

# **The concept of physical protection of nuclear facilities in Sweden**

Stig Isaksson  
Swedish Nuclear Power Inspectorate (SKI)  
SE-106 58 Stockholm, Sweden

## **Abstract**

This paper will discuss the physical protection philosophy used to protect nuclear facilities in Sweden. It will also discuss the systematic approach used to develop the protection system starting from the development of a design basis threat. Furthermore it will in more detail discuss the pillars, all equally important, on which the protection is built i.e. multiple protective barriers, access control, system engineering and response forces. Finally the process to revise the present physical protection regulations will be described.

## **Introduction**

The techniques used for the physical protection of nuclear facilities and transports of nuclear material depend on the type of facility and mode of transport. This paper will focus on protection of nuclear power plants in Sweden and the philosophy on which the protection concept is built. The Swedish Nuclear Power Inspectorate, SKI is the competent nuclear regulatory body in Sweden and therefore responsible for the supervision of nuclear activities. During the build up of the nuclear power program in the late seventies SKI early recognised the need for physical protection measures at nuclear facilities. It took SKI a couple of years to develop a suitable concept for protection which then led to the publication of regulations requiring operators to take proper measures. The regulations have remained unchanged and served its purpose well but due to changes in the supervisory policy of SKI and requirements to modernise regulations there is now a need to rewrite also the physical protection regulations.

## **Threat assessment**

The starting point in the process to develop regulations for physical protection was to assess the threat against Swedish nuclear power plants i.e. what today is known as a design basis threat, DBT. In co-operation with national intelligence and security authorities SKI arrived to the conclusion that the major threat is a terrorist act or a sabotage leading to a radiological accident i.e. a release of radioactivity to surrounding areas. This could lead to serious damage to the plant, to personnel, or to the loss of lives. Furthermore SKI has assessed that an attack in which a threat of damage is made and in which the threat later can be realised is more likely than an attack solely intended to do damage to the reactor. The basis for this philosophy is that if the aggressor has the qualifications to occupy a well-protected power plant and he also has the knowledge to endanger the safety of the reactor, then he probably also has goals e.g. political or economical, other than just to damage the reactor. This forces him to get in contact with other people than the operator for negotiations. This will then provide time for countermeasures. However, in the process to revise the regulations SKI will take into account the more violent and ruthless terrorist actions that have occurred in recent years and were clearly demonstrated in September last year.

SKI has also assessed that sabotage in the plant during periods of normal operation will not, in most cases, lead to more severe situations than those for which the plant is designed to handle safely. A nuclear power plant is however vulnerable to sabotage even during its shutdown period when the accessibility of the reactor building is greater compared to the periods of normal operation.

A nuclear power plant can be protected against a majority of threats and attacks. Only when considering the probability and consequences of a realised threat or attack against a plant it is possible to provide it with sufficient protection. However a plant's physical protection must be based on a number of assumptions as to the threat situation.

SKI has thoroughly assessed the question of having armed guards at the facility to neutralise the aggressor. The conclusion was that the benefit of having such a force does not outweigh the drawbacks. Furthermore having an armed plant security force in addition to the police would not be in compliance with the public spirit. We also agreed that the deterring effects of armed guards are minor since the force we could have at the plant will be quite limited. Even with armed guards at the plant, we cannot assure that an aggressor will not be able to occupy the plant. The force would probably not have the power to reoccupy it. Therefore, the guards at the Swedish facilities are not armed. They are rather considered as watchmen and have no obligation to neutralise an aggressor if such would endanger their lives. The responsibility to act as a response force and reoccupy the plant lies instead with the Swedish police.

With this in mind SKI came to the conclusion that the reactor has to be protected against unauthorised manoeuvres which can be performed from the control room or from local areas of operations e.g. at a switch gear. However performing these operations in areas outside the control room is appreciably more difficult. Physical damages either directly to the systems necessary for the cooling of the reactor or to the controls of the necessary systems can also occur in connection with an attack. Intervention capabilities, built into the reactor system design, are clearly important in mitigation of physical damages and unauthorised operations. Furthermore SKI concluded that we need a well-organised response force outside the plant trained to reoccupy it.

SKI based the regulations for physical protection of nuclear power plants on the following threat situation:

- The aggressor has knowledge of the design of the plant, its technical function and its surveillance routines.
- The aggressor is armed and has explosives. The types of weapons and amounts of explosives are based on national experience.
- The aggressor can be several people who force their way into the plant.
- The forced entry will cause a verified alarm.
- The aggressor will, some time after a verified alarm has sounded, occupy the plant's most important area of operation, the control room.

