Department for Energy Security & Net Zero

NDA

ONR Office for Nuclear Regulation

Sellafield Ltd

AWE

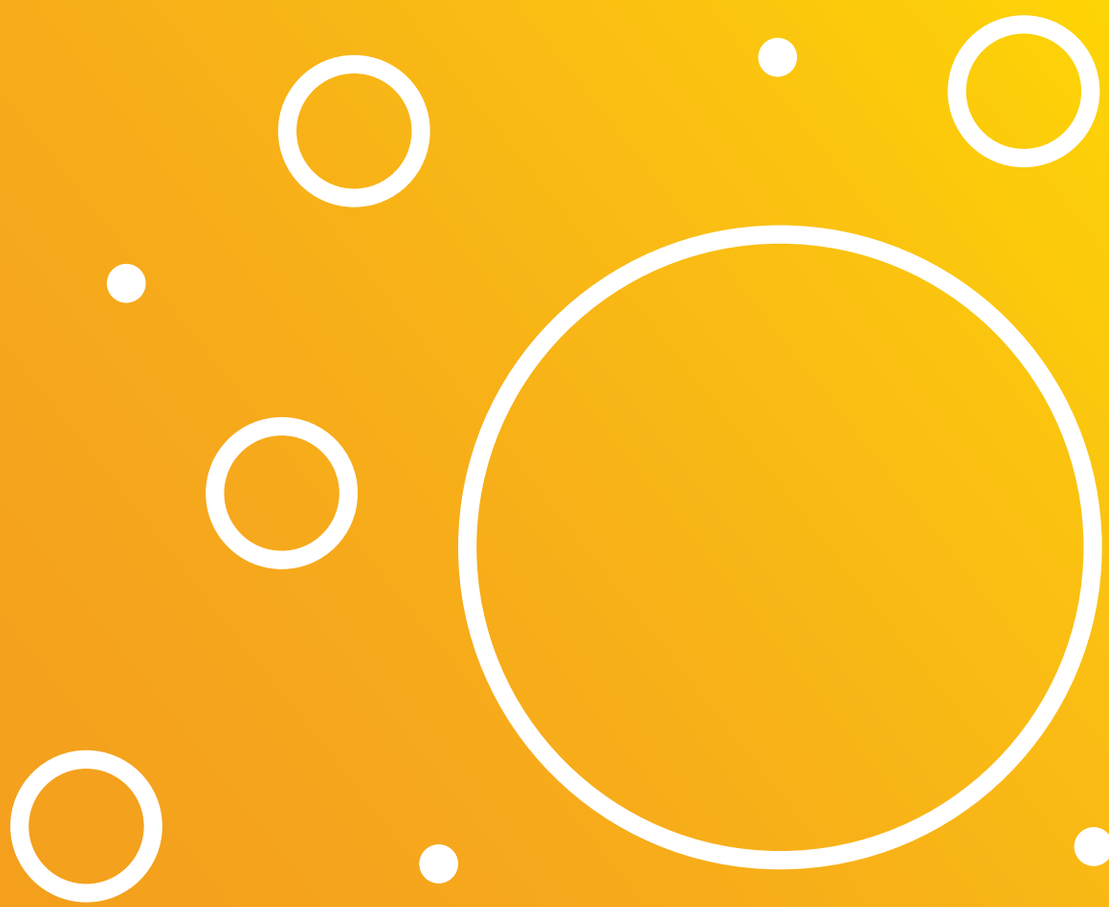
NATIONAL NUCLEAR LABORATORY

NRS

NSSG

Nuclear Security
Awareness Guide

# Vulnerability Assessments



Department for Energy Security & Net Zero
NDA
ONR Office for Nuclear Regulation
Sellafield Ltd
AWE
NATIONAL NUCLEAR LABORATORY
NRS
NSSG

# Contents

This Nuclear Security Awareness Guide has been produced with funding from The UK Alpha Resilience and Capability (ARC) Programme. ARC is a proactive, long-term collaboration between the UK government, nuclear industry and wider nuclear sector which seeks to identify targeted projects and investments in specialist nuclear skills, expertise and facilities.

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.

Drafted in collaboration between The National Nuclear Laboratory and Global Nuclear Security Partners.

