Nuclear Power Plant Cyber-Risk Assessment with Real-Time Reactor Operations
Topic Area 10 – Licensing, Safety, and Security

R. A. Borrelli (PI); Michael Haney (co-PI) – University of Idaho · Idaho Falls Center for Higher Education
Thomas A. Ulrich – Idaho National Laboratory

Summary of the Proposed Project

1. Proposed Research We propose to assess risk to safety and safe operations of the domestic Nuclear Power Plant (NPP) fleet due to cyberattacks (cyber-risk). The domestic fleet is a necessity to the energy independence and security of the United States. Cyber-risk assessment is required for NPP licensing and license extensions. Technically savvy or insider-aided adversaries can target vulnerable plant systems; the consequences of which will challenge safety to personnel and the public. We propose a novel, cyber-risk assessment that is *consequence*-based and can be integrated into a formalized Probabilistic Risk Assessment (PRA). We will use the Western Services Corporation (WSC) Pressurized Water Reactor (PWR) high fidelity experimental platform to simulate both real-time NPP operations and cyberattacks targeting plant systems to simulate cyberattacks on the WSC platform to generate much needed real-time results and assess overall plant risk for cyber hazards leading to a breach of physical safety. We will apply a Cyber-Informed Engineering (CIE) approach [1] to develop risk mitigation strategies. This proposed research into cyber-risk is an ongoing effort into the field of cybersecurity of critical infrastructure under the Adversary-As-A-Service (AAS) strategy at the Idaho Falls Center for Higher Education (UIIF).

2. Motivation Cyberattacks against critical energy infrastructure have gone from possible to eventual to actual. Now, they occur with alarming regularity [2], costing billions of dollars in damages and productivity loss. Gartner analysts starkly predict [3] – '*By 2025, threat actors will have weaponized operational technology environments successfully enough to cause human casualties.*' A casualty at a NPP would be catastrophic. In this unstable world climate, energy independence from foreign oil should be a high national security priority of which maintaining the domestic nuclear fleet is critical. Extension of NPP lifetimes into the 2050s will result in a hybrid mixture of analog and digital technologies that will invariably challenge plant risk and regulatory compliance.

3. Importance & Relevance to Office of Nuclear Energy Objectives Project outcomes will enhance understanding of licensing and safety requirements to create a better cyber-informed PRA for the new threat landscape though the use of an innovative risk assessment methodology. This project is relevant to the Office of Nuclear Energy (NE) mission to keep existing United States (US) nuclear reactors operating and secure and sustain our nuclear fuel cycle. This project is a collaboration between a national laboratory and a university.

4. Background

4a. NRC guidance NRC addresses cybersecurity in 10CFR73 (2009) and RG5.71 (2010). 10CFR73.54 requires protection of digital computers, communications systems, and networks. However, guidance is reactive; focused on remediation once vulnerabilities are found [4]. Cyberattacks are *malleable* in that a single one could hit multiple targets, or multiple attacks could hit a single target. There has not been an evaluation of what classes of cyberattacks are feasible in a nuclear plant, what targets are vulnerable, and to what degree.

4b. Risk-informed paradigm NRC assesses risk by addressing the seminal three questions [5] – (1) What can go wrong? (2) How likely will it happen? (3) What are the consequences? Quantifying risk as a pure number or multidimensional function facilitates comparisons across different systems. Mitigation involves designing redundant and diverse systems and multiple barriers that provide defense-in-depth. NRC suggests

five principles for assessing risk (Fig. 1). Translating these principles to the cyberdomain is a challenge. A cyberattack is a binary event; it either 'hits' or fails. However, the *attempts* are limitless.

4c. Related research Literature focused on recently funded NEUPs relevant to cybersecurity were surveyed. Due to the current page limit, a full summary will be provided if the preproposal is invited. There were seventeen citations investigated. Overall, the NPP cybersecurity landscape focuses on detection and defense. Current approaches lack a focus on safety-related consequences and quantitative risk determination [7]. Major cyberattack incidents at NPPs and other critical infrastructure is summarized in Ref. [8].

