A Conceptual Risk Assessment Framework for Nuclear Power Plants Coupled with Data Centers

Stefano Marchetti[a] and Katrina M. Groth[a]
[a]Systems Risk and Reliability (SyRRA) Lab, Center for Risk and Reliability, Reliability Engineering, University of Maryland, College Park, 20742, MD, USA.
Emails: smachet@umd.edu and kgroth@umd.edu

Abstract: The rapid growth of Artificial Intelligence (AI) and cloud computing infrastructure is driving an unprecedented increase in electricity demand from data centers. Nuclear Power Plants (NPPs) are increasingly being considered as reliable low-carbon energy sources capable of supplying the firm baseload power required by these facilities. However, the co-location of NPPs with data centers introduces new hazards arising from operational coupling, shared cooling and backup systems, and cybersecurity threats. Existing Probabilistic Risk Assessment (PRA) methodologies for nuclear installations explicitly account for component and system reliability within plant boundaries, but they do not typically consider tightly integrated external infrastructures whose operational behavior may influence nuclear safety through electrical, thermal, and cyber dependencies. To overcome these limitations, this work proposes a conceptual framework for extending nuclear PRA to account for the integration of data center infrastructures as coupled external systems. Adopting a system-of-systems perspective, the framework models data centers as dynamic semi-dispatchable loads and captures the shared electrical and thermal dependencies among the systems. The additional cybersecurity risk arising from operational coupling is incorporated by extending the initiating event set to include cyber-induced plant disturbances, such as load rejections and voltage transients resulting from compromised digital control pathways. The framework provides a foundation for risk-informed deployment and operation of data centers powered by NPPs.

1. Introduction

The rapid development of Artificial Intelligence (AI) and cloud computing infrastructure is causing a major increase in electricity demand from data centers, which are projected to consume up to 6-12% of U.S. electricity by 2028 [1], creating the need for reliable, low-carbon, and dispatchable power sources. Nuclear Power Plants (NPPs) are increasingly being considered to supply this demand, thanks to their large capacity factors and stable electricity generation [2]. In particular, the development of small modular reactors enables enhanced operational flexibility, making nuclear systems well suited to accommodate the variable power requirements of large-scale data centers. However, the integration of NPPs with data centers introduces new operational and infrastructural interdependencies [3]. Data centers have strict availability and power-quality requirements that must be maintained to ensure continuous operation of latency-sensitive AI workloads [4]. To meet these requirements, automated operational responses, such as rapid load rejection or voltage ride-through protection may be activated in response to grid or facility disturbances, resulting in rapid downstream load variations that propagate through the shared electrical interface and induce NPP operational transients, potentially affecting plant safety margins. Furthermore, shared resources (e.g., cooling systems), electrical coupling configurations, and cyber-physical interfaces required for monitoring and control also introduce new risk pathways [5]. As a result, failures originating in the data center or in the coupling infrastructure, including both random failures and cyber-attacks, may propagate through complex dependency chains and affect nuclear safety. Accurately capturing these cross-system interactions is therefore essential for assessing the impact of the coupling on plant risk.

Probabilistic Risk Assessment (PRA) has long been used to evaluate the safety of nuclear power plants, typically relying on event trees and fault trees to model accident sequences and system failures ([6], [7]). While these approaches provide a well-established framework for risk quantification, they are limited in their ability to represent complex dependencies across tightly coupled systems. At the same

time, reliability modeling of data centers has largely been developed independently, without explicitly considering their integration with nuclear systems ([8], [9], [10], [11]).
In this context, Bayesian Networks (BNs) provide a suitable modeling framework because they allow the representation of cross-system causal dependencies, support probabilistic inference under uncertainty, and enable the integration of heterogeneous sources of information such as expert knowledge and simulation data [12]. BNs have been widely applied in risk and reliability engineering to enhance traditional PRA approaches ([13], [14]). In particular, they have been used to represent complex dependencies among components and failure mechanisms [15], model human reliability ([16], [17], [18]), and account for the aging of safety systems ([19], [20]). This work leverages the capabilities of BNs to propose a conceptual framework for the PRA of NPPs coupled with data centers. The BN structure is expert-defined to explicitly capture the causal relationships linking component failures and cyber-attacks in the data center and coupling infrastructure to nuclear initiating events and their progression to core damage. The BN conditional probability tables can be characterized using both expert knowledge and data-driven learning. Epistemic uncertainty is accounted for through probabilistic parameter representations. In addition to estimating the impact of coupling in terms of Core Damage Frequency (CDF), the framework enables the identification of critical components and cyber vulnerabilities, as well as the extraction of the most probable causal paths leading to core damage. The present work focuses on the conceptual formulation of the framework; detailed parameterization, validation, and quantitative application are outside its scope.
The proposed approach aims to extend traditional PRA by providing a unified and interpretable framework for analyzing risk in coupled cyber-physical energy systems. By explicitly modeling cross-system dependencies and supporting causal analysis, the framework can support early-stage design evaluations and risk-informed decision-making for emerging NPP-data centers integrated configurations.
The remainder of the paper is organized as follows: Section 2 presents the problem formulation, Section 3 describes the proposed conceptual framework, Section 4 discusses the framework capabilities and suitability and in Section 5, conclusions are drawn.