# 1 Introduction

**Nuclear and other radioactive materials (ORM) present an attractive target to a range of malicious actors, who would seek to use them to cause maximum disruption, harm, or to raise the profile of their cause.**

The need for protection of radiological materials, ORM and sensitive nuclear information (SNI) is to protect against a threat to public health and the environment and prevent significant disruption and cost associated with a potential malicious event.

It is therefore essential to ensure any vulnerabilities in the security component performance are identified, acknowledged and resolved to ensure they cannot be exploited.

This document is intended to provide an awareness of Physical Security Vulnerability Assessment (VulA) to non-security specialists. It is written to explain the key principles only and is not a best practice guide.

## 1.1.

## International

The United Kingdom became a member state of the International Atomic Energy Agency (IAEA) on 29th July 1957 and since its membership has become signatory to various international agreements.

One agreement 'The Convention on the Physical Protection of Nuclear Material' (CPPNM) and its amendment, establishes legal obligations for member states regarding effective worldwide physical protection of nuclear material used for peaceful purposes.

The UK's Nuclear Industries Security Regulations 2003 (as amended) takes the CPPNM and enshrines components into law. The Energy Act 2013 creates the Office for Nuclear Regulation (ONR) as an independent, statutory regulator of nuclear safety, security, and conventional health and safety at nuclear sites. They became a public corporation on 1 April 2014.

ONR, recognised as a world-leading regulator, has recently used this legislative framework in 2017 to create 'Security Assessment Principles' (SyAPs); an outcome based, non-prescriptive regulatory framework.

The primary objective is for a duty holder to provide claims, arguments and evidence to underpin how it is meeting its Physical Protection System (PPS) outcome. How this is achieved is down to the duty holder to establish. ONR has created a series of open-source Technical Assessment Guides (TAGs) thereby making the assessment process transparent.

It is worth noting that SyAPs success is not guaranteed, due to its nonprescriptive nature. In some cases, duty holders may not follow the ONR guidance and look at the underpinning law to establish a different methodology.

## 1.2.

## ONR Vulnerability Assessments

TAG 6.4 states Vulnerability Assessments are undertaken by Dutyholders to satisfy themselves that their PPS achieves the required security outcome.

The vulnerability assessment should be proportionate to Fundamental Security Principle (FSyP) 6 regarding the implementation and maintenance of a proportional and effective PPS.

Throughout the entire vulnerability assessment process, reference should be made to Office for Nuclear Regulations (ONR) Security Assessment Principles (SyAPs), Technical Assessment Guide (TAG) and IAEA Nuclear Assessment Methodologies for Regulated Facilities (IAEA TECDOC-1868).

The purpose of the vulnerability assessment is to assess the security component performance and the overall system effectiveness. This is done through identification of exploitable weaknesses in asset protection. If a vulnerability is identified, recommendations to reconsider the design of the system and specific recommendations of improvements/countermeasures should be suggested.

A vulnerability assessment should also be undertaken in the following circumstances:

- If the designated site or facility undergoes major modification
- If there is a change in categorisation for theft or sabotage
- If there is a change in design basis threat assessment (DBT and/or local site)
- If there is a change in any founding assumptions

The vulnerability assessment should also be reviewed periodically throughout the lifetime of the designated site or facility to ensure it remains valid.

## 1.3.

## Terminology

Undertaking an accurate vulnerability assessment will require understanding and using the correct terminology.

To aid in a common understanding of terminology, the IAEA defines vulnerabilities and vulnerability assessments as follows:

**Vulnerabilities:**

A physical feature or operational attribute that renders an entity, asset, system, network, facility, activity or geographic area open to exploitation or susceptible to a given threat.

**Vulnerability Assessment:**

A process which evaluates and documents the features and effectiveness of the overall security system at a particular target.

Throughout this Nuclear Security Awareness Guide (NSAG), the terms facility and site will be used. The following definitions underpin the use of these words.

**Nuclear Facility:**

A facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored, or disposed of and for which a specific licence is required (IAEA – INFCIRC/225/Revision 5).

**Site Area:**

A geographical area that contains an authorised facility, authorised activity or source, and within which the management of the authorised facility or authorised activity or first responders may directly initiate emergency response actions.

This is typically the area within the security perimeter fence or other designated property marker (IAEA Nuclear Safety and Security Glossary).

