INL/CON-23-75972-Revision-1

# Digital risk analysis in nuclear engineering projects: Designing for safety, performance, reliability, and security

June 2024

Shannon Leigh Eggers, Robert Walker Youngblood III

Changing the World's Energy Future

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

INL/CON-23-75972-Revision-1

# Digital risk analysis in nuclear engineering projects: Designing for safety, performance, reliability, and security

**Shannon Leigh Eggers, Robert Walker Youngblood III**

**June 2024**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**

# Digital Risk Analysis in Nuclear Engineering Projects: Designing for Safety, Performance, Reliability, and Security

**Shannon L. Eggers[1,*], Robert W. Youngblood[1]**

[1]Idaho National Laboratory, Idaho Falls, ID

*doi.org/10.13182/T130-43314*

## ABSTRACT

Cyber-informed engineering and security-by-design frameworks are important in promoting the need to identify cybersecurity concerns early in the systems engineering lifecycle so risks from adversarial cyber-attacks can be eliminated or reduced through engineering design practices. In addition to adversarial risk, risk in operational technology systems also includes non-adversarial and unintentional risk from other factors such as human performance errors, environmental conditions, design flaws, and device degradation or failure. This paper introduces a new concept for characterizing digital risk, both adversarial and non-adversarial, and provides the basis for initial research into a novel digital risk analysis approach focused on incorporating attack difficulty into a multi-attribute analysis technique using robust decision-making. This digital risk characterization is also used to frame a discussion on the challenges of competing objectives and competing stakeholder requirements in an integrated energy system project that incorporates a small modular reactor and industrial facility.

*Keywords*: Digital Risk Analysis, Cybersecurity

## 1. INTRODUCTION

According to the International Atomic Energy Agency (IAEA) [1], there are more than seventy small modular reactor (SMR) designs developed or under consideration based on multiple reactor types, including light water reactor designs as well as those using alternative fuel and coolant designs. This nuclear renaissance is accelerating the digital transformation and use of digital instrumentation and control (I&C) systems in nuclear power plants (NPP), reinforcing the need to incorporate security- and digital-related concerns in design decisions throughout the systems engineering lifecycle.

In early nuclear engineering design phases, there are often competing objectives and competing internal and external stakeholder requirements. Competing objectives, such as performance, safety, security, reliability, and resilience, must be balanced and prioritized, taking into consideration project constraints and stakeholder requirements (e.g., mission-level, facility-level, and systems-level requirements). The need in nuclear digital engineering projects is to evaluate, document, and track digital risk and cybersecurity decisions along with all other safety and engineering decisions, such as those involving nuclear engineering, mechanical engineering, electrical engineering, and controls engineering disciplines. This decision analysis requires an integrated digital risk management process to systematically evaluate how the inclusion of digital I&C systems impact the balance between performance, safety, reliability, and security.

Numerous methods have been proposed for analyzing cyber risk. Many of these concepts estimate the likelihood that an adversarial threat will exploit a vulnerability to successfully cause an adverse consequence. Generally, these cyber risk analysis methods are focused on adversarial threats and do not

*shannon.eggers@inl.gov

integrate the impacts from non-adversarial threats, such as those from human performance errors, environmental conditions, design flaws, and device degradation or failure. Furthermore, these techniques often have a limited analysis scope for NPPs and are not readily adoptable or repeatable for large facilities with thousands of digital assets [2]. To avoid limitations associated with only analyzing adversarial risk during the design of new nuclear reactors, the term digital risk is used in this paper to holistically reflect both adversarial and non-adversarial threats.

Early risk analysis methods were driven by concerns in the aerospace, chemical, and nuclear industries. WASH-1400 was the first full-scale model that attempted to fully quantify severe accident risk in NPPs [3]. Subsequently, Kaplan and Garrick proposed that risk analysis should answer the following three questions: "What can go wrong?," "What is the likelihood it will go wrong?," and "What are the consequences if it goes wrong?" [4]. Incorporating these three questions is still the basis for many safety risk analysis techniques today. In fact, current probabilistic risk analysis (PRA) methods at NPPs still answer these three questions by using historical data and operating experience to quantitatively estimate core damage frequency, frequency of accidents that result in radiation release from the plant, and the adverse consequences to public health and the environment [5].

