ENISS
European Nuclear Installation Safety Standards

REPORT

INSIDER RISK MITIGATIONS IN NUCLEAR POWER PLANTS

OPERATORS' GOOD PRACTICES

September 2025

Summary

The key to ensuring an effective insider risk mitigation in a Nuclear Power Plant (NPP) is that the licensee/operator should implement an effective 'Barriers Model' which provides concentric layers of security to protect the most vital areas on the NPP site. This should be a comprehensive security solution based on a mix of cultural, procedural, and physical controls. The intention of these arrangements is to ensure that all mitigations work together to reduce the likelihood of insider success to a minimum.

Table of Contents

1. INTRODUCTION

This paper is intended to provide operator good practice for mitigating against the potential of an insider risk within a Nuclear Power Plant (NPP). It sets out a range of guidelines and mitigation measures which can be used by operators to enhance their security arrangements.

All good practices in this position paper are provided for guidance purposes only.

2. INSIDER RISK

It was agreed within the ENISS members that whilst the Design Basis Threat (DBT) and national regulatory arrangements vary across NPP operators, the potential for an insider risk is relevant to all.

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 or other acts determined by the State to have an adverse impact on nuclear security'.*[1]

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

- Access: Insiders have authorised 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. Access also includes remote computer access to a facility, such as access to computer systems and networks that control processes, provide safety, contain sensitive information or otherwise contribute to nuclear security.

- Authority: Insiders are authorised to conduct tasks 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.

[1] Source: IAEA Nuclear Security Series No8-G (Rev. 1) Preventative and Protective Measures against Insider Threats.

- 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 dedicated physical protection systems and other facility systems that contribute to nuclear security.[2]

In order to identify the potential threat, it is appropriate to define what constitutes the various elements of potential insider activity and these are defined below:

- Insider Risk: The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.

- Insider Threat: An insider, or group of insiders; that either intends to or is likely to cause harm or loss to the organisation.

- Insider Event: The activity conducted by an insider (whether intentional or unintentional) that could result in, or has resulted in, harm or loss to the organisation.

From the above, it is important to recognise that there are different categories of insider, which have legitimate and approved access to a NPP and therefore have the potential to exploit their authorised access for malicious acts. These different categories can be defined as follows and the potential end result is the same:

- The **'unwitting insider'** – This can be defined as an individual without the intent and motivation to commit a malicious act who is exploited by an adversary without the unwitting insider's awareness.

- The **'insider adversary'** – This can be defined as an individual that commits malicious activities with awareness, intent and motivation. An insider adversary may be passive or active. It is worth highlighting, that the insider adversary could be motivated prior to joining the nuclear industry or subverted after joining.

Both of the above scenarios are plausible, but with differing degrees of motivation. However, the 'insider adversary' is likely to be more motivated and hence harder to deter, as they will be dedicated, driven and focused on their aim, motivation or intention to subvert site security or cause a malicious activity. It is also worth highlighting, that an 'unwitting insider' could be an individual under pressure, because their family has been threatened or held hostage.

[2] Source: IAEA Nuclear Security Series No8-G (Rev. 1) Preventative and Protective Measures against Insider Threats.

3. SECURITY CULTURE AND ORGANISATIONAL MITIGATIONS

In order to provide a comprehensive and effective security model for a NPP, it is important to ensure that the security culture is set to provide an environment which will make it difficult for an insider to successfully operate. Against this context, NPP operators should ensure that their security culture is one which reflects the following:

- Security is not just the responsibility of security staff and it is important that all NPP employees have the capacity to detect a behaviour change and report accordingly; using the concept of 'see something, say something'.

- The site promotes the message that security is an integral part of nuclear professionalism; ensuring that safety & security have the same priority.

- The site conducts a periodic self-assessment of security culture in order to help detect and address potential weaknesses, reinforce staff awareness and accountability. In addition, this will ensure compliance with regulations, enhance preparedness in case of malicious acts and support continuous improvement of the security regime.

- Security is a critical business enabler and should be considered by NPP senior management to be not just another overhead, but a key requirement.

- Operators should clearly state the security requirement and why arrangements are in place to staff, in order that they are better able to enhance the arrangements and provide additional 'eyes and ears', to act as a security multiplier.

- Effective site security induction training for all who require unescorted access; this will ensure staff have received adequate and appropriate security training and are aware of their role, requirements and why they must comply with the security arrangements.

- That staff receive regular, timely and appropriate security communication, which will refresh & inform staff on why they are required to comply with the security arrangements.

- Use of the established safety challenge culture and recognition that all staff and contractors have a part to play in order to ensure that the security arrangements are maintained.

- A culture where all staff are able to identify *the "absence of the normal"* or "*the presence of the abnormal"*.