## 1.4.

## Vital Area Identification versus Vulnerability Assessment

The Vital Area Identification (VAI) process is used to define a boundary around the vital equipment, systems, devices, or nuclear material to which physical protection can be applied.

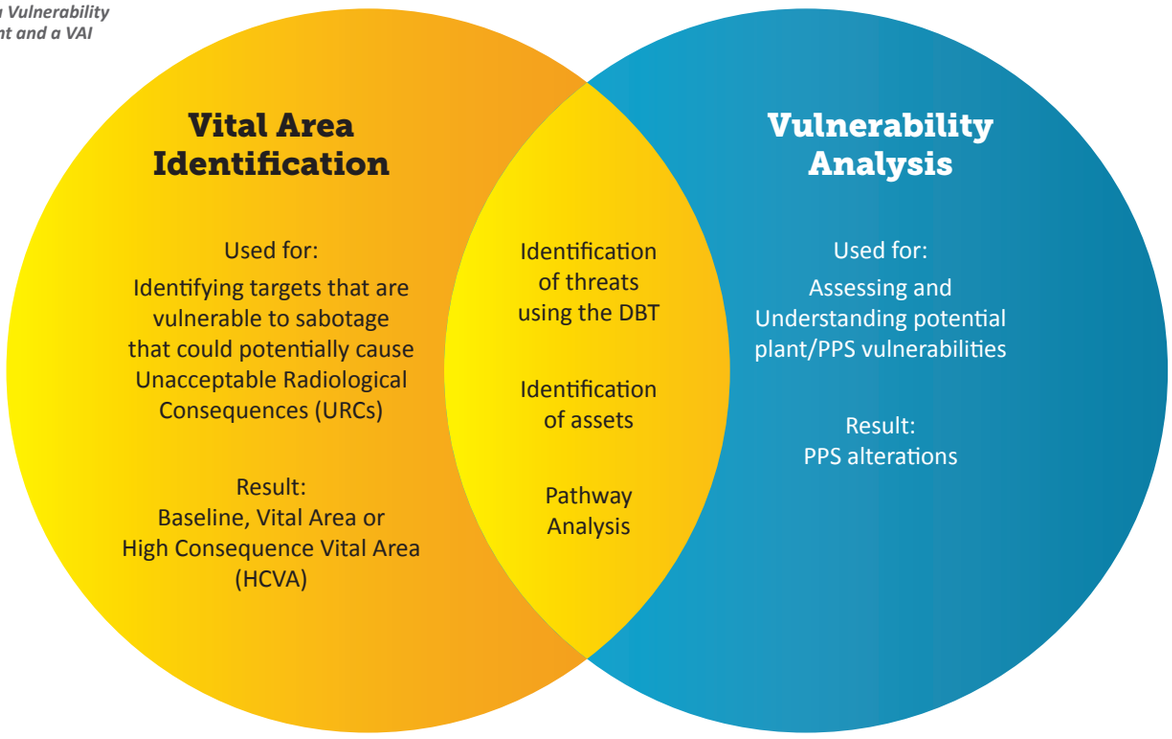
The objective of the VAI process is to identify a set of areas of a facility containing the equipment, systems, structures, components and / or designated items of plant that, if adequately protected, will prevent Unacceptable Radiological Consequences (URCs) (IAEA, Identification of Vital Areas at Nuclear Facilities).

Undertaking a VAI requires many of the same processes as that of a vulnerability assessment, such as identifying assets and threats, and using the DBT to assess possible threat/adversary scenarios. However, their outcomes and purposes are different, and it should be made clear that this NSAG is written specifically for the process of a vulnerability assessment, not a VAI.

The main difference between a VAI and vulnerability assessment is their focus and purpose. VAIs are concerned with identifying critical assets or areas that require protection to ensure mission success, while vulnerability assessments are concerned with identifying and assessing weaknesses or vulnerabilities in systems and processes, to reduce security risks through the implementation of appropriate security controls.

Both processes are essential components of a comprehensive security program, with the VAI informing where to allocate protective resources and the vulnerability assessment helping to secure the identified critical assets.

***Figure 1:***
***Venn Diagram showing the overlap and distinctions between a Vulnerability Assessment and a VAI***



# 2

# Vulnerability Assessment Process

## 2.1.

## Formation of a Suitably Qualified and Experienced Persons (SQEP) Team

A vulnerability assessment should only be undertaken by those who are experienced and qualified.

