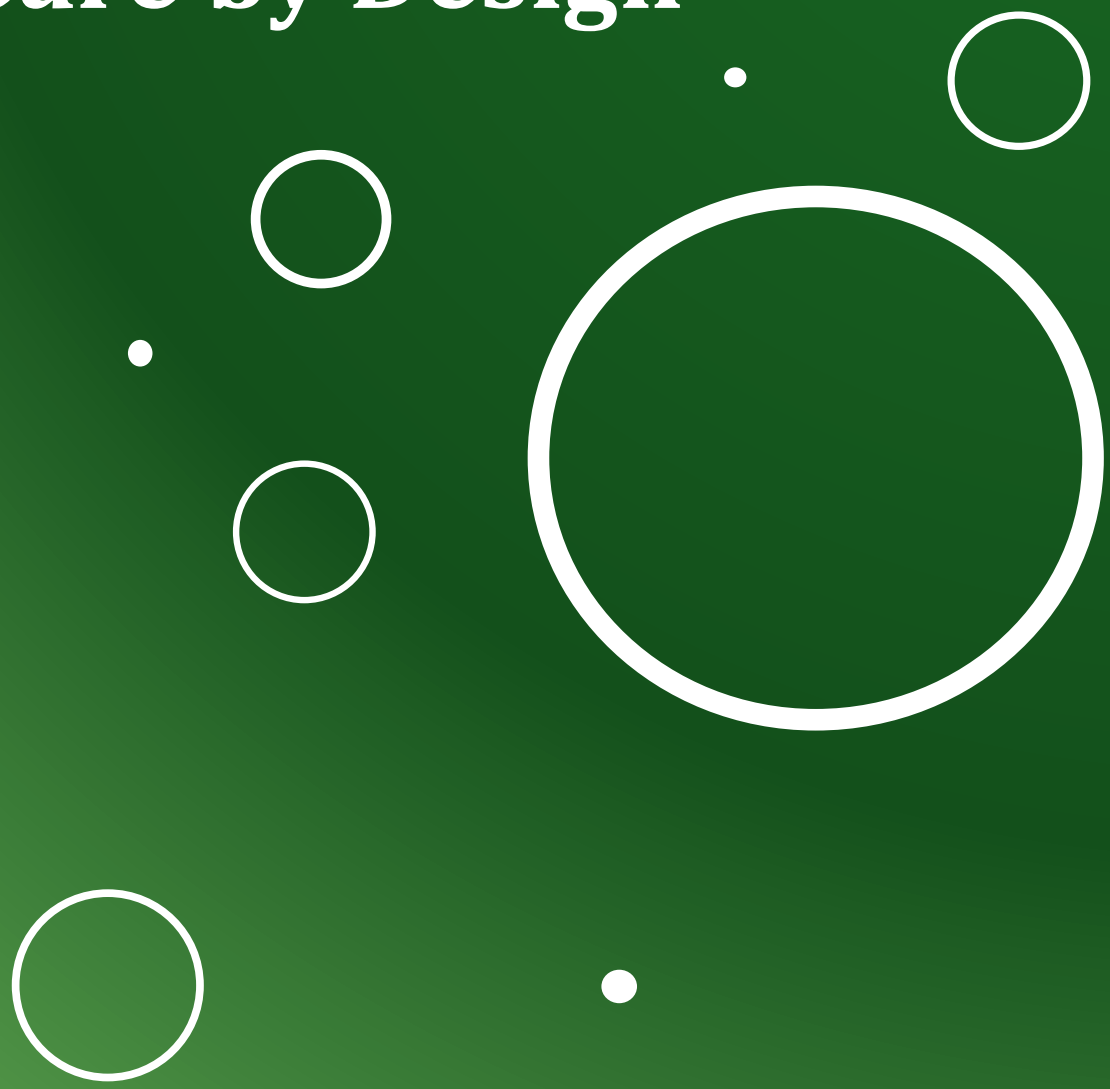
Nuclear Security
Awareness Guide

Secure by Design



Contents

1. Introduction 3
1.1. Why Does This Guide Exist 3
2. What is Secure by Design 4
3. Why Secure by Design Matters 6
3.1. Industry Testimonies 6
3.2. Case Studies 7
3.2.1. Case Study 1 8
3.2.2. Case Study 2 8
3.2.3. Case Study 3 9
4. Principles of Secure by Design 10
4.1. Early Engagement 10
4.2. Proportionality 10
4.3. Collaboration 10
4.3.1. Understanding the Threat 12
4.4. Long-Term Outlook 12
4.4.1. Upfront Costs vs Future Savings 12
4.4.2. Changing Threat Landscape 12
4.5. Technical Security Principles 13
5. When to Apply Secure by Design 14
5.1. Concept 14
5.2. Pre-Enabling 15
5.3. New Build or Enhancement 15
5.3.1. New Build 15
5.3.2. Existing Facility 15
5.4. Operations and Maintenance 15
5.5. Decommissioning 16
5.6. Triggers 16
6. How to Apply Secure by Design 17
6.1. Starting Point 17
6.2. Existing Processes and Procedures 17
6.3. Guidance for Application 18
7. Summary 20
Appendix 1. Useful Resources 21
Appendix 2. Acronyms 22

1. Introduction

As the pursuit of energy security intensifies, and the global ambition to achieve net zero continues, nuclear power will play an increasingly central role in energy generation for both existing nuclear nations and new nations currently developing nuclear energy programmes. It will be critical to maintain the global public acceptance of nuclear as a safe and secure source of energy whilst balancing the investment necessary to construct and operate nuclear facilities.