Subsequent to publication of WASH-1400, multiple attempts were made to adopt its methods to nuclear safeguards and security. However, as summarized in [6] and [7], there are fundamental problems in applying PRA to security. For instance, the premise of PRA for severe accidents is that initiating events randomly occur and it is unlikely that multiple random events occur simultaneously. This assumption is invalid for digital risk, especially when considering intentional, adversarial actions. PRAs are not intended to model intelligent adversaries who intentionally perform an action and who can change their strategy at will. They also are ill-suited to model intentional human actions in digital I&C systems, regardless of whether they are adversarial or non-adversarial, as they can typically only model failure of a human to perform a required action.

Additionally, traditional methods used in PRA are insufficient for analyzing holistic digital risk in early design phases because consequences are limited to the health and safety of the public. Other consequences, such as generation loss or equipment damage, are not considered. Furthermore, PRAs are typically performed on completed designs or existing facilities, rather than conceptual or partial designs. These completed designs are specified at a high level of detail providing thousands of distinct cut sets (e.g., combinations of component failures, human errors, system outages, etc.) that could cause a given scenario.

Moreover, quantification of the likelihood of security-related scenarios has long been recognized as a fundamental challenge. The original Nuclear Regulatory Commission (NRC) safety goal policy explicitly excluded comparison of physical security risks with safety goals noting that there was no basis on which to provide a measure of risk related to the possible effects of sabotage or theft of special nuclear material (SNM) [8]. Thus, the ability to analyze risk using PRA during early design phases is challenging, especially given that the purpose of early design phase digital risk analysis is to decide on solutions or risk treatments to engineer sufficiently low-likelihood for severe-consequence scenarios rather than performing judgement-based assessments on likelihood.

Therefore, a new approach is needed to analyze digital risk during early design phases of nuclear engineering projects. The challenge is to understand the behavior and risks of new reactors and new reactor applications (e.g., integrated energy systems) to identify a higher-level, less detailed, more qualitative approach to digital risk to enable the capability to design for performance, safety, and security. This paper begins to address this gap by first describing information flow and then proposing a new approach for holistically understanding the threats, vulnerabilities, and consequences in nuclear digital I&C systems.

# 2. NEW APPROACH FOR UNDERSTANDING DIGITAL RISK

## 2.1. Information Flow

System-theoretic process analysis (STPA) is a digital risk analysis technique that views accidents as resulting from unsafe control actions corresponding to flaws in, or failures of, a control structure leading to violations of constraints that enforce design intent (or function) [9]. In STPA, the term "unsafe" refers to actions whose affects are adverse to design intent; thus, the term unsafe in STPA includes safety but is not limited to safety. The Electric Power Research Institute's hazards and consequence analysis (HAZCADS) approach combines STPA with a PRA-based fault tree to derive conditional adverse impacts from a digital asset's unsafe control action [10]. While these techniques provide useful insights for digital risk, they are cumbersome to implement in a large facility and may be challenging to implement during early design phases.

A hazard and operability (HAZOP) study is a risk management technique used in the process industry in which a multi-disciplinary team carries out a structured analysis of a system, process, or operation to identify deviations from the intended design that could lead to potential hazards [11]. In a HAZOP, the team evaluates segmented sections of the process to identify deviations (e.g., more flow), causes for the deviation (e.g., valve opens), and the potential consequence of the deviation (e.g., reactor power increases leading to further impact). The team can further evaluate the cause of the deviation as it relates to modification of information or data (e.g., valve opens due to command from I&C system).

It is important to understand the concept of information flow in an I&C system. Information is derived from data. Data in a digital I&C system includes data that is processed, stored, and transmitted. This data may be in analog or digital format and includes data such as sensor data (e.g., pressure, temperature, or flow values), calculated/converted data (e.g., programmable logic controller data, analog to digital conversion, digital to analog conversion), control system commands (e.g., open/close valve, start/stop pump), human machine interface data (e.g., monitored values, trendlines, alerts), computer and application data, and network data. Operational technology (OT) data at a nuclear facility also includes physical protection system data required for monitoring and control of the security system (e.g., door sensors, cameras, detectors, central alarm station computers and monitors). Additionally, data may be present in different formats or protocols based on the system and application. Information flow is, therefore, flow of this OT data between and throughout a system, system of systems, and interconnected systems.

