# Modelling and Simulation for Nuclear Security Planning and Assessment

# A WINS International Best Practice Guide

## WHY YOU SHOULD READ THIS GUIDE

This WINS International Best Practice Guide introduces processes and practices to help your organisation make the best use of modelling and simulation for nuclear security planning and assessment. Computer modelling and simulation (M&S) is a key methodology in assessing security at nuclear facilities. M&S is much less costly than live exercises, is more informative and defensible than purely probabilistic assessment, and can encompass a much broader array of threat and configuration scenarios. Recently, M&S is seeing increasing use in the planning and design phases of security enhancements, as well as predictive analysis for previously unplanned or unforeseen events.

M&S can be a central component in a systems approach to nuclear security planning and analysis. Existing applications include:

- Evaluation of safety and security of initial facility designs
- Vulnerability analysis for an existing facility
- Integrated safeguards and security management (ISSM)
- Cost benefit analysis of security enhancements
- Predictive analysis in the face of new threat scenarios
- Security planning during the staged implementation of security enhancements
- Integrated assault, cyber, and insider threat analysis
- Adaptive adversaries

A sound approach to modelling and simulation for nuclear security planning and assessment is more than just cost-effective: it is a proactive step in ensuring the security of your facility and the safety of the public.

### *About the Appendices*

Appendices A and B provide a series of questions and levels of organisational competencies relating to modelling and simulation for nuclear security planning and assessment that will enable you to see how well your organisation is doing and be able to benchmark its performance. Results of this benchmarking process may indicate possible gaps in your security infrastructure and could provide you with a starting point for improving the situation.

### *About the Preparation of the Guide*

In preparing this Guide, we have taken note of the real-life experiences of nuclear security professionals who have firsthand experience of using modelling and simulation systems, and hope to supplement this Guide with a specialist workshop in 2012.

*We Welcome Your Comments*

We plan to update the information in this Guide frequently to reflect best practices and new ideas. Therefore, we ask that you read it carefully and then let us know how to improve it. If you need help or assistance with any aspect of this Guide, please email us. You can also contact us via the WINS membership portal.

Dr Roger Howsley
Executive Director
[Insert Month, Year of publication]

Revision 1.0

**WINS Contact Information**

World Institute for Nuclear Security
Graben 19
AT-1010 Vienna
Austria
Email: info@wins.org
Fax: +43 (0) 1230 606089
Phone: +43 (0) 1230 606088
www.wins.org

# WHAT IS MEANT BY MODELLING AND SIMULATION FOR NUCLEAR SECURITY PLANNING AND ASSESSMENT?

Computer modelling and simulation (M&S) has been an important methodology in assessing security at nuclear facilities for a number of years. M&S is much less costly than live exercises and can encompass a much broader array of threat scenarios. More recently, M&S is seeing increasing use in the planning and design phases of security enhancements, as well as predictive analysis of scheduled changes. In M&S, a number of common terms are used with very specific meanings, so you may find the following definitions useful as you read this guide.

**Definitions**

A **design basis threat** (DBT) is a threat or attack scenario against which the nuclear security of a facility is officially evaluated. Some organisations may designate multiple DBTs, such as an open assault DBT versus a theft DBT. The DBT is usually used as the basis for evaluating proposed changes in the security configuration.

A **model** is a representation of reality. In this document, a model is an abstract numerical representation of reality that is programmed into a computer. Parts of the programme may be intended to represent buildings, in a simplified way, and parts may represent humans, in even more simplified ways. Well-understand technologies or physical processes (e.g. nuclear fission) may behave in predictable ways very similar to the computer model for them. The extensive use of modelling and simulation in nuclear safety reflects this. Nuclear security, however, is more concerned with the behaviours of humans, which can only be represented in a general way, allowing for wide variations across individuals, and varying at different times under different circumstances.

**Simulation** in this document refers to using a computer to simulate the interactions within – and outcomes from – a computer model. That is, it is the use of a computer model to simulate reality. Typically, though not necessarily, the dynamics of the system are encoded in the model, and simulation is simply a representation of the advance of time and the changes in the model that result. Simulation is often used as a design tool.

