Office for Nuclear Regulation

ONR paper

Security modelling and simulation software to support risk decision-making

ONR paper

Security modelling and simulation software to support risk decision-making

April 2024

Executive summary

Within the security context, ONR's enabling approach to regulating the civil nuclear industry includes facilitating innovation to advance established security risk ways of working. The ONR innovation hub provides pathways for proposals to be considered by subject matter experts.

The routine use of security modelling and simulation (SyM&S) software to support physical protection systems evaluation and security risk decision making has been proposed. This paper sets out ONR's key regulatory considerations, informed by an expert panel discussion. These include the need for thorough validation and verification, use of suitably qualified and experienced persons (SQEP), data quality and information assurance, and an understanding of how the and long-term savings and value potential of adopting SyM&S software may offset initial cost and resource outlays.

The expert panel concluded that SyM&S software could help support risk decision-making, complementing traditional methodologies through dynamic appreciation of risk and providing suitable levels of complexity for rigorous testing of incident and emergency response plans. However, its potential contribution to decision-making will depend on user competence as well as the integrity of the software and contained data.

Acknowledgements

We gratefully acknowledge the contributions of the National Nuclear Laboratory, who provided the problem statement and technical advice to inform this guidance. We also thank the other members of the expert panel.

Glossary

Acronym	Description
CPPNM	Convention on the Physical Protection of Nuclear Materials
DBT	Design basis threat
IAEA	International Atomic Energy Agency
ISO	International Organization for Standardization
NISR	Nuclear Industries Security Regulations
NNL	National Nuclear Laboratory
NPSA	National Protective Security Authority
ONR	Office for Nuclear Regulation
ORM	Other radioactive material
PPS	Physical protection systems
RGP	Relevant good practice
SNI	Sensitive nuclear information
SQEP	Suitably qualified and experienced persons
SRM	Security risk management
SyAPs	Security assessment principles
SyM&S	Security modelling and simulation
TAG	Technical assessment guide
VA	Vulnerability assessment
VAI	Vital Area Identification

Contents

1. The ONR innovation hub

The Regulator's Code [1] states that regulators should carry out their activities in a way that supports those they regulate to both comply and grow. The ONR innovation hub provides a pathway for innovative ideas to be given an appropriate level of regulatory scrutiny. This facility is available to licensees, dutyholders or requesting parties and their supply chain (where they are sponsored by the licensee, dutyholder or requesting party). It is applicable, for example, where experience in the nuclear sector of a particular technology or practice is limited.

A dutyholder, leading on behalf of a wider benefit to the nuclear sector, has asked the innovation hub to consider the regulatory aspects for the use of security modelling and simulation (SyM&S) software in support of security risk decision-making, in particular for evaluating the performance of physical protection systems (PPS). An expert panel was convened to review the concept and provide input to aid ONR's judgement. Their discussions have helped inform the contents of this paper.

While this paper should not be regarded as a full examination of the concept, it nevertheless identifies key regulatory considerations and expectations. This review focuses on assessing the principles of using modelling and simulation for security decision-making, and is not a review of any specific product or tool, noting that commercially available products are already available. Consistent with ONR's enabling approach to regulation, this paper is intended to help dutyholders make informed decisions on the use of SyM&S software to support decision-making for physical security risk management.

ONR welcomes feedback on these key considerations to help us identify other areas to explore and continue our iterative learning process. Please email contact@onr.gov.uk if you have any comments or queries.

2. Security modelling and simulation (SyM&S) software tools

The use of modelling and simulation tools to support risk management and decision-making is not in itself an innovative concept. Such tools are used extensively to underpin nuclear safety assessments and the International Atomic Energy Agency (IAEA) recognises computer simulation as a security risk performance assurance mechanism [2]. Security technology such as this is used extensively in the US: it is endorsed by the Department of Defence for force-on-force modelling and used across the Department of Energy estate.

Within the UK civil nuclear industry, there is some acceptance of the merits of SyM&S software with a limited number of dutyholders having used such tools as a supplement to traditional PPS evaluation methodologies. There is however, no UK regulatory guidance specifically for the use of SyM&S software in the civil nuclear

context. Lack of clarity or misperception of regulatory expectations may present an unnecessary challenge to security decision-makers. The risk to users and regulators is a failure to realise potential benefits.

