THE APPLICATION OF DEFENCE IN DEPTH IN NUCLEAR SECURITY

O. Gregoire

Moltex Energy Canada Inc., Saint John, New Brunswick, Canada
oliviergregoire@moltexenergy.com

Abstract

The design of reactor facilities requires the application of the concept of defence in depth when it comes to safety and security. As a nuclear safety concept, defence in depth is well defined, and its application can rely on a broad base of guidance material. Conversely, there is no such guidance for the provision of independent levels of defence in depth in nuclear security.

The multiple barriers of the physical protection system can be seen as a form of application of the concept of defence in depth, but the layers are not independent as they all contribute to detection and/or delay functions that need to be associated to a response function. The concept of defence in depth can, and should, be applied to those functions individually but this is essentially a means to provide redundancy to each function for a specific aspect of nuclear security, and does not relate to the wide-ranging requirements of an overall defence in depth as applied in nuclear safety.

To apply the concept of defence in depth coherently in both domains of safety and security, specific objectives and essential means are proposed, commensurate with the generic objectives, across the five levels defined in the nuclear safety concept. Based on this approach, a comprehensive framework for the structure of nuclear security provisions is proposed, that opens up new opportunities for improvement in areas wider in scope than the traditional physical protection system. The underlying structure can be applicable to both physical and cyber security considerations.

1. Introduction

The concept of nuclear security refers to the prevention of deliberate malevolent acts potentially affecting nuclear facilities and systems. The main international legal instruments in the area of nuclear security, adopted under the auspices of the International Atomic Energy Agency (IAEA), are the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment [1]. The Amendment to the CPPNM significantly strengthens the original document in a number of important ways. It extends the scope of the original treaty to cover physical protection of nuclear facilities and nuclear material used for peaceful purposes in domestic use, storage and transport. In Canada, plant-level security requirements for a nuclear facility are outlined in the Nuclear Security Regulations [2].

As specified in the obligations for high-security sites, physical protection measures need to be applied to counter a design basis threat (DBT), whose adequacy needs to be validated by a facility-specific threat and risk assessment [2]. Although it is specified that “potential adversaries” considered in the DBT and specific threat assessments may or may not have authorized access to

the facility, the vast majority of the provisions prescribed relate to the prevention of unauthorized access to protected, inner or vital areas. Only a handful of provisions related to searches can apply to individuals or vehicles with or without legitimate access. As such, these measures hardly address concerns such as an insider threat. As mentioned in section 6.2 of REGDOC 2.12.3, technical security measures should include measures to prevent unauthorized personnel from gaining access to nuclear material, but also protect against an act or attempted act of unauthorized removal and protect against an act or attempted act of sabotage [3]. Although the prevention of access by unauthorized individuals obviously supports protection against both theft and sabotage, further provisions can and should be applied to address these specific issues.

More generally, nuclear security provisions are traditionally regarded as corresponding to the "physical protection system" (PPS) of a facility, which is essentially designed to counter external threats by the early detection of a breach or bypass of the site perimeter and the delay of the intruder progression, therefore giving enough time to a response force to intercept the adversary before he/she reaches his/her target. This tendency to draw a direct link between nuclear security and the PPS is for example highlighted in references [4] and [5], where proposals related to the concept of "security by design" are specifically related to the improvement of the detection, delay or response functions of the PPS, or in reference [6] where it is clearly stated that the application of the "defence in depth" concept in the security approach relies on the multiple barriers of the PPS. These approaches are heavily derived from both prescription- and performance-based requirements related to the prevention of unauthorized access and is influenced by past practices when a PPS had to be provided around already existing facilities or around facilities not optimized to prevent theft or sabotage.

Although the PPS is an important component of nuclear security, further considerations can address high-level nuclear security requirements in the design of new facilities, and these can especially address some threats that are hardly prevented by physical protection alone. As mentioned previously, insiders are by definition individuals having a legitimate access and are therefore hardly affected by "unauthorized access" prevention measures. Besides, the multiple barriers of the PPS do not suitably defeat some other specific threats such as stand-off attacks with missiles or deliberate aircraft crashes, which are hardly addressed by the application of detection and delay of the adversary progression. The amended version of the CPPNM specifies that the concept of defence in depth (DiD) is a fundamental principle, reflecting a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order "to achieve his(/her) objectives" [1], and not only to reach a physical target.

