

JUNE 2025

A RISK-INFORMED FRAMEWORK
FOR MANAGING NUCLEAR
FACILITY SECURITY RISKS



Excellence—Every project. Every day.



OUTLINE

1. JCNRM Security Working Group
 2. Risk-Informed Security Framework
 3. A Case for Quantifying Attack Likelihood
 4. Key Points to Consider
- 

Risk-Informed Security Working Group



JCNRM

Joint Committee on Nuclear Risk Management

SCoRA

Sub-Committee on Risk Applications

SWG

Physical / Cyber Risk-Informed Security Work Group



SWG Mission



Develop guidance to:

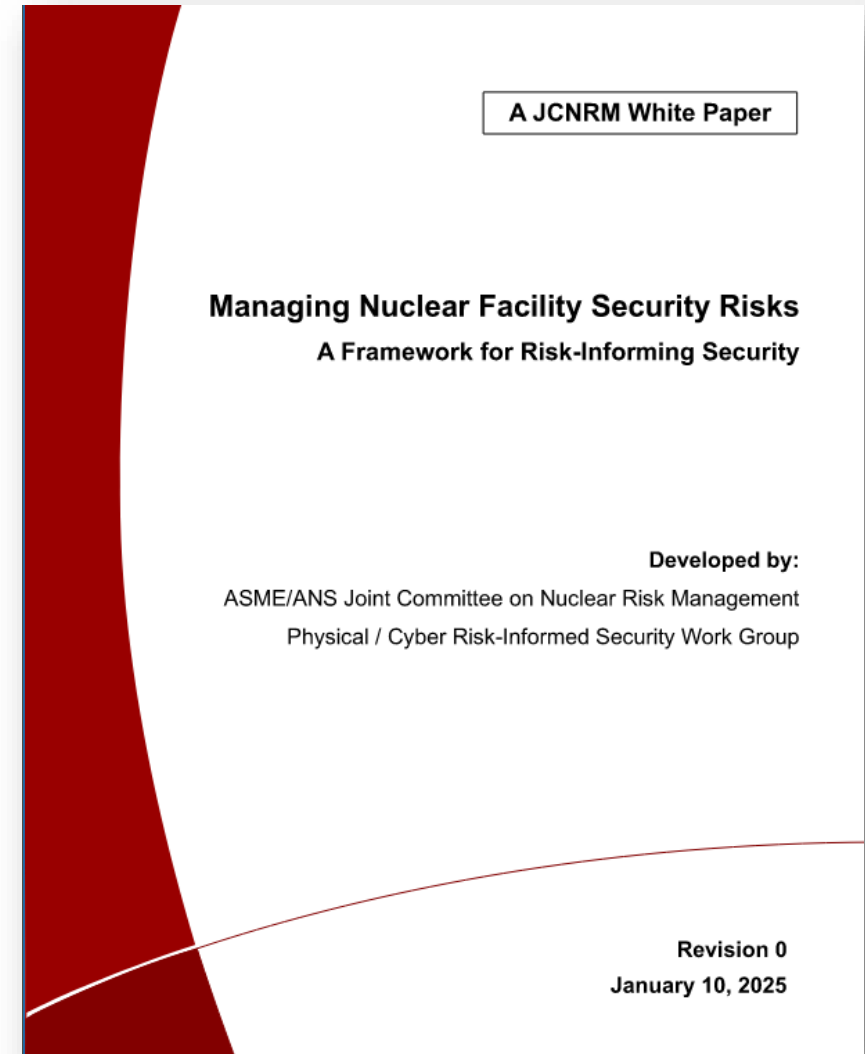
- Improve effectiveness and efficiency of nuclear facility physical and cyber security programs through application of risk assessment methods and insights
- Integrate nuclear facility safety and security considerations into a more uniform decision-making framework such that facility resources can be allocated more consistent with a facility's risk profile



Risk-Informed Security Framework

White paper serves two purposes:

- Communication tool with industry and regulatory stakeholders to appropriately shape and tailor the incorporation of risk into nuclear facility security programs in accordance with state-of-the-art risk practices
- Foundation for use by the SWG in identifying and developing work products to address security risk management for multiple types of nuclear facilities and security scenarios





