ORNL/TM-2021/2034

Methods for the Enhancement of Security Probabilistic Risk Assessments

Alexander J. Huning
Thomas J. Harrison

March 2021

Approved for public release.
Distribution is unlimited.

OAK RIDGE National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

DOCUMENT AVAILABILITY

Reports produced after January 1, 1996, are generally available free via US Department of Energy (DOE) SciTech Connect.

Website www.osti.gov

Reports produced before January 1, 1996, may be purchased by members of the public from the following source:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone 703-605-6000 (1-800-553-6847)
TDD 703-487-4639
Fax 703-605-6900
E-mail info@ntis.gov
Website http://classic.ntis.gov/

Reports are available to DOE employees, DOE contractors, Energy Technology Data Exchange representatives, and International Nuclear Information System representatives from the following source:

Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831
Telephone 865-576-8401
Fax 865-576-5728
E-mail reports@osti.gov
Website https://www.osti.gov/

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/TM-2021/2023

Nuclear Energy and Fuel Cycle Division

METHODS FOR THE ENHANCEMENT OF SECURITY PROBABILISTIC RISK ASSESSMENTS

Alexander J. Huning
Thomas J. Harrison

March 2021

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

ABSTRACT

The US Department of Energy is exploring the methods associated with probabilistic risk assessment (PRA) and how they could be used to enhance physical security evaluations for nuclear facilities. A brief review of both international and US Nuclear Regulatory Commission physical security assessment methods is presented. From this review, and with an understanding of the technical elements associated with a traditional nuclear safety PRA, several observations are made pertaining to where physical security analysis methods could be enhanced. These observations principally support and enhance the answers within a physical security context to the risk triplet: *(1) What can go wrong? (2) What is the likelihood? and (3) What are the consequences?* Finally, benefits and technical challenges toward the development of a full security PRA are presented.

1. INTRODUCTION

This report was developed to support the US Department of Energy (DOE) in exploring the methods associated with probabilistic risk assessment (PRA) and how they could be used to enhance physical security evaluations for nuclear facilities. Any existing or planned facility that has the potential for significant radiological consequences deriving from sabotage and/or theft of nuclear material may benefit from additional risk insights in performing security evaluations. Any observations or conclusions of this report associated with where risk models may substitute for or complement existing approaches are not limited to minor technical areas or assumptions, if the benefit of such a change may outweigh its development effort. However, it is beyond the scope of this report to adequately estimate such development costs and fully address any regulatory, design, or other implications of including additional risk models or changes to the existing security evaluation methodologies. Both domestic (Nuclear Regulatory Commission [NRC], DOE) and international (International Atomic Energy Agency [IAEA]) security evaluation methodologies are explored.

The inclusion of risk information has both focused safety improvements and improved overall plant economics at existing commercial nuclear power plants. NRC has steadily increased its use of risk information over the years. Additionally, any future commercial reactors licensed in the United States will likely rely on risk models for parts of their safety basis.

Although increased fidelity and realism of safety and security assessments is desirable, many other factors contribute to the need for exploring PRA methods as way to enhance the security evaluation process for nuclear facilities. These factors include the following:

- Recognizing that security costs have increased, especially since the September 11, 2001, terrorist attacks, and are a major component of the operating cost for a nuclear power plant,
- Advanced reactor designs employ many novel features (e.g., autonomous control, microreactors with hazards equivalent to a research reactor) that may justify reduced security requirements,
- The use of probabilities and threat scenarios mimics concepts employed by nuclear safety PRAs,
- The scattering of deterministic variables without a sufficient basis might be inadvertently placing overly prescriptive requirements on plant physical security systems.

