Hungarian Atomic Energy Authority

(This is an unofficial translation of the text)

Guideline PP-13

Protection against insiders

Version number:

2.

September 2015

Issued by:

Gyula Fichtinger

Director General of the HAEA

Budapest, 2015

The publication can be acquired from:

Hungarian Atomic Energy Authority

Budapest

Hungarian Atomic Energy Authority

FOREWORD FROM THE DIRECTOR GENERAL

The Hungarian Atomic Energy Authority (hereinafter referred to as HAEA) is a central state administration organ (a so-called government office) having nation-wide competence in the field of peaceful use of atomic energy; it operates under the direction of the Government, it has independent tasks and scope of authority. The HAEA was established in 1990 by the Government of the Republic of Hungary with Govt. decree 104/1990. (XII. 15.) Korm. on the scope of tasks and competence of the Hungarian Atomic Energy Commission and the HAEA.

The public service of the HAEA as defined in law is to perform and coordinate, independently of organizations having interest in the application of atomic energy, the regulatory tasks in relation to the peaceful and safe use of atomic energy, including the safety of nuclear facilities and materials, nuclear emergency response and nuclear security, and the corresponding public information activity, and to make proposal to develop and amend, and to offer an opinion on proposed legislations corresponding to the use of atomic energy.

The fundamental nuclear safety objective is to ensure the protection of individuals and groups of the population and of the environment against the hazards of ionising radiation. This is ensured with effective safety measures implemented and adequately maintained in the nuclear facility.

The radiation protection objective is to keep the radiation exposure of the operating personnel and the public all times below the prescribed limits and as low as reasonable achievable. This shall be ensured in the case of radiation exposures occurring during design basis accidents, and as far as reasonably possible during beyond design basis accidents and severe accidents.

The technical safety objective is to prevent or avoid the occurrence of accidents with high confidence, and the potential consequences occurring in the case of every postulated initiating event taken into account in the design of the nuclear facility shall remain within acceptable extent, and the probability of severe accidents shall be adequately low.

The HAEA determines the way how the regulations should be implemented in guidelines containing clear, unambiguous recommendations in agreement with the users of atomic energy. These guidelines are published and accessible to every members of the public. The guidelines regarding the implementation of nuclear safety, security and non-proliferation requirements for the use of atomic energy are published by the director general of the HAEA.

FOREWORD

The internationally accepted bases of physical protection are represented by the Law Order 8 of 1987 on the promulgation of the International Convention on the Physical Protection of Nuclear Materials, the Act LXII of 2008 on the promulgation of the Amendment to the Convention on Physical Protection of Nuclear Materials approved in the frame of the International Atomic Energy Agency and promulgated by Law-decree 8 of 1987 amended by a Diplomatic Conference organized by the IAEA signed on July 8, 2005, and the Act XX of 2007 on the promulgation of the International Convention for the Suppression of Acts of Nuclear Terrorism.

The realization of the stipulations undertaken by Hungary, at the highest level, is represented by the Act CXVI of 1996 (hereinafter referred to as Atomic Act), which includes the fundamental security principles and establishes the frame of the detailed physical protection regulations.

The Govt. decree 190/2011. (IX. 19.) Korm. published based on the authorization of the Act (hereinafter referred to as Government Decree) establishes the legal requirements for the physical protection of the use of atomic energy and for the connecting licensing, reporting and inspection system.

The HAEA is authorized to develop recommendations regarding the implementation of requirements established in laws, which are published in the form of guidelines and made accessible on the website of the HAEA.

For the fast and smooth conduct of licensing and inspection procedures connecting to the regulatory oversight activity, the Authority encourages the licensees to take into account the recommendations of the guidelines to the extent possible.

If methods different from those laid down in the regulatory guidelines are applied, then the Authority shall conduct an in-depth examination to determine if the applied method is correct, adequate and full scope, which may entail a longer regulatory procedure, involvement of external experts and extra costs.

The guidelines are revised regularly as specified by the HAEA or out of turn if initiated by a licensee.

