|  |
| --- |
|  |
| ONR Technical Assessment Guide  Secure by Design |



ONR Technical Assessment Guide (TAG)

Secure by Design

Authored by: Principal Inspector

Approved by: Superintending Inspector

Professional Lead: Protective Security

Issue No.: 1.1

Publication Date: Jan-23

Next Major Review Date: Jan-28

Doc. Ref.: CNS-TAST-GD-11.4.1

Record Ref. No.: 2022/7673

Table 1: Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 1 | New document. |
| 1.1 | Minor formatting updates. |

Contents

[1. Introduction 4](#_Toc126226855)

[2. Purpose and Scope 5](#_Toc126226856)

[3. Relationship to Relevant UK Legislation and Policy 6](#_Toc126226857)

[4. Relationship to International Standards and Guidance 7](#_Toc126226858)

[5. Advice to Inspectors 9](#_Toc126226859)

[6. A Secure by Design Approach 11](#_Toc126226860)

[References 17](#_Toc126226861)

[Glossary and Abbreviations 19](#_Toc126226862)

# Introduction

1. To assess the safety, security and safeguards submissions for nuclear facilities or transport of nuclear material that may be operated by potential licensees, existing licensees, or other dutyholders, our inspectors use a suite of established assessment principles. These assessment principles are supported by a further suite of Technical Assessment Guides (TAGs).   
   The TAGs assist ONR’s inspectors in making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This document is the Secure by Design (SbD) TAG. The TAG is consistent with other TAGs and associated guidance and policy documentation.

# Purpose and Scope

1. Throughout this guide, the term ‘security plan’ is used to cover all dutyholder submissions such as approved security plans for nuclear premises, temporary security plans and transport security statements.   
   Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 (‘NISR 2003’) [1] may also use our Security Assessment Principles (SyAPs) [2] as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI).
2. This document refers to the ‘Requesting Party (RP), developer or dutyholder’. The term ‘dutyholder’ is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation. It is also used to refer to those holding SNI. A ‘developer’ refers to those carrying out work on a nuclear construction site and approved carriers, as defined in NISR. An ‘RP’ will normally be the vendor for a Nuclear Power Plant (NPP), although it may also be a consortium including the vendor and other partner organisations. The term RP is therefore used throughout this document to identify the organisation(s) undertaking Generic Design Assessment (GDA), irrespective of its composition. These terms are grouped collectively to acknowledge the change in responsible persons as the project develops from concept through to operation.
3. SbD relates to all aspects of a facility’s lifecycle although it might be applied differently to each stage. For example, during the conceptual design stage of a new plant the opportunities to influence the design may differ from a plant during decommissioning, as risks in each case will be different. However, general principles should apply to both cases.
4. This TAG aims to provide general advice and guidance to our inspectors on how the implementation of SbD should be assessed. It does not set out how we regulate the dutyholder’s arrangements. It does not prescribe the detail or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholders responsibility to determine and describe this detail within their submission and for us to assess whether the arrangements are adequate.
5. In addition to providing guidance to dutyholders and developers, this TAG is particularly important to RPs. RPs are those who request, and subsequently undertake our Generic Design Assessment (GDA) process for the assessment of new Nuclear Power Plants (NPPs). Introducing SbD at the design phase provides for optimised security risk reduction. SbD principles form a key part of the Generic Security Report (GSR) which is developed in the latter stages of GDA and goes on to inform the Nuclear Site Security Plan (NSSP). Separate guidance exists pertaining to the wider GDA process [3].

# Relationship to Relevant UK Legislation and Policy

1. ‘The responsible person’ for a ‘nuclear premises’ (both terms as defined by NISR) is required to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. We consider CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.
2. The SyAPs provide our inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to our inspectors when assessing a dutyholder’s submission demonstrating they have effective processes to ensure a SbD approach is adopted within project management.
3. The Government Functional Standard on security [4] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties.   
   The security principles, governance, life cycle and practices detailed within the Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.
4. The Government Security Classifications document, together with our Classification Policy [5] describes types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

# Relationship to International Standards and Guidance

1. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [6] and the IAEA Nuclear Security Fundamentals [7]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.
2. Fundamental Principle J of the CPPNM refers to quality assurance and states that a quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.
3. A more detailed description of quality assurance is provided in Recommendation’s level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities [8]. This document states:

And goes on to state:

“The quality assurance policy and programmes for physical protection should ensure that a physical protection system is designed, implemented, operated and maintained in a condition capable of effectively responding to the threat assessment or design basis threat and that it meets the State’s regulations, including its prescriptive and/or performance-based requirements.”

