Preventive and protective measures against insider threats in nuclear facilities.

Dimitar Dimitrov
Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: *One of the main threats to nuclear facilities can involve external or insider adversaries or both together in collusion (coop eration for an illegal or malicious purpose with another insider adversary or with an external adversary). In these case, the main effort is to prevent and protect against unauthorized removal of nuclear material and sabotage of nuclear material and facilities by insiders. This report applies to any type of nuclear facility - notably nuclear power plants, research reactors and other nuclear fuel cycle facilities - whether in design, construction, commissioning, operation, shutdown or decommissioning.*

KEYWORDS: *NUCLEAR FACILITIES, MALICIOUS PURPOSES, MALICIOUS ACTS, EXTERNAL OR INSIDER ADVERSARIES, UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL, SABOTAGE OF NUCLEAR MATERIAL AND FACILITIES BY INSIDERS.*

1. Introduction

The Nuclear Security Fundamentals publication [1] provides the objective and essential elements for the entire nuclear security regime. Recommendations indicate what a nuclear security regime should address for the physical protection of nuclear material and nuclear facilities [2], radioactive material and associated facilities [3], and nuclear and other radioactive material out of regulatory control [4]. These publications recognize the particular threats that could be posed by insiders, as well as the need to implement specific measures against insider threats and to evaluate those measures accordingly.

The objective of this report is to provide updated guidance to competent authorities and operators, shippers, and carriers on selecting, implementing and evaluating measures for addressing insider threats [5]. Threats to nuclear facilities can involve external or insider adversaries or both together in collusion (cooperation for an illegal or malicious purpose with another insider adversary or with an external adversary).

The report applies to preventing and protecting against unauthorized removal of nuclear material and sabotage of nuclear material and facilities by insiders. Also applies to any type of nuclear facility - notably nuclear power plants, research reactors and other nuclear fuel cycle facilities (e.g. enrichment plants, reprocessing plants, fuel fabrication plants, storage facilities) - whether in design, redesign, construction, commissioning, operation, shutdown or decommissioning.

2. Identification of insider threats

The term "adversary" is used to describe any individual performing or attempting to perform a malicious act. An adversary could be an insider or could be external.

The term "insider" is used to describe "an individual with authorized access to nuclear material, associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities to have an adverse impact on nuclear security" [1].

The term "external adversary" is used to describe an adversary other than an insider.

2.1 Attributes of insiders

Insiders possess at least one of the following attributes that provide advantages over external adversaries when attempting malicious activities:

(a) Access: Insiders have authorized access to the areas, equipment and information needed to perform their work. Access includes physical access to nuclear facilities, nuclear materials and associated systems, components and equipment and computer systems;

(b) Authority: Insiders are authorized to conduct operations as part of their assigned duties and may also have the authority to direct other employees. This authority may be used to support malicious acts, including either physical or computer based acts such as digital file or process manipulation.

(c) Knowledge: Insiders may possess knowledge of the facility, associated activities or systems, ranging from limited to expert knowledge. This may include knowledge that could enable an insider to bypass or defeat dedicated physical protection systems and other facility systems that contribute to nuclear security.

2.2 Motivations of insiders

Insiders may have different motivations for initiating malicious acts, including money, ideology, revenge, ego, coercion or a combination of these motivations.

An insider may independently develop sufficient motivation to perform a malicious act, including as the result of a mental health issue. An insider may also be recruited by an external adversary seeking to exploit the insider's access, authority or knowledge. An insider could be forced to commit a malicious act through coercion (e.g. blackmail).

An insider could hold any position within an organization, from the highest level to the lowest. Insiders at all levels could have sufficient motivation to perform a malicious act.

2.3 Categories of insiders

An unwitting insider is an insider without the intent and motivation to commit a malicious act who is exploited by an adversary without the unwitting insider's awareness. For example, in a computer based attack, an unwitting insider may not be aware that certain actions (e.g. clicking a malicious link in an email that is disguised as being from a trusted source) may provide information or authenticated access to an adversary.

An insider adversary is an insider that commits malicious activities with awareness, intent and motivation. An insider adversary may be passive or active, and an active insider adversary may be either violent or non-violent.

A passive insider adversary assists another adversary by providing information to be used in performing a malicious act. A passive insider adversary would not participate in the malicious act in any other way and would likely cease involvement if there was a high probability of being identified.

An active, non-violent insider adversary uses stealth or deceit to facilitate or conduct a malicious act and may provide information to another adversary. For example, an active, non-violent insider adversary may attempt an abrupt or protracted theft of nuclear material or may assist external adversaries in performing a malicious act by disabling or ignoring alarms or by opening doors.