The regulations listed are supplemented by the internal regulations of the licensees and other organizations contributing to the use of atomic energy (designers, manufacturers etc.), which shall be developed and maintained according to their quality management systems.

Before applying a given guideline, always make sure whether the newest, effective version is considered. The valid guidelines can be downloaded from the HAEA's website: http://www.oah.hu.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Scope and objective of the guideline

The guideline contains recommendations on how to meet the provisions of Government decree.

This guideline lays down the methodology for the identification of an insider, prevention of his/her act and the evaluation methodology of the mitigation of the consequences thereof.

1.2. Corresponding laws and regulations

The legal background of the nuclear safety requirements is established in the Atomic Act and the Government decree.

2. TERMINOLOGY

This guideline used the following terminology in addition to the terms determined in Section 2 of the Atomic Act and Section 2 of the Government decree.

Unacceptable radiological consequences:

The consequence of a sabotage against a nuclear facility, nuclear material, radioactive source or radiative waste is unacceptable, if it causes or may cause a nuclear emergency; and if the sabotage entails significant exceedance of the dose limit of certain individuals or a group of individuals, or it can induce such overexposure.

Threat:

Potential to cause damage to the people, property or environment by a person or group of persons with motivation, intention and possibility to commit a malicious act.

(Design Basis) Threat:

Hazard or act threatening the peaceful users of atomic energy determined by the state in an updated threat assessment.

Authority:

The HAEA and the Hungarian Police Headquarters.

Preventive measures:

Those measures, which prevent or terminate the potential for insider threat or minimize the threat situations or prevent the execution of malicious acts.

Motivation:

The set of motivation forces, which encourage the adversary to commit or to attenmpt the malicious act.

3. RECOMMENDATIONS OF THE GUIDELINE

3.1. General considerations

Section 16 of the Government decree states that:

"16. Insiders

Section 16

(1) The obligant, in compliance with the stipulations of the Act on National Security Services, shall check the trustworthiness of the persons who have knowledge of sensitive information, high-level access rights and authority in relation to the effective operation of the physical protection system.

(2) Vital area and inner area can be accessed only by at least two persons authorized to access and perform the duty."

The nuclear and other radioactive materials, as well as the nuclear facilities are subjected to several various potential threats. Severe environmental consequences and economical loss may be resulted by causing public danger and damaging to the environment with the illegal use of nuclear and other radioactive materials, sabotage.

The basic goal of the protection measures is to prevent unauthorized removal of materials and sabotage acts committed against materials and facilities. Effective physical protection measures should be applied to eliminate the potential hazards. The efficiency of the physical protection measures essentially depends on the accurate knowledge of the potential threats.

These threats might be divided into two parts: external threats that are discussed in separate guidelinea, as well as internal threats. Detection of internal threats means a serious problem from the aspect of design of physical protection measures. The insider has access to the area of the facility and could take advantage of the knowledge of data of the material or facility to be protected, of the security and protections systems and of the awareness of operational safety features. The insider threat thus presents a unique problem. The insiders could access protected locations. Additionally, they have access to such sensitive information, which ensures the safe operation of the facility. Insiders could potentially tamper the operation of certain protection systems, falsify or block the signals of the protection systems. An insider means serious threat for the facility, because he/she may make use of the advantages from having authorized entry, is authorized and able to falsify actual data and evade security measures. The insider might

fulfill any position within the facility. Detailed analysis of the insider threat is dependent on the facility and its environment, since the facilities may substantially vary one to other (e.g. research reactor, nuclear power plant or nuclear fuel cycle related facility).

3.2. Analysis of inseider threat

3.2.1. Identification of potential insider threats

As initial data, the guideline uses the information defined in the design basis threat (DBT) or in the national threat assessment about insider threats in order to identify the potential insider threats for facilities. Then it determines the specific insider threats based on the precise assessment of the licensee's organizational features.

Design Basis Threat should be taken as basis for the design, implementation and assessment of physical protection systems. The State should take into consideration the features, characteristics of potential insiders and should include them into the design basis threat.

