September 2001, the perception of the potential terrorist threat to nuclear installations has changed significantly. Both the sophistication of the planning and the suicidal nature of the act are important aspects to consider in future physical protection measures for nuclear installations.

The physical protection of nuclear installations comprises a number of important components. This paper specifically addresses the component that deals with plant design and engineering safety. In order to provide a consistent and coherent protection for the nuclear installation, safety and security specialists need to work together in close cooperation. Furthermore, there are different levels of responsibility in providing protection against sabotage. Part of the responsibility lies with the state itself. This could involve the intelligence services, armed forces, police, local governmental authorities, municipalities, civil defence organizations, etc. The level of responsibility that will be the focus of this particular presentation is that of the nuclear installation management.

The IAEA has initiated a number of activities under the general title "IAEA Plan of Action to Protect Against Nuclear Terrorism". This is an extrabudgetary programme comprising eight main activity areas. Two of these areas have a direct bearing on this article. Activity Area I relates to Physical Protection of Nuclear Material and Nuclear Facilities. It is an area where all components of Physical Protection are brought together. For our present discussion, only some part of this is relevant (i.e. those parts related to sabotage of installations). The second area of interest is Activity Area V, entitled Assessment of the Safety/Security Related Vulnerability of Nuclear Facilities. This area identifies the areas of similarity between the design/re-evaluation/upgrade process of nuclear installations for external events of accidental origin to those of malevolent origin. A companion paper is being presented to cover this topic more explicitly in this Conference.

After this brief Introduction, a perspective on safety and security synergies and interaction will be summarized as related to the sabotage of nuclear installations. In this section, some terminology will also be introduced. The next section of the paper will deal with the presentation of a methodology to assess the engineering safety aspects of the physical protection of existing nuclear installations. Finally some concluding remarks will be provided and future outlook will be discussed.

Overview of Safety/Security Perspectives

It is possible to consider the "sabotage of a nuclear installation" from various perspectives. For example, the safety point of view would consider the act of sabotage as another external event (although malevolent) that has the potential to cause radioactive release beyond the prescribed regulatory limits. In fact, it is true that safety improvements that may benefit the plant in relation with accidental type external events will also do so if the initiator is malevolent. However, in this case, the definition of "hazard" is very different and commonly non-stationary and adaptive. It is in the definition of the "hazard" and also throughout the evaluation and upgrading process, that an interaction is needed between specialists in nuclear safety and security. The involvement of only one type of expertise will lead to an incomplete evaluation and probably an unsatisfactory result.

Before proceeding further in the subject, some definitions are needed because common terminology is the first requisite of an interactive programme. The following three definitions are taken from the IAEA INFCIRC/225/Rev.4 entitled "The Physical Protection of Nuclear Material and Nuclear Facilities".

Sabotage: Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances.

Design Basis Threat: The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.

Vital Area: An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences.

The definition of "sabotage" is clear and coincides fairly well with the "malevolent external event" to some extent. Sabotage, however, has a broader meaning in that the deliberate act could be external or internal to the plant. In fact, one of the more significant threats in relation to sabotage is the insider threat, i.e. a plant employee or employees who provide information to adversaries, assist the adversaries or even take part in the terrorist act. Because the sabotage of a nuclear facility involves the acquisition of sophisticated and detailed information about safety systems, plant employees may be targets of recruitment by terrorist groups.

Design Basis Threat is determined by the competent authority. Plant management has the responsibility to protect the plant from this threat by designing and evaluating the physical protection system. The physical protection system includes measures to detect, delay and respond to the adversaries. It also includes plant design considerations and engineering safety measures. However, the extreme loads such as airplane crash to a nuclear installation may also be considered as Beyond Design Basis Threat. The consideration given to the BDBT may be different from the rigorous way the Design Basis Threat is treated, e.g. less conservative acceptance criteria may be used.