- The creation of a workplace environment that is hostile to an insider. This will ensure that any potential insider, finds it challenging to undertake malicious activity, due to the potential to be detected or challenged.

- The targeted use of vetting – ensuring that unescorted staff hold appropriate levels of national security vetting.

In order to provide appropriate organisational arrangements, effective Personnel Security measures should be implemented or considered as follows:

- That staff update any changes in their personnel circumstances.
- That vetting is renewed in accordance with national arrangements and does not lapse.
- Formal functional collaboration between Occupational Heath, Security and Human Resources functions, to establish an effective 'Golden Triangle' which is able to share information about NPP staff and ensure that any potential risks can be managed accordingly by senior management.
- Sites should consider their 'aftercare' or ongoing personnel security arrangements for any potential risks, whether identified through the site 'Golden Triangle' (see above bullet point) or from other means.
- Consideration of 'two persons working' in key areas, such as critical systems and access control, in order that one person is not able to conduct a malicious act. The key to the 'two persons working' is that both members of staff are suitably qualified and experienced in order that they can monitor each other's activity.
- Periodic questionnaire submitted to all employees in order to assess security culture and this could include a targeted survey to assess the psychological risk of employees to become an insider.
- Social-media profiling prior to hiring employees, in compliance with the General Data Protection Regulation in the EU, national data protection and privacy laws, in order to evaluate the potential risk of insider activity.
- Inclusion of a drug & alcohol testing regime for current NPP staff, but also as part of the pre-employment screening for new employees.
- Consideration to conducting an insider threat exercise in order to test readiness of the security regime and ensure that the arrangements are adequate.
- Develop a robust incident response plan which will provide clear procedures and strategy to respond and investigate potential insider threats effectively.
- Consideration to use psychometric assessment testing for NPP staff operating in the most sensitive areas.
- Collaborating and engaging with security partners to ensure alignment and that best practice is implemented.

- Clear articulation to staff of what constitutes a breach of standards and a potential disciplinary matter; ensuring that site staff fully understand what is required of them.

Understanding what security risks a NPP faces is essential for developing appropriate and proportionate security insider risk mitigation measures. A role-based risk assessment, conducted by suitable stakeholders, should:

- Identify the critical assets in the organisation.
- Identify the threat (based on intent and capability), in compliance with the DBT.
- Assess the likelihood of the threat happening in the organisation.
- Assess the impact to the business if the threat occurred.
- Review the adequacy of existing countermeasures.
- Propose new proportionate measures where required to reduce insider risks, to as low as reasonably acceptable.

4. PHYSICAL AND TECHNICAL SECURITY MITIGATIONS

Some good practices in order to maintain effective security arrangements:

- Access control system across the entire site which is aligned with a staff pass and requires a personal identification number (PIN) in order to access authorised areas. This could include authentication measures with biometric control to enter the most sensitive areas within a NPP. At the design stage, technical measures should be implemented which ensure multiple validation stages by different persons so that a single individual is unable to provide a site entry pass.
- Security systems should be integrated in order that they can interrogate site access control, access pass status, vetting status and details of searches. This ensures that security staff have full visibility and situational awareness of site staff movements, and this therefore provides a more challenging environment for the insider.
- Clear rules for access to information systems with mandatory identification and authentication, with strong password with periodic changing and robust access control management to sensitive information assets. The key feature is that a ‘need

to know, right to know' principle is applied, ensuring that access to sensitive information is restricted to those who need it.

- Comprehensive search & explosive screening at access control points to site with various methods: visual search, explosive screening equipment and explosive search dogs.

- Minimise the number of vehicles on site and where possible use an off-site delivery point. All site deliveries should be scheduled and security staff aware of vehicles requiring site access.

- All vehicles requiring site access to be searched, including the use of explosive screening equipment, visual search and thermal imaging cameras. This is to provide mitigation against the potential for a 'Trojan Horse' scenario where a potential adversary attempts to gain access to a site hidden within a vehicle.

- Further searches of staff are conducted prior to their entry into the most sensitive areas of a NPP from a security perspective, which may include additional explosive screening. This will ensure that concentric layers of security are applied across the NPP to protect the most important asset. In addition, this may include biometric control of access.

- All unaccompanied site visitors are searched on entry and always escorted, whilst on site. In addition, it is imperative that the escort understands their role and what is required of them.

- Conduct randomised schedules for security patrols to avoid setting predictable patterns in order to reduce the potential for exploitation by an insider or external adversary.

- Effective cyber security controls with effective management and tracking of removal media; this is to include laptop computer registration, with a supporting pass. This is to be implemented for both site access and exit to ensure sensitive important and mobile media is suitably protected.

- Conduct regular vulnerability assessments of physical security arrangements and plans to ensure that any weaknesses, such as poorly maintained barriers or gaps in the arrangements, are corrected.