Nuclear facilities require significant investment in time, cost and effort to ensure that proportionate levels of safety and security are maintained throughout their operational lifetime. This coupled with the multi-disciplinary teams and numerous stakeholders involved in their delivery mean that all projects associated with nuclear facilities tend to be very complex. Changes to any design or construction are therefore expensive and often lead to extensive project delays. Historically, security has been of lower priority and has only been considered late in the project lifecycle, therefore negatively impacting both costs and timelines.

Secure by Design (SeBD) aims to reduce vulnerabilities by making security a fundamental design consideration from the outset, and at every stage of the project lifecycle. By reducing or removing vulnerabilities from the outset, costs can be reduced as additional security measures, arrangements, and procedures are not required to mitigate these vulnerabilities at a later stage.

SeBD can be applied across all projects, whether that's designing a nuclear new build, maintenance and improvement work, or business-as-usual activities. It is an important consideration at all stages of nuclear-related projects and the broader nuclear fuel cycle, including the transport of nuclear and other radioactive material. It is not solely reserved for new reactors and new facilities.

To be implemented effectively, SeBD requires a collaborative approach, with engagement across a range of stakeholders. Applying SeBD is not something that the security function can do on their own.

This document is intended to promote awareness of Secure by Design to non-security practitioners. This guide is not intended to act as relevant good practice.

1.1. Why Does This Guide Exist

This awareness guide was developed to support non-security practitioners understand the value of applying Secure by Design early and continuously throughout the project lifecycle, and the positive impact and benefits it can deliver.

Furthermore, despite SeBD not being a new concept, the application of SeBD in the nuclear industry in practice is still in its infancy. For SeBD to be implemented and integrated into processes, procedures, and standard practice, it needs to be recognised and valued amongst non-security practitioners. This guide aims to enable such wider recognition.

2. What is Secure by Design

Secure by Design is an internationally recognised approach to security. However, the definition and interpretation of SeBD varies depending on the State and the individual interpretation by organisations.

The United States of America's National Nuclear Security Administration (an agency within the Department of Energy) have published a definition of 'Security by Design' as part of their International Nuclear Security for Advanced Reactors programme:

> **SeBD is an approach whereby protection-related elements are considered and incorporated early, frequently, and continuously throughout the design of a new nuclear facility to achieve cost and risk-informed results. This can occur during the design, siting, construction, operation, and decommissioning of any nuclear facility.**

A paper from the French Nuclear Security Authority, submitted to an International Atomic Energy Agency (IAEA) Conference in 2020, described the current French approach to 'Security by Design' as below:

> - **An intrinsically secured design, with inherent features of the installation that contribute to reduce the number of targets, to facilitate nuclear security and allow a better mitigation of the potential consequences of the remaining vulnerabilities and;**
> - **An early identification of physical protection requirements, to cope with the vulnerabilities of the installation.**

SeBD has also been recognised by the UK's independent nuclear regulator, the Office for Nuclear Regulation (ONR), and is one of the Key Security Plan Principles used by the ONR to assess the adequacy of security plans across the civil nuclear industry.

The ONR defines SeBD as below:

> **'Secure by Design' is an approach that seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design. It mitigates specific threats by using an approach, design or arrangement tailored to address malicious acts.**

For the purposes of this awareness guide, SeBD can be defined as below:

> **Secure by Design is an approach that aims to ensure that security is included as a primary function during all phases of a project life cycle, from concept to closure. It means that security is introduced at the outset of a project, and the project can be designed with security in mind, rather than introducing it further down the line.**

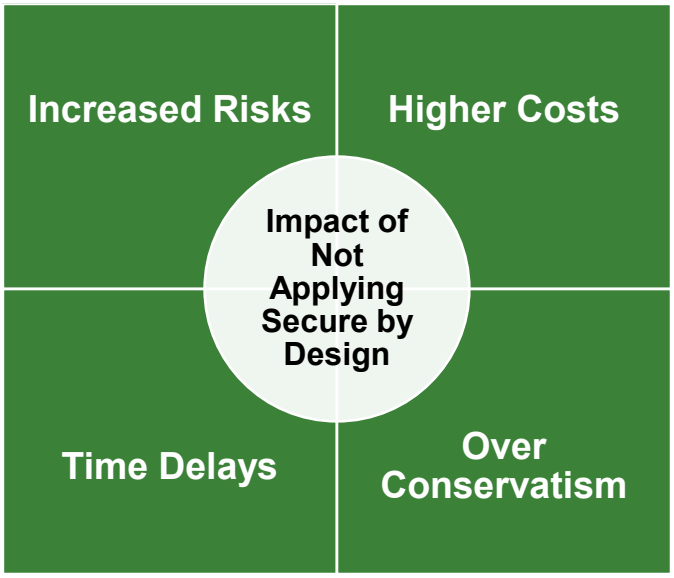
It is important to note that SeBD is not exclusively linked with physical security; the concept of SeBD has been used across multiple sectors, including outside of the nuclear industry. SeBD is particularly well-established within the cybersecurity field, with various frameworks and guidance available.