FRAMEWORK SCOPE

- Scope of the SWG charter is very broad and encompasses:
 - All nuclear facilities (power plants, fuel processing facilities, etc.)
 - Physical, cyber, and combined physical/cyber attacks
 - A range of potential consequences (public health and safety, financial, etc.)
- The guidance may include both qualitative and quantitative risk assessment methods
- Framework had to be defined at a high enough level to address this broad scope

FUNDAMENTAL RISK ASSESSMENT PRINCIPLES

- The framework for risk-informed security is based on the fundamental principles of risk assessment including the risk triplet
 - What can go wrong?
 - How likely is it?
 - What are the consequences?
- Likelihood includes two elements
 - Likelihood of an initiating event
 - Likelihood of a series of subsequent failures that result in an undesired consequence
- A risk-informed approach should be realistic where conservatism is avoided or used with caution
- Uncertainty must be addressed
- The assessment should focus on the ultimate consequence of concern (e.g., radiological release) rather than an intermediate “consequence” (e.g., an adversary accesses a restricted area)

FRAMEWORK

- A framework is “a supporting structure around which something can be built” (Cambridge Dictionary)
 - Defines the essential elements
 - Shows how these elements fit together

“

An important feature of frameworks is that the very contestation over their nature is perhaps their main value. A framework can only be an effective boundary object if it catalyzes deliberation and scholarly debate — thus contestation over what it is and its value is seeded into the toolbox and identity of a scholarly field. Although most frameworks are likely to have shortcomings, flaws or controversial features, the fact that they motivate engagement around common problems and stimulate scholarly engagement is a value of its own.

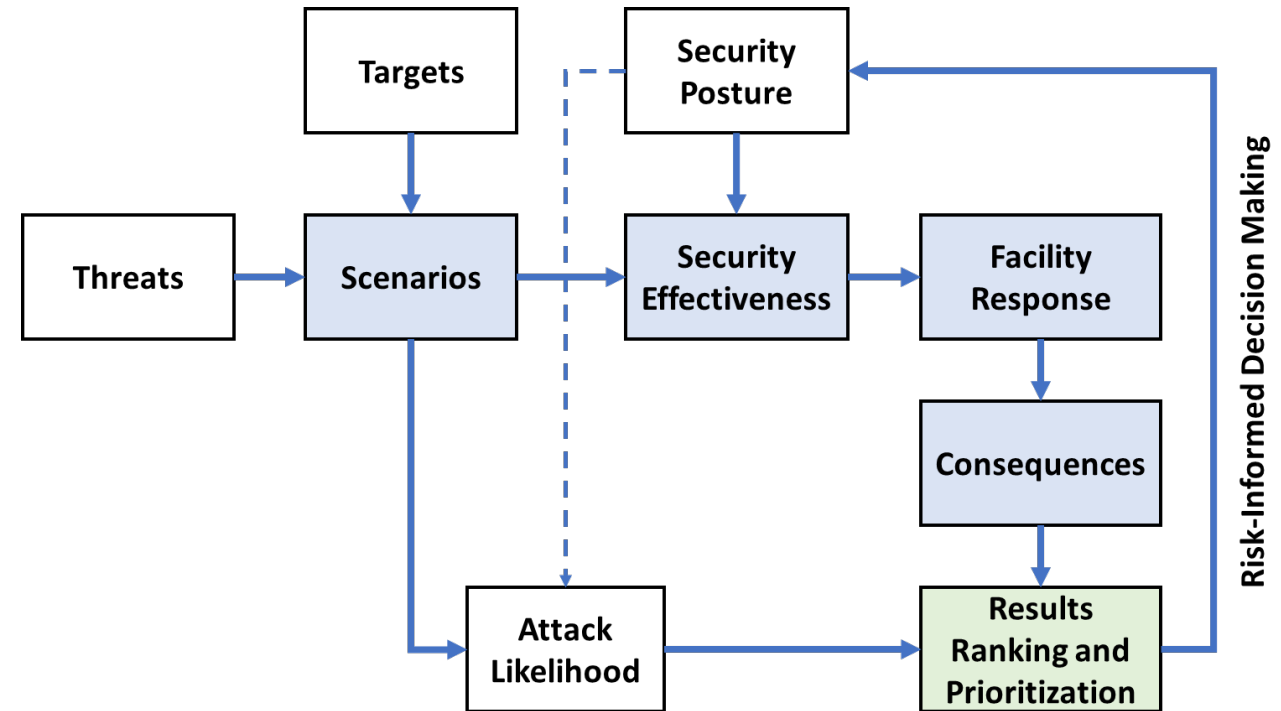
”