- A hostage may be used. The hostage is assumed to perform ordered operations within his knowledge, but without access to hard-to-obtain information.
- The aggressor may have help from an insider.
- The aggressor is able to get control of the rest of the plant's vital areas after a defined time limit. The time limit is based on the time needed to get control of the areas outside the control room and the time needed to assure the operation of the reactor, to get personnel to the spot and to take over operation of the reactor from these areas.
- Explosions outside vital areas may occur.
- The plant personnel are unarmed.

### **Protection level**

The overall purpose of the protection of a nuclear power plant is if possible to deter and prevent a threat or an attack and in case of a realised threat or attack to neutralise it. This is achieved when the aggressor is unable to do damage which would lead to the fuel not being cooled. No protection system can assure that the reactor can be protected from a maximum attack. SKI's assessment is that if the reactor is protected against the assumed threat situations, there is a high probability that attacks likely to occur can be neutralised.

The various parts of the protection system must be co-ordinated to reach the overall goal. On the whole, the protection can be said to consist of:

- multiple protective barriers
- system engineering measures
- administrative measures
- armed outside response force

Of course, there is still a probability that the aggressor will succeed in damaging the reactor. This could cause a core melt down with the risk of releases of fission products into the environment. In this case the physical protection goes hand in hand with what is known as the mitigation of consequences from severe accidents and which also demands system-engineering measures such as containment cooling and filtered venting.

### **Protection barriers**

Access to a nuclear power plant must be controlled. A physical barrier providing detection of an unauthorised entry must surround the plant. For this purpose fences surround the surveilled areas of the plants. Detectors are placed on the inside of the fences and cameras covering the surveilled area will verify an alarm from the detectors.

Areas that contain equipment for the safe operation of the reactor must be placed inside a protected area. Walls, ceilings, doors, windows, etc., enclosures to a protected area are to consist of a sturdy construction with strength enough to stop or delay an unauthorised entry. Entrances to the protected area must be closed, locked, and equipped with an alarm.

Areas outside the control room, from which the reactor can be operated, are very important in the Swedish physical protection system. From these areas threats against the reactor can be neutralised. These areas are included in the plant's vital areas, which are to be mechanically

protected and have boundaries of sufficient strength to resist an attack for a defined time limit. Entrances to vital areas must be equipped with an alarm. If an acceptable level of redundancy protects these areas, they do not need a higher degree of mechanical protection than what is required for protected areas. They are then called safely closed areas.

In order to facilitate control and restrict the movement of persons within the plant, it is divided into sections. The sections are physically cut off and access is controlled by for instance a card reader. Access to the different sections is limited to only the people who need to enter to perform their duties.

The target of an attack is likely to be the reactor control room. Therefore, this room must be especially protected in order to allow the personnel to take the actions necessary to prevent the aggressor from damaging the reactor. Entrances to the control room must be closed, locked and equipped with an alarm. Before an aggressor can enter the control room, three barriers must be passed: the surveilled area, the protected area and the entrance to the control room. The entrance to the control room is locked to give its personnel full control over who gets in. From the time an alarm indicating an attack against the plant is verified, point zero, the aggressor must be delayed at least long enough for the control room personnel to take necessary operational steps and have the option to evacuate the control room. For the safety of the personnel, there must be more than one way to evacuate the control room.

### **System engineering measures**

System engineering measures are intended to prevent the aggressor from damaging the reactor and to make recovering control over the reactor easier for the operator. The goal is to have the plant designed in such a way that necessary areas of the plant can be kept under safe control in the event of deliberate damage or occupation of the control room. This can be achieved with the aid of automation or operation personnel.

Since we have assumed that the aggressor will be able to occupy the control room, certain steps have to be taken to assure that the reactor will be in a safe mood when the personnel evacuate the control room. We also have to make the aggressors attempt to make operations or to influence the safety of the reactor difficult by disconnecting parts of the control room. Other parts vital for the safe operation of the reactor have to be considered and protected. These parts of the reactor shall be protected by redundant systems and by physical separation of the systems. Later, the operator has to re-man the reactor to be able to take control of it again. This has to be done within a certain time limit. To reoccupy the control room within this time is not considered feasible, and the control room may also be damaged. To be able to control the reactor, the operator needs information on the status of the plant conditions like cooling and subcriticality. For this purpose, instrumentation for the surveillance of the plant conditions is installed at local areas in the plant. The information is used to operate the reactor from local operating areas. Such an area is meant to be a place from where the operation of equipment such as feed water pumps can be taken over. These operations are difficult to perform and the area is physically protected. The local operating areas are spread over the plant to get redundancy as high as possible. This means that a second control room normally is not acceptable. Occupying and damaging both control rooms would be too simple for an aggressor.