2. Problem formulation

The coupling of nuclear power plants with data centers creates an integrated system in which disturbances originating outside the nuclear power plant may affect its safety. Unlike conventional off-takers, data centers can behave as large, dynamic loads whose operating conditions, automated responses, and support infrastructures may interact with the plant through electrical, thermal, and cyber-physical interfaces. The problem addressed in this work is therefore the extension of nuclear PRA to represent and assess the additional risk introduced by such coupling.

2.1. Coupling-induced risk mechanisms

A coupled system is considered in which the nuclear power plant supplies electricity to the data center and may also provide steam for cooling. In these configurations, the data center is not treated as a passive external load, but as a coupled infrastructure whose operating conditions, control actions, and failure modes can influence overall plant operation and safety. The coupling may introduce electrical dependencies, thermal dependencies, shared support systems, and cyber-physical interfaces for monitoring and control. From a risk perspective, these interdependencies create additional pathways through which disturbances originating in the data center or in the coupling infrastructure may propagate to the nuclear side. Examples include rapid load variations induced by data center-side failures or control actions, disruptions affecting shared cooling systems, and cyber-attacks. These disturbances may in turn trigger plant-level transients or abnormal conditions, alter the availability of safety functions, and affect the progression of accident sequences. As a result, the coupled system must be analyzed as an integrated energy system in which failures and disturbances can propagate across infrastructure boundaries.

2.2. Risk assessment objective and modeling requirements

The objective of the proposed framework is not to perform a full PRA of the integrated system, but rather to quantify the impact of the coupling on nuclear safety. Specifically, the framework is intended to estimate the increase in core damage frequency associated with the introduction of the coupled data

center infrastructure, relative to a baseline configuration without coupling. To support this objective, the framework must satisfy three requirements. First, it must enable the systematic identification of coupling-induced hazards and their mapping to nuclear initiating events. Second, it must represent electrical, thermal, and cyber dependencies within a unified probabilistic structure capable of modeling the propagation of failures from the data center and coupling infrastructure to plant-level safety outcomes. Third, it must support risk-informed interpretation by accounting for epistemic uncertainty and by providing interpretable outputs, including the identification of influential contributors to risk and the most plausible causal paths leading to core damage.

3. The proposed framework

Consider a Nuclear Power Plant (NPP) coupled with a data center through electrical and thermal interfaces, supplying electricity and steam for heat-driven cooling via an absorption chiller [21]. Since the objective is to assess the increase in nuclear risk induced by the coupling, rather than to perform a full PRA of the integrated system, the analysis focuses on the data center, the coupling infrastructure, the associated safety systems, and cyber-attacks targeting these elements.

The proposed framework consists of three main steps (**Fig. 1**):

1. identification and characterization of the hazards introduced by the coupling;
2. definition and parameterization of the BN model;
3. estimation of the CDF increase, identification of the most influential contributors and extraction of the most probable causal paths leading to core damage.

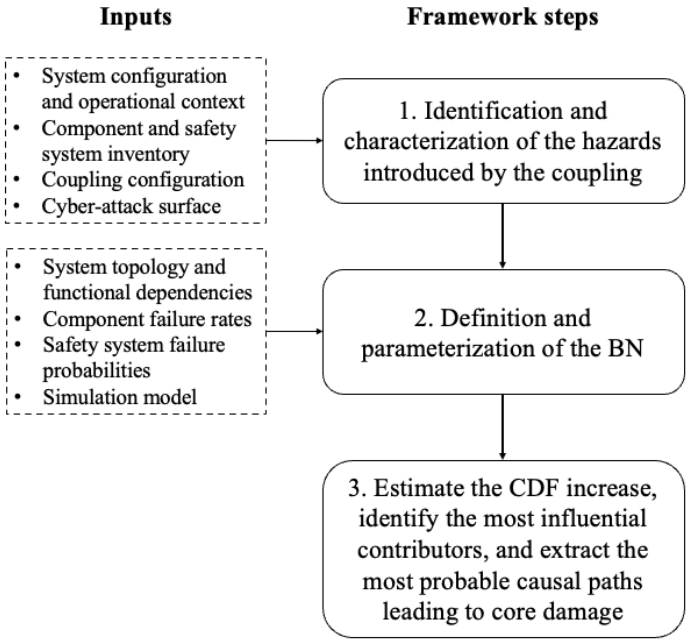

Figure 1: Steps of the proposed framework.