Consider, as an example, an integrated energy system (IES) in which an SMR provides thermal heat to industrial processes via thermal storage and electricity to the bulk electric system (BES) interconnected to renewable energy sources. Figure 1 shows a simplified, notional IES in which a nuclear steam supply system (NSSS) provides steam and electricity to interconnected assets. Examples of information flowpaths for these interconnections are overlaid in dashed lines.

In this example, high-pressure steam is directed to the turbine generator or thermal storage based upon the position of the bypass valve. The control knob implies there are influences on reactor power other than demand from the grid or thermal storage. For instance, as shown in Figure 1, status information for planning purposes (e.g., planned or forced outages) may influence I&C system settings. Understanding the entire set of information flow in a system or interconnected system and the potential impacts from disruption, degradation, falsification, destruction, or loss of this information is necessary to identify functional constraints, design requirements, and security concerns.

For instance, information flow may involve a range of time scales. If a reactor trip quickly separates the SMR from the BES, there is likely an immediate need for the balancing authority to rapidly recover and rebalance the load and supply on the BES. This could include requesting other energy suppliers to ramp up generation. In comparison, a planned shutdown will proceed much slower and will not require such an immediate response. Similar to energy supply, energy demand may also have a range of time scales. For

example, while long-term forecasts will enable generation planning, an interconnected industrial facility may unexpectedly go offline or ramp up production requiring faster changes to SMR output. Additionally, market forces, contractual obligations, and economic decisions may impact both supply and demand.