A **simulator** is a computer model in which some parts of the model are represented by real objects, some are represented strictly within the computer, and one or more objects in the model are replaced by real human beings. When this model is subject to the simulation of advancing time, this is often called a man-in-the-loop simulation. A flight simulator, for example, presents the cockpit instruments and controls as real devices, possibly simulates the cockpit attitude, and displays a computer representation of the surroundings on screens that simulate the windows. The data shown on the instruments, the feedback to the controls, and the behaviours of other pilots, flight controllers, birds, and the weather are all represented numerically within the computer. A simulator is a training tool. This document does not cover simulators; that topic will be taken up in another guide.

**Modelling and simulation** is the process of producing a computer representation of some small part of reality and running simulations to represent outcomes from the objects and behaviours that are built into the model. To be useful, the amount of detail in the model must be sufficient to reproduce plausible behaviours and outcomes. Because many aspects of reality may be unknown or be poorly understood, the model may allow for a wide distribution of behaviours and outcomes, making it necessary to run large numbers of simulations to understand both the average outcomes and the extreme outcomes. Based on the statistics of those outcomes, an analyst is able to report a degree of confidence in the outcome, given the accuracy of the model. This latter topic, model accuracy (sometimes called *validity* or

*fidelity*), may be the topic of a complete study in itself before the results of simulations are accorded any degree of significance.

**Fidelity** refers to how closely a computer model represents reality. A computer model of a room that includes carpet, furniture, wall coverings, lights, switches, and electrical outlets is said to have high fidelity.

**Abstraction** is the process of simplifying a computer model so that it as simple as possible whilst its behaviour in simulation is still accurate. If a room functions solely to provide passage between one place and another, the details of carpet, furniture, wall coverings, lights, switches, and electrical outlets are irrelevant. In this sense, abstraction is the opposite of fidelity.

**Granularity** is for the passage of time what abstraction is for model details. For example, a simulation of the change of seasons requires only very coarse granularity, while a simulation of the trajectory of a bullet requires very fine granularity.

## HOW DO ORGANISATIONS USE MODELLING AND SIMULATION FOR NUCLEAR SECURITY PLANNING AND ASSESSMENT?

Typical uses of M&S in nuclear security include vulnerability or risk assessment, force allocation planning, cost/benefit analysis of security enhancements, and predictive analysis. In any of these cases, security systems may be assessed by simulating multiple threats, such as

- The design basis threat (DBT)
- Worst case scenarios, such as overwhelming force
- Theft
- Sabotage
- Insider
- Exploit of a natural disaster

The simulations may also include multiple security configurations, for example

- Normal daytime operations
- Normal night-time operations
- Material transport operations
- Maintenance operations

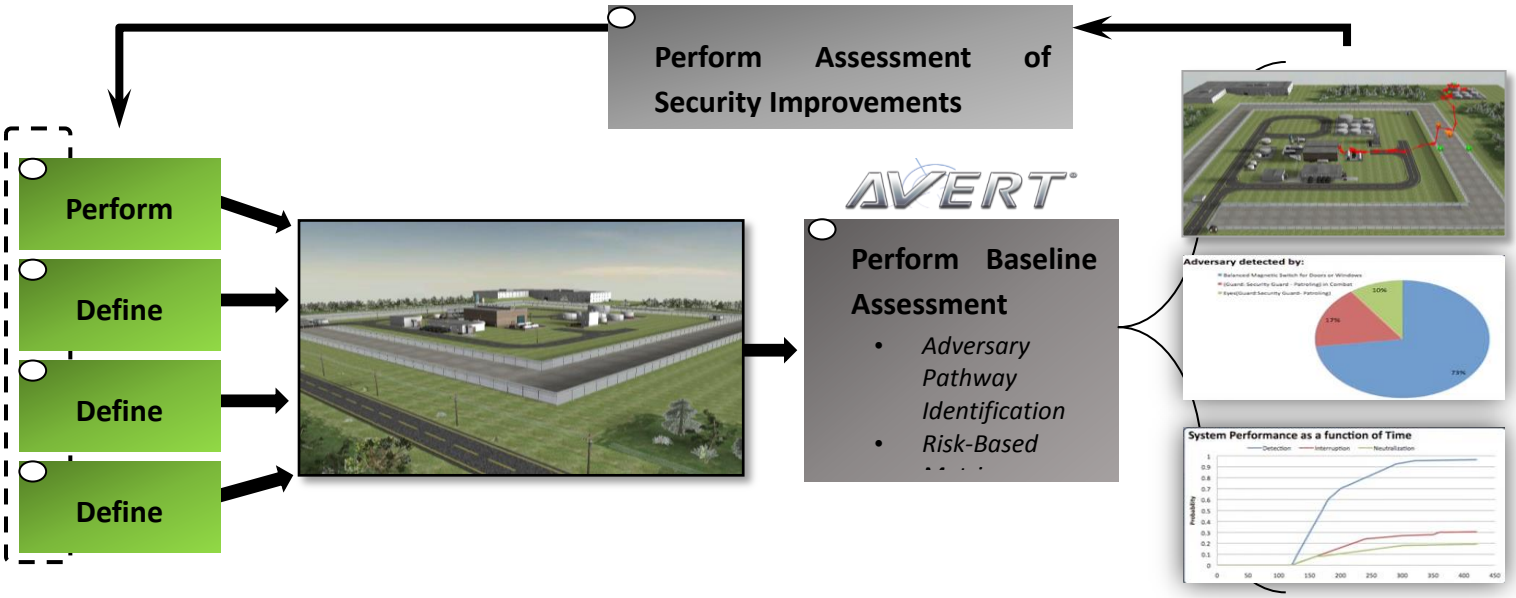
Often, the result of simulation is reported as either a probability of system effectiveness or as a probability of failure (threat success). The probability of effectiveness is usually one minus the probability of threat success, and either of these may be stated as a percentage. Which measure is used depends on the goal of simulation. Some example goals are listed in the table below, along with the simulation products and how they're used.