This is to ensure the vulnerability assessment is carried out accurately and appropriately using integrated methods, showing clear links between any analysis and engineering/ technical corroboration, as required by ONR guidance.

The team should be a multidisciplinary team formed of an assessment lead with appropriate subject matter experts (SMEs). SMEs are individuals with significant experience operating plants and/or exploring vulnerabilities. Other individuals involved may include, but are not limited to, system owners, radiological protection staff, security systems engineer and relevant operational personnel.

This approach should be taken to ensure that staff members involved have the appropriate knowledge and skills to undertake their responsibilities and ensure that credible and appropriate processes, methods, and standards are used for undertaking the project.

Important considerations:

- **Expertise:** Vulnerability assessments require a diverse set of skills and knowledge.
- **Independence:** An independent SQEP team is less likely to overlook or downplay vulnerabilities due to conflicting interests. They can provide an unbiased assessment of the security posture and prevent detailed knowledge of threat pathways not apparent in open source.
- **Accountability:** Having an accountable team for vulnerability assessments ensures that this critical aspect of security is not overlooked or treated as an afterthought.

## 2.2.

## Assessment Input Required

A variety of information and data is needed to ensure the assessment is informed; it should be collected and collated by the SQEP team undertaking the vulnerability assessment.

The following data is usually required for the assessment:

| | |
|---|---|
| **Identifying Critical Assets and Infrastructure** | a. Nuclear material |
| | b. Other radioactive material |
| | c. Equipment |
| | d. Structures |
| | e. Systems |
| | f. Components |
| **Identifying Threats** | a. Adversary identification – insider and outsider |
| | b. Adversary characterisation (refer to DBT, the site specific interpretation of the DBT and relevant NPSA guidance) |
| | c. Identify what information is easily available to adversaries on the internet and other open-source literature. |
| **Deciding/Creating Scenarios** | a. Scenarios should be site-specific, challenging, and realistic, in line with the DBT and local/site specific threats. |
| | b. Any threats discounted should be evidenced as to why that threat is unlikely for the specific site. |
| **Site or Facility Characterisation** | a. Determine the PPS components (dependant on the lifecycle status of the site or facility, this could be carried out at the beginning of this process) |
| | b. Determine how to quantify or demonstrate the PPS component's performance measures. |

## 2.3.

## Undertaking the Assessment

The vulnerability assessment seeks to assess the adversary task time required to overcome the individual PPS functions (delay, detect, assess, unauthorised access control and insider mitigation) when compared with the PPS response and its required effect.

The assessment may incorporate, where available, empirical data such as data from the operational environment and performance testing for the physical, technical, and operational components of the PPS. Where subjective information is used this should be supported by SME input and fully documented.

The outline of the process for undertaking the assessment is as follows:


***Figure 2:***
***The Vulnerability Assessment Process***

- **Step 1:** Following the gathering of all the data, the first step is usually performing adversary pathway analysis. This will clearly illustrate the potential pathways an adversary could take to reach critical assets and will help determine the most vulnerable pathways on the site.

- **Step 2:** Scenario Analysis- Evaluate specific scenarios using the initial input data, this will determine attack scenarios that would compromise the security of an asset.

  Dependant on the site this step may come first, preceding pathway analysis, as high-level scenarios could be formed in which multiple pathways may consequently present themselves.

  Credible scenarios are critical to ensure measures identified remain proportionate to the threat and risk posed.

- **Step 3:** It is suggested for high consequence sites to undertake additional analysis to substantiate the claims, arguments and evidence made, it is not mandated for other sites. There are a range of methodologies and techniques available to be used, these include (but are not limited to):
  - Wargaming
  - Tabletop
  - Force on Force
  - Subject Matter Expert (SME)
  - Modelling and Simulation

  It is essential that the correct technique is chosen which accurately addresses the specific purpose and scope of the vulnerability assessment being undertaken and which provides a quantitative or qualitative assessment appropriate to the purpose of the assessment and the methodology used for performance evaluation.

  A table including some of the capabilities and limitations of these different tools can be found in the Appendix. There is no regulatory expectation any particular technique should be selected, this remain Dutyholder specific.