PRA is a broad term that encompasses a variety of technical elements for both nuclear and non-nuclear applications. For example, the ASME/ANS PRA standard for non–light water reactors (non-LWRs) [1] contains high-level and supporting requirements for 18 different technical elements. These elements include areas of statistical and engineering analysis such as initiating event analysis, seismic and other hazard analyses, human reliability analysis, and mechanistic source term analysis, among others. Capability categories are also defined in PRA standards that allow for graded requirements for the given design stage and level of detail that are available. Note also that a PRA meets these standard requirements on an element-by-element basis. This means that not all technical elements need to be developed to meet the definition of a PRA for a given application. The standard also generally does not define “how” or what method to use to construct a model that meets the requirements. In many cases, an example or suggestion is provided but is not mandatory should another method be preferable. Based on this description, a few observations can be made which benefit or support the use of PRA methods for the enhancement of security risk assessments:

1. A security PRA may need to develop only a few of the technical elements to have a PRA that meets standards, as defined in those industry PRA standards.

2. Only lower-level capability requirements may be sufficient for security applications.

3. Alternate techniques or methods more common to security assessments may be sufficient to meet technical requirements traditionally developed for nuclear safety risk assessments.

2. REVIEW OF DOMESTIC PHYSICAL SECURITY ASSESSMENT METHODOLOGIES

Within the United States, nuclear facilities are primarily regulated by DOE and NRC. Order DOE O 473.3A applies to all DOE elements and provides requirements and responsibilities for physical protection program operations [2]. NRC encourages new applicants to use NUREG/CR-7145 as their guidance [3] for meeting the general security performance objectives in 10 CFR 73.55(b). Physical security assessment methodologies are similar and revolve around the evaluation of a design basis threat (DBT). For DOE, the DBT represents an absolute extreme malevolent act based on the adversary characteristics defined in DOE O 470.3C [4]. NRC also maintains a set of DBT scenarios for nuclear power plants. Both documents are either classified or restricted because of security concerns surrounding the specific events contained within the DBTs.

Methodology options for evaluating DBT scenarios include the following:

- vulnerability of integrated security analysis (VISA) tabletop
- design evaluation and process outline (DEPO)
- the process outlined in NUREG/CR-7145

These methodologies follow a similar process. For example, the process outline in NUREG/CR-7145 is shown as **Error! Reference source not found.**.

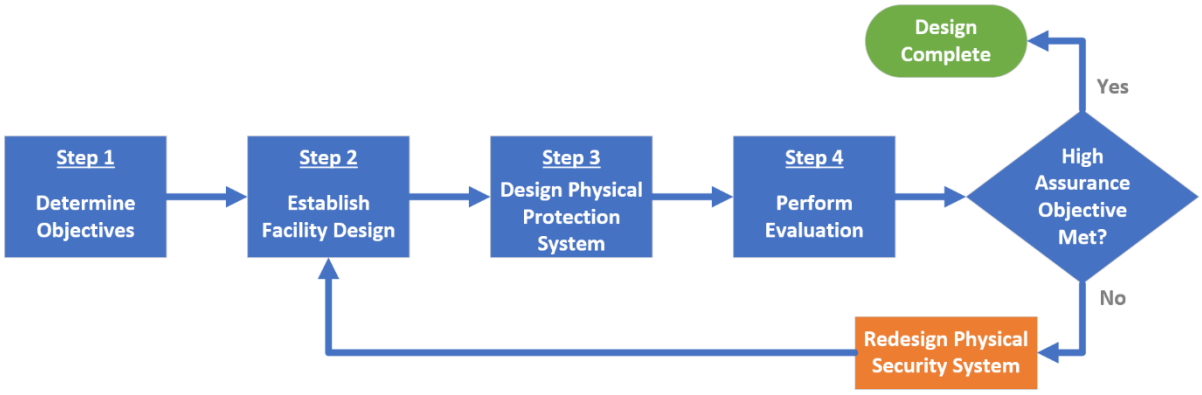

Figure 1. Security assessment process as outlined in NUREG/CR-7145 [3].

