IMSR400'S HOLISTIC APPROACH TO NUCLEAR SECURITY

J M Llambias[1] and R Ion[2]
[1] Risktec Solutions Limited, Warrington, United Kingdom
[2] Terrestrial Energy Inc., Oakville, Ontario, Canada
john.llambias@risktec.tuv.com, rion@terrestrialenergy.com

Abstract

Nuclear security has traditionally been retrospectively applied to nuclear facilities based on prescriptive national regulations. These regulations have aimed to protect the facility from the 'outside-in' via the provision of a physical protection system and armed response force. Developments in the adversarial threat over the recent years, in particular the insider and cyber threat, are challenging this approach to nuclear security. This paper presents an alternative approach which starts with the asset requiring protection and applies an understanding of the reactor design and safety systems to deliver a pragmatic and holistic nuclear security solution founded on a defined clearly defined hierarchy of controls. This paper illustrates the practical implementation of the security by design approach by Terrestrial Energy Inc. (TEI) for the IMSR400 design, a Small Modular Reactor (SMR) technology, as part of its Basic Engineering program and presents the benefits of this new approach compared to the traditional approach.

1. Introduction

Nuclear security has traditionally been retrospectively applied to nuclear facilities based on prescriptive national regulations. These regulations have aimed to protect the facility from the 'outside-in' via the provision of a physical protection system and armed response force and have, in general, withstood the test of time.

However, developments in the adversarial threat over the recent years are now challenging this approach. The 'outside-in' physical protection is ineffective in preventing a knowledgeable insider who has authorised access to the facility from carrying out a malicious act. Similarly, it is ineffective in protecting against a cyber threat that may originate from a different geographical location and may not require any physical malevolent act on-site for its pursuit. Additionally, SMRs and their intended deployment are challenging the traditional approach.

This paper presents an alternative holistic approach to nuclear security. It is in the form of a nuclear security case that effectively addresses these challenges and delivers proportional risk informed security. The approach starts with the identification and understanding of the assets requiring protection, and applies the hierarchy of risk control principle to manage the security risks with the aim of developing a blend of inter-related layers of protective physical, cyber and procedural measures around the asset to provide proportional protection. The approach provides an opportunity to security inform the design at the earliest opportunity, integrate

safeguards with security. It also provides an opportunity to integrate safety, security and environmental, including the removal of any conflicts.

2. Fundamental nuclear security objectives

Nuclear security aims to deliver two fundamental security objectives, as follows:

1. The prevention of sabotage of nuclear material; and

2. The prevention of unauthorized removal of nuclear material or prescribed information from the site.

The second objective is closely aligned with the delivery of the nuclear safeguards obligation, which aims to prevent the unauthorised diversion of certain types of nuclear material by the nation-state. To this end, the alternative approach integrates nuclear security with nuclear safeguards under the second objective.

3. Nuclear security case

The nuclear security case aims to demonstrate to stakeholders that the nuclear security risks at the plant are understood, managed and adequately controlled, and that the above fundamental nuclear security objectives are met. In support of this, the nuclear security case makes the following eight high level security claims.

1. The nuclear material inventory within the nuclear facility is identified and categorized.

2. The prescribed information held within the nuclear facility is identified.

3. The assets and areas within the nuclear facility requiring protection to prevent the sabotage of the nuclear material are identified.

4. The assets and areas within the nuclear facility requiring protection to prevent the theft of the nuclear material or prescribed information are identified.

5. The national Design Basis Threat (DBT) is interpreted to define the adversary capability and threat against the nuclear facility.

6. Protection against theft and sabotage is provided via a combination of robustness in design, physical, cyber and procedural protective measures, supplemented by safeguards, to provide defence in depth.

7. Areas within the nuclear facility are security classified to facilitate the provision of proportional protection, which is delivered to each area by an Integrated Security Solution (ISS).