Modelling and Simulation Goals and Simulation Products

| Goal | Simulation Products and Their Use |
|---|---|
| **Vulnerability Analysis** | The goal of vulnerability analysis is to identify vulnerabilities in a nuclear security system. M&S will frequently identify multiple vulnerabilities, and either effectiveness or failure may be used to priority-rank those vulnerabilities. |

| | |
|---|---|
| **Risk Assessment** | Risk is the probability of an attempt, times the probability of its success, times the impact of the successful attempt. Often it is the goal of risk assessment to find multiple vulnerabilities (like vulnerability analysis), to assign a probability of each occurring, and then to associate an impact with each vulnerability. For example, consider an attempted theft of a small quantity of low-level waste:<br><br>• Low attempt probability<br>• Low success probability<br>• Medium-high impact<br><br>Compare this with the attempted destruction of a waste-containment facility<br><br>• Lower attempt probability<br>• Lower success probability<br>• Much higher impact<br><br>Modelling and simulation provides a framework in which to document component probabilities and assess outcomes for probabilistic risk assessment (PRA). |
| **Force Allocation Planning** | The goal of force allocation planning may be to allocate current personnel, or to plan for a change in the number or type of personnel. For example, as a government facility makes the transition to privately operated, soldiers are replaced by civilian security personnel. M&S may also be used to evaluate multiple ways to group security staff for patrols. |
| **Response Planning** | The goal of response planning is to anticipate different kinds of threat scenarios and plan the appropriate response. For example, an identified hostile assault may call for activation of automated security barriers and concentrated deployment of security personnel, while the response to a natural disaster would be quite different. |
| **Evaluation of Proposed Security Enhancements** | M&S is often used to evaluate competing costly security enhancements. The benefit versus cost of proposed enhancements such as a fortified perimeter, an automated surveillance system, or increased staffing may be complicated by unforeseen conflicts (or synergies) with existing security features. |
| **Predictive Analysis** | M&S can be used to assess vulnerability to a previously unforeseen threat in much less time than it would take to organise a live exercise. |

Many issues discussed in this Guide are addressed by tools designed specifically for modelling and simulation for nuclear security planning and assessment. These tools can make the M&S process more efficient, consistent, and cost-effective. Some tools include authoritative data sets for components such as detection, barrier and defensive technologies. The availability and acceptance of tools for modelling and simulation for nuclear security planning and assessment varies across industries and across jurisdictions. In 2009, for example, the U.S. Department of Homeland Security approved the AVERT ("Automated Vulnerability Evaluation for Risks of Terrorism") software product as the first tool for modelling and simulation for nuclear security planning and assessment, designating it an Approved Product for Homeland Security. Regulators, nuclear safety organisations or other industry groups in your industry and jurisdiction may be able to recommend appropriate software tools. The diagram below illustrates a typical ongoing modelling and simulation project using the AVERT software tool.