3.1. Identification and characterization of the hazards introduced by the coupling

The first step consists of identifying and characterizing the hazards introduced by the coupling between the nuclear power plant and the data center. These hazards are defined as failures originating in the data center or in the coupling infrastructure that may affect nuclear power plant operation and safety. Hazard identification can be performed using established system safety analysis methods, such as Failure Modes and Effects Analysis and Functional Hazard Analysis, which support the systematic identification of failure modes, affected system functions, and associated preventive and mitigative safety systems ([22], [23]). The identified hazards are then analyzed to determine whether they can induce plant-level transients or abnormal conditions and are then mapped to the corresponding nuclear initiating events, consistently with standard PRA practice [6]. Cyber-attacks are also considered through a complementary hazard identification step, since they may act as triggering mechanisms for the same initiating events. The resulting set of hazards, safety systems, and cyber-induced disturbances provides the input for the subsequent modeling steps.

3.2. Definition and parametrization of the BN model

The second step concerns the definition of the BN structure and its CPTs. The BN is constructed to represent the causal relationships from component failures and cyber-attacks to NPP initiating events, and from initiating events to core damage. The node categories considered in the framework are reported in **Tab. 1**.

Table 1: BN node categories.

Node category	Description
Data center size	Percentage of the nuclear power plant power needed to operate the data center at peak utilization
Shared cooling	Presence of shared cooling infrastructure between the nuclear power plant and the data center
Cyber-attack	Occurrence of a cyber-attack affecting components or safety systems
Component	Physical components belonging to the data center or to the coupling infrastructure
Safety system	Safety systems responsible for preventing or mitigating accident scenarios
Initiating Event	Events that initiate accident sequences in the nuclear power plant
Core Damage	Occurrence of core damage

The high-level BN structure, shown in **Fig. 2** for a generic initiating event, follows the logical progression from component failures to core damage while explicitly representing the underlying causal relationships. Component failures and cyber-attacks are linked to the corresponding initiating events together with the relevant safety systems. The initiating events are then connected to the core damage node together with configuration-related nodes, such as data center size and the presence of shared cooling. The BN structure is constructed to reflect standard PRA logic, and its consistency is verified by ensuring that the modeled dependencies reproduce the expected propagation from component failures to initiating events and from initiating events to core damage.

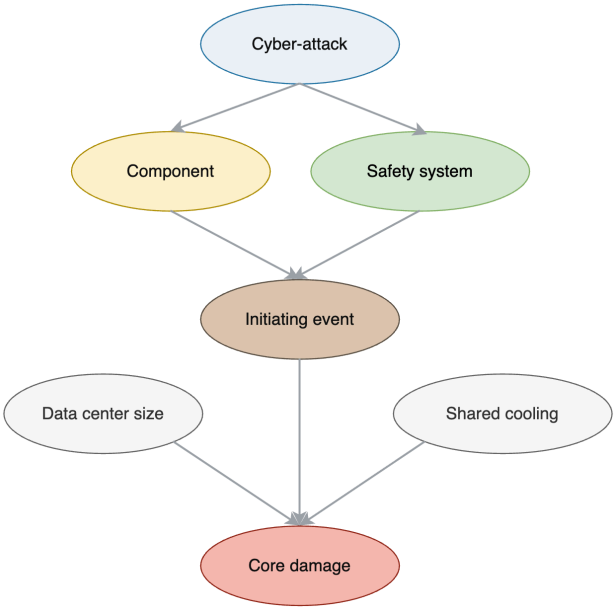

Figure 2: High-level structure of the BN model.

Regarding the CPTs of the BN, the proposed framework supports their characterization using both expert elicitation and data-driven learning [24]. In this way, the framework allows combining engineering knowledge, probabilistic modeling, and simulation-informed learning within a unified structure.