8. The site security operations deliver the ISS, which is regularly tested and reviewed to confirm its ongoing validity and effectiveness during the plant lifecycle.

Figure 1 presents an illustration of the nuclear security case showing how these eight claims integrate to deliver the fundamental nuclear security objectives.

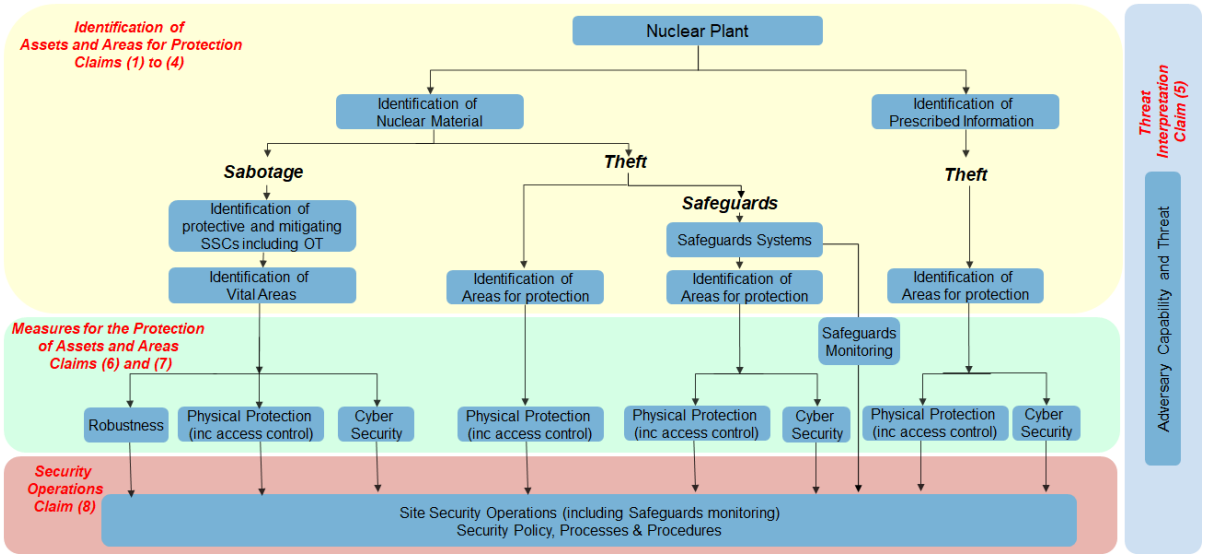

Figure 1 Nuclear security case.

These eight high level security claims also provide a roadmap for the development of the nuclear security arrangements at a nuclear plant. This roadmap is of benefit in non-prescriptive and risk-informed regulatory regimes as it provides a structured approach for the development and justification of plant-specific nuclear security arrangements by a prospective licensee. Furthermore, this approach is well suited for new nuclear power plant designs and projects and especially for Small Modular Reactors (SMRs).

The development of plant specific security arrangements using the eight high level security claim roadmap is discussed further in the subsequent sections, with a focus on design development activities.

3.1 Identification and categorization of nuclear material (Security Claim 1)

The starting point for the nuclear security case is the development of a nuclear inventory for the nuclear plant, as the primary aim of the nuclear security case is to protect the nuclear material from theft or sabotage. The nuclear material in this context refers to both fissile material and other irradiated material, which are referred to in this paper as Nuclear Material (NM) and Other Radioactive Material (ORM), respectively. The nuclear inventory includes the characteristics of the material, its quantity, form and location, as well as information on changes during the lifetime of the plant.

Having established the nuclear inventory, the material comprising the nuclear inventory needs to be categorized for theft and sabotage in order to provide the basis for developing proportional security arrangements.

Categorization of the plant for theft is based on the characteristics and quantity of the NM within the plant nuclear inventory. It is informed by national regulations, for example Schedule 1 of the Canadian Nuclear Security Regulations (Ref. 1). All nuclear material, whether NM or ORM is required to be protected from theft.