The intended output of this initial innovation hub engagement is the provision of a regulatory note on how SyM&S software may be used to provide evidence that supports claims and arguments about PPS adequacy to the satisfaction of both the dutyholder and regulator.

3. Problem statement

National Nuclear Laboratory (NNL), the lead dutyholder acting as proponent, provided the following problem statement for review.

Security modelling and simulation software to support security risk decision-making

Request: Dutyholders will look to use SyM&S software for performance evaluation of a PPS to provide an objective, quantitative physical security risk assessment for civil nuclear sites, particularly those which carry the greatest consequence for theft or sabotage.

Key potential benefits: A common and repeatable approach to provide quantitative and statistically relevant assessment of PPS performance, increasing transparency and enabling better and more comprehensive security risk management (SRM) and decision-making.

Perceived shortfalls: Existing methodologies do not, arguably, reflect the broad range of factors that can influence adversary and response patterns of behaviour. Nor do they easily allow for the running of multiple adversary pathway scenarios to facilitate objective, time and cost efficient consideration of PPS performance including upgrade and reduction permutations in existing measures.

Proposed solution: SyM&S software allows for a standardised, objective and data rich approach to SRM, providing confidence to the dutyholder and assurance to the regulator through the use of statistical evidence as a decision support tool with regard to changes to the PPS environment (e.g. UK Design Basis Threat (DBT)), threat level, response level), providing for a standardised process which enables the isolation of specific PPS performance aspects through variation analysis. A modelling and simulation approach can remove some of the subjectivity and bias associated with approaches based purely upon Subject Matter Expertise, and provide the transparency and evidence upon which to underpin and justify decisions. In so doing, this will potentially enable more effective and robust decision-making, and more effective interaction between dutyholder and ONR.

4. Expert panel

The expert panel comprised subject matter experts from within ONR and the dutyholder community. This is consistent with ONR's commitment to providing an environment that will foster creative thinking and solutions by focusing practices and behaviours on principles which include:

- Being enabling, accessible, open-minded and providing stimulating challenge;
- Working collaboratively; and
- Being adaptable and responsive to our environment and the needs of others.

5. Scope

The following assumptions informed the expert panel discussions and subsequent scope of this report:

- The UK DBT is the framework threat document for scenario modelling and adversary pathway simulations which will be used to inform vulnerability assessments (VA) [3];
- The UK DBT has a probability factor of 1, that is, an attack will happen;
- The proposer's assertion is that use of SyM&S software provides a mechanism to quantify security performance, which is key to underpinning claims, arguments and evidence in regulatory submissions as well as enabling risk management decision-making; and
- Use of SyM&S software for vital area identification (VAI) is beyond the scope of this report. There is existing relevant guidance within ONR TAG 6.2 [4].

6. Responsibilities

As a signatory to the IAEA Convention on the Physical Protection of Nuclear Materials (CPPNM) [5], the UK recognises its obligations to protect civil nuclear facilities, nuclear materials and sensitive nuclear information (SNI) when in use, during storage and in transit.

The Nuclear Industries Security Regulations (NISR) 2003 [6] identifies responsible persons (i.e., the dutyholder) and requires them to implement arrangements for the protection of nuclear material, other radioactive material (ORM), associated facilities and SNI. This includes the requirement for an approved security plan demonstrating how security outcomes are achieved. As reflected in its Security Assessment Principles (SyAPs) [7] and consistent with an outcome-based philosophy, ONR

expects security plans to reflect how PPS adequacy has been validated through the performance-based vulnerability assessments using one or more proven methodologies. Computer-based modelling and simulation is one such methodology, which the dutyholder may choose to support claims arguments and demonstrate PPS efficacy.

7. Regulatory observations

7.1. Security risk management

- Any software solution intended to support risk decision-making should undergo thorough validation and verification covering the underpinning software code and its ability to repeatably, reliably and consistently perform its calculations and analysis. This should be consistent with ONR TAG GD-042 [8].