Stefan Partelow
Journal of Environmental Studies and Sciences



RISK-INFORMED SECURITY FRAMEWORK

- **Consequences** represent the undesired outcomes that are being assessed
- **Threats** represent classes of adversaries
- **Targets** represent SSCs and operator actions that need to be protected to prevent the consequences
- **Scenarios** are defined by combinations of threats and target sets that could result in the consequences
- **Security Posture** includes all security measures in place to protect the facility
- **Security Effectiveness** is an assessment of the likelihood for an adversary to partially or fully accomplish their objectives
- **Facility Response** is an assessment of the likelihood that the consequences of concern will occur following adversary neutralization
- **Attack Likelihood** is the likelihood that an initiating event (i.e., attack) will occur for a given scenario
- **Results Ranking and Prioritization** is a comparison of scenario results to gain necessary insights for risk-informed decision-making



FRAMEWORK FROM JCNRM RISK-INFORMED SECURITY WHITE PAPER

NEXT STEPS

- Methods and tools currently exist for many elements of the framework, but guidance is needed to address gaps and show how methods can be properly integrated for a risk-informed assessment
- The SWG has chosen to narrow our near-term focus on:
 - Commercial power reactors (existing fleet and advanced reactors)
 - Health and safety of the public (radiological release)
- Our near-term focus still includes physical, cyber, and combined attacks
- We are currently working on guidance for two important elements:
 - Attack likelihood
 - Scenario development

ATTACK LIKELIHOOD

- A challenging and controversial topic
- Developing a robust technical solution for attack likelihood is difficult but valuable

The Value of Developing Quantitative Estimates of Attack Likelihood for Risk-Informed Security

Tim Sande*

Enercon Services, Inc., Albuquerque, NM

ABSTRACT

The insights gained from probabilistic risk assessment (PRA) models and risk-informed applications over the past five decades provided significant benefits to the nuclear industry in terms of improved plant safety and operational efficiency. The successes achieved in plant safety risk management provide a strong motivation for expanding the use of risk-informed methods within the nuclear power industry. The NRC has supported this expansion as they strive to be a risk-informed, performance-based, and technology-neutral regulator.

Nuclear power plant PRA models are based on the answers to three questions: What can go wrong? How likely is it? What are the consequences? Although many people have suggested using a similar risk triplet approach for assessing security risk, the second question (how likely is it) has been a roadblock. With respect to safety, likelihood is assessed based on the frequencies of initiating events and the probabilities of various equipment and human (operator action) failures. With respect to security, methods currently exist to estimate the probability of the plant protection system to mitigate adversary attack prior to achieving the desired target set (i.e., security effectiveness modeling). However, there are no currently accepted methods for addressing the frequency of occurrence for an adversary attack (i.e., the equivalence of an initiating event frequency).

Quantifying attack frequencies presents some unique challenges, and the methods that have previously been developed to quantify initiating event frequencies cannot be directly applied to an attack scenario. However, these challenges can be addressed in a meaningful and technically robust manner.

Solving the difficult issues associated with quantifying attack likelihood will allow the nuclear industry to implement a risk-informed approach that is consistent with safety risk assessments. This will allow for risk-informed decision-making that holistically encompasses both safety and security.