The multiple barriers of the PPS are often seen as a form of application of the concept of DiD, as is for example reported in reference [6], but the layers are not independent as they all contribute to detection and/or delay functions that need to be associated to a response function. For instance, adversaries that could neutralize response forces or disrupt detection assessment capabilities for example could defeat the whole system at once. The concept of DiD can, and should, be applied to those functions individually but this is essentially a means to provide redundancy to each function for a specific aspect of nuclear security and does not relate to the wide-ranging requirements of an overall DiD as applied in the field of nuclear safety.

As a nuclear safety concept, DiD is well defined, and its application can rely on a broad base of guidance material. Conversely, there is no such guidance for the provision of independent levels of defence in depth in nuclear security. To apply this concept coherently in both domains of safety and security, specific objectives and essential means need to be identified, commensurate with the generic objectives, across the five levels defined in the nuclear safety concept.

2. Application of the defence in depth in nuclear security

REGDOC 2.5.2 reports five different levels of DiD as a fundamental safety concept in the development of nuclear reactors [7]. These levels are the ones described in the IAEA report "Defence in Depth in Nuclear Safety" [8]. Although no such description can be found for security considerations, the same classification can be applied to nuclear security if it is assumed that the concept of "failure" or "abnormal operation" in safety can be considered as an attempt of malevolent act (sabotage or theft of nuclear material), and an "accident" in nuclear safety would relate to the actual perpetration of a malevolent act in nuclear security. Based on these distinctions, specific objectives corresponding to the different levels of DiD may be defined, as reported in Table 1.

Table 1 Application of the five levels of defence in depth in nuclear security. The first column corresponds to the objectives reported in reference [8] for the different levels of DiD in the field of nuclear safety. The next column corresponds to a translation of these objectives when "failures" and "accidents" are seen as "attempts of malevolent acts" and "successful malevolent acts" respectively.

DiD Level	Generic objective	Objective in Nuclear Security	Essential means
1	Prevention of abnormal operation and failures	Prevention of attempts of malevolent acts	Deterrence
2	Control of abnormal operation and detection of failures	Detection of attempts of malevolent acts and interception after detection	Prevent unauthorized access (physical protection / cyber)
3	Control of accidents within the design basis	Limitation of the possibilities for malevolent acts by a Design Basis Threat	Robustness of the plant systems important to safety
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Mitigation of the consequences of a successful malevolent act / Limitation of the possibilities for malevolent acts by a Beyond Design Basis Threat	Complementary measures and accident procedures
5	Mitigation of radiological consequences of significant releases of radioactive materials	Mitigation of radiological consequences of significant releases of radioactive materials in case of sabotage (or recovery of stolen nuclear material)	Off-site emergency response

2.1 First level of defence in depth: Deterrence

The first level of DiD is the prevention of malevolent acts being attempted or even contemplated by potential adversaries. It essentially refers to deterrence aspects, rooted in the reduction of the (perceived) impact vs risk ratio in the adversary's calculus. Although some aspects of deterrence refer to a visibly robust PPS, it also includes the increase of uncertainty for potential adversaries through the protection of prescribed information. In the assessment of a PPS as mentioned in the following section, it is assumed that the adversary has a comprehensive knowledge of the system, whereas it is mandatory to protect this information from unauthorized disclosure. Considering that the efficiency of the PPS and the non-disclosure of its characteristics relate to two different levels of defence provides a rationale for this distinction and highlights its importance.

Another important aspect of deterrence relates to the legal framework of the host nation, and strong penalty prospects for nuclear-related offenses. Although this is out of the scope of the security provisions at a specific facility, it nevertheless contributes to deter potential adversaries and has an impact on the level of threat to protect against. The responsibility of the State in this framework is specifically highlighted in the legally binding international convention [1].

The upkeep of a comprehensive and coherent culture of security in the operator's structure also contributes to prevent malevolent acts from insiders in addition to assure the effectiveness of the nuclear security framework at large.

Finally, the risk of theft of nuclear material can be mitigated by a reduction of the attractiveness of the material, which is a contributing feature to both security and safeguards provisions.