- Consistent with the use of other modelling and software-based analysis methods, the dutyholder should ensure requirements governing the use of SyM&S software are included in site SRM framework documents and approved security plans and made available for inspection. Levels of complexity associated with operating instructions and other guidance should not negatively impact their use.

- SyM&S software is one of a number of tools and approaches to aid effective SRM. It will not be a one-size-fits-all solution, but could help inform effective decision-making through quantifying risks more objectively than some other methods. Decisions on the choice and use of technical approaches should be made by suitably qualified and experienced persons (SQEP) and should be consistent with key themes in security decision-making [9].

- The subjectivity of SQEP security appointment holders should be carefully considered as part of the SRM process.

7.2. Data validation

- Modelling and simulation methods operate using a reference library of performance measures, for example, effectiveness of detection, delay provided by barriers, or speed of a responder over different surfaces. These performance measures are consistent with those currently being used for other security and vulnerability assessment activities. Most software tools are equipped with a pre-populated and accurate but unclassified performance library. A central repository could be beneficial through supporting consistency across the sector.

- Any dataset should meet international and national standards for performance evaluation; for example, the equipment cited in the Catalogue

of Security Equipment [10] has met National Protective Security Authority (NPSA) security performance standards. This is consistent with the requirements and expectations specified within ONR TAG 6.4 [3].

- Obsolescence should be addressed as the software and performance data changes.
- Proof of concept exercises (or similar) may provide evidence of data validity.

7.3. Information assurance

- To ensure compliance with the NISR 2003, information management measures should align with relevant good practice (RGP) such as the International Organisation for Standardisation (ISO) 27000 series. This includes classification, information ownership, information guardianship (especially pertinent if there is to be a central repository), information sharing, use of cloud-based solutions and information assurance counter compromise measures.
- When aggregating data, dutyholders should consider potential risks as well as how its availability may be affected. For example, aggregation may increase the classification of the information held and so require additional information assurance controls. There may also be security clearance implications for those with regular access to the software or its outputs.

7.4. Enduring commitments

- There should be an appreciation of the financial liabilities associated with accredited SyM&S software. To mitigate unanticipated and sudden loss of a key capability once installed, security leaders are fundamental in promoting understanding and buy-in at senior levels.
- Potential savings should be balanced against enduring costs, including for software licences, software developer support, maintenance and training. These should be clearly articulated to the leadership and security budget holder, and made available for inspection.
- For low hazard and risk sites, it may be difficult to justify the cost of SyM&S software where traditional methodologies can provide adequate outcomes.

8. Conclusion

The expert panel discussion saw a consensus supporting the use of SyM&S software for PPS evaluation. It was noted that such tools help focus attention on areas where the risk gap is greatest, which aligns with the graded approach.

Where risks to nuclear material and SNI are greatest, complementing traditional decision support methodologies with the use of SyM&S software should facilitate dynamic appreciation of the security risks. SyM&S software should be considered to be an optional enabler and provider of suitable levels of complexity for rigorous testing of incident and emergency response plans.

It is important to understand that not all SyM&S software is equal. Notwithstanding user competence, its potential contribution to qualitative and quantitative decision-making will depend on the integrity of the software and contained data.

References

[1] The Regulators' Code, 2014.

[2] IAEA, Nuclear Security Assessment Methodologies for Regulated Facilities, 2019.

[3] ONR, CNS-TAST-GD-6.4 – Vulnerability Assessments, 2022.

[4] ONR, CNS-TAST-GD-6.2 – Categorisation for Sabotage, 2023.

[5] IAEA, The Convention on the Physical Protection of Nuclear Material, 1980.

[6] The Nuclear Industries Security Regulations, 2003.

[7] ONR, Security Assessment Principles for the Civil Nuclear Industry, 2022.

[8] ONR, NS-TAST-GD-042 – Validation of Computer Codes and Calculation Methods, 2023.

[9] ONR, CNSS-TAST-GD-1.3 – Security Decision Making, 2020.

[10] NPSA, Catalogue of Security Equipment, [Online]. Available: https://www.npsa.gov.uk/cse-categories.