Accompanying the definition of Vital Area (given above), INFCIRC/225/Rev.4, provides further explanation on of the definition in Paragraph 7.1.5, as follows:

"Safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malevolent acts, considered in the context of the State's design basis threat, to identify nuclear material, or the minimum complement of equipment, systems o devices to be protected against sabotage. Also measures that have been designed into the facility for safety purposes should be taken into account. When protecting against sabotage, nuclear material or equipment, systems or devices the sabotage of which, alone or in combination based on analysis, could lead to unacceptable radiological consequences, should be located in vital areas. Potential conflicting requirements, resulting from safety and physical protection considerations, should be carefully analysed to ensure that they do not jeopardize nuclear safety, including during emergency conditions."

The role of the safety specialist as well as the required interaction between safety and physical protection specialists is underlined here. Vital area identification is necessary for the simple reason that plant management should know what plant items (structures, systems and components) need to be protected as a minimum and where they are located. The next step involves the question of *how* they may be protected. Whether the "detect, delay, respond" process is sufficient or supplementary engineering safety measures are required depends on the defined DBT, BDBT as well as plant design, layout and configuration.

In Annex 1 of this paper, a flow diagram in which the process of the Physical Protection of Nuclear facilities Against Sabotage is presented. The Annex also includes a brief description of the various boxes that are part of the flow diagram. This is one of several attempts to display the safety/security interaction in the design and evaluation of a physical protection of a nuclear facility. Although the representation reflects current thinking and is based on the concepts provided in INFCIRC/225/Rev.4, it may not coincide with some Member State practices and should not be considered definitive. One aspect of the flow diagram that is very important is its emphasis on the interdependence of nuclear safety and security in this process.

The remainder of this paper will concentrate on the engineering safety aspects of physical protection. In particular, the following three topics will be discussed:

1. Identification of Vital Areas
2. Protection of Vital Areas using engineering safety measures (for DBT)
3. Protection of Vital Areas using engineering safety measures (for BDBT).

Identification of Vital Areas

The purpose for identifying vital areas is to determine the potential targets of an "intelligent" terrorist at a nuclear facility. If all the items within the vital area(s) are protected, then it is ensured that "core damage" will not occur as a result of the terrorist attack. Although, in theory the vital area(s) will not depend on the DBT, in practice knowing the number of intruders, presence (or absence) of an insider, etc. provides for shortcuts in the identification process.

Several methods may be used for the identification of vital areas and the one selected should be compatible with the complexity of the installation as well as the safety documentation already available.

However, before starting the process of vital area identification it is necessary to have clear radiological criteria. These should generally coincide with the radiological criteria already identified for accidents (i.e. non-sabotage event related sequences). In a nuclear power plant, the adversary can cause radiological release to occur either from reactor core damage or directly from a source of radioactivity such as the spent fuel pool. The vital areas related to these two types of events will be different. For the case of reactor core damage one train of safety systems need to be protected. Conditions for having redundancy, physical separation, single failure criteria, off-site power availability, etc. need to be decided by the regulatory authority before the process of vital area identification begins. For the spent fuel pool, the concern is more related to the structural integrity and the vital areas are easier to identify.

As mentioned above, the radiological criteria need to be defined first. Then the vital areas are identified having the objective of preventing core damage. Here the conservative assumption is that every time a core damage occurs, radiological limits will be exceeded. It should be recognized that the containment functions and on-site accident management are not given quantitative credit in this approach. These provisions generally constitute important layers of defence in depth. Especially with the attention this topic has received in nuclear safety recently it is important to include "post-accident" aspects into the analysis.

The identification of vital areas is generally accomplished using a two step process. The first step is to identify the systems and components, and the second involves the locations of these systems and components. The first part of the process already constitutes a part of safety analysis that should be available at the plant. In many plants logic diagrams (fault and event trees) developed for probabilistic safety analysis will serve as a good source of information. Availability of external event PSAs (fire, seismic, etc.) will have the added benefit of providing information on passive system failures that is also useful for malevolent initiators. It is important to check the consistency of the assumptions between the available analyses and the vital area identification. There are also recent attempts to combine these two steps and arrive at the vital areas using one analysis.

After the identification of systems and components, the locations need to be chosen and this is an area where very close co-operation between the safety and security specialists is required. From the security perspective, the chosen areas should be easily defendable. However, potential interference of security measures with the safe operation of the plant should be avoided.