Within this process, step 4, "Perform Evaluation", is the focus of this report investigating where PRA methods could be employed. Within step 4, NUREG/CR-7145 describes three steps:

1. Apply NRC-developed scenarios and evaluate physical protection system (PPS) using an acceptable methodology.

2. Analyze scenarios to ensure adversary action are within DBT capabilities and credible.

3. Analyze scenario to ensure barrier delay time protective force actions are credible.

The basic steps for evaluating the PPS effectiveness include these:

- identify the overall scenarios
- evaluate blast effects

- analyze scenario timelines
- analyze neutralization
- determine overall PPS effectiveness (integration of the first four elements)
- conduct risk-informed evaluation of candidate design features

Throughout the steps, probabilities are constructed to determine the overall PPS effectiveness :

$$P_E = P_I \times P_N \tag{1}$$

where

P_E = probability of effectiveness or overall system effectiveness,

P_I = probability of interruption of the adversary (considers the likelihood that detection will occur early enough in the adversary attack sequence that the response force can arrive before the attack is successfully completed

P_N = probability of neutralization of the adversary

The probabilities are established through simulation and modeling of the event scenarios, also referred to as “force-on-force” simulations. When these simulations are coupled with possible PPS enhancements, such as the placement of bullet-resistant enclosures and defensive posture changes (i.e., a guard staff reduction or increase), the PPS design can be optimized.

In the last step of the NRC methodology, a plant PRA provides some input for informing the selection of candidate design features based on their ability to ensure safety function performance and their contribution to risk metrics such as core damage frequency.

3. REVIEW OF IAEA METHODOLOGY

The IAEA's recommendations for physical protection requirements and evaluation methodology is documented in INFCIRC/225/Revision 5 [5]. This publication is defined as follows:

> *This publication provides a set of recommended requirements to achieve the four Physical Protection Objectives (see Section 2) and to apply the 12 Fundamental Principles (see Section 3) that were endorsed by the IAEA Board of the Governors and General Conference in September 2001.*

The four physical protection objectives are

- To protect against unauthorized removal
- To locate and recover missing nuclear material
- To protect against sabotage
- To mitigate or minimize the effects of sabotage

The 12 fundamental principles include responsibilities of the state, responsibilities during international transport, and others. Of those, "Fundamental Principle G: Threat" is most relevant for discussion here. This principal states "The State's physical protection should be based on the State's current evaluation of the threat."

Within the threat fundamental principal, several requirements are specified. Some of the important aspects of the specified requirements are the following:

- The state should define the threat in the form of a threat assessment, and if appropriate, a DBT.
- Consideration should be given to insider threats.
- DBTs should include both unauthorized removal of material and sabotage that has potentially high radiological consequences.
- The effectiveness of physical protection measures should be evaluated.
- The state should also consider airborne threats and possible stand-off attacks as specified in its threat assessment or DBT.

In terms of security risk management, IAEA recommends the following:

- Reducing the threat (e.g., increasing the deterrence presented by the physical security)
- Improving the effectiveness (e.g., establishing and maintaining a strong nuclear security culture)
- Reducing the potential consequences (e.g., modifying the amount and type of nuclear material and the design of the facility)

In addition to the IAEA recommendations, the IAEA's nuclear security series also includes

- nuclear security fundamentals
- implementing guides

- technical guidance

IAEA recommendations are expanded upon in the implementation guide, IAEA Nuclear Security Series No. 27-G, *Physical Protection of Nuclear Material and Nuclear Facilities* (*Implementation of INFCIRC/225/Revision 5*) [6]. **Error! Reference source not found.** shows the physical protection life cycle.