- **Step 4:** Analyse results. Evaluating the effectiveness of existing security measures, the nature of the radiological hazard, identifying vulnerabilities, and estimating a degree of vulnerability for the site. It can then be determined if the PPS is adequate to counter the postulated threats.

- **Step 5:** The final step is the writing of the assessment report.

## 2.4.

## Writing the Assessment Report

The aim of the report is to provide accurate, unbiased information clearly demonstrating the current effectiveness of the PPS, along with *potential solutions for any ineffective areas identified.*

It is usually written in a manner that is useful to the facility managers, informing them of the current effectiveness of the PPS and helping to support their decision making.

It is typically recommended within such reports that assessments are reviewed throughout the lifetime of the site, to ensure they remain valid.

The vulnerability assessment can be used to determine performance requirements needed to allow the security design team to select the most appropriate PPS components that will meet requirements. At this stage it is for the key risk owner to determine their risk appetite against the overall performance of the PPS installed. An Intelligent Client (IC) is normally nominated ensuring the project team have identified the outcomes needed.

If a vulnerability prevents a response being met satisfactorily this will represent a gap in the security plan. This can be included in the site's Nuclear Site Security Plant (NSSP) Security Improvement Schedule (SIS), or a similar approved document. It should be noted that the SIS is an agreed shortfall in the PPS and the key risk owner has a plan to make it achievable. It is not normal to have items within a SIS that are unachievable.

Figure 3 and its supporting narrative is one example of a number of acceptable methods to present the outcome of a Vulnerability Assessment.

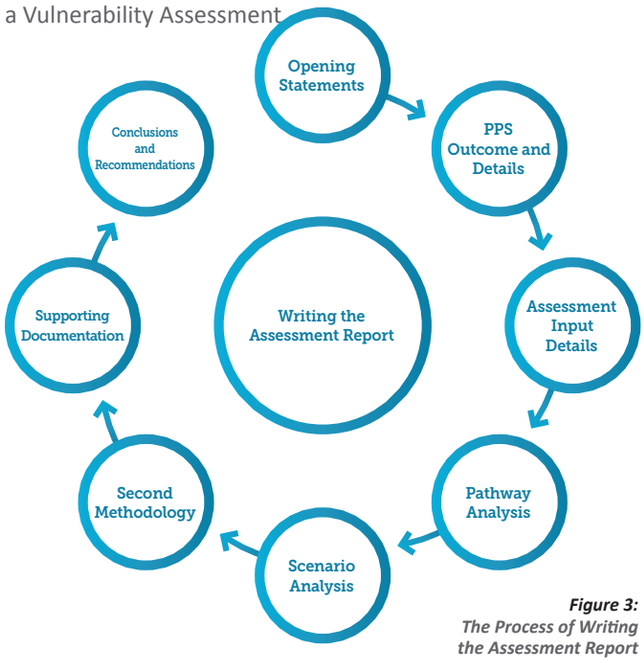



***Figure 3:***
***The Process of Writing the Assessment Report***

1. **Opening statements**
   a. Address why the assessment is being undertaken, where, and an explanation of the makeup of the SQEP team.
   b. It can include the requirements stated in SyAPs or international best practice.

2. **PPS Outcome and Details**
   The PPS outcome expected to be met should be stated and information regarding the PPS in place.

3. **Assessment Input Details**
   Detailed explanation of the assessment inputs (critical assets, infrastructure, threats, and open-source information).

4. **Pathway Analysis**
   Process and results.

5. **Scenario Analysis**
   Process and results.

6. **Second Methodology**
   Data from any other methodologies undertaken. National Protective Security Authority (NPSA) data (or other test house that provides similar levels of rigorous testing) should be used to evidence any timings or claims made during the pathway analysis.

7. **Supporting documentation.**

8. **Conclusions and recommendations.**

## 2.5.

## Peer Review

During production, the submission undergoes a peer review process by a SQEP individual or team before being submitted to ONR (CAT I–III duty holders UK Only).

This individual or team can be from within the organisation, an outside consultancy, or from another site. The essential considerations are the SQEP-ness and objectives of the individual or team undertaking the review. They should not have been immediately involved in the development of the vulnerability assessment in order to provide a level of separation and avoid any possible bias.

A peer review ensures appropriate methods and relevant security standards and specifications have been used, the calculations are correct, and assumptions are realistic.