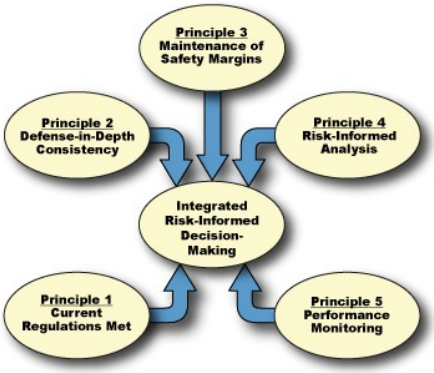

Fig. 1. NRC risk [6].

5. Methodology

5a. Adversary-As-A-Service (AAS) AAS is an innovative cybersecurity methodology that applies physical systems with realistic internet-scale cyberattacks [9]. AAS is novel to the cybersecurity field because we can deploy real-time cyberattacks using using adversarial cyberattack tools and techniques to test the defenses of a given system or technology deployment. We will use the WSC platform to assess NPP vulnerabilities, where the consequences thereof can be directly observed and quantified [8].

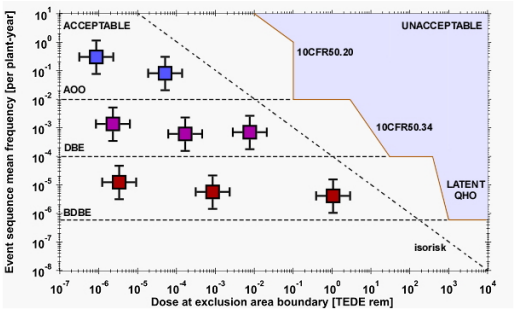

Fig. 2. Notional Farmer's chart.

5b. Visualizing cyber-risk Assessing cyber-risk is challenging. Traditional PRA is frequency-based with a single consequence; e.g., dose exposure. Assuming a cyberattack frequency of unity; i.e., it hits, the risk is then solely derived from the consequences. Defense-in-depth and multiple barriers still provide mitigation. A notional Farmer's chart [10] is shown in Fig. 2. The colored boxes represent hazards with uncertainty bars. Events are classified by frequency (based on NRC regulations) – (1) Anticipated Operational Occurrences (AOOs) – Frequent with low consequences, (2) Design Basis Events (DBEs) – Less frequent with moderate consequences, (3) Beyond Design Basis Events (BDBEs) – Rare with very high consequences. Cyber-risk has to be assessed within these classifications. We intend to use the WSC platform to formulate an augmented Farmer's chart that could characterize cyber-risk within PRA while capturing malleability.

5c. Cyber-Informed Engineering Cyber-Informed Engineering (CIE) fundamentally draws on the risk-informed paradigm to mitigate cyber-risk [1]. CIE is inherently predicated on expert knowledge of the system to identify critical threat vectors [11]. Incorporating defense-in-depth for cyber-risk reduction will involve knowledge of cyberattack vectors and system response *a priori*.

5d. Penetration testing Proof-of-concept has been established to simulate cyberattacks on the WSC platform [8]. By completing a 'three way handshake' and achieving a TCP/IP hijack, cyberattacks can be initiated in real-time during reactor operation on the WSC platform.

Major Outcomes & Deliverables

Workscope 1 – Regulatory analysis.

Task I. Identify gaps in NRC regulations for cyberattacks.

Task II. Determine risk metrics affected by cyberattacks.

Milestone 1. *Establish how cyberattacks challenge, safety, regulatory compliance, and licensing.*

Investigator duties

Borrelli – Gap analysis; Risk metrics.

Haney – Feasibility of cyberattacks.

Ulrich – Risk metrics; Licensing.

Workscope 2 – Cyberattack risk analysis.

Task III. Construct cyber motivated Preliminary Hazards Analysis (PHA). (1) Based on our established approach [8], apply a cyber motivated PHA for plant systems focusing on component, systems damage affecting plant safety. (2) Conduct Delphi analysis with plant personnel to verify results.