2.2 Second level of defence in depth: Unauthorized access prevention

The second level of defence relates to the early detection of attempts of a malevolent act, essentially the detection of unauthorized access to a facility, as well as the interception of adversaries before they reach their target. This is typically the purpose of the PPS, which is designed to counter a threat corresponding to a physical assault on the site with capabilities represented by the generic DBT. This system integrates detection of breaching of the site perimeter as well as means to delay the progression of adversaries so that a suitable response force intercepts them on the path to their target.

The means of detection (including assessment), delay and response should not be considered as different layers of defense since they are all necessary to successfully intercept the adversaries. Instead, a comprehensive PPS represents one layer of defense.

The same concepts of detect, delay and respond can also be adapted to the cyber protection of digital systems or prescribed information in a defensive computer-based architecture.

This level of defence also includes the early detection (and mitigation) of potential insider threats through the programs implemented by the operator in terms of insider risk reduction and employees vetting.

2.3 Third level of defence in depth: Limitation of possible malevolent acts

The third level of DiD addresses the consideration that an adversary actually reaching his/her target (whether physically of by cyber means) should have limited potential to carry out a successful malevolent act. This essentially refers to the inherent capability of the plant systems to withstand such acts and assure the continued provision of fundamental safety functions.

Overall, these considerations of robustness of the systems against malevolent acts represent a further level of DiD against adversaries with capabilities comparable to the DBT if the PPS fails to intercept them. They also address standoff attacks or deliberate aircraft crash and provide a level of defense against "beyond design basis threat," although the robustness of the systems may not be designed to withstand malevolent acts carried out by adversaries having such capabilities.

A fundamental means to reduce the overall vulnerability of the facility through the design of the plant in preference to attempting to secure or mitigate vulnerable aspects post-design is to prevent the potential for sabotage in a way that as few areas as possible in the facility, and ideally none, would be considered as vital.

2.4 Fourth level of defence in depth: Complementary measures

The fourth level of defence addresses the mitigation of the consequences of a successful malevolent act. In the case of an act of sabotage, this is fundamentally provided by the fourth level of DiD in the safety concepts (and covered by corresponding requirements) since at this point of an incident progression a malevolent act is mostly similar to an accidental occurrence.

An important specific feature in terms of nuclear security is represented by compartmentalization to reduce the source term of the release of radioactive material from any area of the facility, therefore contributing to the absence of vital areas.

In terms of theft of nuclear material, the fourth level of DiD refers to a limitation of the amount and the chemical or physical form of available material.

2.5 Fifth level of defence in depth: Off-site mitigation capabilities

The fifth level of defence for an act of sabotage refers to the mitigation of the radiological consequences of significant releases of radiological material, should all other layers of defence fail. This is essentially covered by off-site capabilities provided by local, provincial or federal units. As for most of the considerations of the fourth level of DiD in the case of an act of sabotage, this is already considered as a specific layer of defence in nuclear safety.

For an act of theft of nuclear material, it relates to state-level (host nation as well as international partners) capabilities to track and retrieve stolen material.

3. Application of a graded approach in the provision of each level of defence in depth

In accordance with the concept of a "graded approach," the efforts to address security considerations within each level of DiD will be commensurate to the level of risk if this level of protection fails. It is therefore dependent on the protection that can already be provided by other levels of defence against the same threat. For instance, if it turns out that security provisions recommended to prevent a certain type of sabotage are not reasonably achievable or in conflict with safety considerations, compensatory measures could relate to improvements at other levels of DiD such as the identification of a specific vital area and its consideration in the performance requirements of the PPS.

The application of a risk-informed graded approach also brings some flexibility where the protection against a given threat is already robust. It is important to keep in mind that the high-level performance-based requirements apply to the facility in general, not to each system at each level of DiD. This could especially be important to consider in the perspective of the fielding of a fleet of small modular reactors in remote areas, for which the level of capabilities associated with current physical protection systems and response forces for large generating stations could hardly be applied.

4. Security by design provisions across the different levels of defence in depth

To identify a set of security provisions addressing high-level requirements across the different levels of DiD as comprehensively as possible, a list of specific security considerations has been derived from the descriptions of the five levels of DiD highlighted previously and is reported in Table 2. Each identified security provision is associated with a reference to the implementation level and corresponding stakeholder responsibility, whether it can be considered by the plant designer, implemented by the operator or addressed by local, provincial or federal authorities. Elements associated with "facility design" highlight opportunities for security-by-design considerations.