## 2.6.

## Drawing Conclusions

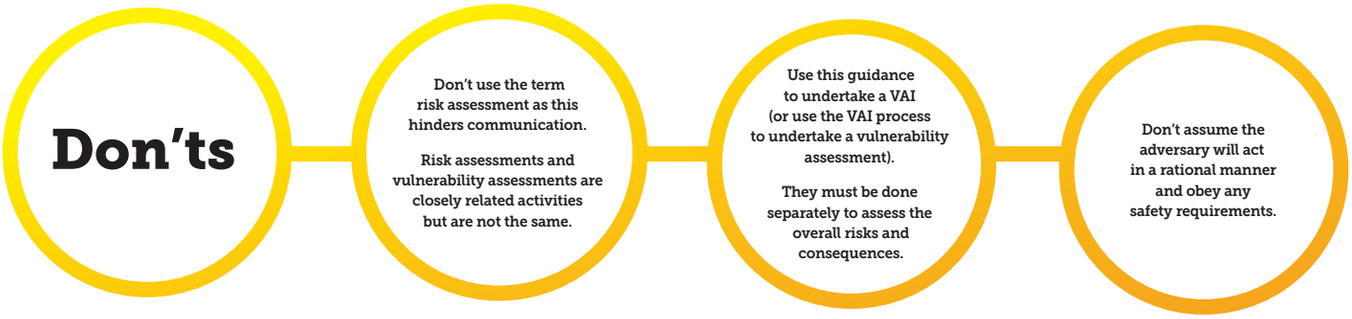
Any conclusions made on the performance of the PPS or recommendations for alterations are written into the final assessment report.

The key risk owner decides upon timescales and tolerability of risks for completion. If risks are allocated each should have a specific owner and be tracked for completion via an appropriate process.

Additionally, any lessons identified, or further conclusions should be recorded and made available for future reference.

## 2.7.

## Do's and Don'ts

# 3 References

[1] DSRL Vulnerability Assessment, PowerPoint, 2023, Dounreay.

[2] Frontiers, 'Advanced Modelling and Simulation of Nuclear Reactors' https://www.frontiersin.org/research-topics/36576/advanced-modeling-and-simulation-of-nuclear-reactors/magazine

3] Garcia, Mary Lynn (2005) 'Vulnerability Assessment of Physical Protection Systems', Sandia National Laboratories.

[4] International Atomic Energy Association (IAEA) (2011) 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities', (INFCIRC/225/Revision 5) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

[5] International Atomic Energy Association (IAEA) (2012) 'Identification of Vital Areas at Nuclear Facilities' https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf

[6] International Atomic Energy Association (IAEA) (2019) 'Nuclear Security Assessment Methodologies for Regulated Facilities' https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1868web.pdf

[7] International Atomic Energy Association (IAEA) (2022) 'Nuclear Energy Series No. NG-G-6.1, Guide to Knowledge Management Strategies and Approaches in Nuclear Energy Organisations and Facilities https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1957_web.pdf

[8] International Atomic Energy Association (IAEA) (2022) 'Nuclear Safety and Security Glossary' https://www-pub.iaea.org/MTCD/Publications/PDF/IAEA-NSS-GLOweb.pdf

[9] International Atomic Energy Association (IAEA) Collection (1995) 'Guidance for a Large Tabletop Exercise for a Nuclear Power Plant' https://inis.iaea.org/collection/NCLCollectionStore/_Public/26/059/26059981.pdf

[10] International Atomic Energy Association (IAEA) 'Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment' https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material-and-its-amendment

[11] Office for Nuclear Regulation (ONR), Security Assessment Principles (SyAPs) https://www.onr.org.uk/syaps/security-assessment-principles.pdf

[12] Office for Nuclear Regulation (ONR), Technical Assessment Guide (TAG) https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.4.pdf

[13] Office for Nuclear Regulation (ONR), 'ONR Strategy 2015-2020' https://www.onr.org.uk/media/yedn1n23/onr-strategy-2015-2020.pdf

[14] RAND Corporation, 'Wargaming', https://www.rand.org/topics/wargaming.html

[15] Rolls Royce Civil Nuclear UK (2020), 'Secure by Design – Guidance Document Principles and Methods'

[16] Security Protected Plant dentification (SPPI), PowerPoint, 2022, Technical Client Organisation.