Insiders may have various motivations and may be passive or active, non-violent or violent. Motivations may include ideological, personal, financial and psychological factors and other forces such as coercion.

Insiders could act independently or in collusion with others. They could become malicious on a single impulse, or act in a premeditated and well prepared manner, depending upon their motivation.

Passive insiders are non-violent and limit their participation to providing information that could help adversaries to perform or attempt to perform a malicious act. It is also possible that an insider provides information unconciouosly, and thus facilitates the conduct of the maclicious act (e.g. social engineering).

Information may be obtained about active insiders during the preparation of the action. They may also be violent or non-violent. Active insiders are willing to open doors or locks, provide hands-on help and aid in neutralizing response force personnel.

Passive insiders are non-violent and may limit their activities to damaging to and tampering with accounting and control systems, or safety and security systems.

Violent active insiders may use force regardless of whether it enhances their chances of success; they may act rationally or irrationally.

Insiders may hold any position in an organization or can be an indirectly employed member of a contractor who also have access.

Insiders may have:

a) Access to some or all areas of a facility, systems, equipment or tools;

b) Authority over instrumentation and control systems or personnel;

c) Knowledge of facility layout, transport arrangements and/or processes, physical protection, safety systems and other sensitive information;

d) Technical skills and experience;

e) Authority to acquire and ability to use tools, equipment, weapons or explosives.

3.2.2. Situations to be considered in the analysis of insider threats

Certain situations at nuclear facilities may be favourable or conducive to insider threats.

Situations inside the facility or regarding transport, including those related to the workforce, employment issues such as performance appraisals, industrial relation policies and an absence of security culture, security awareness and trustworthiness programmes may all be favourable or conducive to insider attempts to perform malicious acts.

Temporary situations, such as maintenance operations, may lead to a significant increase in the number of access authorizations delivered, for example, to contracting companies.

The general attitude of the community, like discontented faction among the population and social and political animosities should be considered. Special attention should be paid to possible connections between these groups and individuals with experience in facility operations or with access to the nuclear facility.

3.2.3. Target identification

Target identification is important with regard to the determination of potential targets for unauthorized removal of and sabotage against nuclear and other radioactive materials, especially of targets being attractive ofr insiders.

Target identification is an evaluation of what to protect a priori, including nuclear material and other radioactive materials, associated areas, buildings and equipment, components, systems and functions, without consideration of the difficulty of providing protection.

Consideration should be given to safety analysis and the associated vital area identification analysis as the starting point to identify potential sabotage targets, to categorization of nuclear material and equipment in order to identify potential targets for unauthorized removal.

Insider targets are somewhat different from those of outsiders. For example, insiders could commit protracted theft of small amounts of nuclear material from several locations, in each of which the quantity of material is not attractive to an outsider. Moreover, in some cases an insider's sequence of malicious acts leading to sabotage may not be time constrained, which contrasts with the outsider's dependence on time.

3.3. Measures against potential insiders

3.3.1. General approach

The measures to preclude or remove possible insider threats can be grouped into two groups: preventive and protective measures. Prevention of and protection against malicious acts can be implemented as follows:

Prevention:

1. Exclude potential insiders by identifying undesirable behaviour or characteristics, which may indicate motivation, prior to allowing them access;

2. Exclude further potential insiders by identifying undesirable behavior or characteristics, which may indicate motivation, after they have access;

3. Minimize opportunities for malicious acts by limiting access and authority.

Protection:

4. Detect, delay and respond to malicious acts;

5. Mitigate or minimize consequences.

3.3.2. Development of a comprehensive approach

The overall approach consists of implementing several layers of defence, including both administrative aspects (procedures, instructions, administrative sanctions, access control rules, confidentiality rules) and technical aspects (multiple protection layers fitted with detection and delay) that insiders would have to overcome or circumvent in order to achieve their objectives.