Categorization for sabotage is dependent on the radiological consequence of a release of radiation due to the sabotage of the nuclear material. Nuclear material with the potential to result in Unacceptable Radiological Consequences (URC) is protected from sabotage. The URC is defined in terms of off-site dose limit, the level of which is normally set by national regulators. In some regulatory regimes more than one category of URC is defined to enable proportional security to be provided against sabotage.

3.2 Identification of prescribed information (Security Claim 2)

An inventory of nuclear sensitive information requiring protection (i.e., Prescribed Information) is developed. The definition of the sensitive information is also informed by national security regulations; for example a definition of Prescribed Information is given in Section 21 the General Nuclear Safety and Control Regulations (Ref. 2). The inventory of sensitive information will include its form (e.g., digital or hard copy) and details on the location(s) where the information is stored and handled.

3.3 Identification of assets and areas requiring protection to prevent sabotage (Security Claim 3)

3.3.1 Identification of Vital Areas

The protection of nuclear material against sabotage requires the identification of the Structures, Systems and Components (SSC) that keep the material in a safe and stable state in response to sabotage events. The SSCs that maintain, in a safe and stable state, the nuclear material capable of creating a URC if sabotaged together with the nuclear material itself are referred to as Critical Assets (CAs). The areas in which the CAs are housed are defined as Vital Areas (VAs).

The VA Identification (VAI) is carried in four phases, as illustrated in Figure 2 and summarised below. It is informed by and consistent with the IAEA guidance (Ref. 3). The opportunity is taken during each of stages to eliminate or minimise the number of CAs and VAs in accordance with the security hierarchy of control principle (see Section 3.6.2 (a)).

Phase 1 – Analysis of NM/ORM inventory: This first phase analyses the nuclear material inventory to determine which NM/ORM is capable of delivering a URC. This phase is carried out in support of Security Claim 1 as noted in Section 3.1 above. NM/ORM which is capable of creating a URC if unprotected and unmitigated is considered further in Phase 2. It is noted that this analysis considers also the potential for an accumulation of NM/ORM in one place to deliver a URC.

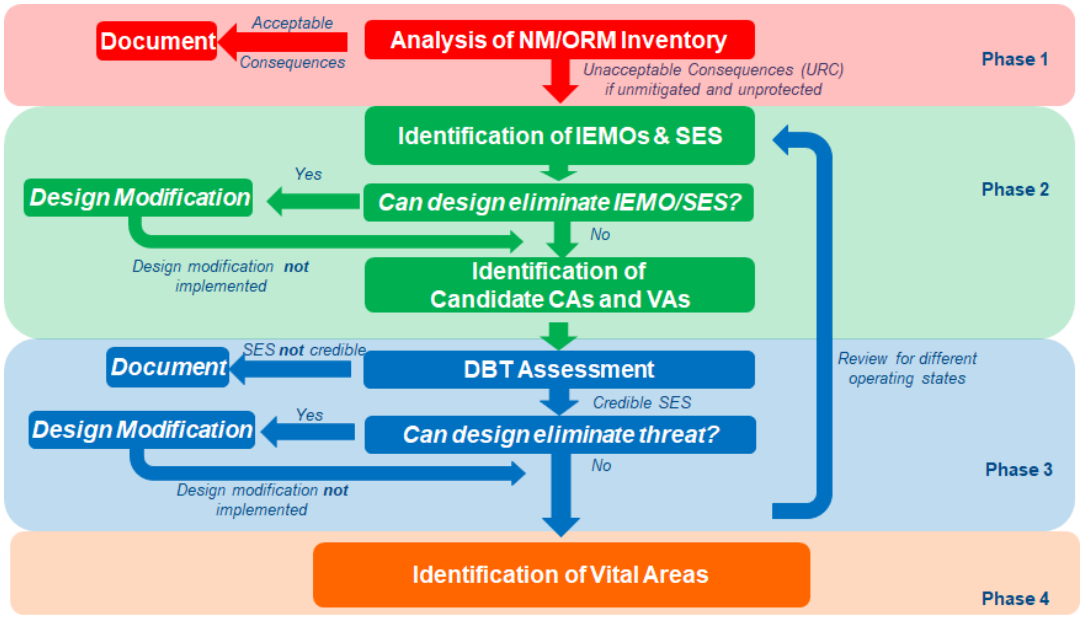

Figure 2 VA Identification process.