An active, violent insider adversary is similar to an active, non-violent insider adversary but is also willing to use physical force against personnel to facilitate or conduct a malicious act. Depending on the circumstances, an insider adversary may move from non-violent to violent.

3. Target identification

Target identification, as described [6], determines which material and equipment needs to be protected from an adversary. Targets may include nuclear material, associated areas, buildings, equipment, components, information, systems and functions.

3.1 Targets for unauthorized removal

Nuclear material targets for unauthorized removal can be assigned to one of three categories (I-III) according to the relative attractiveness and characteristics of the nuclear material as well as the potential consequences if it were used in a nuclear explosive device.

The identification of potential targets for unauthorized removal of nuclear material by an insider adversary should take into account the possibility of both abrupt and protracted theft.

Abrupt theft is the unauthorized removal of a target or a significant quantity of nuclear material during a single act.

Protracted theft is the repeated unauthorized removal of potentially small quantities of nuclear material from either a single location or multiple locations.

3.2 Sabotage targets

Sabotage targets in a facility are determined by analyzing the potential for the facility's radioactive material inventory and waste, including nuclear material and radioactive sources [3], to result in unacceptable radiological consequences or high radiological consequences.

The identification of possible combinations of actions (scenarios) an insider adversary might take to degrade facility structures, systems and components that may result in unacceptable radiological consequences or high radiological consequences should be part of the target identification process [7].

3.3 Identification of systems that contribute to nuclear security

A target identification process should consider all systems that could require additional protection from insider threats. Physical protection systems, NMAC systems and safety and process control systems should be considered as potential targets for malicious acts, including those initiated by an insider adversary [8].

An insider adversary may have authorized access to the facility or to information about the facility and might attack other structures, systems or components to indirectly perpetrate an attack, mask malicious acts or aid an external adversary.

The compromise of computer based systems in a facility could adversely affect safety, the security of nuclear material or accident mitigation. The operator should evaluate and protect computer based systems that contain information related to safety or security in accordance with the risk and the potential consequences of the release of this information [9].

The operator should consider providing additional training to employees and contractors with access to sensitive systems to raise security awareness. External adversaries may target insiders with access to a facility, sensitive information, sensitive information assets or the facility's networks to gain assistance in facilitating or masking malicious activities.

4. Measures against potential insider threats

Nuclear security measures used to protect against insider threats should include both preventive and protective measures [10]. The term “preventive measures” refers to measures used to reduce the number of potential insiders before individuals are granted access, to minimize opportunities for an insider to undertake a malicious act if access is granted or to prevent a potential insider adversary from carrying out a malicious act. The term “protective measures” refers to measures used to detect or delay malicious acts, respond to malicious acts or mitigate the consequences of a malicious act.

4.1 Implementing measures against insider threats

Preventive and protective measures should both be used to protect against potential insider threats.

Preventive measures can be used as follows:

(a) To reduce potential insider threats before allowing individuals access by identifying undesirable behaviors or characteristics that may indicate motivation;

(b) To further reduce potential insider threats after insiders have gained access by identifying undesirable behaviors or characteristics that may indicate motivation;

(c) To minimize opportunities for malicious acts by limiting access, authority and knowledge of insiders.

Protective measures can be used as follows:

(a) To detect, delay and respond to malicious acts;

(b) To mitigate or minimize the consequences of a nuclear security event and, if necessary, locate or recover the material.

4.2 Implementing preventive measures

The goal of preventive measures is to reduce the number of potential insider threats and to minimize the opportunity for insiders to perform a malicious act. Preventive measures should be applied before employment, during employment and upon termination.

In addition, preventive measures include quality assurance and specific computer security measures.

Measures to be applied before employment.

Individuals applying for work that requires access to a facility should be subject to identity verification, personal document verification and trustworthiness assessments.

Measures to be applied during employment.

Insiders who have passed the pre-employment checks and have been granted authorized access, including access to critical assets, sensitive information and vital areas, should be subject to the various measures. A security awareness programme for staff and contractors should be developed and implemented.

The security awareness programme should include clear security policies, the enforcement of security practices and continuous training. The purpose of training is to establish an environment in which all employees are aware of security policies and procedures so that they are able to aid in detecting and reporting suspicious or erroneous behaviour as well as unauthorized acts. Training should include methods to evaluate security awareness and training effectiveness as well as processes for continuous improvement or retraining. In addition to preparing personnel for the possibility of a physical incident at the facility or against its assets, the training should prepare personnel for the possibility of a cyber-attack.

Measures to be applied upon termination.