Implementing preventive and protective measures to counter the insider threat is usually much more difficult than implementing measures to counter the outsider threat, due to the access, knowledge, authority and attributes of

insiders. Thus, although already partially addressed for the outsider threat, any element that could provide protection against the insider threat should be considered. These elements include detection, delay, response, nuclear safety, radiation protection and accountancy provisions.

For nuclear safety purposes, design criteria such as redundancy or diversity in systems and equipment that are important to safety, or layout criteria such as physical or geographical separation or segregation of these systems or equipment should be taken into account. These provisions can improve protection against sabotage by requiring more preparation, more means and more time for an insider to commit a malicious act. Consequently, they could be of significant efficiency to deter, prevent or delay acts of sabotage by insiders or to mitigate radiological consequences.

Radiation protection measures, such as the limitation of access to specific areas as well as radiation protection devices could contribute to both deterring and preventing unauthorized removal or sabotage by insiders.

Accountancy provisions require keeping a strict inventory of all nuclear and other radioactive materials and triggering an alarm if the material balance shows a discrepancy.

The accountancy rules also enable the operators to:

a) know precisely the quantity and type of all inputs and outputs of nuclear material in their facilities;

b) always be aware of the location, use, movement and transformation of nuclear and toher radioactive material; and

c) detect any anomalies concerning the inventory of nuclear or other radioactive material.

The accountancy system should be able to detect unauthorized transfers in or the repeated unauthorized removal of small quantities from a facility, which might not be detected by the physical protection system. The detection of anomalies should be supported, in particular, by the use of seals, tamper indicating devices and a computerized accounting system.

3.3.3. Preventive measures

The aim of preventive measures is to exclude potential adversaries and to minimize the likelihood of insiders attempting to commit a malicious act. The following are recommended as preventive measures:

Identity verification. This confirms that the name and personal particulars of the individual in question are correct.

Trustworthiness check. Trustworthiness checks are initial and ongoing assessments of an individual's integrity, honesty and reliability as pre-employment checks and checks during employment. These checks attempt to identify motivational factors such as greed, financial factors, ideological interests, psychological factors, desire for revenge (e.g. due to perceived injustice), physical dependency (e.g. on drugs, alcohol or sex) and factors due to which an individual could be coerced by outsiders. Such factors might be indicated by a review of criminal records, references, past work history, financial records, medical records and psychological examinations/records. Periodic checks should be conducted during employment period as some of these conditions may not be apparent or may change over time. These reviews are of particular interest in the case of temporary employees and workers whose duties may place them close to sensitive targets. The depth of the trustworthiness checks should be graded according to the level of access the individual has.

Escort and surveillance of casual visitors. Temporary workers, such as maintenance, service or construction workers often come from contracting or subcontracting companies. The trustworthiness of temporary workers and visitors may not have been determined prior to their access. Escorting such people is a way of making sure that they are in the right place and that they are performing their duties properly. To be effective, the escort should know about their approved activities, including access to specific places and actions they should not perform. In addition, guard patrols may deter or detect any attempt by individuals to carry out malicious acts.

Security awareness. Implementing a strong security awareness programme for staff members and contractors supports the security culture within the organization. A strong security awareness programme requires clear security policy, the enforcement of security practices and continuous training. The purpose of the training programme is to establish an environment in which all employees are mindful of security policies and procedures, so that they can aid in detecting and reporting inappropriate behaviour or acts. Everyone, irrespective of his/her role or function, should be aware of the threats and potential consequences of malicious acts and of their own role in reducing the risks and in developing a comprehensive and effective security framework. Security awareness programmes should also provide for measures to reduce risks of blackmail, coercion, extortion or other threats to employees and their families, and should promote the reporting of such coercions or attempts thereof to the security management.