Phase 2 – Identification of candidate CAs and VAs: The identification of CAs is informed by the safety analysis and provides a direct link back to the nuclear safety case. A review of Postulated Initiating Events (PIEs) developed for the safety analysis is carried out to identify which of these events can be initiated maliciously, and these become potential Initiating Events of Malicious Origin (IEMOs). Through structured workshop expert elicitation, other potential IEMOs are then identified from a review of those considered and excluded from the safety analysis on the basis of incredibility of occurrence, for example, and from brainstorming with operators and designers who have been informed of potential adversary capabilities. The latter is generally done on the basis of a generic adversary capability rather than site-specific adversary capability to facilitate the involvement of as wide a participation as possible during the workshops without compromising national information security requirements.

Informed by the safety analysis, the SSCs that prevent the potential IEMOs from developing into an accident sequence leading to the loss of a fundamental safety function (e.g. cooling, containment, control of reactivity) are identified. Similarly, the SSCs that mitigate the consequences following the loss of the fundamental safety function are also identified. The potential IEMO and the associated protective and mitigating SSC create a potential Sabotage Event Scenario (SES). This is because should the adversary successfully initiate the IEMO and compromise the associated protective and mitigating SSCs, then the IEMO will develop into an accident sequence leading to a URC.

The SSCs associated with the potential SESs become the candidate CAs, and the areas of the plant housing these candidate CAs become candidate VAs. This identification of candidate CAs and candidate VAs provides an early opportunity to security inform the design.

An illustration of this process based on the Bowtie approach is given in Figure 3.

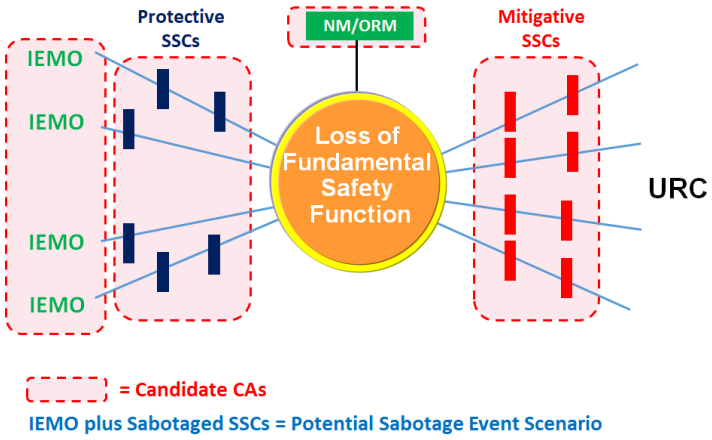

Figure 3 Identification of potential SESs and candidate CAs.

Phase 3 – DBT assessment: In this phase, the potential SESs are assessed relative to the adversary capability (see Section 3.5 below). The objective is to determine whether the adversary is capable of pursuing the potential SESs. Unless it can be clearly demonstrated that the adversary capability is insufficient to pursue the potential SES, then the potential SES is considered to be credible and considered further in Phase 4. It is noted that should the threat change, a re-assessment of all the potential SESs is required.

Phase 4 – Identification of VAs: A consolidated list of CAs is derived from a review of all the credible SESs identified in Phase 3 and a consolidated list of VAs is subsequently derived based on plant location data. This is repeated for different plant operating states and consideration given to the VAs during the plant lifecycle phases.