Table 2 Security provisions to address high-level requirements across the five levels of defence in depth.

Security DiD Level	Security Provision	Implementation level
1	State-level deterrence provisions	National policy and legal framework
	Plant-level deterrence provisions	PPS-related visible aspects (plant operator)
	Insider threat deterrence	Trustworthiness program / Security culture (plant operator)
	Limitation of attractiveness of NM for a theft perspective	Plant / process design option; Also a Non-Proliferation consideration
	Increase of uncertainty for potential perpetrators	Prescribed information protection (plant operator)
2	Access control to nuclear material	Access control procedures (plant operator) / Facility design (reactor designer / vendor)
	Detection of, Delay and Response to potential intrusions	PPS - Central Alarm Station - On-site response force (plant operator) / Facility design (reactor designer / vendor)
	Limitation of accesses for potential insider threat	Facility design (reactor designer / vendor)
	Limitation of accesses to systems by cyber means	Facility design (reactor designer / vendor)
3	Limitation of the potential for malicious manual intervention to impair safety functionality	Facility design (reactor designer / vendor)
	Limitation of the potential for sabotage inside of the facility	Facility design (reactor designer / vendor)
	Limitation of the potential for physical stand-off attack	Facility design (reactor designer / vendor)
	Limitation of the potential for cyber attack	Facility design (reactor designer / vendor)
	Prevention of unauthorized removal of material	Facility design (reactor designer / vendor)
4	Limitation of the source term	Safety case / Facility design
	Limitation of the release potential of radioactive material (chemical / physical form)	Safety case / Facility design
	Complementary mitigation features	Accident mitigation claims / safety case
5	Out-of-plant response capabilities for the management of radioactive release	Provincial / national / transnational response capabilities
	Out-of-plant capabilities for the retreival of stolen material	Provincial / national / transnational response capabilities

Elements identified in Table 2 highlight areas where the concept of security-by-design can be implemented. It is unsurprisingly of critical importance for the third level of DiD and the improvement of the robustness of the plant systems. It is also apparent that the design of new facilities provides opportunities of improvement for its physical protection system. Although there are some security provisions related to the plant design in the fourth level of DiD, most of these aspects are already being addressed as safety requirements.

5. Conclusions

The security provisions identified in this work are not new and are actually already implemented in most high security facilities. The novel aspect is to propose a framework for nuclear security, built on the best practices in the field of safety, that would integrate all these provisions in a comprehensive and structured approach rather than applying some of them as complementary means to compensate for the shortcomings of a physical protection system alone.

This framework would in turn open up new opportunities for improvement of security provisions in areas wider in scope than traditional physical protection, especially for the application of the concept of security-by-design for new nuclear facilities The underlying structure can be applicable to both physical and cyber security considerations. Security-by-design would specifically be important for plants where Category I nuclear material would be handled, or in the context of the deployment of small reactors in remote areas, for which the reliance on a full-scale traditional physical protection system may not be the most suitable option.

Finally, this framework highlights the relationship of nuclear security elements provided by, as well as the opportunities for improvement for, stakeholders such as the plant designer and the operator but also provincial or federal authorities.

6. References

[1] "Convention on the physical protection of nuclear material and nuclear facilities", Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod. 1 – corrected, 2021.

[2] "Nuclear security regulations", SOR/2000-209, Government of Canada Statutory Orders & Regulations.

[3] "Security of nuclear substances", REGDOC 2.12.3, Canadian Nuclear Safety Commission regulatory document.

[4] A. Evans et al., "New security concepts for advanced reactors", *Nuclear Sciences and Engineering*, 2022.

[5] "Proposed physical security requirements for advanced reactor technologies", Nuclear Energy Institute white paper, 2016.

[6] "Conceptual design of a pilot-scale pyroprocessing facility", Summary report revision 1, Argonne National Laboratory, 2018.

[7] "Design of reactor facilities: Nuclear power plants", REGDOC 2.5.2, Canadian Nuclear Safety Commission regulatory document.

[8] "Defence in depth in nuclear safety", International Atomic Energy Agency report INSAG-10, 1996.