Confidentiality (security of information). Information on security measures or sensitive targets (e.g. location of the nuclear and other radioactive materials, site maps, specific drawings of equipment, systems or devices that represent the design features of specific targets, lock combinations, passwords and mechanical key designs) could help insiders to perform a malicious act successfully. This information should be kept confidential so that only those who need to know are permitted access to it. In addition, information addressing potential vulnerabilities in physical protection systems should be highly protected. A possible solution is compartmentalization (dividing information into separately controlled parts) to prevent insiders from collecting all the information necessary to attempt a malicious act. Special attention should be paid to electronic information. Ensuring confidentiality will mean that insiders would have to make additional efforts to carry out unauthorized removal of nuclear material or an act of sabotage, during which they could be deterred or detected.

Quality assurance. A quality assurance policy and related management programmes should be established and implemented that specify requirements for all activities important for the prevention of and protection against insider threats.

Employee satisfaction. It cannot be assumed that just because an individual is an employee or a contractor, he or she will be free from dissatisfaction. Therefore, good relations among workers and between management and workers should be given due consideration and should be part of the security culture. Managers should be trained to identify and raise any concerns about an employee's behaviour.

Physical compartmentalization of areas. Compartmentalizing facility access by means of measures for access control minimizes the opportunity for sabotage or the unauthorized removal of nuclear material by insiders, since this makes more difficult to obtain data on security and targets, as well as regarding the full capability needed to perform a malicious act. Every effort should be made to ensure that a single person does not acquire all the necessary access authorizations that would enable such an individual to commit a malicious act.

The significance of the physical compartmentalization of areas has to be consistent with the potential risks; therefore, the most sensitive targets should be located in more protected areas, whereas less sensitive targets could be located in less secure areas. The access rules should be assigned to physical protection areas. Strictly limiting the number of persons with access to a sensitive area and also the number of persons empowered to give access

authorization to sensitive areas can minimize opportunities for insiders. In the design phase, specific attention should be paid to minimizing unnecessary access to protected areas.

Compartmentalization of activities. Compartmentalization of activities will limit the ability of insiders to obtain the set of capabilities necessary to conduct a malicious act. Such capabilities might include the ability to use special tools and equipment required for operations or for handling material. Transfer of tools, material and equipment between areas should be formalized and should involve more than one person.

Sanctions (disciplinary actions and prosecution). It is important that potential insiders be aware that deliberate violation of laws and regulations or the instructions of the operator may be severely sanctioned. The certainty of disciplinary action and prosecution may deter insiders from committing malicious acts. A megelőző intézkedések célja az elrettentés és a belső elkövetők által elkövetett rosszindulatú cselekmények elkövetési valószínűségének csökkentése. A javasolt megelőző intézkedések a következőek:

3.3.4. Protective measures

The aim of protective measures is to detect, delay and respond to malicious acts after their initiation, and to mitigate or minimize their consequences.

When designing and implementing protective measures, efforts should be made to ensure that these measures have minimal impact on radiation protection, safety systems or emergency response. In case of conflict, such solution must be reached when the overall risk to the workers and the public is minimized. The following items are recommended as protective measures.

3.3.4.1. Detection

Malicious acts can be detected by means of physical protection sensors, personnel surveillance and/or monitoring of operational processes. In the case of outsiders, detection measures focus on detecting penetration of protective layers by adversaries. Detection of malicious acts committed by insiders is more difficult. Insiders may be able to bypass many detection measures, owing to their access or by other available means. Therefore, protection measures in respect of insider threats should focus on the detection of insiders both during performance of adversary actions and during preparatory (unauthorized) acts such as the manipulation of safety equipment or the falsification of accountancy records. Therefore, the

detection of insiders may occur far later in the incident sequence than the detection of outsiders.

To be effective, detection must be assessed. It may be difficult to assess properly and quickly the nature of an act committed by an insider. This difficulty may seriously weaken the ability to provide respond in a timely manner.

An increase in a physical barrier or the complexity of achieving the malicious act can provide additional opportunities for detection or even deter insiders from attempting the malicious act.

The objectives of surveillance measures are to ensure that the activities of any authorized employee are always monitored by at least one other experienced, authorized employee in order to ensure that unauthorized acts can be immediately detected and reported (the 'two person rule'). This method of detection can afford a rapid means of both generating and assessing an alarm. Surveillance may be provided through co-workers, managers or closed circuit television coverage. In the event of a malicious act, recorded videos can be useful to put together a list of possible suspects. Surveillance may be a good tool to check whether unauthorized activities are occurring.