Even when used within the context of physical security within the nuclear sector, SeBD does not relate to extrinsic security measures only. For example, when applied early in the design stage, it can shape key decisions such as site selection, the type of nuclear material used in a reactor, or the form that the waste material is stored in, therefore inherently mitigating risk through design. However, the application of SeBD must be cognisant of the change in risk over the lifetime of a project or facility (see Section 4.4). For example, different risks may be present across the different stages of a power plant's lifetime, from construction through to decommissioning. The optimal security design will therefore differ over this period.

To successfully implement SeBD, collaboration across a broad range of disciplines is required. This includes both technical and non-technical staff.

3. Why Secure by Design Matters

Secure by Design matters because of the potential consequences of failing to apply it. These consequences may include increased complexity in managing vulnerabilities, higher costs, project delays, and overly conservative design choices. These consequences often give rise to other issues, such as putting a stop to operations, creating friction between stakeholders, and the formation of negative perceptions surrounding security.



When SeBD principles are integrated at the earliest stage of a project, they can enable the design of a balanced security system which is proportionate to the risk at that time.

Security infrastructure can be expensive to install, operate, maintain and replace throughout the lifetime of a nuclear facility, and in addition to this, response forces are often one of the highest costs associated with security. By implementing security in a way which is proportionate to the risk, an optimised security solution that is less reliant upon a response force can be developed, and significant costs can be saved whilst still achieving regulatory compliance.

3.1. Industry Testimonies

Responses to a survey of nuclear professionals frequently cited both additional costs and delays as a direct consequence of not recognising security requirements from the outset, thus illustrating the detrimental impact of not giving security appropriate consideration during the early stages of a project, where key design decisions are made and changes can be implemented most efficiently.

Participants were asked: **Have you delivered a project where security requirements were not recognised at the outset? What impact did this have?**

[Security] have been blamed on many occasions for holding up projects by requiring them to meet the regulatory requirements, which were not known about until late in the project. This can be stressful and could be avoided if the security requirements are considered at the outset.

Independent Assurance

Yes … as security is always retrofitted. This impacts project milestones, has significant financial implications and can be detrimental to operations.

Nuclear Safety

Yes. As with any project that doesn't include the right stakeholders from Day 1, it resulted in an elongated programme and additional cost (plus frustration from all involved).

Delivery Operations

When security is not considered during design phase, it is much more costly to retrofit later on. This will also have a negative impact on project milestones and completion times.

Compliance

Yes, a number of times.

Impact:

- **Inadequate assurance of security performance**
- **High levels of performance ambiguity**
- **Higher costs of post design and build systems integration**
- **Over designed parameters with associated cost inflation beyond a risk managed optimal design**

Nuclear Security

3.2. Case Studies

The benefits of SeBD are also evident when looking at real-life case studies from nuclear sites and facilities. Case Study 1 and Case Study 2 illustrate the impact when SeBD is not implemented, and security is absent at the start of projects. Case Study 3 provides an example of positive engagement with security, where changes could be made at an early stage.

3.2.1. Case Study 1

Case Study 1 – Landscape Design

- A nuclear new build project in the UK underwent an optioneering process, and security subject-matter experts were actively involved to identify and eliminate potential vulnerabilities in the design choices.
- A decision was made to change the plant layout, however, shortly after the optioneering process concluded, the developer appointed a new supply chain partner as the lead delivery partner for construction.
- The supply chain partner was tasked with creating a new design for drainage, mounding, and grading of landscaping.
- This design process was carried out in isolation, without input from the security team.
- The process no longer followed the SeBD philosophy.
- The resulting landscape inadvertently created elevated areas that could provide ideal vantage points for hostile reconnaissance or to launch attacks against the operational power station.
- The issue was discovered only by chance when the construction security lead reviewed the designs and raised their concerns.
- This led to a costly redesign process which could have been avoided if the organisation had embedded SeBD principles into its culture.

3.2.2. Case Study 2

Case Study 2 – Security Enhancements to an Existing Facility

- A security enhancement project was initiated in an operational nuclear facility in the UK, as proposed future work would result in a requirement to increase the security categorisation of the facility.
- Security practitioners were engaged during the initial concept phase of the project where they identified areas for enhancement to meet the regulatory requirements. This led to the development and approval of Operational Requirements (see Section 6.3).
- On appointment of the lead contractor a breakdown in communication occurred resulting in some of the requirements being misinterpreted within the subsequent security system design phase.
- This led to an overly conservative design, with significant capital and operational expenditure implications and adverse impacts on project schedule and delivery.
- This led to the design being reassessed, and a revised solution being developed that adopted a pragmatic, risk-informed approach whilst still meeting organisational and regulatory requirements.
- Because of the breakdown in communication, the operator incurred a substantial and avoidable additional cost.