3.3.2 Identification of Operational Technology requiring protection from sabotage

The sabotage of a CA can be as a result of a cyber-attack on digital Operational Technology (OT). A cyber-attack can be carried out on a digital or embedded digital component within the CA itself; the Instrumentation and Control (I&C) system for the CA; or a supporting I&C system (e.g. power supply). This will include the plant or reactor control system if these have not been identified as a CA in the VAI study. There is also the possibility that other nuclear safety related digital systems and devices can be manipulated via a cyber-attack to initiate an incorrect plant response which facilitates rather than prevents the pursuit of a SES. This digital OT and its location is identified so that it can be protected from sabotage.

3.4 Identification of assets and areas requiring protection to prevent theft of nuclear material of prescribed information (Security Claim 4)

3.4.1 Nuclear material

All nuclear material within the plant is required to be protected against theft. The nuclear material and its location are obtained from the nuclear inventory (see Section 3.1).

3.4.2 Prescribed information

The theft of prescribed information can provide intelligence to an adversary to enable them to cause harm and hence any prescribed information at the plant needs to be identified for protection against theft either physically or electronically. The prescribed information, its form and location are obtained from the prescribed information inventory (see Section 3.2).

3.4.3 Safeguards equipment

The safeguards arrangements contribute to the protection of the nuclear material against theft, as an aim of the safeguards program is to prevent the untimely diversion of material (i.e., theft) for malicious use by the nation-state. The safeguards arrangements will comprise of equipment and digital systems which, if tampered with, could facilitate the theft of nuclear material. Hence the extent of the safeguards equipment and its location need to be identified so that it can be afforded the necessary protection against tampering and theft of nuclear material.

The safeguards equipment and its location are site and design specific and is the responsibility of the IAEA. However, the expected safeguards systems and equipment and their locations are identified in general terms for protection.

3.5 Threat interpretation (Security Claim 5)

Having identified the assets and areas requiring protection from either sabotage or theft, there is a need to consider the potential adversarial threat to the plant. The potential adversarial malicious acts can be physical or cyber or blended (i.e., combination of physical and cyber) and can include an “insider”.

The characteristics of the potential adversary are defined by national regulators and include the number of adversaries and their knowledge, capability and weapons, and include potential intentional aircraft crash. This information is interpreted for use in support of:

- The identification of CAs and VAs (Security Claim 3).
- The design of protective measures (Security Claim 6).
- The development of the overall security solution (Security Claim 7).
- The evaluation of the site security operations (Security Claim 8).

3.6 Measures for the protection of assets and areas (Security Claim 6)

3.6.1 Introduction

Having identified the assets and areas requiring protection from sabotage and theft and established the adversarial threat and capability, protection needs to be provided to ensure that the security fundamental objectives are delivered.

The protection is provided via an ISS for the plant. This ISS comprises a blend of robustness in design, physical and cyber protection measures and the on-site nuclear/off-site response

force capability, as required by category of nuclear material on-site. The development of the protection measures is based on a number of key protection principles.

3.6.2 Protection principles

Protection against sabotage or theft for the plant is built upon the following key protection principles.

(a) **Security informed design** which aims to eliminate or reduce security vulnerabilities through design (i.e., robustness in design) in preference to protection or mitigation via the use of a secure by design hierarchy of controls illustrated by the diagram below.