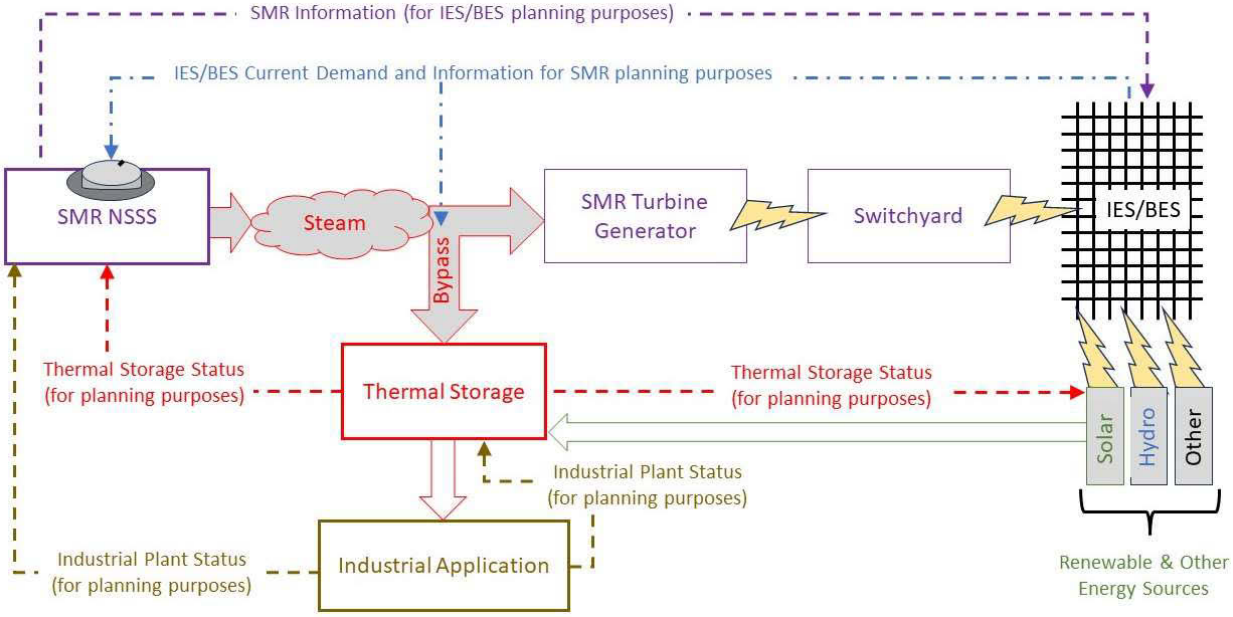


**Figure 1. Information flow for a notional IES, internal and external to the SMR.**

The various information flows in an IES require consideration of both adversarial and non-adversarial incidents. It is important to recognize that one set of constraints and requirements may not adequately preclude both types of incidents. Understanding these concerns is necessary during early design phases so competing requirements and competing objectives can be appropriately analyzed in a digital engineering decision analysis framework. For example, consider how a performance objective may negatively influence a security objective on the notional IES in Figure 1. There may be a requirement to monitor and control the SMR and integrated industrial application from one system in one central location. This tighter coupling may lead to improved communications and system performance but may inherently increase the digital risk to the SMR and interconnected facilities due to the introduction of new pathways.

## 2.2. Digital Risk Scenario Classification

Risk can be viewed more broadly as the potential for performance shortfalls relative to management intent based on stakeholder requirements. Figure 2 provides a new approach for holistically considering digital risk. Rather than only focusing on public health and safety consequences or theft of SNM when critical digital asset functions are adversely impacted, the goal is to consider additional consequences, such as undesired impacts to worker safety, environmental damage, reduction in capacity factor, financial loss, and damage to organizational/industry reputation.

Figure 2 represents a systematic way of considering stakeholder requirements by recognizing the need to prevent the larger set of consequences occurring through scenarios omitted in traditional safety analysis. Moving from left to right through the tree structure corresponds to a class of scenarios, characterized by the symbols in Table I and the examples in Table II. These are potential tools for evaluating stakeholder requirements, recognizing there are likely different scenarios or sequences that can be identified for a given project or system. For instance, while D and P are defined as digital and physical “impacts” in this example, another analysis could evaluate D and P as “pathways” (e.g., digital-enabled attack, physical-enabled

attack). Regardless, during the design of new reactors and applications it is important to analyze both digital and physical impacts as well as digital and physical pathways to characterize overall digital risk.