Protection of Vital Areas Using Engineering Safety Measures (for DBT)

The protection of vital areas using engineering safety measures should not be seen as an alternative to physical protection of vital areas through the detect/delay/respond process. It is always assumed to have the latter present and engineering measures are needed to supplement these or to cope with some malevolent initiators for which the latter systems are not specifically designed. Although these malevolent initiators are more likely to be found as part of "Beyond Design Basis Threat", it is also possible that they are considered part of DBT depending on the original plant design and the decision of the Competent Authority.

Airplane crash is one example of an event that cannot be dealt with by the detect/delay/respond type of a plant physical protection system. In this case it is necessary to protect plant vital areas using engineering safety measures. The protection should cover a multitude of effects, both primary and secondary, that an airplane crash may induce. These include impact from primary and secondary missiles, vibration due to the impact and fire. The significance of the fire will depend on the amount of fuel present at the moment of the impact as well as the ingress of the

fuel into safety related structures. Most nuclear power plants are either designed for (or can be shown to withstand) the impact from small planes such as Cessna or general Aviation aircraft. If the threat assessment includes this type of an event into the DBT then it is necessary to check the capacity of the plant against this event. In doing so, it is important to consider any differences between the original assumptions made on the mass, velocity, angle of incidence and contents of the plane and those related to the new event included in the DBT. A suicidal malevolent act may on purpose lead to parameters that are unfavourable in relation to the above mentioned parameters. This was the case for the crashes of 9/11 on the World Trade center buildings. The angle of incidence, velocity and the fire potential were more unfavourable than an accidental type of an airplane crash. Moreover, it is also possible that explosives may have been taken on board in order to make the defence more difficult. In this case, aside from impact, vibration and fire, the plant structures also need to be designed against the detonation of the explosives.

Engineering safety measures are also important as part of the "delay" aspect of the physical protection system if the intrusion of the adversary into the site is accomplished by means of a vehicle (e.g. a pick up truck). In this case the barriers need to be positioned and designed together by the safety and security specialists.

Finally, engineering safety measures constitute a level of defence in depth. If prevention of the sabotage act is not accomplished for some reason even though the physical protection system for detection/delay/response is designed for the DBT, then it may still be possible to avoid core damage through robust design of items in vital areas and/or through physical separation of items.

Protection of Vital Areas Using Engineering Safety Measures (for BDBT)

Some events that may cause excessive loads on nuclear installation structures, systems and components may have been left outside the coverage of the DBT for a variety of reasons. In some cases the Competent Authority may decide to require the nuclear installation management to consider these events in a special way. This category is called Beyond Design Basis Threat and includes events that are still credible but more demanding than those in the DBT. When a new threat situation is identified, this could either be made part of the DBT or considered as BDBT. This is not very different from the approach taken by the Competent Authorities when a new issue is discovered relating to accidental (not malevolent) external events. This can either be made part of the design basis, i.e. reconstitution of design basis is required, or the capacity of the plant can be checked for the new challenge. The design basis reconstitution requires all the rigors of the design process to be in place whereas the latter approach can take advantage of less demanding acceptance criteria.

Similarly, the BDBT may be treated in a way that uses different assumptions and acceptance criteria than for the DBT. These need to be discussed and decided by the Competent Authority in consultation with the utility as well as other stakeholders of the process. The objective is to be able to demonstrate that no event of significant radiological impact occurs even in the case of the BDBT.

Concluding Remarks

Physical protection of nuclear installations (both against material theft and against sabotage), especially nuclear power plants, is a well established process. Use of engineering

measures to prevent core damage in the case of a malevolent external event has been considered implicitly in the design of installations as part of the protection against external events of accidental origin. Design of barriers against the so-called malevolent vehicle intrusion has been considered by both security and safety specialists jointly.

This paper is an attempt to explore ways to put the security and safety aspects of the problem of "protection of nuclear installations against sabotage" within a common framework.

A rational and interactive effort is needed between the security and safety specialists in order to provide for a robust design and process to: (1) prevent the sabotage act from succeeding, (2) prevent core damage even if the act succeeds (fully or partially), (3) manage the post core damage crisis on site, and (4) provide effective emergency measures offsite. In the implementation of items 3 and 4, it is important to recognize additional difficulties of dealing with continuing adversary presence that may intend to disable or disrupt these efforts.