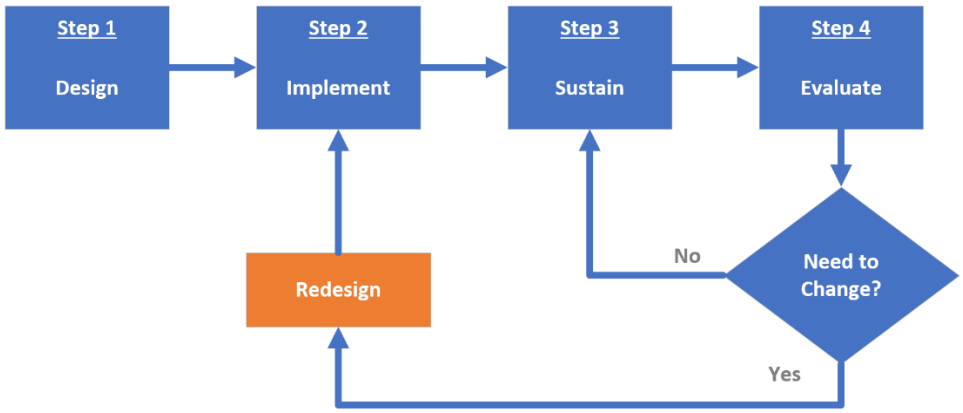

Figure 2. Recommended IAEA physical protection lifecycle in INFCIRC/225/Revision 5 guidance [6].

Both IAEA and NRC documents place a strong importance on the identification of threats or DBTs. IAEA does not identify specific threat scenarios and charges this task to the individual member state governments. However, guidance for developing the DBT scenario is provided in IAEA Nuclear Security Series No. 10, *Development, Use, and Maintenance of the Design Basis Threat* (2009) [7]. Within that document, guidance is provided regarding what items it would be necessary to include in the development of a DBT. The process is defined as follows:

> *The process for the development of the DBT include further analysis and, most importantly, decision making. The analysis and decision making process has three major phases:*
>
> *[1] Screening the threat assessment output for those threats with motivation, intention, and/or capability to commit a malicious act;*
>
> *[2] Translating the resulting screened list into a statement of representative attributes and characteristics of the postulated adversary;*
>
> *[3] Modifying the statement of representative threat attributes and characteristics on the abasis of relevant policy considerations.*

After these phases are completed, the potential DBT is dispositioned or endorsed as a DBT.

IAEA and NRC identify similar methods for evaluating the effectiveness of physical security systems. The IAEA guidance document specifically mentions the following:

- *Path analysis*, which involves constructing timelines for different credible paths that an adversary might attempt. Task and response times are measured or deterministically computed, with detection feature effectiveness values being probabilistic.

- *Simulation methods*, which include both computer simulation and tabletop exercises that predict PPS effectiveness.

- *Exercises,* which include force-on-force exercises that measure the effectiveness of specific scenarios.

Of these methods, the IAEA guidance cautions against using only simulations, as they may fail to reflect practical aspects of the response and may miss important aspects of attack scenarios. More detailed guidance on the analysis and design aspects of the PPS is provided in IAEA Nuclear Security Series No. 4, *Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage* [8].

One difference between the methodologies is that IAEA guidance is much broader, allows for a graded approach to physical protection requirements, and does not force a state or applicant to use a specific methodology in the assessment of threats and the physical security system. It advises member states to consider the varying consequences of malicious acts. IAEA also directs member states to decide what level of risk is acceptable and what level of protection against threats should be provided.

4. ASSESSMENT OF SECURITY PRA METHODS

A risk evaluation is commonly expressed as obtaining the answers to three questions, also known as the "risk-triplet":

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

(For technical completeness, a fourth is often included:

4. What is the uncertainty?)

When these questions are compared with the steps described earlier, they are partially answered to varying degrees. PRA methods could be employed to enhance physical security evaluations to better address these questions.

1. What can go wrong? — Identify the overall scenarios

In terms of PRA technical elements, this question is answered through the identification of initiating events (IEs) and initial event sequence development. In terms of physical security evaluations, this question is largely adverted by using deterministically selected DBT scenarios. It is unclear whether this issue is adequately addressed in the supporting DOE or NRC guidance documents.