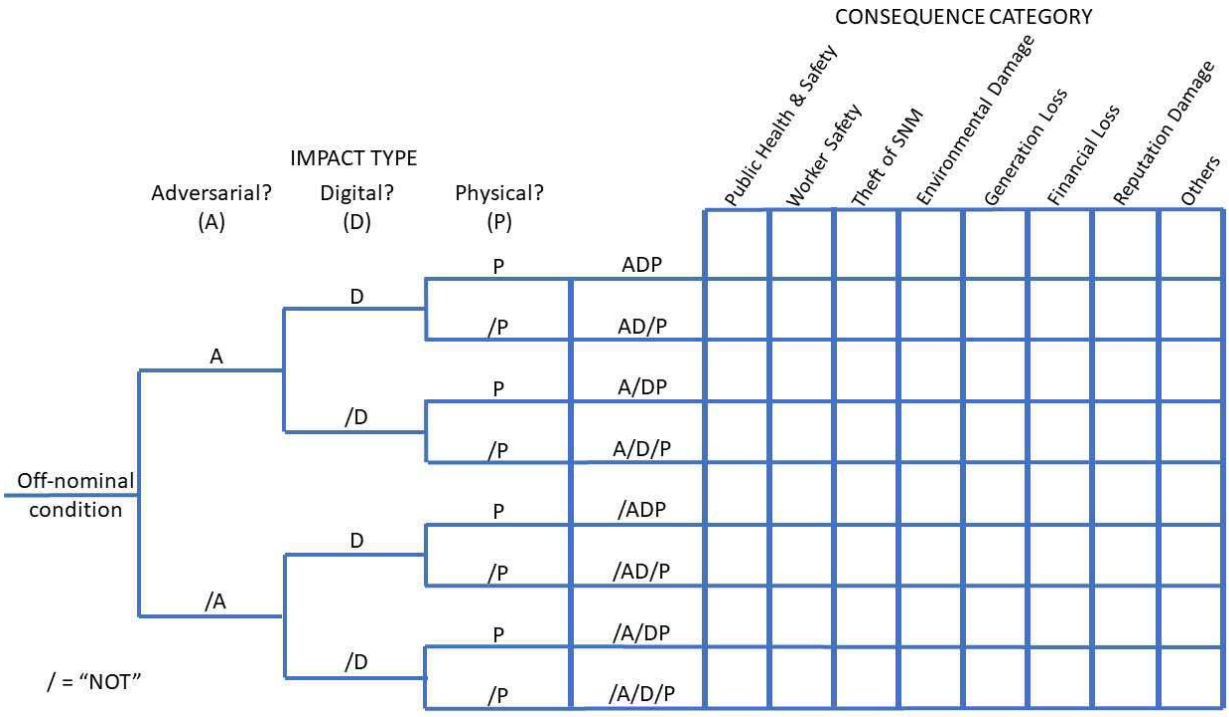


**Figure 2. Digital risk event tree with impact types and consequence categories.**

Much of the conventional wisdom regarding risk management views the decision problem (e.g., what actions are needed, if any, to manage risks) as being adequately handled with classical (utility-based) decision analysis. Within that paradigm, uncertainties are handled with probability distributions in which expected utility (or a convenient proxy) is calculated for each possible course of action, and the risk management actions taken are the actions that maximize expected utility. For example, it is unknown whether a large earthquake will occur in the future—in fact, there is very significant uncertainty about earthquake hazards—but the belief is that enough is known about earthquake likelihood to make rational risk management decisions.

**Table I. Description of each symbol indicated in Figure 2.**

| Symbol | Definition | Description |
|---|---|---|
| **A** | Adversarial action | Caused, at least partly, by a bad actor. |
| **/A** | Non-adversarial action | Not caused by adversarial means. For instance, caused by unintentional human actions, failure or degradation of components, or environmental hazards. |
| **D** | Impact to digital SSCs | Involves denial, degradation, disruption, or destruction of information flow, including failure of digital structures, systems, or components (SSCs) or corruption of data flow. |
| **/D** | No impact to digital SSCs | Information flow and digital SSCs are not impacted. |
| **P** | Impact to physical SSCs | Involves denial, degradation, disruption, or destruction of physical SSCs. |
| **/P** | No impact to physical SSCs | Physical SSCs are not impacted. |

**Table II. Scenario classes derived from Figure 2.**

| Sequence | Description | Examples |
|---|---|---|
| **ADP** | Adversarial attack with impact to both digital and physical SSCs | Adversary creates a denial-of-service attack to disrupt function of a feedwater controller, which results in automatic shutdown of a feedwater pump and plant trip. |
| **AD/P** | Adversarial attack with impact to digital SSC | Adversary gains access into an NPP digital I&C network to insert malware, which corrupts heat balance calculations. |
| **A/DP** | Adversarial attack with impact to physical SSC | An adversary sabotages a facility by drilling a hole in reactor coolant piping to cause a loss of coolant accident. |
| **A/D/P** | Adversarial attack with no impact to digital or physical SSC | An adversary gains access into a facility but is captured prior to adverse impact.<br>An adversary gains entry into a networked system but security information and event monitoring software flags the incident and personnel mitigate the situation before damage occurs. |
| **/ADP** | Non-adversarial incident with impact to both digital and physical SSCs | Digital I&C software is programmed incorrectly on a crane, which causes a load to fall.<br>Severe weather causes rain to leak into a building on top of a fire control panel, which results in short-circuit of the control panel and failure of the fire system to actuate. |
| **/AD/P** | Non-adversarial incident with impact to digital SSC | Unintentional human performance event in which the configuration of a network switch is improperly performed, allowing unauthorized access into network components. |
| **/A/DP** | Non-adversarial incident with impact to physical SSCs | An environmental event (e.g., earthquake, fire) occurs, which damages equipment.<br>Project personnel de-tension the reactor building in preparation to cut a hole for a steam generator replacement project, which results in delamination of the containment building. |
| **/A/D/P** | Non-adversarial incident with no impact to digital or physical SSCs | Normal plant operation. |

The problem is more complicated if the risks are due to adversarial or intentional actions. For instance, while earthquake likelihood is independent of political policies or criminal intentions, likelihood of adversarial action may be dependent on these political and socio-economic factors. In fact, security risk is often characterized by the knowledge, capability, intention, and motivation of the adversary and their ability to exploit vulnerabilities. It is very difficult to know what to believe about attack likelihood, and there is no reason to believe that attack likelihood is constant in time. Under these conditions, digital risk decisions based on likelihood are difficult if not impossible.