Some readers may be familiar with the use of modelling and simulation in the nuclear safety arena. Nuclear safety covers a wide range of postulated nuclear accidents including those caused by system or structural failures, natural phenomena and intentional actions. These are computer models and simulations of the physics of materials, nuclear and non-nuclear. This kind of modelling and simulation is quite mature, and is used to analyze design-basis accidents like pipe ruptures that could occur operationally, and to simulate beyond-design-basis accidents like natural disasters that result in a core meltdown and radiation dispersion. Modelling and simulation for nuclear security is also concerned with the responses of mechanical and electronic systems, but is primarily focused on the behaviours of hostile actors and on the defensive personnel assigned to thwart them. This is a relatively new and maturing application of modelling and simulation.

## SOME GUIDING PRINCIPLES IN MODELLING AND SIMULATION

The only thing that is exactly the same as reality is reality itself. Computer modellers face a constant trade-off between fidelity and abstraction in their models. Sometimes, a model of the same thing may have high fidelity for one purpose, and low fidelity for another. For example, a parked car may serve as something to hide behind in one simulation, while it may be used to escape in another. A low-fidelity model is easier and faster to design and implement. More importantly, in most cases, a low-fidelity model takes much less time and effort to validate and verify, much less computing power and time to simulate, and much less time and effort to analyse the results. These concepts are described in the following table.

**Guiding** Principles **in Modelling**

| Principle | Application to Modelling |
|---|---|
| **Abstraction and simplification** | Building a model you can use and understand. Some of the ways in which a model can be abstracted or simplified include:<br><br>• Variable elimination – don't include irrelevant people or equipment |

| | |
|---|---|
| | • Enumeration – either open or closed, not everything in between<br>• Reduction – don't model an entire campus if only one building matters<br>• Non-determinism – stochastic simulations rather than every possibility<br>• Grouping – combine players, components, or actions when relevant<br>• Decomposition – model areas separately before combining them |
| **Validation** | These are ways to make sure you have the right model to answer the questions being asked:<br><br>• Site walk-down – visit the physical site early and often<br>• Peer review - get more, fresh eyes on the model<br>• Domain expert review – make sure abstractions make sense<br>• Error tracking and resolution – write down problems and follow up<br><br>These steps may be repeated many times in the course of modelling project. |
| **Verification** | These are ways to make sure your model does what you designed it to do, and that it stays that way. Uses the same techniques as validation, but may require simulation results to be sure that the model behaves consistently after changes. This is typically done using regression testing. |
| **Version Control** | Keeping a recoverable record of how a model got to be the way it is. The best way to do this is to use version control software. The things you will need to keep under version control include:<br><br>• Models<br>• Supporting documents (CAD data, GIS data, drawings, etc.) and assumptions documents (what was abstracted or simplified, why, and how)<br>• Reported errors and how they were resolved<br><br>Develop and use a process document as a best-practices template for configuration control of models and scenarios |

Guiding Principles in Simulation

| Principle | Application to Simulation |
|---|---|
| **Goal Orientation** | The goal drives simulation choices like granularity, number of alternative scenarios, and how many stochastic samples to run. There are many possible goals, but common ones include:<br><br>• Threat assessment (what are a site's vulnerabilities?)<br>• Risk assessment (how do equipment or personnel trade-offs affect risk?)<br>• Target ID (given a specific threat scenario, what is the likely target?)<br>• Evaluation of countermeasures (which technology works best?)<br>• What-if simulations (what if there's a blackout during a storm?) |

| | |
|---|---|
| **Controlled Experimentation** | A systematic approach to understanding how changes in simulation affect the results<br><br>• Turn one dial at a time – vary just one thing, then another<br>• Look for convergence – don't trust the results from a single simulation<br>• Reality-check results – understand both unexpected and expected<br>• Document, document, document – write everything down |
| **Validation** | Review the goals and the simulation parameters regularly to be sure that the simulation is answering the question being asked. This may involve some of the procedures already in place for model validation, including:<br><br>• Peer review – verify that simulation choices answer the question<br>• Domain expert review – verify that simulation choices are realistic<br>• Error tracking and resolution – record problems and their resolutions |
| **Verification** | Make sure that simulation results remain consistent. This can involve some of the same procedures as validation, with a focus on results rather than goals and assumptions. For example:<br><br>• Peer review – verify that results continue to answer the question<br>• Domain-expert review – verify that results are still realistic<br>• Formal Procedures – use spreadsheets, statistical analysis, other tools<br>• Error tracking and resolution – record problems and their resolutions |
| **Documentation** | Keeping track of what has and has not been explored in simulation<br><br>• Keep a record of all simulation parameters<br>• Verify one thing at a time<br>• Record Everything.<br>• Assure valid comparisons – don't compare apples to oranges.<br>• Be sure to record ideas for further investigation: what you didn't do but think you should have, or which might be interesting. Those insights probably won't come back later.<br>• Develop and use a process document as a best-practices template for configuration control of models and scenarios |

## PROCESS CONTROLS

Some organisations will have formal processes like ISO 9000 in place, while others will have to develop their own. In either case, it is important to have documents that define your processes and, importantly, how your process can change over time, or to adapt to unusual circumstances.