1. In addition to quality assurance, the importance of issues relating to the graded approach is recognised in [6], specifically:

* Essential Element 9: Use of Risk Informed Approaches – 3.9.   
  A nuclear security regime uses risk informed approaches, including the allocation of resources for nuclear security systems and nuclear security measures and in the conduct of nuclear security related activities that are based on a graded approach and defence in depth, which take into consideration:
  1. The State’s current assessment of the nuclear security threats, both internal and external.
  2. The relative attractiveness and vulnerability of identified targets to nuclear security threats.
  3. Characteristics of the nuclear material, other radioactive material, associated facilities and associated activities.
  4. Potential harmful consequences from criminal or intentional unauthorised acts involving or directed at nuclear material (NM), other radioactive material (ORM), associated facilities, associated activities, sensitive information or sensitive information assets, and other acts determined by the State to have an adverse impact on nuclear security.

1. NSS 13 [8] also refers to the graded approach that should take account of the current evaluation of the threat, the relative attractiveness of the site in terms of malicious activity, the nature of the material stored or used, and the potential consequences associated with the unauthorised removal of material and with the sabotage against nuclear material or nuclear facilities. It states that a graded approach is used to provide higher levels of protection against events that could result in higher consequences. For protection against sabotage, the state should establish its threshold(s) of Unacceptable Radiological Consequences (URCs) to determine appropriate levels of protection considering existing nuclear safety and radiation protection.
2. The IAEA also publish Technical Guidance documents NSS 16 ‘Identification of Vital Areas at Nuclear Facilities’ [9] and NSS 4 ‘Engineering Safety Aspects of the Protection of Nuclear Power against Sabotage’ [10] where further relevant information can be found.
3. It is at these early stages during the development cycle of a facility, when risk reduction should be carried out through the analysis of the inherent security risks using such methodologies as Vital Area Identification (VAI), NM categorisation and a Cyber Security Risk Assessment (CSRA). That analysis sets the conditions for considering SbD so to optimise risk reduction measures.

# Advice to Inspectors

1. In terms of other Relevant Good Practice (RGP), the Sandia National Laboratories (SNL) Security by Design Handbook [11] provides a trusted source of thinking, although this work was published in 2013. Since its publication it is now necessary to consider all security risks and therefore not just a physical security regime but also cyber protective arrangements.   
   The SNL Security by Design Handbook refers to the Idaho National Laboratory (INL) definition of security by design which includes safeguards, physical security and cyber security. INL highlights the Cyber-Informed Engineering (CIE) body of work [12] as an emerging method to integrate cybersecurity considerations into the conception, design, development, and operation of any physical system that has digital connectivity, monitoring, or control.
2. The National Cyber Security Centre as the UK National Technical Authority for cyber security, provides Secure Design Principles [13] which are intended to help ensure that the networks and technologies which underpin modern life are designed and built securely. These principles are aimed at those who design systems, since the principles are most useful in the design and build phases of a project, although they can also be used to review existing systems. NCSC also promote a Secure by Default [14] approach which recognises that to be effective security needs to be built-in from the ground up. NCSC work with vendors to develop technologies that mitigate the latest threats so that users can have confidence in products at root.
3. Further RGP is provided by the World Institute for Nuclear Security (WINS) [15]. WINS states that SbD is based on the concept that security should play an integral role in the design process from the very beginning. It is a risk-informed approach that requires multi-discipline teamwork and a clear security strategy. WINS also identifies what they call ‘intrinsic security’ rather than ‘inherent security’. Both concepts relate to the security benefits inherent in any design. For example, certain types of fuel may have a lower enrichment level that has a positive benefit in terms of categorisation for theft; or a new facility design may have inherent structural advantages when a large part of the plant is underground.
4. While SbD is a Key Security Plan Principle (KSyPP), its application within the civil nuclear industry is still developing. Therefore, it is possible that dutyholders, developers or RPs may have different interpretations of the concept. However, SyAPs provides an overview of this approach to risk management