The entity relationship diagram in Figure 3 illustrates another way to consider digital risk. This diagram is an adaptation of the risk informed approach to computer security measures in IAEA NSS 42-G [12] and demonstrates how an adversary (bad actor) can intentionally exploit a vulnerability to adversely impact an asset and function leading to a high consequence event. Figure 3 also demonstrates how unintentional actions, non-adversarial events, and equipment degradation or failure can lead to a similar result. Adding protections, such as technical, physical, and administrative security controls, can reduce vulnerabilities. Use of cyber-informed engineering and nuclear safety-related design processes (e.g., design simplicity, defense

in depth, redundancy, diversity, physical separation, and electrical isolation) can reduce vulnerabilities as well as reduce loss or degradation of function. Additionally, detection and response capabilities may reduce the threat prior to an incident occurring or may reduce or prevent the loss of function upon incident occurrence by stopping incident propagation.

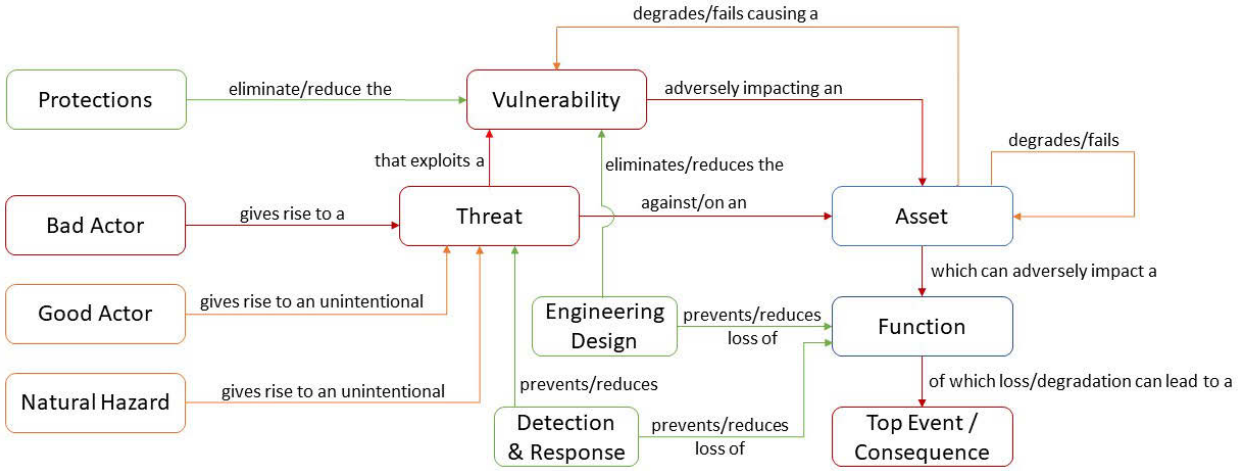


**Figure 3. Entity relationship diagram for digital risk (adapted from IAEA NSS 42-G).**

## 2.3. RIMES and Robust Decision-Making

For physical security, some researchers have advocated the Risk-Informed Management of Enterprise Security (RIMES) approach. RIMES is motivated, in part, by the fundamental challenges associated with using attack likelihood within a classical (utility-based) risk management paradigm. The history of classical approaches, and arguments against them, are summarized in a recent review article [7]. RIMES prioritizes scenarios for mitigation according to their consequences and the difficulty faced by an attacker in causing those consequences; "attack likelihood" is not explicitly invoked. The authors of RIMES argue that one does not, and cannot, know enough about "likelihood" to reason in the classical way. Similarly, in digital risk, both future adversarial and non-adversarial actions are unknown and difficult to model, leading to unsubstantiated assumptions about likelihood and the inability to quantifiably determine digital risk.