The following table shows a sample outline of a Modelling and Simulation Process Document. This would be a document to describe how modelling and simulation projects will be run. It typically references a number of other documents, such as a Statement of Work, Process Management Plan, and possibly a

number of industry-wide, organisation-wide, or facility-wide process documents. This will be a living document – it will be refined, improved, and otherwise changed regularly.

Sample Outline of a Modelling and Simulation Process Document

| Section | Description |
|---|---|
| **Introduction** | Places this document in the overall process, gives an overview of the document, identifies the intended audience, and defines the document's scope. |
| **Project Planning and Organisation** | Defines the documents to be associated with each project. Typically these will include:<br>• Statement of Work<br>• Project Management Plan<br>• Model Specification<br>• Supplier Agreement<br>• Configuration Management Plan<br>• Security Plan<br>• Quality Assurance Plan<br>• Project Organisation<br>• Project Controls<br>• Documentation Plan |
| **Project Management** | Defines the role of Project Manager and sets out the phases of the project, which typically include a Planning Phase, a Modelling Phase, and a Delivery Phase. |
| **Configuration Management** | Defines the roles and responsibilities of the committee responsible for overseeing the project and, importantly, responsible for approving any changes in the project documents listed in the Project Planning and Organisation section. This committee, often called a Change Control Board, is also responsible for managing risks to the project associated with changes and uncertainties. |
| **Data Management** | The procedures for acquiring data, for controlling data, to justify or otherwise document estimations and approximations, and for periodic reviews of data used for appropriateness and consistency. Modelling and simulation for nuclear security planning and assessment usually involves large amounts of official data as well as data that must be estimated or otherwise approximated. Often the official data is proprietary or otherwise sensitive, which usually requires that the origins be well documented and the use be strictly controlled, in accordance with the Security Plan referenced in Project Planning and Organisation. |
| **Model Development and Simulation Testing** | The procedures for developing a computer model and the simulations used for testing it are outlined. All assumptions made during the modelling must be documented and related to the data documentation developed in the Data Management activity. Model testing and validation are often done using both desk checks and test simulations. |
| **Simulation Results** | The procedures for running simulations are outlined along with the kinds of results to be collected and how and where they will be kept. |
| **Delivery and Maintenance** | The procedures and documentation for delivering results to the client, including outlines of standard reports and procedures for refining results and resolving |

| | |
|---|---|
| | problems. |
| **Process Improvement** | The procedures, documentation, roles and responsibilities for incorporating lessons learned from one project into future projects. |
| **Bibliography** | A list of documents referenced in this one, including other process documentation, industry-standard documents, and so on. |
| **Appendices** | Sample forms and reports. |

## GETTING STARTED WITH MODELLING AND SIMULATION FOR NUCLEAR SECURITY PLANNING AND ASSESSMENT

Given the growing interest in using modelling and simulation for nuclear security planning and assessment, we have outlined in the table below a few best-practice considerations you may wish to take into account if you are new to the topic.

Ten Steps in Undertaking Modelling and Simulation for Nuclear Security Planning and Assessment