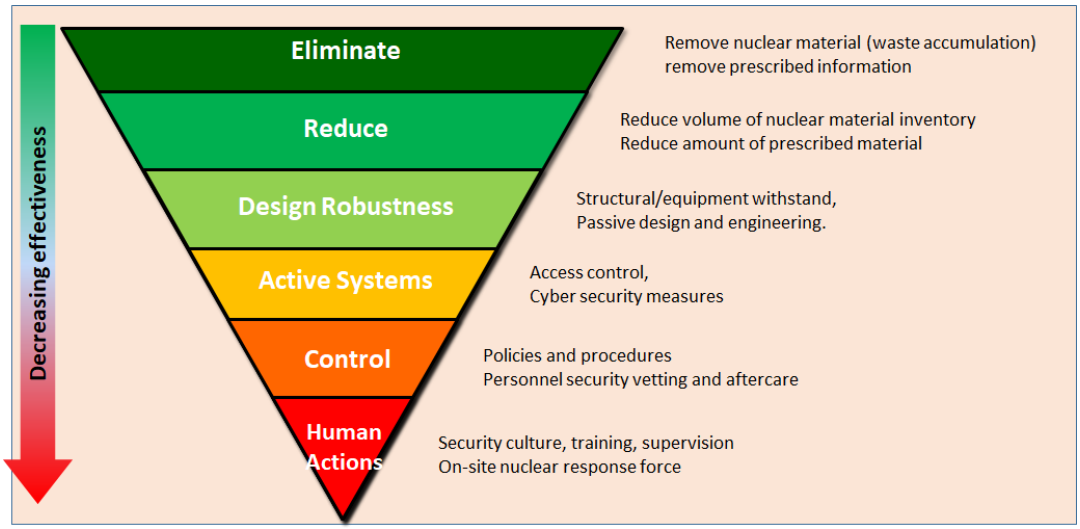

Figure 4 Illustrative secure by design hierarchy of controls.

(b) A blend of **security risk control enablers** including design and engineering, management systems and behaviour is adopted, as illustrated below.

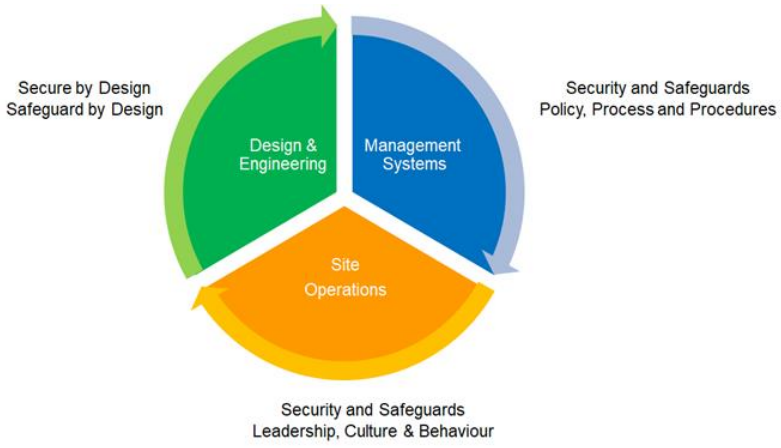

Figure 5 Security risk control enablers.

(c) **Defence in Depth (DiD)** which involves the multiple, interlocking, and integrated and independent layers of security protection measures designed to detect and delay any potential adversary, thereby allowing the nuclear security officers to mount the appropriate response, as illustrated below.

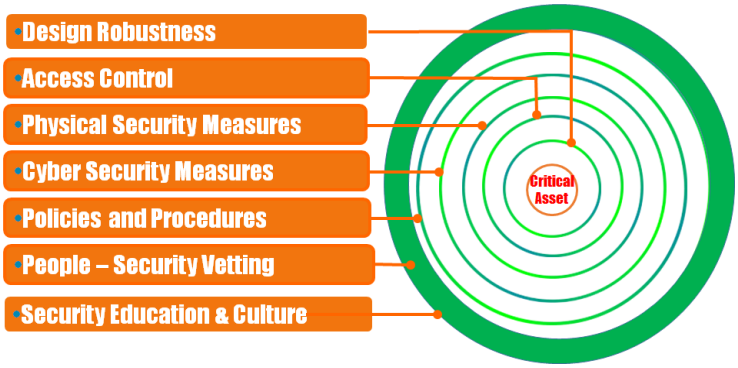

Figure 6 Illustrative layers of protection principle.

(d) **A proportional (graded) approach** to security whereby the higher the potential consequence, the greater the level of protection.