An individual's access and authority, including computer access, should be cancelled upon termination of the individual's position, employment or contract.

Termination procedures should be established and should include revoking physical access to the facility; using a non-disclosure agreement to protect sensitive information; and changing encryption keys, passwords,access codes and quality assurance programmes.

The quality assurance programmes should include all facility systems that contribute to nuclear security to ensure adequate protection against insider threats.

Quality assurance should require configuration management of the nuclear security systems to ensure that they continue to meet the desired performance criteria of these systems and to understand any potential consequences when changes are made to the systems, for example by an insider.

Measures for computer based systems.

While certain measures, such as escorting, may be effective in limiting insider access to nuclear and radioactive material, they do not provide sufficient protection against potential insider threats to computer and network systems; such protection may be provided by information security measures [11, 12].

The facility operator should define and implement a policy addressing the acceptable use of computer based systems. This policy may define the approved use of computer based systems, outline employer expectations for monitoring approved use of these systems, provide for training and explicitly identify prohibited actions on computing systems. The facility operator should also consider the use of technical measures to enforce or enhance the systems policy.

4.3 Implementing protective measures

The purpose of protective measures against insider threats is to detect, delay and respond to a malicious act after it has been initiated and may include mitigation of consequences and recovery of nuclear or radioactive material. When designing and implementing protective measures, efforts should be made to ensure that these measures are supportive of and do not have an adverse effect on facility operations and safety. In case of conflict, particularly with safety, a solution should be reached in which the overall risk to the workers and the public is minimized and sufficient security is maintained.

Detection measures.

The detection of malicious acts attempted by external adversaries focuses on detecting the penetration of any one of a facility's protective measures. By contrast, insiders could bypass or defeat certain physical protection owing to their authorized access, authority and knowledge. Operators should implement multiple and diverse protective measures for these systems to detect potential malicious acts performed by an insider and to provide the information needed for investigation and analysis. The facility operator should investigate all of the information provided by these detection measures in a comprehensive manner. Individual signals that seem insignificant might produce an indication of a malicious act when examined together.

Facility detection measures implemented against insider threats typically include measures related to:

Access control; Personnel tracking; Detection of prohibited items; Surveillance and computer security.

Delay measures

Multiple layers of different physical protection or procedural measures, including compartmentalization and separation of duties, can complicate the progress of an insider adversary by requiring a variety of tools and skills, thus providing additional time and opportunity for detection. By delaying the malicious act in this manner, an insider adversary could be detected and defeated. Delay may also deter insiders from attempting malicious acts.

Response measures.

Both operations and security personnel may respond to an irregularity (e.g. an inventory difference, an opened door that should be locked). Typically, operations personnel respond to an irregularity to investigate its cause. If an irregularity is suspected to be due to a malicious act, security personnel should be notified and should respond if necessary.

5. Comprehensive elements that reinforce preventive and protective measures

5.1 Nuclear security culture

Nuclear security culture plays a key role in ensuring that individuals, organizations and institutions remain vigilant and that sustained measures are taken to counter insider threats. The effectiveness of preventive and protective measures against insider threats depends on the attitudes, behaviors and actions of individuals [13].

Management should promote a robust nuclear security culture to counter insider and external threats. The nuclear security culture creates the overall conditions for personnel to implement both preventive and protective measures. A facility's nuclear security culture should improve loyalty and adherence to security policies. For example, management should emphasize the employees' responsibility to report unusual activities or suspicious behavior without fear of suffering disciplinary actions [14].

5.2 Contingency plans

The contingency plans developed by the operator should address measures to respond to both insider and external threats. Protective measures against insider threats should be coordinated with contingency plans in accordance with agreed procedures. The contingency plan should require that personnel evacuating a building during a real or simulated emergency be controlled and examined for contamination and nuclear material to protect against insider threats.

5.3 System maintenance and recovery programme

A maintenance and recovery programme for all facility nuclear security systems that need to be protected may mitigate the consequences of a malicious act by an insider adversary. The maintenance programme should include the capability to rapidly repair operational and other vital systems, to rapidly replace parts that have been damaged and to implement compensatory measures as needed. Rapid repair and replacement limit the duration of the system outage and the time available for any subsequent malicious actions and may mitigate the consequences of the insider adversary's malicious act.

6. Evaluation of measures

6.1 Objectives and overview of the evaluation process

Evaluating the effectiveness of preventive and protective measures against insider threats is a key component of a risk assessment that is intended to identify systems vulnerable to insider threats.