3.3. BN-based risk, importance, and causal analyses

Once defined and parameterized, the BN is used to support three complementary analyses.
First, it enables the estimation of the increase in core damage frequency due to the coupling by conditioning the network on the selected coupling configuration and evaluating the probability of core damage. This allows comparison with the baseline configuration (i.e., without coupling) and with applicable risk acceptance criteria. Second, the BN supports importance analysis to identify the component failures and cyber-attacks that contribute most to the increase in risk. This provides a basis for prioritizing mitigation measures and identifying critical coupling-related vulnerabilities. Third, the BN supports causal analysis through most probable explanation inference ([25], [26]), allowing the extraction of high-probability combinations of failures, initiating events, and safety system states that lead to core damage. These causal paths provide interpretable insight into the mechanisms through which disturbances originating in the data center and coupling infrastructure can affect nuclear safety.

4. Discussion

The proposed conceptual framework is designed to represent the dependencies between nuclear power plants and data centers, enabling the explicit modeling of failure propagation from the data center and the coupling infrastructure to plant-level initiating events. This allows the analysis of how disturbances originating outside the nuclear power plant can influence plant-level safety outcomes within a unified probabilistic structure. In addition, the framework supports the integration of heterogeneous sources of information, including system knowledge, failure data, and simulation outputs, enabling the characterization of BN parameters through both expert elicitation and data-driven learning. This is particularly relevant for coupled systems, where limited operational data are available and simulation-based approaches are required to explore a wide range of operating and failure scenarios.
The framework also supports the explicit treatment of epistemic uncertainty through probabilistic modeling of BN parameters, which is a key requirement for risk-informed decision-making in early design stages. Finally, the use of probabilistic inference also supports importance measure analyses to identify the most influential components and cyber-attacks, as well as the extraction of the most likely causal paths leading to core damage. These capabilities enable interpretable outputs that support not only risk quantification but also the identification of key risk contributors and the understanding of the mechanisms through which coupling may affect nuclear safety.

5. Conclusion

This work proposed a conceptual BN-based framework for the PRA of nuclear power plants coupled with data centers, with the objective of quantifying the impact of operational interdependencies and cyber-attacks on plant safety. The proposed approach represents operational interdependencies, shared-support-system interactions, and cyber-induced disturbances within an interpretable probabilistic structure, enabling estimation of coupling-related changes in core damage frequency. The framework also supports the treatment of epistemic uncertainty, importance analysis, and causal-path extraction, thereby providing insight into the mechanisms through which external infrastructure can affect nuclear plant safety. Rather than replacing established PRA methods, the framework extends them by offering a structured means to represent cross-system dependencies that are difficult to capture with conventional methods. As such, it can support early-stage design screening, comparison of coupling configurations, and risk-informed decision-making for emerging integrated energy systems.

Acknowledgements

This research is funded in part by the Department of Energy's Nuclear Energy University Program (NEUP) under grant DE-NE0009406. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] A. Shehabi, S. Smith, D. Sartor, and R. Brown, “LBNL-2001637 2024 United States Data Center Energy Usage Report,” Berkeley, CA, USA, Dec. 2024. doi: 10.71468/P1WC7Q.
[2] U.S. White House, “Deploying Advanced Nuclear Reactor Technologies for National Security,” *Executive Order 14299*, May 2025.