The foundation for the system engineering measures is:

- The built-in natural protection obtained in a plant as a consequence of the conventional safety requirements.
- The technical specifications for the use of the plant.
- The plans for evacuation of the control room and the manning of other operating areas in the plant intended to be used e.g., in case of fire in the control room.

The physical protection might mean that additions to the system engineering measures are necessary. An example of what has been done in Swedish reactors is making the unauthorised operation in the control room after an evacuation more difficult to perform. Furthermore in later reactors all safety-related systems are four-subbed, each subsystem with 50 % redundancy according to design and with a high degree of physical separation. This leads to a higher safety in case of sabotage as well as other failures. Finally additional instrumentation at local operating areas for surveillance of plant conditions have been installed.

### **Response force**

The intention is to re-man the areas of the plant necessary to secure the cooling of the reactor after a possible occupation. As mentioned earlier we cannot be sure that we can prevent the aggressor from occupying the facility. In Sweden, only the police have the means to organise a response force with the power to reoccupy a nuclear power plant occupied by terrorists. For this purpose the police are specially equipped and trained to respond on short notice and to act within a limited time. As a matter of fact the police continuously have the opportunity to train together with the operator even inside reactor buildings. Training and exercises are planned in close co-operation between the operators and the regional police authorities. Furthermore emergency plans and procedures are shared and subject to joint exercises.

### **Regulatory review**

As mentioned earlier the requirement to take measures to ensure proper physical protection are laid out in regulations being in force for more than 20 years. In the light of the new, activity-oriented, supervisory policy of SKI, to clearly put the full responsibility on the licensee to take appropriate measures, the regulations are being revised. The basis for the revision is the Design Basis Threat, DBT. The DBT is just being formulated after having been subject to a revision process involving SKI personnel as well as representatives from other relevant Swedish authorities, including the intelligence community. Experiences from the tragic events of September 2001 have been taken into account in the process.

The objective is to have transparent regulations laying out functional requirements which the licensee has to meet. The licensee should then have the obligation to show SKI how the regulatory requirements are met.

The process that has been established by SKI to rewrite the regulations could be divided into the following formal steps:

- Development or review of the existing design basis threat, to be co-ordinated with other national authorities.

- Proposed regulations, first draft
- Review of the internal SKI regulatory group
- Comments from relevant offices in SKI
- Proposed regulations, second draft
- Information to the Director General and the Board of SKI
- Request for informal comments from operators, police authorities and other relevant bodies
- Meeting with interested operators and other relevant bodies to review comments
- Proposed regulations, final draft
- Formal request for comments from operators, police authorities and other relevant bodies
- Proposed regulations presented by the Director General to the Board of SKI for approval
- Regulations in force

As shown above the process is quite lengthy but it gives the opportunity to include external comments into the final regulations. Furthermore there is a greater possibility that the final regulations will meet a better acceptance by the licensees given that they have had the opportunity to influence them. SKI has had very good experiences using this process in developing regulations during the last years.

The plan is to have the revised regulations in force before the end of 2003.

### **Conclusions**

On the whole the Swedish physical protection system is based on the following fundamentals:

- A high loyalty level within the personnel of the facility
- A good system of multiple protective barriers and detection devices
- System engineering measures to neutralise unauthorised operations and sabotage
- A response force, well organised, trained and equipped with the obligation to reoccupy the reactor and to ensure re-manning of the controls

The objective of the physical protection system is to deter and hopefully to prevent an aggressor from getting into the plant. If the physical protection system fails to do so, then it shall minimise the aggressors opportunities to damage the reactor or to release radioactive substances. The system shall also give the operator as many options as possible to operate the reactor safely even with parts of the reactor occupied by an aggressor. Only a system, which has a great deal of system engineering measures, will fulfil all these demands.

What an acceptable physical protection system shall look like when it is implemented is dependent on many factors. To say "what is good to you is good for us" would be serious misjudgement. In fact important factors such as the actual threat situation in the country, or even in part of the country where the reactor is sited, the social order of the country and also type of reactor have to be taken into account. Therefore the Swedish experience is, to make the physical protection system as effective as possible it should be based on specific national conditions.