Keywords: Risk-Informed, Security, Attack Likelihood

1. INTRODUCTION

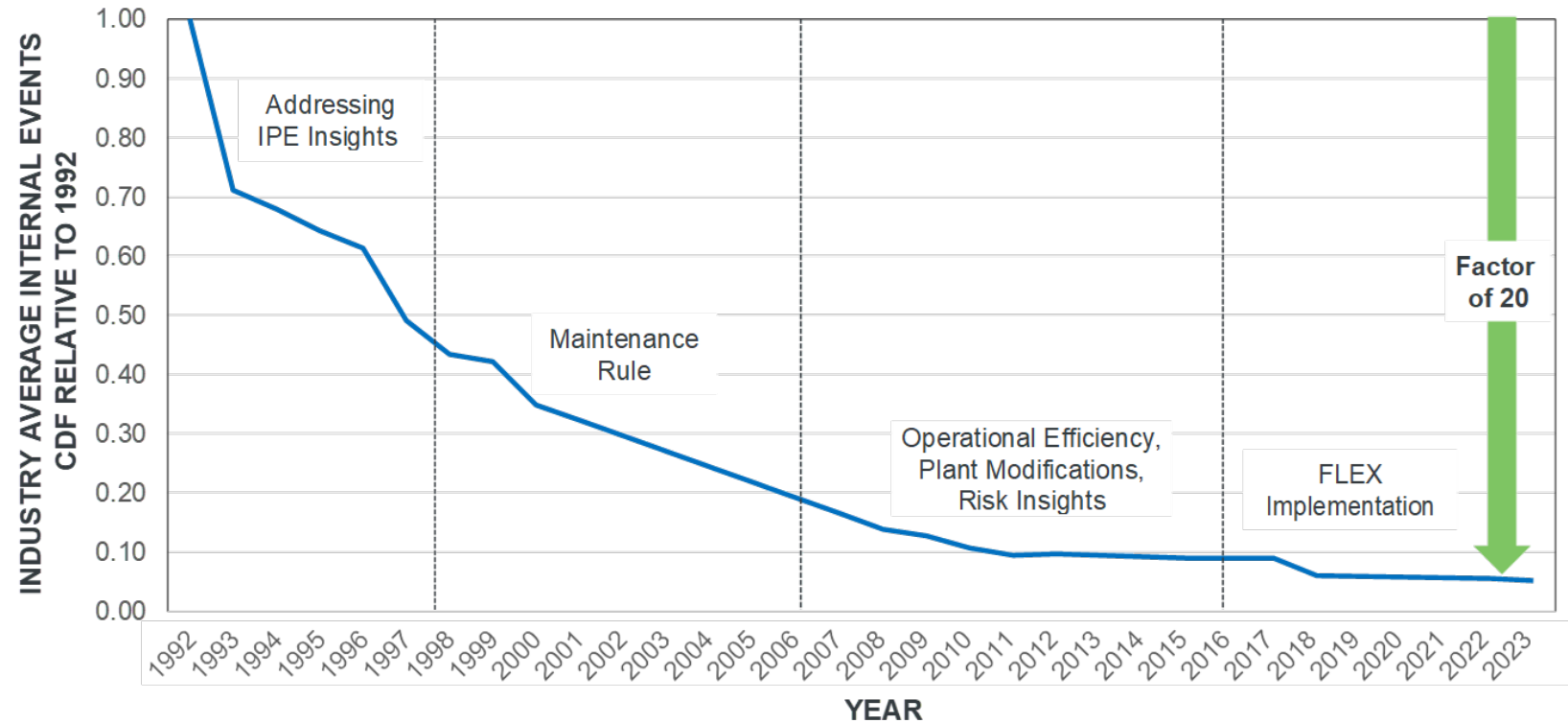
Probabilistic risk assessment (PRA) and risk-informed engineering are broadly accepted methods for managing risk associated with the safety of nuclear power plants. These methods are fundamentally based on the quantitative definition of risk described by Kaplan and Garrick as the risk triplet [1]:

What can go wrong?

*tsande@enercon.com

PRA BENEFITS FOR SAFETY

- The current nuclear fleet was designed and built using deterministic safety analysis methods with defense-in-depth
- Over the past 30+ years, PRA methods have been developed and effectively used to reduce plant risk
- Risk-informed applications have improved safety and reduced cost by focusing on what matters most



INDUSTRY AVERAGE CORE DAMAGE FREQUENCY TREND PRESENTED BY NEI AT 2024 NRC RIC (ML24082A179)

CURRENT ASSESSMENT METHODS

	DETERMINISTIC	PROBABILISTIC
SAFETY	<ul style="list-style-type: none"> • Standard design basis accident (DBA) scenarios • Evaluated based on prescriptive rules and acceptance criteria • Focused on bounding scenarios due to implicit assumption that DBA will occur • Uncertainties implicitly addressed through use of conservatism 	<ul style="list-style-type: none"> • Wide range of scenarios evaluated including beyond design basis (BDB) • Combinations of active failures, common cause failures, and human failures evaluated based on probabilities • Initiating event frequencies estimated • Uncertainties explicitly addressed
SECURITY	<ul style="list-style-type: none"> • Standard design basis threat (DBT) scenarios • Evaluated using force-on-force exercises with prescriptive rules and acceptance criteria • Focused on bounding scenarios due to implicit assumption that DBT will occur • Uncertainties implicitly addressed through use of conservatism 	<ul style="list-style-type: none"> • Not currently performed • Methods exist for probabilistically assessing security effectiveness (likelihood of success given attack) • Methods have not yet been developed for estimating attack frequencies • Uncertainties could be explicitly addressed