A PRA takes in as many sources and methods that are available to construct as complete a set of events as possible. Very low-frequency and nonapplicable events can later be screened when the supporting data and systems models are developed. Many of the methods used to identify events come from the field of process hazard analysis (PHA). These methods include but are not limited to "what-if" analysis, checklist approach, master logic diagrams (MLDs), hazards and operability analysis (HAZOP), failure modes and effects analysis (FMEA), and the more detailed fault tree methods common to commercial LWR internal event PRAs.

Of these PHA techniques, the MLD approach has proved useful for advanced reactors at an early design phase for identifying events that could result in a release of radionuclides. The MLD approach is a deductive technique that starts with the consequence, a release of radionuclides, and works backward (or downward) to basic events that lead to this consequence. An MLD approach could also be employed for the identification of security-related events that can lead to a radiological consequence.

2. How likely is it? — Blast effects, timelines, neutralization, and PPS effectiveness

With consideration of the PRA methods, data, systems models (fault and event trees), human reliability analysis, and other technical elements are used to construct event probabilities. Multiplying these event probabilities by their respective IE frequencies, individual event sequence frequencies are constructed. The steps for evaluating PPS effectiveness are similar to this process in that probabilities are constructed for the various success or failure for the interruption and neutralization of adversaries.

In the context of nuclear safety PRAs, accident scenarios are commonly simulated using thermal hydraulic and severe accident tools to estimate the consequences and timeframes of those consequences (i.e., if a release occurs, is it large, small, early, late, etc.). This approach is similar to force-on-force simulations for establishing the effectiveness of the PPS. A systematic assessment of events within the DBT scenarios, using an event tree or similar event sequence development tool, could be beneficial for

assessing PPS effectiveness. Given the dynamic and dependent nature of the interactions among events, dynamic event trees that can automatically initiate the simulation of different event sequence pathways may be more beneficial than the traditional accident scenario modeling process for security events.

To complete the assessment of likelihood, some consideration must be given to frequency. It is not clear whether DBT frequencies are discussed in PPS evaluations. This is a much more challenging problem and is described briefly in the next section.

3. What are the consequences?

Potential consequences of both a security-related event and a non–security-related event (e.g., nuclear safety accident) include a radionuclide release, to a varying degree. In a safety PRA, source term calculations (either mechanistic/best estimate or bounding) are used to estimate the consequences for the various accident scenarios. It is unclear whether security-related events use or rely on best-estimate tools for consequence estimation. Added complexity is associated with security events because of the various malicious acts (e.g., fires, explosions) that could magnify a potential release. Source term and atmospheric transport and dispersion tools, such as MELCOR and MACCS, could be used for security-related event consequence information; but it may be necessary to include modules for fire effects and consideration of the integrity of surrounding structures. Alternatively, security-related consequences could be approximated by using assumed equivalent values for similar scenarios from the safety PRA.

4.1 CONSIDERATIONS TOWARD THE DEVELOPMENT OF A FULL SECURITY PRA

The potential benefits of having a full security PRA (i.e., one that would satisfy all applicable standard requirements) would mirror the benefits seen for traditional safety PRAs in terms of risk-informed safety classification (e.g., 50.69 process), technical specifications, reactor oversight processes, and other applications. It would translate to a potential reduction of security costs by focusing protection away from non–risk significant events or plant areas. It could also be used a tool for risk-informing PPS design. Additionally, it could serve as one way for advanced reactor developers to justify reduced security requirements for new reactors.

However, there are many challenges associated with developing a full-scope security PRA. It is unlikely that a full-scope PRA will be developed for the following technical reasons:

1. IE Frequencies

It is unlikely that any developed probabilistic representation of security-related IEs will provide an acceptable level of uncertainty for the application of deriving event sequences as substitutes for deterministically derived DBT scenarios. For internal events—those event sequences initiated by some random failure within the plant—the uncertainty surrounding the frequencies and types of event sequences can be easily bounded by established component failure data. Similarly, for external hazards—such as seismic or wind-related IEs—exceedance frequency hazard curves can be constructed from region-specific historical data. The difference for security-related event sequences is that these are not initiated by random failure and have not occurred frequently enough to establish a reasonable uncertainty distribution. Additionally, humans are generally intelligent enough not to repeat scenarios or events and can learn in a way for which nature shows no regard.