3.2.3. Case Study 3

Case Study 3 – Security Integration from the Outset

- A Design Modification Committee was created for the Generic Design Assessment of a Pressurised Water Reactor design.
- This Committee included members across multiple disciplines, including Safety, Security, and Environment.
- All technical changes were reviewed by the security function to assess whether they affected any security arrangements or created any new vulnerabilities.
- A proposed change in the Centralised Instrumentation and Control Systems was reviewed, and the security team identified a potential cyber vulnerability with the interlinkages between the safety trains, which could allow an attack to move laterally and affect vital control systems within the power station.
- The security team therefore raised concerns to the Committee, and a design change was made to remove the vulnerability.

4. Principles of Secure by Design

Secure by Design may be characterised by a range of principles that are covered below.

Although SeBD is complemented by a range of other technical security principles, these will only be touched on briefly, as this section will focus on the principles relevant to all stakeholders, including non-security practitioners.

4.1. Early Engagement

As illustrated in the Case Studies above, early and continuous engagement is one of the key principles of SeBD and is fundamental in ensuring its effective implementation. When security is engaged early, costly mistakes can be avoided, and opportunities for cross-disciplinary interdependencies can be identified. For example, thick concrete shielding around radioactive material not only serves as radiological protection but can also be considered a security feature, as it increases the delay time for an adversary to gain access. As a result, fewer additional external security layers are necessary.

However, often the security function is not involved in key conversations and processes at these initial stages. Therefore, work must be done to ensure security is not overlooked in the early stages of projects.

4.2. Proportionality

Proportionality is also key to the SeBD approach, as SeBD provides the opportunity for utilising risk-informed approaches. This is especially true in the early optioneering stages of a project, where there is opportunity to choose a different solution that could remove or reduce future security burden. SeBD should be guided by the analysis of the threat and vulnerabilities, thus ensuring that the security design is fit for purpose and is not solely based on conservative judgements or prescriptive requirements.

The UK's outcome-focused security regulations provide the flexibility to take a risk-informed approach. This approach encourages practical and efficient security solutions that enable an optimal design to be achieved when implemented in conjunction with other stakeholders.

4.3. Collaboration

Nuclear infrastructure projects are extremely complex, with the involvement of many different technical disciplines, all with specific and often preferred requirements. A collaborative approach is required to successfully implement SeBD to ensure an optimised design solution is identified. Effective communication is essential to establishing an integrated, iterative process that is applied consistently across the entire lifecycle of the site. Failure to engage security increases the risk of delays to a project and may mean potentially significant changes are needed in order to meet regulatory or operational requirements. Security should be considered at the start of every project, with the involvement of security professionals being non-negotiable and automatic, in the same way that the safety function is considered at the start of most projects.

Collaboration is also beneficial to help identify any easy wins and opportunities for integrated security, which could lead to reduced capital or operational expenditure, or both. When it comes to security, people don't know what they don't know. For example,

there may be passive safety measures that also provide a security function which could be implemented easily into a new design, but as the engineers are not aware of these measures or the security requirements, they may not be recognised and may be overlooked.

The table below illustrates the importance of engagement with various stakeholders, although it is by no means an exhaustive list.

Stakeholder	Reason for Engagement
Security	Suitably Qualified and Experienced Persons (SQEP) from the security function must be fully engaged with to guide decision-making. This prevents incorrect assumptions from being made, which otherwise may steer projects in the wrong direction (see Case Study 1).
Environment and Safety	Like security, environment and safety are essential functions that must be engaged with at the outset of a project. However, sometimes the interests of environment, safety, and security conflict. For example, safety may seek to include additional doors in active areas for use as emergency exits, whereas security will want to reduce the possible access points that an adversary may be able to use. It is vital that all teams work together to ensure that any decisions made consider all disciplines to find the optimal solution, otherwise additional measures will be required to mitigate the issues created.
Project Management	Project management has a key role, as they must ensure that the project delivers an optimised solution to meet client requirements. To do so requires the involvement of all stakeholders, including security. To ensure this engagement happens, security should be included in project management forms and documentation, thus ensuring that projects cannot progress without security involvement.
Executives	SeBD requires leadership commitment. Executives must be bought into the benefits of SeBD, and the importance of security in general. If the value of security is not recognised at the top of the organisation, then other disciplines may feel less compelled to value security, potentially leading to engagement with security being less than optimal, or even missed entirely.
Engineers	Engineers should be engaged with to facilitate the inclusion of security requirements in designs. This enables engineers to incorporate security measures from the outset, and design with security in mind.
Regulators	Early and continuous engagement with the regulator will help ensure key regulatory expectations are met, enable timely advice and guidance, and foster relationships built on trust.

4.3.1. Understanding the Threat

A potential barrier to effective collaboration is failure to understand the threat. To effectively design a security system, the threat that you are designing against must be understood, as this will affect the type and quantity of security measures and procedures to be implemented.

The threat against which dutyholders must design and implement their security arrangements is defined by the State in the threat assessment or the Design Basis Threat (DBT), which describes the capabilities of the adversary. However, due to the document classification and the 'need to know' principle, not all stakeholders will have access to it. Therefore, to ensure that project and design decisions are made with the threat in mind, it is essential that stakeholders engage with the security practitioners in their organisation who have access to the DBT and who can advise on the requirements necessary to address the threats within the design. For example, security practitioners may be able to advise engineers as to the blast level that a wall must be able to withstand whilst not disclosing the details of the threat, and as a result, the engineers can design the wall with the threat in mind.