[17] Security Vulnerability Assessment F-879 Issue 2, Magnox.

[18] Security Vulnerability Assessment: Process, Assessment Methods and Considerations Issue 1, 16 January 2023, National Nuclear Laboratories (NNL).

[19] Sellafield Ltd Practice, March 2021, Sellafield Ltd.

[20] IAEA Nuclear Assessment Methodologies for Regulated Facilities (IAEA TECDOC-1868)

[21] Vulnerability Assessment, PowerPoint, 13 June 2023, Rolls Royce SMR.

[22] World Institute for Nuclear Security (WINS), Webinar on Effective Vulnerability Assessment https://www.wins.org/wp-content/plugins/weventsv2/display_event.php?id=7800

## 3.1.

# Acronyms

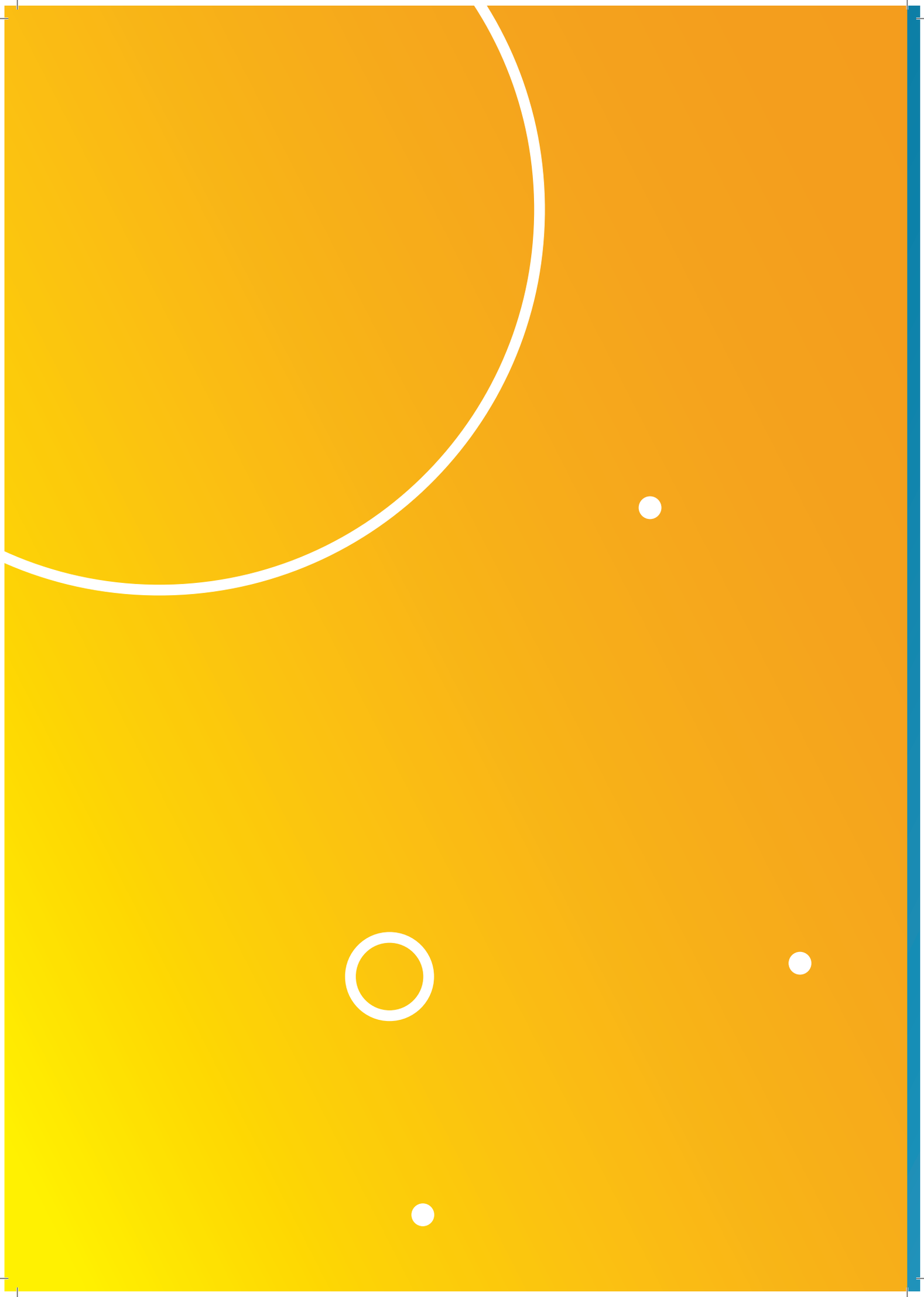
| Acronyms | Meaning |
|---|---|
| CPPNM | Convention on the Physical Protection of Nuclear Material' |
| DBT | Design Basis Threat |
| FSyP | Fundamental Security Principle |
| IC | Intelligent Client |
| IAEA | International Atomic Energy Agency |
| NPSA | National Protective Security Authority |
| NSAG | Nuclear Security Awareness Gude |
| NSSP | Nuclear Site Security Plan |
| ONR | Office for Nuclear Regulation |
| ORM | Other Radioactive Material |