| Section | Description |
|---|---|
| **1. Suppliers** | The most common route is to contract the services of experts in modelling and simulation for nuclear security. There aren't many, and most of them are also suppliers of software tools for modelling and simulation in nuclear security. Some users develop in-house expertise to support the modelling and simulation projects begun as service engagements, taking advantage of training provided by the service provider. An increasing use of suppliers is as a resource to initiate a modelling and simulation process for your organisation. Suppliers can provide training on tools and techniques, allowing your organisation to see immediate benefit while rapidly developing internal capabilities. |
| **2. Cost** | A typical initial engagement includes creation of the initial computer model, an assessment of an identified threat scenario via simulation, and analysis of the results. Costs and timescales for the study might range from €25k and three weeks for a small, non-secure facility to upwards of €250k and two months for a campus of buildings with extensive security features. Typically, the original model is reusable, significantly reducing the cost of subsequent engagements. |
| **3. Benefits** | The cost of a single live exercise can be greater than the cost of developing a computer model and running multiple simulations for assessment and the flexibility of modelling and simulation makes it possible to explore options. Additionally, modelling and simulation for nuclear security planning can lead to important cost savings in the implementation of security programmes, helping make security more effective and efficient (see Lessons Learned, below). |
| **4. Drawbacks** | Perhaps the biggest drawback to modelling and simulation is that it requires extensive, high-quality data for the results to be valid. Another difficulty arises in reporting results: a simple success or failure from a live exercise is easy to communicate and understand, while a distribution of probabilities for |

| | |
|---|---|
| | outcomes – typical output from modelling and simulation – is difficult. Expert analysis is important. To overcome these drawbacks, tools and/or suppliers can be chosen where existing industry data are immediately available and standard output emphasize good risk communication. |
| **5. Prerequisites** | Some modelling and simulation projects begin with a satellite photo of the site, a few blueprint drawings of the interior, and many hours of building up a computer model from this information. Most sites, however, begin with digital maps (GIS data) and digital engineering drawings (CAD data). The availability of GIS and CAD data not only speeds up the model-building process, it also improves the fidelity and can help ensure that the model reflects current information. With the rapid growth of online sources of geo-spatial data, the availability of high-quality data will continue to improve. |
| **6. Security** | Classification considerations vary by jurisdiction but, in general, in increasing order of restriction:<br>a) The layout of the physical site is unclassified<br>b) Details such as floor plans are controlled<br>c) Security features and personnel deployments are classified<br>d) Simulation results are highly classified<br>Given that the layout of the physical site can be obtained online from satellite photos, it is usually possible to complete a majority of the computer model in an unrestricted environment. Depending on your jurisdiction, your supplier may have personnel with security clearances. Otherwise, your supplier can provide training for your cleared personnel |
| **7. Involving the Regulator** | It is important to start this dialog with the regulator early. Often, it is sufficient to demonstrate that a simulation of the design-basis threat shows parallels to already accepted results. The sophistication of regulators continues to improve as they look to incorporate risk-informed regulations, an area in which modeling and simulation excels. |
| **8. Including Multiple Stakeholders** | Modelling and simulation can be an effective results-oriented tool to get buy-in from disparate stakeholders to agree on a path forward. The CEO, plant operations, security personnel and safety managers can all provide input to the model and share in the results. |
| **9. Lessons Learned** | One example of the effective use of M&S was reported at the Y-12 facility belonging to the US Department of Energy. Security planners estimated that, by using modelling and simulation for nuclear security planning, they reduced security costs by up to US$5 million. You can read about their experience at<br>http://www.y12.doe.gov/news/report/toc.php?vn=3_4&xml=p10 |
| **10. When to Start** | The use of modelling and simulation for nuclear security has expanded in recent years and this trend is expected to continue. The sooner you get going, the sooner you begin realizing benefits and cost savings. |

# APPENDIX A

## QUESTIONS TO ASSESS PERSONAL CONTRIBUTIONS TO MODELLING AND SIMULATION FOR NUCLEAR SECURITY PLANNING AND ASSESSMENT

Appendix A contains a series of questions that members of an organisation can use to evaluate their approach to modelling and simulation for nuclear security planning and assessment. The questions also make excellent prompts for generating discussion. Such a process helps individuals at all levels of an organisation reflect critically on their personal involvement. It also helps them understand how they can contribute personally to enhancing modelling and simulation for nuclear security planning and assessment within their organisation.

## QUESTIONS FOR FACILITY OWNERS/DIRECTORS

| | |
|---|---|
| Is modelling and simulation approved for nuclear security planning and assessment by your industry's regulators, or are you currently advocating that it be? | ☐ Yes<br>☐ No |
| Does your industry sponsor standards committees or other forums for setting standards for the use of modelling and simulation for nuclear security planning and assessment, or are you currently advocating that it do so? | ☐ Yes<br>☐ No |
| Do you participate in industry-wide standards activities for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you encourage managers to support the adoption and dissemination of best practices for your modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you provide a positive environment for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |

## QUESTIONS FOR FACILITY MANAGERS

| | |
|---|---|
| Do you understand your industry's use and acceptance of modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you require the development, documentation and deployment of best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you perform regular reviews of practices and standards for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you encourage continuous improvement in practices and standards for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Are you incorporating modelling and simulation into all aspects of nuclear security planning and assessment (e.g. design, staffing and acquisition)? | ☐ Yes<br>☐ No |
| Do you provide a positive environment for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you have open and direct communication between all stakeholders in modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |

## QUESTIONS FOR NUCLEAR SECURITY MANAGERS

| | |
|---|---|
| Do you understand your facility's use and acceptance of modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you require the development, documentation and deployment of best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Are you familiar with your facility's best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you perform regular reviews of practices and standards for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you encourage continuous improvement in practices and standards for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you have open and direct communication between security operations and the modelling and simulation team(s)? | ☐ Yes<br>☐ No |

## QUESTIONS FOR MODELLING AND SIMULATION MANAGERS

| | |
|---|---|
| Do you understand your facility's use and acceptance of modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you drive the development, documentation and deployment of best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you have thorough knowledge of your facility's best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you drive continuous improvement in practices and standards for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you require that all modelling and simulation practitioners read and frequently review your facility's best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you encourage your modelling and simulation practitioners to participate in continuous improvement activities? | ☐ Yes<br>☐ No |
| Do you ensure use of best practices in project launch meetings, regular status meetings, and in project conclusion meetings? | ☐ Yes<br>☐ No |
| Is participation in best practices and continuous improvement an integral responsibility for your practitioners as opposed to an "added on" activity? | ☐ Yes<br>☐ No |
| Do you regularly review and improve your own practices? | ☐ Yes<br>☐ No |

## QUESTIONS FOR MODELLING AND SIMULATION PRACTITIONERS

| | |
|---|---|
| Do you understand your facility's use and acceptance of modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you participate in the development, documentation and deployment of best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you read, review, and implement your facility's best practices for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you participate in continuous improvement in practices and standards for modelling and simulation for nuclear security planning and assessment? | ☐ Yes<br>☐ No |
| Do you share your experiences and insights in project launch meetings, regular status meetings, and in project conclusion meetings? | ☐ Yes<br>☐ No |
| Is participation in best practices and continuous improvement something you treat as a core responsibility in your modelling and simulation work? | ☐ Yes<br>☐ No |
| Do you document every modelling assumption? | ☐ Yes<br>☐ No |
| Do you document every simulation parameter? | ☐ Yes<br>☐ No |
| Do you take ownership for the quality of your modelling and simulation products? | ☐ Yes<br>☐ No |

# APPENDIX B

## DEFINING DIFFERENT LEVELS OF ORGANISATIONAL SUCCESS

**The following chart presents five stages of maturity in modelling and simulation for nuclear security planning and assessment, each with its own set of characteristics. By identifying where your organisation falls on this chart, you will know what you need to do to move to the next stage to improve your ability to accredit your use of modelling and simulation for nuclear security planning and assessment.**

| LEVEL | CHARACTERISTICS |
|---|---|
| 1 | Level 1 describes an organisation that is not currently using modelling and simulation for nuclear security planning and assessment. It is relying on security technologies and practices that were tested in a single live exercise run a year ago against an outdated design-basis threat. |
| 2 | Level 2 describes an organisation that is in discussion with experts in modelling and simulation for nuclear security assessment. Its security personnel have met with the security staff from a facility that uses modelling and simulation for nuclear security assessment routinely. The security staff is collecting the data needed for a modelling and simulation assessment. |
| 3 | Level 3 describes an organisation that has an on-going project using modelling and simulation for nuclear security assessment. Security assessment personnel have had training on modelling and simulation for nuclear security assessment. Security planning personnel are observing the assessment and are taking the training, as well, in anticipation of upcoming security planning. |
| 4 | Level 4 describes an organisation that has completed one or more projects using modelling and simulation for nuclear security assessment. They have begun a project using modelling and simulation for nuclear security planning. Assessment and planning personnel have completed modelling and simulation training and have begun to institute best practices like document and version control and formal validation and verification. |

| | |
|---|---|
| 5 | Level 5 describes and organisation that is actively using modelling and simulation for nuclear security planning and assessment. In-house modelling and simulation personnel have instituted best practices like document and version control and formal validation and verification. All personnel involved in nuclear security planning and assessment participate in activities for continuous improvement of their modelling and simulation processes. |