QUANTITATIVE DEFINITION OF RISK

- Risk triplet defined by Kaplan and Garrick:
 - What can go wrong?
 - How likely is it?
 - What are the consequences?
- Likelihood is a key element for assessing risk
- If it is removed, the remaining doublet would be a hazard assessment



LIKELIHOOD IN SAFETY APPLICATIONS

- Likelihood is a general term that encompasses:
 - Frequency: A rate of occurrence over a given period (units of time⁻¹)
 - Probability: An event outcome ranging between 0 and 1 (unitless)
- Both aspects of likelihood are used to assess safety risk
 - Initiating event frequencies for LOCAs, reactor trip, ATWS, etc.
 - Probabilities for basic event failures (e.g., pumps, valves), human failures, and common cause failures
- Assessing the likelihood of rare events is challenging
 - Frequency of a large LOCA is one example
 - No historical occurrences to use as the statistical basis
 - Addressed through expert elicitation (NUREG-1829)
 - Large uncertainty bands (orders of magnitude)
 - Estimated frequencies provide meaningful risk insights



LIKELIHOOD IN SAFETY APPLICATIONS

Initiating Event	Initiating Event Frequency (yr ⁻¹)	Conditional Core Damage Probability	Core Damage Frequency (yr ⁻¹)
Reactor/Turbine Trip	1.1	2.6×10^{-7}	3.0×10^{-7}
Loss of Offsite Power	2.4×10^{-2}	2.4×10^{-5}	5.9×10^{-7}
Small LOCA	3.8×10^{-3}	1.0×10^{-7}	3.9×10^{-10}
Medium LOCA	1.2×10^{-4}	4.4×10^{-5}	5.3×10^{-9}
Large LOCA	7.8×10^{-6}	9.8×10^{-6}	7.6×10^{-11}
Reactor Vessel Rupture	1.3×10^{-8}	9.0×10^{-1}	1.2×10^{-8}

LIKELIHOOD IN SECURITY APPLICATIONS



- Several concerns have been raised regarding quantification of likelihood for security:
 - Equipment failures are intentional rather than random
 - A simple Bayesian approach can't be used to estimate attack likelihood
 - An adversary decision to attack is dependent on the level of security
 - Attack likelihood changes over time
 - High uncertainty could make it difficult to achieve statistically meaningful insights
 - Regulatory requirements don't allow it



KEY POINTS TO CONSIDER

- The challenges of quantifying attack likelihood have led many people to some form of the following conclusions:
 - It is an impossible problem to solve
 - It might be possible, but would have so much uncertainty that the results would not be meaningful
 - It's just not worth the effort
- These same arguments could have been made with respect to safety PRA models
- The value of PRA could have been lost to the nuclear industry if the TMI accident hadn't validated a major conclusion in WASH-1400 (small LOCAs can be more risk-significant than large LOCAs)

“

some hold a philosophic view that there is no such thing as a numerical value for the probability of occurrence of a catastrophic accident; that such a thing is unknowable.

”

WASH-740 (1957)



NORM RASSMUSSEN REMARKS IN FALL 1976

“ I do not believe that the safeguards risks can be quantified using these procedures. ”

“ an overall quantitative risk assessment of the safeguards issues is at present beyond the capability of the methodology. ”

“ If this type of work continues, and I hope it will, it is reasonable to hope that these methods may someday produce meaningful quantitative assessments of the effectiveness of various systems. These assessments would be particularly valuable in the early stages of facility design when modifications can be readily made. ”



CONCLUSIONS

- There are real technical challenges with quantifying attack likelihood, but the problems are not impossible to solve
- After 50 years of PRA model development and application, we have the tools we need to quantitatively estimate attack likelihood and address the uncertainties
- We can achieve the same benefits for security that we have gained for safety and it is absolutely worth the effort

“

There is nothing that we know absolutely nothing about.

”

Bob Budnitz

“

Statistics is the science of handling data; probability is the science of handling the lack of data.

”

Stan Kaplan



Tim Sande

Senior Manager
PRA and Risk-Informed Engineering

Phone: 505.261.2442

Email: tsande@enercon.com

THANK YOU



Excellence—Every project. Every day.