## Regulatory Expectation

1. The regulatory expectation is that the dutyholder should demonstrate within their security plan how they implement a SbD approach within their project management arrangements.

|  |  |  |
| --- | --- | --- |
| **Key Security Plan Principles** | Secure by Design | KSyPP 1 |
| The underpinning aim should be an inherently secure design, consistent with operational purposes. | | |

# 

# A Secure by Design Approach

1. SyAPs describes SbD as an approach that seeks to reduce security vulnerabilities within a given design (a large project such as a new nuclear power plant or smaller one such as a new storage facility) rather than attempting to secure or mitigate them post design. Emphasis is placed upon eliminating or reducing risk to design out the requirement for protection measures. An RP, or later a dutyholder, has the flexibility on how they achieve security outcomes so to meet regulatory expectations. ONR should be prepared to assess all claims made by an RP, developer or dutyholder as to how risks are managed.
2. Previously RGP has assumed retrofit of mainly physical security arrangements during construction or, at best, designing in security systems during later detailed design stages having to deconflict first with safety requirements. Whilst seeking a retrofit approach may, on occasion be necessary, seeking security benefits during the conceptual design stage may ultimately achieve greater risk reduction in addition to attracting wider corporate and commercial benefits over the lifecycle of the plant. Nevertheless, such claims will need to be argued credibly and appropriately evidenced by a well-informed dutyholder.
3. With an outcome-focussed regulatory approach, that encourages dutyholder and designer innovation, there is scope to consider security risks and vulnerabilities within a design and, equally, any security benefits inherent within the proposed plant or facility. This analysis is best conducted by a multi-discipline team, through a detailed understanding of the threat and design, thereby addressing all risks at their source and managing any conflicting requirements. Security vulnerabilities might be considered as potential weaknesses within the design that could be exploited by an adversary leading to theft of NM, ORM or sabotage of associated facilities.
4. Such vulnerabilities, that might be targeted by malicious actors, would include structures, systems and components (SSCs) that deliver nuclear safety functions (notably reactivity control, cooling and containment with means to control them) ensuring the plant is operated safely. In most cases these SSCs would include Vital Areas (VAs) of various magnitudes and attractiveness in terms of target profile. With such a detailed understanding of risks, experts could identify potential security benefits inherent in the design itself.
5. Passive safety systems might reduce the magnitude of an offsite release created through sabotage affecting a number of VAs. New fuels, and their nature and management, may reduce the proliferation risk arising from theft. Therefore, before any security regime is designed-in, the design itself may offer benefits to risk reduction that are inherent and intrinsic.
6. Identifying and assessing security and safety vulnerabilities in parallel, requires suitably qualified and multi-disciplinary project teams. RGP suggests that delivering SbD requires several enablers or preconditions that are organisational, and process based. There are two important preconditions: Firstly, there needs to be a risk informed decision-making process that seeks to understand and manage both safety and security risks (and maybe safeguards and environmental risks as well). Secondly, a set of design principles, practices, and processes for assessing risk.
7. It is accepted that some aspects of safety and security risk assessment will not be similar, while others will be more easily aligned. Also, security assessments of consequences based on VAI studies, and similar cyber based assessments, will draw from a safety case, with specific consideration for initiating events. Whilst the dichotomy between safety, security and safeguards (3S) needs to be understood, the expectation in this TAG is not to explore the 3S interface, although understanding their different methods and RGP is a precondition to applying an effective SbD approach that cannot be achieved in isolation.
8. The expectation is that engineers and designers would understand the plant vulnerabilities and collectively seek engineering solutions to eliminate or reduce the risk. SyAPs refers to ‘inherent security’ that describes how safety measures may deliver security benefit or might be strengthened to reduce risk further. This might be referred to as designing-out security vulnerabilities and is the first part of any SbD approach. For example, pipe work that is part of the cooling system might be protected by the structure of the design but access to it may create a security weakness that could be reduced further by a small plant modification.
9. Another example might be the choice of crane for moving fuel within the plant. One crane design might have inherent security benefit in terms of reducing the potential for malicious interference. This could be argued by the security specialists when modifications are made that could attract such benefits. A designer may have placed vehicle routes, loading/unloading bays and made choices of on-site vehicle types in a way that, if changed, could reduce the security risk while meeting other requirements so it is fit for purpose. Internal building structural design could be such that it creates stand-off against a vehicle borne improvised explosive device threat. For cyber security, design features may be such that they make compromise and disruption by malicious means more difficult.
10. Inherent security is illustrated in SyAPs by a model of various risk controls that might be applied to a design, that reflects broader risk management RGP. The model illustrates schematically how design teams, having identified and categorised the risks to safety and security, might design-out risk (eliminate or reduce) or, if that cannot be achieved, then to design-in security protective systems (physical and cyber) to mitigate the risk further. Both aspects of SbD could take place within the early conceptual design stage and subsequent detailed design before construction (in regulatory terms within GDA and licencing). This is the choice of the designer.   
    For some designs it may not be advisable to choose the exact technologies to deliver security effects (such as detection capability), during the design stage. If this is so, it may nonetheless be necessary for the designer to plan for physical and cyber protection systems. For example, in terms of space for such security systems, their power requirements and an awareness of what systems will be shared with safety, safeguards and environmental functions.