RIMES has been promoted as an approach for physical security, not cybersecurity in particular. RIMES presumably uses a large body of work for modeling "difficulty" in physical attacks while complementary data does not exist for cyber-attacks. However, the technique has certain items in common with other decision-analytic ideas that may be applicable to digital risk analysis. RIMES focuses on determining (and mitigating) scenarios with high consequences that are easier for adversaries to achieve; alternatively stated, the approach attempts to limit worst-case consequences an attacker can achieve at a given level of attack difficulty. Risk reduction in RIMES is predicated on the ability to eliminate the scenario, reduce the consequences if the scenario is successful, or make a successful scenario more difficult.

Another decision tool, robust decision-making (RDM), is an approach that informs decision-making under deep uncertainty. Deep uncertainty occurs when there is disagreement, lack of knowledge, or low confidence in the likelihood of future scenarios which is similar to those conditions found in predicting the likelihood of a cyber incident. RDM is an iterative process for decision-making that uses models and data to appropriately frame complex decisions by analyzing different sets of assumptions to describe how the plans perform in a range of plausible futures, considering trade-off and vulnerability analyses. RDM inverts the "predict-then-act" approach of PRA to an "agree-on-decisions" approach, eliminating the need to make predictions [13]. Thus, RDM supports the selection of robust, short-term actions that are consistent with long-term goals over many alternative futures [13].

Applying the RIMES concept of attack difficulty to cybersecurity is not yet formalized in literature. Similarly, there is not currently a body of knowledge on the use of RDM for decision-making in cybersecurity or digital risk. Therefore, there is unmet potential for using these techniques along with the concepts of information flow and multi-attribute digital risk (Figure 2) to holistically evaluate digital risk in early nuclear digital engineering project design phases.

## 3. DISCUSSION

While SMR vendors are constrained by the need to satisfy regulatory requirements aimed at preventing radiological release and theft of SNM, there are other competing objectives and competing stakeholder requirements impacting digital risk decisions that must be included in the project's overall engineering decision framework. Table III lists potential samples of mission-level, facility-level, and systems-level performance objectives for an SMR-driven IES.

**Table III. Examples of mission-level, facility-level, and systems-level performance objectives for an SMR IES.**

| Objective Level | Objective Examples |
|---|---|
| **Mission-Level** | • Optimization of the number of interconnected entities.<br>• Maximized participation of renewable energy sources on the IES. |
| **Facility-Level** | • Maximized profitability for the SMR and interconnected entities.<br>• Minimized entity/facility investments. |
| **Systems-Level** | • Optimization of the SMR steam bypass control.<br>• Optimization of the SMR and interconnected entity I&C systems. |

Each of these objectives can be translated into digital engineering questions. And, while most nuclear engineering projects focus on balancing performance, safety, and reliability, there is a need to incorporate and balance digital risk as part of the decision-making process during early design phases. Considering digital risk early in the systems engineering lifecycle will lead to risk reduction and/or elimination during design and enable integrated risk treatments, thereby reducing the need to add additional risk reduction measures after installation or operation.

It is anticipated that new SMRs and advanced reactors will be designed with passive-safety features that will reduce the overall number of safety systems with a reduced, or limited, emergency planning zone. However, even though the footprint of digital safety systems may be reduced (or eliminated) in new reactor designs, there is likely a greater interest in maintaining capacity factor of the SMR (i.e., supplying electricity to the BES) to ensure profitability and IES mission scope. The use of the broader multi-attribute risk analysis using impact and consequence types in Figure 2 enables digital risk evaluations for nuclear reactors to be expanded outside the current focus on maintaining safety, important-to-safety, security, and emergency preparedness (SSEP) functions. Incorporating a digital risk difficulty metric (i.e., difficulty of successful cyber-attack, difficulty of unintentional cyber incident) along with an RDM tool will provide further insights into overall digital risk. Goals of this novel digital risk analysis technique will be to:

1. Identify and prioritize high-consequence events (SSEP and non-SSEP) that should be addressed in early engineering design phases.
2. Evaluate information flows and identify adversarial and non-adversarial scenarios leading to unsafe control actions and/or deviations that may cause a high-consequence event (or adverse impact).
3. Identify measures that can make the scenarios more difficult to achieve, including both adversarial and non-adversarial scenarios.