The delivery of threat briefings is also another method that can be used to ensure key stakeholders recognise the threat and are therefore more conscious of the requirement to consider security needs within the design.

4.4. Long-Term Outlook

Due to the significant investment required, nuclear facilities have long operational and decommissioning lifecycles. Therefore, even small operational expenditures are magnified across many decades of operation. Thus, it is important to take a long-term view of security. This involves considering what will create the most benefit long-term, rather than taking advantage of quick wins which may have a detrimental effect overtime and potentially require further work and investment.

4.4.1. Upfront Costs vs Future Savings

A key part of having a long-term outlook involves the consideration of cost. While implementing integrated security measures early in a project may incur a significant cost, if security is not integrated and is simply 'bolted on' at the end of a project, this will likely incur a far larger cost.

For example, when addressing blocked sightlines at a facility, a series of cameras may be proposed as a security solution, rather than changing the layout of a perimeter wall. Cameras might be favoured as they would avoid the cost of a redesign. However, the camera systems will require ongoing, frequent inspection and maintenance, plus replacement for obsolescence; and place additional burdens and demands on the security centre operators responsible for monitoring video surveillance or CCTV systems. Therefore, when considering a long-term outlook, the short-term redesign cost to change the layout may be more economical.

4.4.2. Changing Threat Landscape

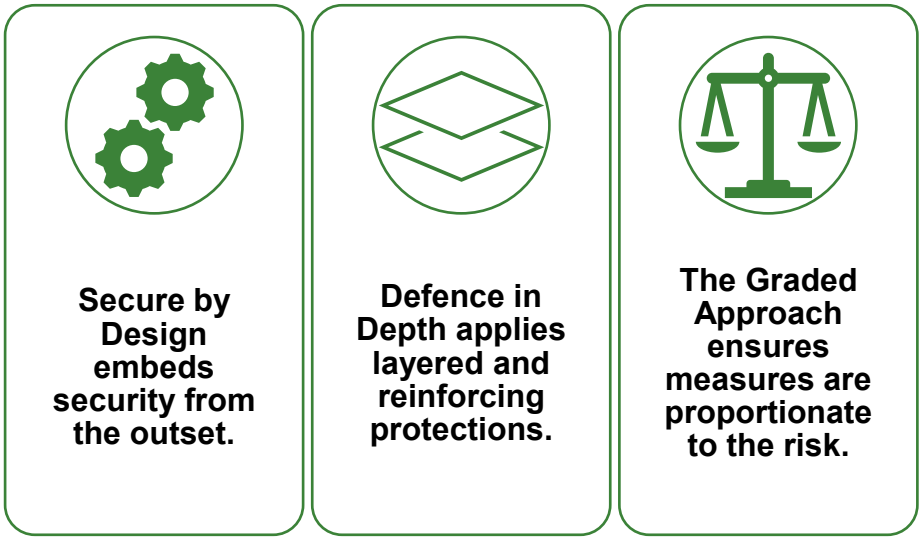
Considering a long-term outlook also requires an understanding that the threat can change over time, and therefore a security solution which adequately addresses the threat today, must also be sufficiently flexible to adapt in years to come.

This principle can be challenging to reconcile with the purpose of SeBD, which aims to ensure that security is applied proportionately. Therefore, integrating a higher level of security than is required now to mitigate any potential evolution of the threat, counters the primary objective of SeBD.

A balance must be struck whereby a design is futureproofed but is not overly conservative and disproportionate to the current threat. This will require thoughtful consideration and detailed discussions with security subject-matter experts.

4.5. Technical Security Principles

SeBD is complemented by other technical security principles, such as the Graded Approach and Defence in Depth. Together they collectively deliver a risk-informed and proactive security framework.



These principles create a balanced system that is fundamentally secure, operationally robust, and aligned with the assessed threat and consequence.