Task IV. Conduct Failure Modes and Effects Analysis (FMEA) on system targets. (1) Define a failure mode as a specific cyberattack vector on a specific system. (2) Establish consequences per vector. (3) Determine detectability of vector. (4) Assign a Risk Priority Number (RPN) per vector.

Milestone 2. *Determine and quantify plant systems vulnerable to cyberattacks that challenge safe plant operations.*

Investigator duties

Borrelli – PHA; FMEA; RPN.

Haney – Failure modes (vectors).

Ulrich – Verify practicality of FMEA & RPN; Delphi analysis.

Workscope 3 – Cyberattack execution & Experimentation.

Task V. Cyberattack execution. (1) Determine means of cyberattack based on vectors. (2) Prepare attack graphs per vector.

Task VI. Establish operations suite for cyberattack experimentation.

Task VII. Operate WSC subject to cyberattacks. (1) Set up virtual machines for WSC and cyberattack adversary. (2) Execute vectors during WSC operation. (3) Observe consequences – physical damage, safety (regulatory) violations. (4) Collect relevant operational data. (5) Compare results to predictions from FMEA.

Milestone 3. *Execute cyberattacks on selected targets to determine challenges to safe operations.*

Investigator duties

Borrelli – Attack graphs; Operations suite; WSC operation; Operations analysis.

Haney – Cyberattack execution; Attack graphs; Operations analysis.

Ulrich – Operations suite; Operations analysis.

Workscope 4 - Cyber-risk assessment.

Task VIII. Compile system risk. (1) Define a consequence-based metric for cyberattacks. (2) Develop augmented Farmer's type charts for cyberattacks, consequences. (3) Establish cyber defense-in-depth mitigation strategies.

Task IX. Risk mitigation. (1) Incorporate defense-in-depth strategies into WSC platform. (2) Operate WSC platform under cyberattacks. (3) Determine risk based on mitigation strategies.

Task X. Regulatory compliance. (1) Compare results to existing regulations to assess compliance (licensing). (2) Determine effect of cyberattacks on existing risk metrics. (3) Suggest new risk metrics.

Milestone 4. *Quantify cyber-risk and assess regulatory compliance.*

Investigator duties

Borrelli – Cyber-risk assessment; Defense-in-depth; Operations; Compliance; Risk metrics
Haney – Cyber-risk assessment; Defense-in-depth; Compliance; Risk metrics
Ulrich – Cyber-risk assessment; Compliance; Risk metrics

Workscope 5 - Crosscutting discussions & Follow on activities.

Task XI. Identify lessons learned. (1) Lessons learned will be applied to identify technical gaps and uncertainties related to regulatory compliance and licensing.

Task XII. Develop future work. (1) Pathways to testing on a specific NPP control room simulator. (2) Application to advanced nuclear energy systems. (3) Develop additional experimental approaches for cyber-risk assessment. (4) Engage the community in future partnerships for ongoing research.

Task XIII. Reproducibility & validation (R&V). (1) Reproducibility – Engage with colleague Prof. Fan Zhang [12] with the iFAN WSC platform. (2) Validation – Engage with colleague Dr. Ronald L. Boring [13] with the Human System Simulation Laboratory.

Milestone 5. *Apply lessons learned for future research and engage colleagues in new collaborations.*

Contribution to Advancing State of the Art

We will advance the state-of-the-art in NPP cyber-risk assessment to – (1) Develop a novel framework for cyber-risk assessment within the context of PRA; (2) Establish new risk metrics to capture cyber-risk malleability; (3) Demonstrate visualization for cyber-risk.