Integral to the delivery of these key protection principles are the establishment of security zones and protection measures for the plant, as follows:

3.6.3 Security Zones

A series of security zones is established to provide protection from sabotage and theft based on the principles outlined above. These security zones are illustrated conceptually in Figure 7.

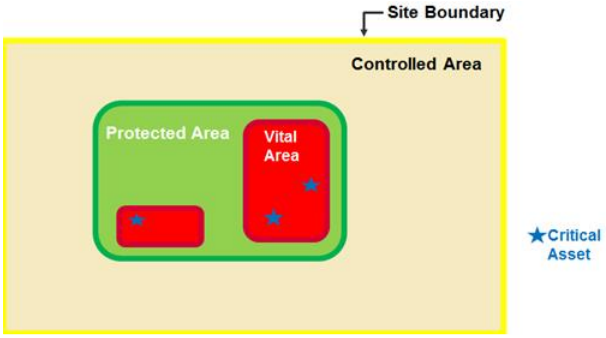

Figure 7 Illustration of security zone principle.

Figure 7 shows that the CAs are protected via three security zones with increasing level of protection, as follows:

1. A Controlled Area.
2. A Protected Area within the Controlled Area.
3. VAs within the Protected Area.

Further protection to a VA is provided by the building within which it is located.

3.6.4 Protection measures

Protection in each of the security zones is delivered via an integrated security solution comprising a combination of multiple measures consistent with the protection principles outlined above and on-site nuclear/off-site response force capability, as required by the categorization of the nuclear material. Referring to Figure 6, the delivery of an effective protective solution requires the consideration of design and engineering aspects, management systems aspects and site operation aspects. This is illustrated in Figure 8 which also identifies the types of protection measures comprising the protective solution.

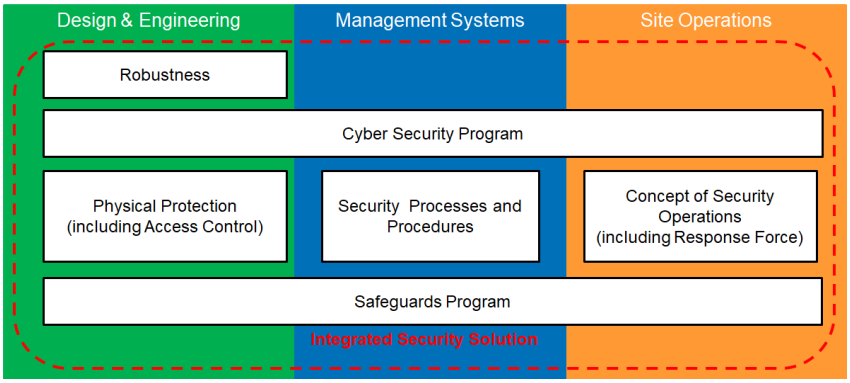

Figure 8 Protective measures and integrated security solution.

3.7 Protection of plant areas by an integrated security solution (Security Claim 7)

As illustrated in Figure 8, protection of the plant is provided by an ISS comprising a mix of protective measures and on-site nuclear and/or off-site response force capability, managed and delivered on a day to day basis by the nuclear site security officers.

In order for this ISS to provide proportional protection and defence in depth to the different plant areas, the plant areas are security classified depending on the potential consequences of any sabotage or theft of assets housed within that area. An illustration of the Security Classification (SyC) of plant areas is tabulated below.

Security Classification	Definition of Area
SyC 1	A VA.
SyC 2	All plant areas which are not VAs but contain assets requiring protection from theft (nuclear material and Prescribed Information), or nuclear safety related OT, or safeguards equipment.

Security Classification	Definition of Area
Baseline	All other plant areas within the protected area.
Commercial	All areas outside the protected area but within the controlled area requiring protection for commercial reasons, e.g. operational and asset protection reasons. (Note that whilst this is outside the scope of the nuclear security, it is included here to show how nuclear security can be integrated with commercial/conventional security).