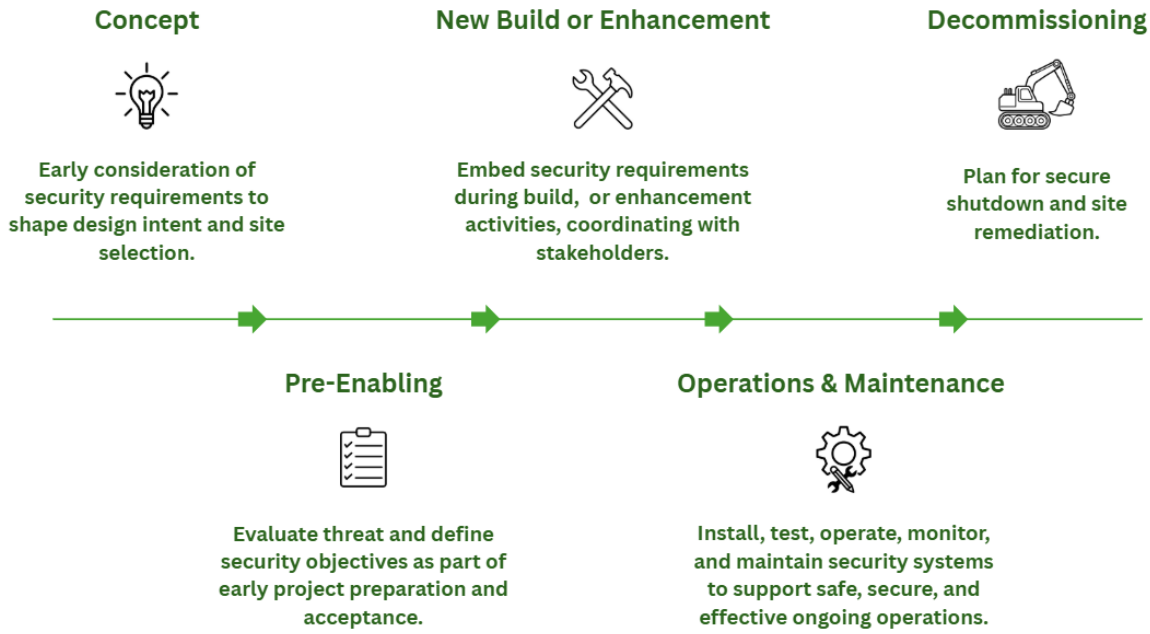
Defence in Depth and the Graded Approach will not be discussed further in this guide, but they should be applied in tandem with SeBD by the security teams engaged with.

Further guidance on the application of these principles can be found in the IAEA Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) and the ONR Security Assessment Principles for the Civil Nuclear Industry.

5. When to Apply Secure by Design

Secure by Design should be applied at every stage of all projects, enabling vulnerabilities to be designed out from the outset and proportionate security measures to be built in to effectively mitigate threats.

The recording of decision logs throughout the project lifecycle is fundamental to providing the rationale for decisions taken. Maintaining clear and accurate decision logs enables consistency as the project evolves. This reduces ambiguity, supports coherent decision-making, and prevents unnecessary rework caused by misinterpretation.



5.1. Concept

Whether you are constructing a new facility or modifying an existing one, either on a new site or existing nuclear licensed site, security must be integrated from the initial concept design phase. Early engagement with cross-disciplinary stakeholders is key to ensuring an optimal design solution.

For example, the location of a facility and its design may affect how vulnerable or secure it is. Consider the impact of the different choices below:

- A facility that is near to a large town may pose a greater radiological risk if there was to be a sabotage event.
- A facility surrounded by flat, bare land, will offer the response force uninterrupted sight of the area surrounding the facility, however, it will also provide adversaries with increased visibility, making it easier for them to target a ballistic attack.
- A facility surrounded by varied terrain with hills and trees may provide adversaries with more hiding places thus making them harder to be detected. Higher ground may also provide adversaries with vantage points for surveillance and launching attacks (see Case Study 1).

In addition, the fuel type and the enrichment should be considered from a security perspective, as these factors directly influence the level of protection required to meet regulatory requirements.

If the security function is not involved in early discussions between the designers, architects, and engineers, then these security considerations may be overlooked.

5.2. Pre-Enabling

Incorporating security conceptually at this stage of a project ensures that security is a key consideration in design reviews, decision gates, and operability studies. When security is embedded at decision points, it supports operations rather than constraining them.

For example, working with designers and architects to ensure understanding of the threat, and early identification of key areas of the facility that will require protection will allow for early consideration of layouts and access/egress routes whilst being cognisant of the threat.

5.3. New Build or Enhancement

Secure by Design applies equally to the construction of a new reactor or facility and to enhancements of existing ones.

5.3.1. New Build

Irrespective of the type of new build, whether a facility or a reactor, and whether intended for land-based or maritime use, SeBD must be integrated from the outset. New builds provide a blank slate in which SeBD can be applied to its fullest extent, with aspects such as facility, location, siting, and design being able to be developed with security considerations in mind. This enables vulnerabilities to be designed out from the start, rather than requiring additional mitigating measures in the future.

At this stage, it is also important to involve the relevant response force, in addition to the internal security function, as it is imperative to ensure that the chosen design allows the response force to protect against the threat, and does not unintentionally hinder the response forces' effectiveness.

5.3.2. Existing Facility

For facilities that were designed to earlier standards, it is important to ensure that risks have been proportionately managed and vulnerabilities have been mitigated. Where modifications or enhancements are proposed, applying the principles of SeBD can help to ensure that unnecessary additions that do not account for existing measures and capabilities are avoided.