Team Synergy Profs. Borrelli and Haney extensively collaborate [2, 4, 8, 14, 15] and lead the State of Idaho in this field. Research includes – (1) Integrating risk due to cyberattacks into PRA, (2) Simulating a Man in the Middle (MITM) cyberattack on an experimental setup using OpenPLC for boric acid controls with mitigating strategies, and (3) Formulating cyberwar nonproliferation policy and technical approaches to cyberweapons attribution. Prof. Haney is the Idaho State Board of Education program manager for the Idaho Cybersecurity Education Initiative. He leads the effort to create standardized cybersecurity curricula across all eight public postsecondary institutions.

Unique Project Features The WSC platform installed and operational at UIIF with a two seat license. The platform provides real-time, reactor operation. A full-featured trending system can monitor multiple operational transients. The developers license and source code provide innovative capabilities that allow for cybersecurity incidents to be coded and input for simulation during reactor operation. Combining expertise in nuclear engineering modeling and simulation with cybersecurity from within the computer science discipline provides robust synergy to develop an innovative cyber-PRA methodology and mitigation strategies.

Estimated Cost of the Project

The maximum amount of $1,000,000 is requested for the full time period. A detailed budget will be provided upon submission of the full proposal. The project timeline is provided in Table 1.

Table 1. Timeframe for Execution

TASKS	Y1				Y2				Y3			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
I. Regulatory gaps												
II. Risk metrics												
III. PHA												
IV. FMEA												
V. Cyberattacks												
VI. Operations suite												
VII. Operate WSC												
VIII. System risk												
IX. Risk mitigation												
X. Compliance												
XI. Lessons learned												
XII. Future work												
XIII. R&V												

References

[1] United States Department of Energy, 2022. National cyber-informed engineering strategy. Office of Cybersecurity, Energy Security, and Emergency Response.

[2] Haney, M., et al., 2021. Cyberweapon Nonproliferation Controls for the Virtual Battlefield - Applying the Nuclear Nonproliferation Regime to an Unseen Enemy. Washington, D. C.: Proc., American Nuclear Society Winter Meeting.

[3] Panetta, K., 2021. The Top 8 Cybersecurity Predictions for 2021-2022. Gartner.

[4] Peterson, J., et al., 2019. An overview of methodologies for cybersecurity vulnerability assessment conducted in nuclear power plants. Nuclear Engineering and Design 346, 75.

[5] Kaplan, S. et al., 1981. On the quantitative definition of risk. Risk analysis 1, 11.

[6] United States Nuclear Regulatory Commission (NRC), 2020. Risk and Performance Concepts in the NRC's Approach to Regulation.

[7] Eggers, S. et al., 2021. Survey of cyber risk analysis techniques for use in the nuclear industry. Progress in Nuclear Energy 140, 103908.

[8] Root, S. J., et al., 2023. Cyber Hardening of Nuclear Power Plants with Real-time Nuclear Reactor Operation - 1. Preliminary Operational Testing. Progress in Nuclear Energy 162, 104742.

[9] Jillepalli, A. A., et al., 2019. Formalizing an Automated, Adversary-aware Risk Assessment Process for Critical Infrastructure. In: 2019 IEEE Texas Power and Energy Conference (TPEC). 1.

[10] Farmer, F. R., 1967. Reactor Safety and Siting: A Proposed Risk Criterion. Nuclear Safety 8, 539.

[11] Tudor, Z., 2020. A focused approach to cybersecurity. Cyber Security Review.

[12] Zhang, F. et al., 2022. Overview and recommendations for cyber risk assessment in nuclear power plants. Nuclear Technology , 10.1080/00295450.2022.2092356.

[13] Boring, R., et al., 2017. Analog, digital, or enhanced human system interfaces? Results of an operator-in-the-loop study on main control room modernization for a nuclear power plant. INL/EXT-17-43188.

[14] Root, S. J., et al., 2022. Simulated boron shimming cyber-attack on pressurized water reactor. Phoenix, Arizona: Proc., American Nuclear Society Winter Meeting.

[15] MacLean, T., et al., 2019. Cybersecurity modeling of non-critical nuclear power plant digital instrumentation. Critical Infrastructure Protection XIII, J. Staggs, S. Shenoi, eds. Chapter 15, 277.