The results of the evaluation should be compared with previously established criteria for the effectiveness of preventive and protective measures. These criteria are usually established by the competent authority and are based on the potential consequences of a malicious act by an insider adversary and its likelihood of success.

Evaluation of the effectiveness of the preventive and protective measures should be based on the operator's security plan. If the evaluation indicates that the preventive and protective measures defined in the security plan do not meet the criteria, upgrades

should be implemented and the evaluation should be repeated until the criteria are met.

6.2. Evaluation of preventive measures

The implementation of preventive measures should be evaluated to ensure that they are implemented as designed. Although difficult to evaluate quantitatively, preventive measures can be effective in reducing the possibility of insider threats.

Preventive measures should be evaluated by conducting performance testing on procedures to determine whether the procedures are adequate to address the threat and whether employees follow the procedures

The opportunity for an insider adversary to perform a malicious act can be minimized by reducing the possibility for an insider to gain the access, authority or knowledge necessary to successfully carry out a malicious act. Credible scenarios for evaluation will incorporate the degree to which and the manner in which opportunity is minimized. A review should be performed to identify what preventive measures are in place and whether they are properly applied.

6.3 Evaluation of protective measures

The effectiveness of the measures used to detect, delay and respond to malicious acts (protective measures) can be quantitatively or qualitatively analyzed. The likelihood of detection and the timeliness of response are often quantifiable and can provide a basis for an evaluation of the effectiveness of the protective measures.

One way to evaluate the effectiveness of the protective measures against insider threats is to develop credible scenarios, including scenarios of collusion with other insider adversaries or with external adversaries, as appropriate. The effectiveness of the protective measures in countering these scenarios can then be evaluated.

The evaluation process should be repeated for credible scenarios that require further analysis. Conclusions about the effectiveness of protective measures should be based on the results of all the evaluations conducted.

7. Conclusions

The process of evaluating a facility for protection against insider threats begins with characterizing insiders according to attributes, motivations and categories to identify potential insider threats. The next step is target identification, which involves an evaluation of the assets that need to be protected from unauthorized removal or sabotage. The result of this evaluation is a prioritized list of targets.

Preventive measures should be implemented using the concept of defence in depth and a graded approach to minimize opportunities for the identified threats and targets to be subject to malicious acts.

Protective measures should be identified to protect targets in protected, inner or vital areas in a prioritized manner. The measures to detect, delay and respond to the insider threat should be increased in depth by using the results of the evaluation.

Preventive and protective measures against sabotage and unauthorized removal of nuclear material should be evaluated using a method such as the development of credible scenarios. Scenarios should be consistent with the threat assessment or DBT and may include physical attacks, cyber-attacks or a combination of both at the facility, along transport routes and within supply chains.

The system should be re-evaluated periodically to ensure that the measures are effectively implemented and sustained. The timing of the re-evaluation might be cyclic, or it might be triggered by changes to the threat or to the facility and its operation.

8. Acknowledgement

The issues discussed in this report are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum communication, intelligent security systems and risk management (Quasar) " , which has received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

Bibliography

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/ Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).
[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, International civil aviation organization, International criminal police organization-interpol, United nations interregional crime and justice research institute, united nations office on drugs and crime, world customs organization, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).
[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and protective measures against insider threats, Implementing guide, IAEA Nuclear Security Series No. 8-G (Pev. 1), IAEA, Vienna (2020).
[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
[7] Panevski V.S., „POSSIBLE APPROACH FOR DEVELOPING A MODEL OF INTELLIGENT SECURITY SYSTEM APPLICABLE IN ITS DESIGN IN THE QUASAR CENTER OF COMPETENCE“, SECURITY & FUTURE, 4, 2, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2020, ISSN:2535-082X, p.p. 47-50;
[8] Panevski V.S., „COMPATIBILITY BETWEEN DESIGN OF MECHATRONIC SYSTEMS FOR CRITICAL INFRASTRUCTURE SECURITY AND TECHNOLOGICAL READINESS LEVELS“, International Scientific Journal “Security & Future”, 4, 3, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2020, ISSN:2535-0668, p.p. 111-114;
[9] Valeri Panevski, “Some standardized peculiarity in defining the processes / stages providing input data for Intelligent Security Systems development – peripheral security systems”, International Scientific Journal “Security & Future”, vol. 5, issue 1, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2021, ISSN:2535-0668, p.p. 3-6;
[10] Valeri Panevski, “Possible integrity framework between the Intelligent Security Systems parameters and the Business Continuity Management processes”, International Scientific Journal “Security & Future”, vol. 5, issue 2, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2021, ISSN: 2535-0668, p.p. 42-45.
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28-T, IAEA, Vienna (2007).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).