Table 1 Security classification of plant areas.

Protection outcomes corresponding to each security classification are developed in terms of security functions that need to be delivered by the ISS. This is illustrated below.

Security Classification	Protection Outcome
SyC 1	PREVENT – Multiple layers of independent protection and procedural measures to prevent the unauthorized interference with the Critical Asset that is being protected within the Vital Area, and to apprehend the perpetrator(s).
SyC 2	RESTRICT – Layers of independent protection and procedural measures to restrict access into Secure Building Areas that contain NM/ORM, OT, Safeguards equipment and emergency response equipment to authorized staff only in the pursuit of their authorized duties and respond to unauthorized access attempts.
Baseline	DETECT – Layers of independent protection measures that will detect unauthorized attempts to enter the Protected Area, maintain observation of the intruder(s) and guide the on-site and/or off-site response force to apprehend the perpetrators.
Commercial	AWARE – Layer(s) of protection (measures) to inform the Security Monitoring Room that an unauthorized attempt to access the Controlled Area has been made.

Table 2 Illustrative protection outcomes.

The outcomes will be delivered by a mix of protection measures in accordance with the protection principles outlined in Section 3.6.2 and on-site nuclear/off-site response force which will be site dependent and the responsibility of the licensee.

3.8 Site security operations (Security Claim 8)

The ISS will be the basis for the day to day protection of the plant from sabotage and theft. This day to day protection will be site-specific. It will be the responsibility of the licensee and delivered via the licensee's site security operations.

The licensee will develop a site security plan which will cover the nuclear site security operations alongside commercial and personnel security. This site security plan will be

compatible with the plant's concept of operations and, in turn, form part of the overall site operational plan.

Nuclear security operations will start with the securing of the site prior to commencement of construction, builds up proportionately as the plant is commissioned and is fully in place and tested prior to the arrival of fresh fuel at the site. It thereafter continues until decommissioning and removal of nuclear material from the site with regular reviews and testing.

4. TEI's security by design update

TEI is currently in the midst of the Basic Engineering phase of the IMSR400 design work. At the end of this phase, the IMSR400 plant will have been designed at the system level before moving into the Detailed Engineering phase (i.e. at component and site-specific design level). The secure by design process has been initiated at the beginning of the Basic Engineering phase and the Security Claims 1 through 4 are expected to be completed by the time this paper is published. By that time, the information about the Design Basis Threat is expected to be received from the Canadian Nuclear Safety Commission (CNSC), and work on IMSR400's security case to continue in Basic Engineering with Security Claims 5 through 7. During the Detailed Engineering phase, an updated iteration of the Security Claims 1 through 7 is expected to take into account any adjustments of the design, and Security Claim 8 be also accounted for based on specific site and licensee's input.

5. Conclusion

This paper has presented an alternative holistic approach for the delivery of nuclear security to the traditional prescriptive approach. Rather than developing a retrospective solution that protects from the 'outside-in', the alternative approach starts with the asset requiring protection and delivers a multiple blend of layers of protection from the 'inside-out' providing an opportunity to security inform the design early in the design development process. The method deals effectively with the insider and the developments in the cyber threat. It integrates safeguards with security and provides a link to the nuclear safety case. The method is well suited to non-prescriptive regulation which permits risk informed proportional security.

The opportunity to security inform design using the secure by design hierarchy of controls is of benefit to the Generation IV SMR designs, like TEI's IMSR400 design, where security risk can be eliminated, minimised or mitigated during the design development process.

6. References

[1] Canadian Government, "Nuclear Security Regulations", SOR/2000-209, June 2015.

[2] Canadian Government, "General Nuclear Safety and Control Regulations", SOR/2000-202, June 2015.

[3] International Atomic Energy Agency, "Identification of Vital Areas at Nuclear Facilities", IAEA Nuclear Security Series No.16, 2012.