5.4. Operations and Maintenance

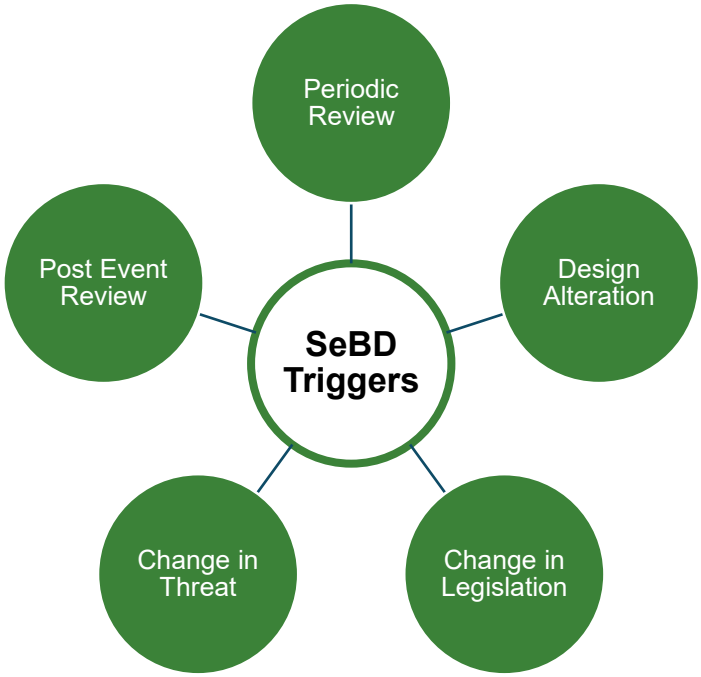
The upfront cost of security is often perceived as significant and disproportionate. However, when security isn't considered from the outset, the ongoing operational expenditure for operating, testing, and maintaining security over the lifetime of a facility frequently exceeds the initial capital expenditure due to the decades-long operational lifetime of nuclear facilities.

5.5. Decommissioning

The final stage of the nuclear lifecycle involves facilities and sites transitioning from active operations to site restoration, including the removal of the nuclear material. SeBD must be applied at this stage to ensure that the security measures remain proportionate to the risk. Once nuclear material is removed and the associated risks reduced, security measures should be adjusted accordingly.

5.6. Triggers

In addition to the points highlighted above, there are additional triggers which should prompt the application of the SeBD approach.



Should any of these triggers occur, the security function should be engaged with to consider whether these events have any impact on security, and if they do, how that impact can be addressed in a cost-effective and proportionate manner, whilst meeting the relevant regulatory requirements.

6. How to Apply Secure by Design

Secure by Design is not a one-size-fits-all process. It is an inclusive, multi-disciplinary approach that involves the integration of security alongside other disciplines throughout a project lifecycle. Therefore, the application of SeBD may differ depending on the nature of the project and the unique approach of the organisation applying it. The application of SeBD may also differ depending on the type of regulations adopted by the State. For example, the UK's outcome-focused regulations will likely enable a more flexible approach to SeBD than a State with prescriptive security regulations. Therefore, a tailored approach is required.

6.1. Starting Point

To truly embed SeBD, an organisation must work collectively to foster a culture that strengthens nuclear security and ensures a security system that is both proportionate and effective. The IAEA Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) states:

> **All organizations involved in implementing physical protection should give due priority to the security culture; to its development and maintenance necessary to ensure its effective implementation in the entire organization.**

With the right organisational culture in place, SeBD can be embedded into everyday practice in the same way as other core disciplines, like safety. This will allow security to be recognised as a valued partner and integrated throughout the entire project lifecycle, from concept and design through to operations and decommissioning.

6.2. Existing Processes and Procedures

One of the easiest ways to apply and sustain SeBD within an organisation is to embed its principles within existing processes and procedures. This will often be quicker and easier to implement than creating new processes and may attract less resistance from other disciplines as it is not increasing their workload with new forms and documents (see Case Study 3).

Some examples of processes and procedures are listed in the table below; however, this is not an exhaustive list. Processes related to engineering and plant modifications should also be adapted to include security input as a requirement.

Process / Procedure	Explanation	Benefit of Integrating Security
Hazard and Operability Study (HAZOP)	HAZOPs are an effective technique for the identification and analysis of hazards and operational concerns.	Integrating security considerations into the HAZOP process enables the identification of vulnerabilities and potential security related failures, alongside safety risks, without introducing an entirely new process.
Quality Governance Model (QGM)	A QGM is a structured framework, or management system, that defines how an organisation directs, controls, and assures quality across its projects and programmes. It establishes clear accountability, standards, decision-making processes, and assurance mechanisms to ensure that outcomes meet defined requirements and manage risk effectively.	Embedding security within a QGM ensures that it is not treated as an 'afterthought' or 'bolt-on' function, but as a core discipline integrated throughout the project lifecycle. This enables a proactive, risk-informed approach that supports the delivery of operationally effective systems.
Gate Process	Most large infrastructure and nuclear projects are delivered in a phased approach to design with formal hold points, or gates.	Integrating security into the existing gated process shifts security from a reactive compliance check to a proactive design parameter, informing decisions at every stage. This prevents costly redesign, over-engineering, and disruption to delivery timelines. Embedding security requirements within each gate also reduces ambiguity and misinterpretation (see Case Study 2).

6.3. Guidance for Application

Specialist national advisory bodies and agencies play a key role in supporting the implementation of SeBD. The UK's National Protective Security Authority (NPSA) provides publicly available guidance and tools to help organisations embed security considerations into projects from the outset.