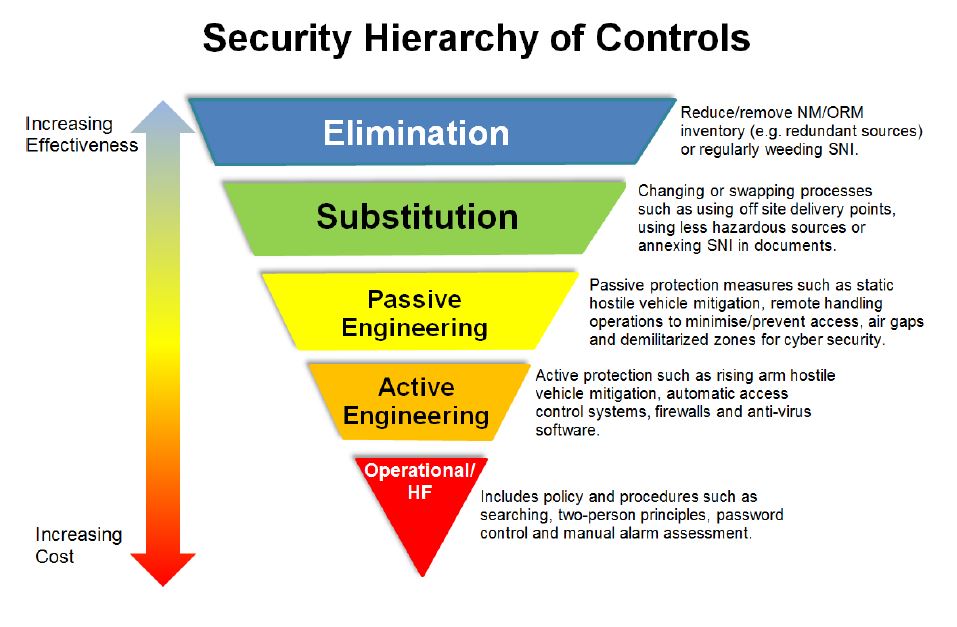


Figure 1 – The Secure by Design Hierarchy of Controls

1. The diagram above offers a simple SbD concept and terminology. It captures the principle of understanding the risks and controlling them if elimination is not possible. It first seeks to reduce the nuclear inventory. Another option is to make that inventory less attractive for proliferation or sabotage purposes. Should risks not be successfully addressed by inherent and passive measures, active security arrangements will need to be added to reduce the risk to acceptable levels. The concept indicates there are potential cost and efficacy benefits.
2. Application of this hierarchy should reduce the need for, and reliance on, protective security systems and the challenges placed on them. In addition to this hierarchy, SbD for cyber can be further enhanced by the following underpinning principles:

**Principle 1: Focus on what is critical**

1. Designers should consciously and methodically focus on including only those system functions that are essential to operations and eliminate access points and susceptibilities associated with unneeded functionality.   
   This reduces the number of potential susceptibilities (and therefore the paths between the attack surface and target systems) in which essential functions, critical systems and controls, or critical data could be compromised.