[3] P. Talbot *et al.*, “Navigating Integration: Key Challenges for Data Centers, Nuclear Stakeholders, and Utility Operators (INL/RPT-25-87663),” Idaho Falls, ID, USA, Aug. 2025.
[4] K. M. U. Ahmed, M. H. J. Bollen, and M. Alvarez, “A Review of Data Centers Energy Consumption and Reliability Modeling,” 2021. doi: 10.1109/ACCESS.2021.3125092.
[5] N. E. Stauff *et al.*, “Preliminary Analysis of Nuclear-Powered Data Center Scenarios (ANL/NSE-25/47),” Lemont, IL, USA, 2025.
[6] US Nuclear regulatory Commission, “PRA procedures guide (NUREG/CR-2300) Vol.1,” *Nureg/Cr-2300*, vol. 1, 1983.
[7] NRC, “An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities,” *Regulatory Guide 1.200*, no. March, 2009.
[8] W. M. Bennaceur and L. Kloul, “Formal models for safety and performance analysis of a data center system,” *Reliab. Eng. Syst. Saf.*, vol. 193, 2020, doi: 10.1016/j.ress.2019.106643.
[9] T. Addabbo, A. Fort, M. Mugnaini, V. Vignoli, E. Simoni, and M. Mancini, “Availability and reliability modeling of multicore controlled UPS for datacenter applications,” *Reliab. Eng. Syst. Saf.*, vol. 149, 2016, doi: 10.1016/j.ress.2015.12.010.
[10] H. Cheung and S. Wang, “Reliability and availability assessment and enhancement of water-cooled multi-chiller cooling systems for data centers,” *Reliab. Eng. Syst. Saf.*, vol. 191, 2019, doi: 10.1016/j.ress.2019.106573.
[11] X. Y. Li, Y. Liu, Y. H. Lin, L. H. Xiao, E. Zio, and R. Kang, “A generalized petri net-based modeling framework for service reliability evaluation and management of cloud data centers,” *Reliab. Eng. Syst. Saf.*, vol. 207, 2021, doi: 10.1016/j.ress.2020.107381.
[12] K. M. Groth and L. P. Swiler, “Use of Limited Data to Construct Bayesian Networks for Probabilistic Risk Assessment,” Albuquerque, NM, Jan. 2013. doi: 10.2172/1095131.
[13] D. Marquez, M. Neil, and N. Fenton, “Improved reliability modeling using Bayesian networks and dynamic discretization,” *Reliab. Eng. Syst. Saf.*, vol. 95, no. 4, 2010, doi: 10.1016/j.ress.2009.11.012.
[14] E. Zarei, N. Khakzad, V. Cozzani, and G. Reniers, “Safety analysis of process systems using Fuzzy Bayesian Network (FBN),” *J. Loss Prev. Process Ind.*, vol. 57, 2019, doi: 10.1016/j.jlp.2018.10.011.
[15] P. Weber, G. Medina-Oliva, C. Simon, and B. Iung, “Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas,” *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 671–682, 2012, doi: 10.1016/j.engappai.2010.06.002.
[16] K. M. Groth and A. Mosleh, “Deriving causal Bayesian networks from human reliability analysis data: A methodology and example model,” *Proc. Inst. Mech. Eng. O J. Risk Reliab.*, vol. 226, pp. 361–379, Jan. 2012, doi: 10.1177/1748006X11428107.
[17] K. M. Groth and L. P. Swiler, “Bridging the gap between HRA research and HRA practice: A Bayesian Network version of SPAR-H,” *Reliab. Eng. Syst. Saf.*, vol. 115, pp. 33–42, Jan. 2013, doi: 10.1016/j.ress.2013.02.015.
[18] K. M. Groth, C. L. Smith, and L. P. Swiler, “A Bayesian method for using simulator data to enhance human error probabilities assigned by existing HRA methods,” *Reliab. Eng. Syst. Saf.*, vol. 128, pp. 32–40, 2014, doi: 10.1016/j.ress.2014.03.010.
[19] S. Marchetti, F. Di Maio, and E. Zio, “A Physics-of-Failure (PoF) model-based Dynamic Bayesian Network for considering the aging of safety barriers in the risk assessment of industrial facilities,” *J. Loss Prev. Process Ind.*, vol. 91, p. 105402, Oct. 2024, doi: 10.1016/J.JLP.2024.105402.
[20] F. Di Maio *et al.*, “Accounting for Safety Barriers Degradation in the Risk Assessment of Oil and Gas Systems by Multistate Bayesian Networks,” *Reliab. Eng. Syst. Saf.*, vol. 216, p. 107943, Dec. 2021, doi: 10.1016/J.RESS.2021.107943.
[21] S. Bin Cho, M. A. Bin Aziz, B. Lindley, T. P. Grunloh, C. Brooks, and N. Stauff, “Evaluating the Benefits of Nuclear–Data Center Tight Integration: Enhancing Plant Utilization via Heat-Driven Absorption Cooling,” in *Transactions of the American Nuclear Society*, 2025. doi: 10.13182/T133-49130.
[22] International Electrotechnical Commission, “IEC 60812: Failure modes and effects analysis (FMEA and FMECA),” 2018. [Online]. Available: www.iec.ch/online_news/justpub

[23] M. Modarres and K. Groth, *Reliability and Risk Analysis*, 2nd ed. Boca Raton, FL: CRC Press, 2023. doi: 10.1201/9781003307495.
[24] R. E. Neapolitan, *Learning Bayesian Networks*. Northeastern Illinois University, 2004.
[25] D. Koller and N. Friedman, *Probabilistic Graphical Models- Principles and Techniques*, vol. 53. 1989.
[26] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. San Mateo, CA: Morgan Kaufmann, 1988.