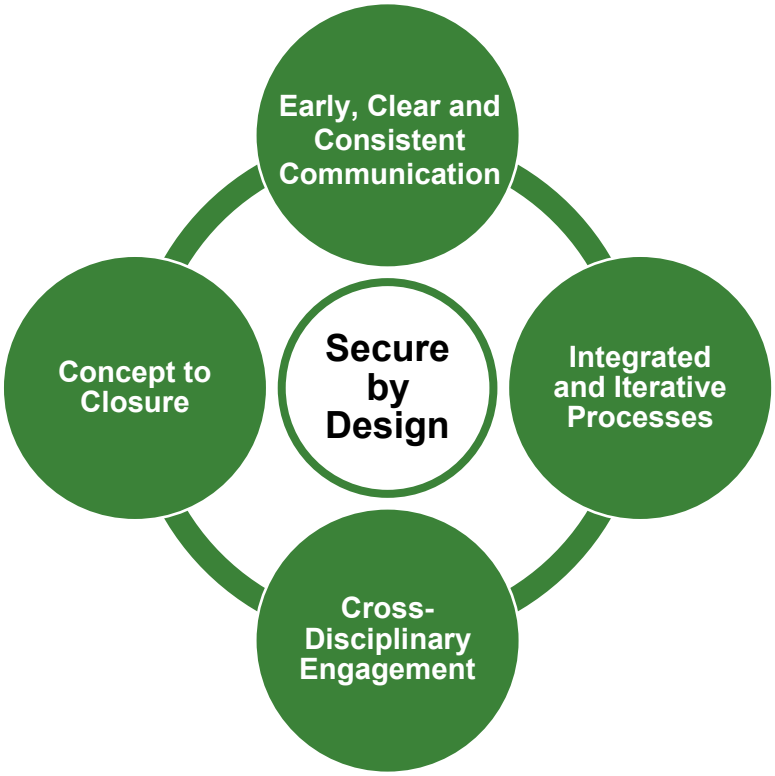
These tools help to ensure that security is integrated into planning, design, and delivery processes rather than being applied retrospectively.

Three of NPSA's key tools are highlighted below.

NPSA Tool	Purpose
Operational Requirements Methodology	For projects where security is the primary driver, the Operational Requirements methodology may be appropriate. This approach enables an organisation to develop a clear, well-considered, high-level statement of its security needs, grounded in an understanding of the risks it faces.
Security Considerations Assessment	Where security forms one component of a broader project, the Security Considerations Assessment methodology may be more suitable. This structured process ensures that potential security vulnerabilities are systematically identified and addressed across a range of activities and processes. It also strengthens the documentation of security-related decisions and improves the consistency and quality of their implementation.
HAZOP Application Guide	This security-informed guide supports the growing need to provide safety and security assurance, which is a variation from the conventional HAZOP.

7. Summary

This Awareness Guide outlines the fundamental principles of why, when, and how SeBD can be implemented across all stages of the nuclear lifecycle to help achieve these goals. It provides practical guidance and highlights the benefits of applying SeBD, demonstrating how its integration can facilitate the successful deployment of advanced nuclear technologies and drive a more efficient approach to nuclear security.



Additional resources are provided in Appendix 1 to offer further information and support for the practical application of SeBD.

Appendix 1. Useful Resources

Resources	
1	International Atomic Energy Agency (2005) *Amendment to the Convention on the Physical Protection of Nuclear Material*
2	International Atomic Energy Agency (2011) *IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*
3	International Atomic Energy Agency (1980) *The Convention on the Physical Protection of Nuclear Material (INFCIRC/274/Rev. 1)*
4	International Atomic Energy Agency (2013) *International Safeguards in Nuclear Facility Design and Construction (No. NP-T-2.8)*
5	International Atomic Energy Agency (2008) *Nuclear Security Culture (NSS no. 7)*
6	Office for Nuclear Security, *Security Assessment Principles for the Civil Nuclear Industry*
7	Office for Nuclear Regulation, *Nuclear Security Technical Assessment Guides*
8	National Protective Security Authority (Last Updated: 2025) *Security Considerations Assessment*
9	National Protective Security Authority (Last Updated: 2023) *Operational Requirements*
10	National Protective Security Authority (last Updated: 2023) *Protecting Your Assets*
11	T. Languin and E. Ducousso (2020) *French Approach to Security by Design: From the Opéra Garnier to SMR*, International Conference on Nuclear Security 2020 (10-14 Feb 2020)
12	Mark K. Snell, Calvin D. Jaeger, Sabina E. Jordan, and Carol Scharmer (Sandia National Laboratories), and Koji Tanuma, Kazuya Ochiai, and Toru Iida (Japan Atomic Energy Agency) (2013) *Security-by-Design Handbook (Sandia National Laboratories, SAND2013-0038)*

Appendix 2. Acronyms

Acronym	Meaning
DBT	Design Basis Threat
HAZOP	Hazard Operability Study
IAEA	International Atomic Energy Agency
NPSA	National Protective Security Authority
ONR	Office for Nuclear Regulation
QGM	Quality Governance Model
SeBD	Secure by Design
SQEP	Suitably Qualified and Experienced Persons
UK	United Kingdom

This guide is part of a comprehensive series of Nuclear Security Awareness Guides that focus on key aspects of nuclear security. These guides have been developed by security specialists for non-security practitioners.

These documents are for guidance only and do not constitute relevant good practice.

Produced by the United Kingdom National Nuclear Laboratory, March 2026.

The United Kingdom National Nuclear Laboratory acknowledges the contribution and input from the Safety Directors' Forum Nuclear Security Standards Sub Group members.