The two person rule requires at least two experienced persons to monitor one another in a sensitive area. This basic procedure is extended to require that at least two persons be present in a sensitive area in order for each person to verify that all actions are performed as authorized. Each of the two persons involved in the task should be technically qualified to immediately detect unauthorized activities. In addition, means should be provided to immediately report suspected malicious acts or suspicious activity. If subsequent investigation shows that no malicious acts were carried out, it is important that no penalty be imposed on either party for the false alarm, otherwise partners will be hesitant to report suspicious behaviour. This should be emphasized in security awareness training. To be effective, these two people must remain in full view of each other at all times, and must be fully informed about the authorized activities of the other. Ideally, the two person rule would assign two competent persons to perform a one person job. The two person rule is effective as long as the individuals do not become complacent through long term friendship or association. Whenever possible, managers should ensure that the members of such two person teams are rotated. Enforcing the two person rule for access to sensitive areas is a deterrent and may be an aid to detection. In addition, the two person rule can help to protect against insiders tampering with sensors.

Access control is used to allow only authorized entry or exit, and to prevent or detect unauthorized entry and exit. Access control is achieved by identifying individuals by means of an identifying device (one or more badges or keys), an access code (a lock combination or a personal identification number) and/or a personal identifier (biometrics). Access control provisions should also cover vehicles. Further, access control can be used to find out when people are present in different areas. If appropriately recorded, access control records can be used during the investigation of a malicious act to determine a list of possible suspects. Specific criteria should be established before authorizing access to a sensitive area (such as need to do a duty, need to be escorted, need to know and trustworthiness). Individuals granted access to a sensitive area should meet these criteria. Equipment used to generate badges and systems to assign access should be protected to prevent unauthorized assignment of access. Further, an access system should be periodically checked to ensure that it is effective.

Tracking the movement and location of personnel within the facility assists in protecting against violation of access rules and also in providing useful information after an incident. Existing technology makes it possible to track each worker throughout a facility by recording the locations and areas visited each day by the worker and the times that each location was visited. Awareness that a facility has a tracking system may deter a worker from carrying out unauthorized activities. Further, tracking records may be used during the investigation of a malicious act to generate an initial list of suspects.

Insiders may require tools, material and weapons that are unavailable or not allowed within the facility to carry out a malicious act. Therefore, checks should be made to prevent and detect the introduction of contraband items into sensitive areas. Contraband items may include unauthorized tools and material, radiation shielding material, weapons and explosives, as these could be used to gain access to or cause damage to sensitive components as well as to steal nuclear or other radioactive material. The stringency of searches should be commensurate with the sensitivity of the area, and searches performed close to the target should also be more stringent.

Methods of contraband detection include manual searches of personnel, packages and vehicles; use of metal detectors, X-ray machines and radiation detectors, or the use of dogs and explosives detectors. These methods should take into account the specifics of the facility and the threats against which protection is required. In specifying the locations at which searches are to be carried out, care should be taken not to place them so far from the

sensitive areas that it would be easy to bypass the checks. For example, insiders might bypass checks on the protected area boundary by throwing contraband over the protected area fence for later retrieval. Since vehicles are more difficult to be searched than personnel, it is advantageous to limit significantly the number of authorized vehicles having permission to enter sensitive areas.

For certain types of nuclear material, radiation detectors should be used on persons, in packages or in vehicles leaving to detect its unauthorized removal. Radiation detectors could be placed at pedestrian exits in tandem with metal detectors to enhance their effectiveness, as shielding material can be used to remove nuclear or other radioactive material from the nuclear facility.

Manual searches may also be used for monitoring persons and material exiting from an area. Random searches can be used to deter the unauthorized removal of nuclear or other radioactive material. If this is not in violation of safety rules, the exits should be locked on actuation of a security alarm.