| Acronyms | Meaning |
|---|---|
| PPS | Physical Protection System |
| SIS | Site Improvement Schedule |
| SME | Subject Matter Expert |
| SNI | Sensitive Nuclear Information |
| SQEP | Suitably Qualified and Experienced Person(s) |
| SyAPs | Security Assessment Principles |
| TAG | Technical Assessment Guide |
| URCs | Unacceptable Radiological Consequences |
| VAI | Vital Area Identification |
| WINS | World Institute for Nuclear Security |

## 3.2.

# Appendix 1:
# Capabilities and Limitations of methodologies and techniques.

| Method | Explanation | Capabilities | Limitations |
|---|---|---|---|
| **Wargaming** | Wargaming is an analytical tool that simulates aspects of warfare at the tactical, operational and strategic levels.<br>(RAND) | • Good for understanding system capabilities, and therefore vulnerabilities.<br>• Can integrate quantitative and qualitative data. | • Human decision making and imperfect data can affect the accuracy of outcomes. |
| **Tabletop** | A structured discussion based on a scenario or set of conditions for potential emergency response situations, among decision makers and responders.<br>They are a teaching and training aid as well as an opportunity to talk through plans and procedures or discuss new systems.<br>(Guidance for a Large Tabletop Exercise for a Nuclear Power Plant) | • Is a good way to familiarise key personnel with their roles and responsibilities.<br>• Simple and more economically friendly than expensive technologies.<br>• Helps with decision making and responses. | • Would not be a realistic test of guard (or other force) reaction. |
| **Force on Force** | A performance test of the physical protection system that uses designated trained personnel in the role of an adversary force to simulate an attack consistent with the threat or the DBT.<br>(IAEA – INFCIRC/225/Revision 5) | • Appropriate for considering the adequacy and concept of operations of an armed response team.<br>• Allow for the resting of the complete system using the full features of the security system.<br>• Good for identifying challenges in communications, interpretation of processes and procedures, human factor issues, and the training and site knowledge of the responders. | • Only relevant where actual force-on-force confrontation between an on-site response force and the adversaries is possible.<br>• Neutralisation is a measure of the outcome of a force-on-force confrontation, again this is only relevant to specific sites, not all.<br>• Less suitable for assessing proposed design for a facility.<br>• Resource intensive, require shadow forces to maintain site security arrangements and involve exercise controllers and umpires.<br>• Expensive and time consuming to plan and execute. |
| **Subject Matter Expert** | An individual who is in possession of comprehensive knowledge and experience in a given subject area.<br>(IAEA Nuclear Energy Series) | • Appropriate for assessing specific areas of concern. | • Lack of number and availability. |
| **Modelling and Simulation** | Tools that enable the reproduction of the behaviour of systems through computational models.<br>(Frontiers) | • Best suited for assessing the adequacy of the performance of the physical and technical components of the PPS.<br>• Statistical significance can be attributed to the results if multiple runs are performed.<br>• Can provide data on numerous variations/scenarios. | • More challenging to model threats which include an insider.<br>• Costly and time-consuming to build initial model. |



Department for Energy Security & Net Zero

NDA

ONR Office for Nuclear Regulation

Sellafield Ltd

AWE

NATIONAL NUCLEAR LABORATORY

NRS

NSSG