2. Other PRA Technical Element Modeling Gaps for Security Events

Beyond IE development, human (plant operator) reliability assessment and the development of level 2 types of system models for security events pose some of the largest challenges to developing a security

PRA that meets standards. Level 2 types of system models are those that model containment or confinement performance, assuming a core disruption event that may lead to an offsite release of radionuclides. For security events, these would have to predict or estimate the probability of small to large radionuclide releases due to malicious acts.

One potential solution, as discussed earlier with respect to addressing consequences, is to link the various security-related consequences to those already developed in the safety PRA. Consideration must be given to potential security-related modifiers that might enhance a potential release.

3. Coupled Safety PRA Modeling Challenges

Assuming that an acceptable probabilistic representation of security-related IEs could be constructed, those IEs would require their own event trees or fault tree model tie-ins to the safety PRA. Any PRA analyst would then need the same level of security access to evaluate traditional or non–security related risk-informed applications, unless separate safety and security PRAs be developed. However, developing separate models is unlikely because any change in the traditional safety PRA would trigger a change in the security PRA. Traditional PRA standards, like those published by ASME and ANS, assert that PRA models must be updated at regular intervals, typically 3 to 5 years, to be consistent with the design and operation of the plant. This added complexity and cost would need to be weighed against the cost of security evaluations from the standpoint of a standard DBT scenario methodology.

5. CONCLUSIONS

A brief review of existing security evaluation methodologies was performed, along with an exploration of where safety PRA methods can be employed to enhance these existing techniques. Although having a full security PRA that meets standards would provide significant benefits, there are many technical challenges that could be prohibitive. One of the main challenges is associated with identifying the spectrum of initiating events and estimating their frequency of occurrence. Without an estimation of frequency, it would be difficult to weigh PPS design decisions in the same context as other safety component design decisions with clear links to preventing anticipated, design-basis, or beyond-design-basis types of events or accidents. In terms of enhancing existing security evaluation methodologies, three observations were made:

1. An MLD or another PHA approach could support the development of other DBT scenarios or security-related events that would lead to a significant consequence.

2. Event trees, along with a robust simulation framework, could enhance the scenario descriptions and potential end states for consequence modeling input.

3. Consequence modeling similar to safety PRAs, using MELCOR/MACCS (or a similar tool), could refine the magnitude of the release for the various security-related scenarios.

These observations could be applied toward either sabotage or theft events. However, theft events would then need to consider additional sites or areas to which the material is transported.

REFERENCES

[1] AMERICAN SOCIETY OF MECHANICAL ENGINEERS and AMERICAN NUCLEAR SOCIETY, *"Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants,"* ASME/ANS RA-S-1.4-2021, (February 2021).

[2] US DEPARTMENT OF ENERGY, *"Protection Program Operations*," DOE Order 473.3A Chg. 1, (January 2018).

[3] US NUCLEAR REGULATORY COMMISSION, *"Nuclear Power Plant Security Assessment Guide,*" NUREG/CR-7145, ADAMS Accession No. ML13122A181, (April 2013).

[4] US DEPARTMENT OF ENERGY, *"Design Basis Threat (DBT),"* DOE O 470.3C Chg.1, (September 2020).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, "*Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,"* IAEA Nuclear Security Series No. 13, INFCIRC/225/Revision 5, (2011).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, "*Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5),"* IAEA Nuclear Security Series No. 27-G, (2018).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, *"Development, Use and Maintenance of the Design Basis Threat,*" IAEA Nuclear Security Series No. 10, (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, *"Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage,"* IAEA Nuclear Security Series No. 4, (2007).