Particular attention should be paid to emergency evacuation conditions, including exercises.

Special care should be taken during the detailed search of a cargo vehicle prior to loading and shipment to ensure that those persons carrying out the search are not able to introduce items that would aid a malicious act.

Monitoring the normal operation of processes or activities can be used to survey an area, to detect an unauthorized action or to provide an early assessment of alarms. The operating parameters of a nuclear facility (temperatures, pressures, flows, radiation monitoring, etc.) are checked continuously to ensure that they remain within the operating limits. An alarm should go off when one of these parameters exceeds a specified threshold. Since sabotage can cause an abnormal situation of the operating parameters, surveillance of operating parameters may help to detect malicious acts. It is crucial that a procedure for reporting of alarms be established between operational personnel and security personnel to ensure that alarms are quickly communicated to security personnel in the central alarm station. The actuation of an alarm should be communicated even prior to operations personnel assessing its cause (malicious or accidental). Operating personnel should monitor sensitive equipment, systems or devices to verify that no tampering or interference has taken place.

These operations may be very effective in detecting possible malicious acts on equipment or systems in relation to protecting nuclear or other radioactive material or sensitive areas. This approach contributes to both prevention and detection.

One measure to mitigate the consequences of a malicious act is to have the capability rapidly to replace parts that have been damaged. To achieve the desired goal successfully, it is prudent to provide protection for spare parts so that it would be difficult to destroy or compromise both the installed parts and the spare parts for vital equipment. Protection can be provided by, for example, installing barriers, storing the spare part at a distance from the installed part, as well as frequently monitoring storage.

Inspections and audits, in particular unannounced ones, might be an efficient way to prevent and protect against unauthorized removal of nuclear and other radioactive materials as well as sabotage. Inspections and audits can detect compromised equipment or abnormal conditions.

3.3.4.2. Delay

Delay is provided by personnel, procedures or physical barriers that increase the task time of an adversary. Most barriers are designed to delay penetration of areas, rather than to delay the carrying out of malicious acts, and thus have only limited impact on insiders. However, it is possible to develop barriers to delay malicious acts close to equipment or material (for example, locking a piece of equipment). Barriers close to equipment or material are especially effective when the area is under continuous surveillance. For insiders who do not have access to certain areas or material, installing barriers that an adversary could not overcome without using contraband items or highly specialized skills further strengthens prevention by deterrence and increases the likelihood of detection. Multiple layers of different physical or procedural barriers along all possible insider paths will complicate the progress of an insider by requiring a variety of tools and skills. Upgrading a barrier to force insiders to use more sophisticated tools complicates the requirements for resources, logistics, training and skills. Sophisticated resources may not be available at the facility and may have to be introduced on the site by insiders. By delaying the malicious act in this manner, insiders could be detected and defeated.

Delays can also be accomplished by the use of specially trained security personnel (such as guards). In some cases, the presence of such personnel may result in a significant delay in order to circumvent them, particularly for insiders with limited resources.

As a result of redundant equipment and automatic equipment shutdown, the task of an insider may be complicated by requiring the insider to defeat multiple redundant and dispersed facilities and equipment. These features can delay a malicious act and prevent it from being successfully carried out.

3.3.4.3. Response

Response to a malicious act committed by an insider can be made by both operating personnel and security personnel. Typically, operating personnel respond to the malicious act in order to reverse, mitigate or minimize it, and security personnel respond to insiders.

Classical analysis of response to outsider threats compares the response time with the time required for a sequence of outsider acts necessary to complete a malicious action. The implicit assumption in an outsider threat analysis is that the outsider will be easily identified anywhere on the site. None of this may be true for insiders, since a malicious act committed by an insider can consist of several acts separated in both time and space.

As mentioned above, an insider would not necessarily need to perform all the acts in a prescribed order, nor in quick succession. An insider may commit single acts and then wait to see if they are detected. The non-continuous nature of acts that insiders might attempt can seriously complicate the security response necessary to identify and apprehend them. As a result, investigation will play a more important role in response to insider threats. Furthermore, operating specialists may be required to assist in the investigation to predict, from the abnormal event, what further malicious acts might be attempted.

