Nuclear Safety Curriculum, Credentialling, and Training in Operations and Cybersecurity to Support a Digitalizing Fleet

PI: Caleb S. Brooks, University of Illinois Urbana-Champaign (UIUC)

Program: Nuclear Reactor Safety Training and Workforce Development Program

Collaborators: *UIUC*: Timothy Grunloh, Tomasz Kozlowski, Kathryn Huff, Syed Bahauddin Alam, Rizwan Uddin, David Nicol, David Emmerich; *Purdue:* Hitesh Bindra, Stylianos Chatzidakis, Xiaoyuan Lou; *Curtiss-Wright*: Majid Mirshah; *Parkland College*: Daniel Meccoli, Wes Cravens, Timothy Newcomb

Unfunded Collaborators: *Sargent & Lundy:* Pareez Golub; *PJM Interconnection*: Steven McElwee

ABSTRACT:

The nuclear industry is changing, sometimes in conflicting ways. A competitive energy market is driving margins down, leaving many to do more with less. At the same time, the global demand for nuclear is rising swiftly. For example, the US joined over 20 countries at COP28 to set a goal of tripling nuclear power by 2050. The net result is that the nuclear industry is in dire need of a workforce development pathway that is responsive, flexible, and adaptable. We propose to design, develop, and implement a targeted curriculum for high impact nuclear safety topics. The approach includes development of formal credentials, classroom topics, hands-on-learning, and accessible virtual laboratories to maximize reach.

Perhaps the fastest changing aspects of nuclear lie in Instrumentation and Control (I&C). Original Nuclear Power Plant (NPP) equipment is becoming obsolete, power uprates are being facilitated with increasingly precise sensors, online maintenance is being rolled out, and digital technologies are becoming more present. The integration of more complex technologies into the nuclear space, dramatically raises the importance of cybersecurity, a topic that is currently absent from most nuclear training and education. Without introducing core concepts to the workforce pipeline, our industry will be caught unprepared, especially in an era of nation-state action and cyberwarfare. Consider by analogy the partial meltdown of Three Mile Island Unit 2. Here a design flaw combined with instrumentation failure leading operators to be presented with conflicting signals. Incorrect diagnosis led to exacerbating operator actions which lead to core damage. The modern analog to this is the completely new class of sensor failures inherent to digital and cyber-enabled technologies. It is critical that all technicians and engineers who configure, calibrate, maintain, or operate nuclear I&C technologies must be trained in the dangers of cyberattacks and the proper response to them.

Previously it was assumed that critical infrastructure, including nuclear facilities, was safe from cyber attacks for several reasons based on security by design. First, these facilities have been physically separated from Internet connections. Second, the control equipment often uses proprietary protocols not compatible with TCP/IP and other common network communications approaches. However, it is simply a fact that no system can be designed with complete immunity to cyber attack. Indeed, several events have indisputably shown that nuclear power plants are vulnerable. At the same time the proliferation of highly capable generative AI technologies has dramatically simplified the process of creating bespoke malware. Exploiting networks, even with proprietary technologies, is a significantly easier task than even a few years ago. Cyberspace is increasingly becoming a theater of war and nations are devoting immense

resources to uncovering vulnerabilities and developing exploits. Ongoing plant-side trends of modernization and digitalization, combined with adversary-side trends will elevate the risk of damaging cyberattacks against a NPP without a properly trained workforce.

In this project we will develop education and training curriculum to ensure a workforce is adequately prepared for a modernizing fleet. One face of the curriculum will be targeted toward nuclear engineers/technicians understanding cybersecurity principles as they apply to the current fleet. This will focus on prior events (e.g., those at Davis-Besse and Browns Ferry) which showed that plants are vulnerable. The types of attacks that might affect I&C, their consequences, and their mitigations will be the focus. Another side of the curriculum will be nuclear technology for cybersecurity-oriented students. Here basic nuclear operation and control topics will be covered. Then the curriculum will focus on details of currently operating plants including network configurations and the unique mix of both analog and digital equipment found in plants. Every aspect of the curriculum will be underpinned with nuclear professionalism topics like quality assurance, safety culture, and industry vernacular.

To implement the curriculum, the project will develop a multifunctional classroom facility that enables virtualization of realistic nuclear plant networks to provide hands-on learning to students, prospective technicians, and practicing professionals. The unique facility design will manifest a wide range of critical curricula to support a nuclear workforce in a growing and modernizing industry. This facility will integrate with a Generic Pressurized Water Reactor (GPWR) simulator already in use at UIUC. Combined with a virtual connection to an operating digitalized research reactor, this facility will provide a unique opportunity for hands-on and experiential learning in this important topic area.

The objectives of our approach are as follows.:

- Establish a cyber safety training curriculum for nuclear technicians and engineers,
- Establish a nuclear training curriculum for cybersecurity professionals,
- Deliver the curricula through a multifunctional educational facility, and
- Establish formal nuclear safety credentials related to operational cybersecurity.

The proposed team was designed to meet these objectives efficiently. UIUC is a major research university in the leading nuclear generation state. Purdue will provide access to the 10 kWth PUR-1 research reactor, the first fully digital controlled nuclear system in the US with a digital twin and remote communications, as well as access to virtual-enabled cyberphysical systems for advanced instrumentation labs. Curtiss-Wright is a leader in NPP technology and plant simulation. Community college partnership with Parkland College provides capabilities to train diverse workforces effectively. Throughout the project, a stakeholder's advisory group will be assembled. Initial members will include leaders in digital energy systems from Sargent & Lundy and PJM Interconnection.