**Principle 2: Move key assets out-of-band.**

1. The designer should consciously differentiate between user access and attacker access to a given system. This is accomplished by moving the data/processes used by essential functions, critical systems and controls, and associated access points out-of-band. i.e., not accessible by the attacker through their preferred or available access methods, either logically, physically, or both. The extent and strength of access differentiation between the user and attacker is greatly influenced by the type of out-of-band mechanism employed and whether it is done in software or hardware and should be proportionate to the risk.

**Principle 3: Detect, react, adapt.**

1. The designer should employ dynamic sensing and response technologies such as security control sensors or reference monitors, that mitigate the threat actor’s capabilities and exploitation attempts through autonomic or automated system behaviour. This makes the system's defences unpredictable and adaptive rather than passive, and therefore confounds the threat actor’s capabilities.
2. For an operating reactor or design, the reduction of both safety and security risk is informed by the systems that deliver fundamental safety functions. New reactor designs depend on more passive safety measures that reduce human error or potentially lessen the risk of a loss of fundamental safety through novel choices of coolant and fuel design.
3. With the necessary expertise, within both security and safety teams, the designer is free to make a claim, supported by appropriate arguments and adequately backed by evidence, that certain UK Design Basis Threat   
   (UK DBT) scenarios have been mitigated inherently by passive measures. Should a design (with or without any modifications) not deliver such security benefits, the dutyholder would be required to design-in active security measures to address the risk (or residual risks) to ensure the required SyAPs security outcome is achieved. That regime, as the diagram suggests, would be based on RGP that includes a mix of physical, cyber and procedural arrangements. Therefore, if security risks cannot be designed-out (that is, through reduction or elimination), then a proportionate security effect, that meets specified SyAPs outcomes, will need to be designed-in.
4. In adopting such an approach to security risk analysis, it should be noted that while security-based claims might be argued successfully in concept design, they will nonetheless need to be reassessed through licensing, construction, and thereafter during operations (as a nuclear power plant or other civil nuclear licensed facility). Once operational, the regime would be explained within an approved security plan that would need to demonstrate, with confidence, that stated outcomes are achieved thereby meeting regulatory expectations.
5. SbD, as an approach to achieving security outcomes with a new facility’s design and thereafter where there is a change to the threat or site operations, assumes a dutyholder will carry out a security risk analysis.   
   That analysis requires identification of what needs to be protected against the UK DBT in order to meet the government’s risk appetite and our regulatory expectations. In terms of managing risk, the expectation is that the RP, developer or dutyholder offers claims, arguments and evidence that such risks, once identified through VAI studies, and a similar CSRA through agreed methodologies, are either designed out, reduced or mitigated in the design stage. This process may need to be iterative in nature, requiring the dutyholder to review their VAI following each design modification to determine if the scenario leading to a URC has been successfully mitigated. Security should be adequately incorporated into any change control procedures.
6. Thereafter, if such design measures are unable to adequately mitigate against the UK DBT (that is, VAs remain identified despite the application of all reasonably practicable design modifications), then a suitable physical and cyber protective security regime is required to be designed-in and evaluated for efficacy to ensure the required SyAPs outcomes are achieved, thereby meeting regulatory expectations.
7. The RP, developer or dutyholder should have an understanding that SbD is dependent on drawing from and achieving the other KSyPPs. SbD should not be viewed in isolation but as an approach that requires an understanding of the design itself, the UK DBT and its application through the conduct of VAI together with other standards.
8. Inspectors should consider:

* During scoping activities an inspector should consider all available regulatory intelligence in respect of the RP before using the points below to frame their intervention plan scope.
* How the RP, developer or dutyholder has demonstrated its understanding of SbD, and the opportunities offered? Do they appreciate that within an outcome-focussed regulatory approach there is scope for innovation in the ways and means to address risk?
* Within the general concept of SbD, how has the dutyholder interpreted their approach, and what RGP have they drawn from to inform their methodology?
* Has SbD been considered in the early stages of the design, including SbD for cyber?
* How will they leverage the importance of cross-specialism coordination to inform holistic and integrated regulatory activity?
* Does the dutyholder have a risk informed decision-making process that enables a multi-discipline team to consider how the design might be modified to meet various design needs across the disciplines of safety, security, safeguards and environmental expectations?
* How has the dutyholder deconflicted the needs of fire safety, power requirements, physical space for foreseeable security equipment and human factors-based risks?
* What RGP has the dutyholder adopted to integrate cyber security considerations into the conception, design, development, and operation of any physical system that has digital connectivity, monitoring, or control?
* How does the dutyholder organise itself to deliver a SbD approach? Does the dutyholder have a policy and related structures for assessing the risks of a particular design, and its intended role, and making design modifications to a design to meet security requirements?
* Does the dutyholder’s security team have the necessary qualifications and experience to adopt and deliver the SbD approach?
* How does the dutyholder team assess the security risk in the design? What methodologies have they used? What interaction has there been between dutyholder designers, security, safeguards and safety experts?
* Does the dutyholder’s choice of security risk analysis methodology include adequate categorisation for theft, sabotage and cyber risks?
* Having carried out a risk analysis what scope has the dutyholder identified to apply the ‘hierarchy of controls’ relevant to SbD?
* Has the dutyholder recorded when modifications have been made or not made along with necessary justifications?
* Have limitations on delivering a SbD solution to a security risk been captured so that they can be addressed later in design development?
* When a design change is not appropriate or possible, and when security arrangements will need to be applied later in the project, has the dutyholder made provisions for foreseeable security systems?   
  (This could include areas for security management systems, fences, access control, searching and screening and the necessary space and power requirements).

# References

|  |  |
| --- | --- |
| [1] | H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003. |
| [2] | ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017. |
| [3] | ONR, “ONR-GDA-GD-007 - New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties. https://www.onr.org.uk/new-reactors/onr-gda-gd-006.pdf”. |
| [4] | HM Government, “Government Functional Standard GovS 007: Security,” 2021. |
| [5] | ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”. |
| [6] | IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”. |
| [7] | IAEA, “Nuclear Security Series No. 20 - Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime,” 2013. |
| [8] | IAEA, “Nuclear Security Series No. 13 - Nuclear Security Recommendations on the Physical Protection of NUclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011. |
| [9] | IAEA, “Nuclear Security Series No. 16 - Identification of Vital Areas at Nuclear Facilities,” 2013. |
| [10] | IAEA, “Nuclear Safety Series No. 4 - Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage,” 2007. |
| [11] | Sandia National Laboratories, “Security by Design Handbook,” 2013. [Online]. Available: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2013/130038.pdf. |
| [12] | Idaho National Laboratory, “Cyber-Informed Engineering,” [Online]. Available: https://inl.gov/cie/. |
| [13] | NCSC, “Secure Design Principles,” 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/cyber-security-design-principles. |
| [14] | NCSC, “Secure by Default,” 2018. [Online]. Available: https://www.ncsc.gov.uk/information/secure-default. |
| [15] | World Institute for Nuclear Security, “Implementing Security by Design at Nuclear Facilities,” 2019. |

# Glossary and Abbreviations

CIE Cyber-Informed Engineering

CS&IA Cyber Security & Information Assurance

CSRA Cyber Security Risk Assessment

UK DBT UK Design Basis Threat

GDA Generic Design Assessment

GSR Generic Security Report

IAEA International Atomic Energy Agency

KSyPP Key Security Plan Principle

NCSC National Cyber Security Centre

NISR Nuclear Industries Security Regulations

NM Nuclear Material

NPP Nuclear Power Plant

NSS Nuclear Security Series

NSSP Nuclear Site Security Plan

ONR Office for Nuclear Regulation

ORM Other Radioactive Material

PPS Physical Protection System

RGP Relevant Good Practice

RP Requesting Party

SbD Secure by Design

SNI Sensitive Nuclear Information

SyAPs Security Assessment Principles

TAG Technical Assessment Guide

URC Unacceptable Radiological Consequences

VA Vital Area

VAI Vital Area Identification

WINS World Institute for Nuclear Security