Every employee and contractor on the facility site should be prepared not only to detect a malicious act but also to react appropriately to protect themselves and the facility, and should know that the first action to take after detecting an event is to transmit the alarm according to a specified set of procedures. The procedures for transmitting the alarm should be a part of security awareness training.

It is important to recognize that any person involved in response may be insider (for example, an insider in the response team might use an emergency, simulate an emergency or create an actual emergency to mask a malicious act).

3.3.4.4. Emergency planning

Emergency plan should be developed to recover stolen nuclear or other radioactive materials and to mitigate or minimize the radiological consequences of sabotage.

Emergency plans do not usually differentiate between insiders and outsiders.

Consideration should be given to the fact that insiders could be members of the emergency response team and could disrupt recovery or mitigation efforts.

Plans should provide for the training of guards and response forces to perform their actions in a coordinated manner in the event of a malicious act.

Emergency plans should ensure coordination and protocols for operational interfaces between operators and local, regional and national authorities. Emergency plans developed for malicious incidents should be designed and coordinated within the general emergency response arrangements.

3.4. Evaluation of preventive and protective measures

3.4.1. Objectives and overview of the evaluation process

This evaluation process is a key component of a risk assessment that is intended to identify vulnerabilities of systems to insider threats. The result of the evaluation process is an evaluation of the effectiveness of preventive and protective measures in countering possible insider actions that could lead to the unauthorized removal of nuclear and other radioactive materials or sabotage.

Effectiveness of the preventive and protective measures should be regularly evaluated.

3.4.2. Evaluation of preventive measures

Exclusion of potential insiders is difficult as with all preventive measures, but the measures applied (such as trustworthiness checks prior to and during employment) are believed to be effective in reducing — but not completely eliminating — the possibility of insiders. These measures are reasonable and prudent precautions, even if their effect cannot be quantitatively evaluated.

However, the effective implementation of preventive measures can be checked and criteria can be specified and analyzed to ensure that the preventive measures are implemented as designed.

Prevention and protection against malicious acts committed by insiders accomplishes reduction of access, authority or knowledge of insiders, which are necessary to carry out successfully a malicious act leading to unacceptable radiological consequences.

3.4.3. Evaluation of protective measures

The measures used to detect, delay and respond to malicious acts can be quantitatively analyzed. Likelihood of detection and timeliness of response are often quantifiable and thus provide a basis for an analysis of the effectiveness of the protective measures.

The development of credible scenarios consists of identifying the combination of events necessary to accomplish the malicious act. For sabotage, consideration should be given to the actions that must be accomplished to initiate a sequence leading to unacceptable radiological or economical consequences.

Sabotage scenarios should include attacks against either single or multiple targets. For unauthorized removal of nuclear or other radioactive materials, the actions that must be successively accomplished to remove material from the facility should be identified. Scenarios involving unauthorized removal of nuclear or other radioactive materials should include situations in which insiders leave the facility directly with materials or hide material on the facility site and then removing it later under more favorable circumstances. Both protracted and abrupt theft should be considered.

Taking into account the design basis threat, the tasks that an insider would need to carry out should be defined in specific terms. The set of actions should consider both general actions and the areas where they are performed. The actions may occur along paths within the facility. All the protection elements that could be encountered by insiders along each of these paths or sets of actions should be defined. As insiders can perform the actions required for the malicious act over an extended period of time, the concept of adversary path analysis may not always be relevant.

By combining protection elements and insider defeat strategies for a set of insider actions, a credible insider scenario can be developed. Once a detailed insider scenario has been developed, the effectiveness of the protective measures is evaluated by considering the accumulated impact of detection, assessment and delay.

The effectiveness of the response will depend on both the effectiveness of interrupting the malicious act and the effectiveness of preventing the

consequences. Possible efforts by insiders to reduce the effectiveness of the response should be considered in the evaluation.