## 4. CONCLUSIONS AND FUTURE WORK

Nuclear engineering projects involving digital I&C systems must balance performance, safety, reliability, and security by considering digital risk in overall mission, facility, and system objectives. Digital risk includes adversarial cybersecurity risk as well as non-adversarial risks arising from the digital nature of the I&C systems themselves. By detailing information flow within and between systems and facilities, project personnel can identify when disruption, degradation, falsification, destruction, or loss of information may result in a deviation or unsafe control action leading to an adverse impact. The modification to or loss of information flow could be from a cyber-attack, or it could be from a non-adversarial incident such as a human performance error. In either case, the result or consequence may be the same. Similarly, the ability to impact information flow can be prevented or reduced. For example, a successful cyber-attack may be more difficult with simplified designs incorporating security protection measures and a human performance error leading to an adverse impact may be more "difficult" to achieve with diverse and redundant designs. Future work will explore the development of a multi-attribute digital risk analysis technique that incorporates this concept of difficulty along with RDM to provide a higher-level, less detailed, more qualitative approach to digital risk that does not rely on quantifying attack likelihood.

## ACRONYMS

| | |
|---|---|
| BES | bulk electric system |
| HAZCADS | hazards and consequence analysis |
| HAZOP | hazard and operability study |
| I&C | instrumentation and control |
| IAEA | International Atomic Energy Agency |
| IES | integrated energy systems |
| NPP | nuclear power plant |
| NRC | Nuclear Regulatory Commission |
| NSSS | nuclear steam supply system |
| OT | operational technology |
| PRA | probabilistic risk analysis |
| RDM | robust decision-making |
| RIMES | Risk-Informed Management of Enterprise Security |
| SMR | small modular reactor |
| SNM | special nuclear material |
| SSC | structures, systems, or components |
| SSEP | safety, important-to-safety, security, and emergency preparedness |
| STPA | system-theoretic process analysis |

## ACKNOWLEDGMENTS

This research was funded by the U.S. Department of Energy Office of Nuclear Energy under DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

## REFERENCES


1. IAEA. *Power Reactor Information System (PRIS)*. Available: https://www.iaea.org/resources/databases/power-reactor-information-system-pris (2021).
2. S. Eggers and K. Le Blanc, "Survey of cyber risk analysis techniques for use in the nuclear industry," *Progress in Nuclear Energy,* **140** (2021).
3. NRC, "WASH-1400, NUREG-75/014, Reactor safety study: An assessment of accident risks in US commercial nuclear power plants," U.S. Nuclear Regulatory Commission, Washington D. C. (1975).
4. S. Kaplan and B.J. Garrick, "On the quantitative definition of risk," *Risk Analysis,* **1** (1), pp. 11-27 (1981).
5. NRC. *Probabilistic Risk Assessment (PRA)*. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html (2020).
6. J. Sandoval, "The use of the PRA risk equation in DOE security: A chronological history," Sandia National Laboratories (2014), Available: https://www.osti.gov/biblio/1140372.
7. G.D. Wyss and A.D. Williams, "Possible does not mean useful: The role of probability of attack in security risk management," *Nuclear Science and Engineering,* **197** (sup1), pp. S80-S94 (2023).
8. NRC, "51 FR 30028. Safety goals for the operations of nuclear power plants. Policy statement.," (1986).
9. A.D. Williams, "System Theoretic Process Analysis (STPA): Overview of Sandia uses to address national security problems," presented at the Conference: Proposed for presentation at the Boiling Water Reactor Owners Group Meeting held June 3-21, 2019 in Albuquerque, NM, United States., United States, 2019. Available: https://www.osti.gov/biblio/1645411
10. EPRI, "HAZCADS: Hazards and consequences analysis for digital systems," Electric Power Research Institute (2018).
11. F. Crawley and B. Tyler, *HAZOP: Guide to Best Practice (Third Edition)*. Elsevier (2015).
12. IAEA, "NSS 42-G, Computer security for nuclear security," International Atomic Energy Agency, Vienna (2021), Available: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.
13. R.J. Lempert, "Robust Decision Making (RDM)," in *Decision Making Under Deep Uncertainty: From Theory to Practice*, V. Marchau, W. Walker, P. Bloemen, and S. Popper, Eds.: Springer, Cham., 2019.