

## **Characterizing Nuclear Cyber Security Using Artificial Intelligence/Machine Learning**

### **BACKGROUND**

Artificial intelligence (AI) and machine learning (ML) technologies have the potential to provide tools for identifying, characterizing, and responding to cyber security events at nuclear power plants, i.e., the nuclear cyber security AI/ML use case or simply the AI/ML use case. For example, AI/ML may enable plant staff to monitor increasingly complex plant systems and detect and evaluate abnormal systems states resulting from a cyber attack.

To prepare to regulate nuclear applications of AI/ML, the NRC plans to conduct research activities to develop insights and fundamental knowledge about AI/ML and the AI/ML use case.

The NRC is seeking a vendor capable of performing research on the AI/ML use case. Tasks performed as part of this research include 1) identification of technologies and approaches applicable to the AI/ML use case, especially those useful for capturing and analyzing the system and cyber security states of nuclear plant systems, 2) evaluation of available technologies and approaches, and selection of a technology/approach suitable for research on and demonstration of the AI/ML use case, 3) implementation of the selected approach with a small test case to develop insights and fundamental knowledge about the application of AI/ML to nuclear cyber security such as the feasibility of detecting and distinguishing abnormal plant and cyber security states, considerations for accuracy and reliability, necessary and availability ML training data, utility for identifying and responding to a cyber-attack, and existing and novel risks inherent to the application of the technology, and 5) producing a technical report documenting the results of this project and generalizing the results of the test case as appropriate.

### **REQUIRED CAPABILITIES**

The vendor must provide and use an existing experimental infrastructure (e.g., personnel, equipment, facilities) to conduct research and implement a test case. The research conducted by the vendor is expected to produce data that evaluates the impacts of AI/ML concepts, technologies, and applications on nuclear power cyber security outcomes and programs, especially those outcomes and programs that may be relevant to new and advanced reactor designs. The vendor shall provide all necessary qualified personnel to conduct this research.

Ideally, the vendor's programs and infrastructure should meet or exceed the following requirements:

1. Capability to represent, simulate, or emulate basic nuclear power plant systems, states, performance, and operations, including integration with physical components, e.g., hardware-in-the-loop
2. Capability to represent, simulate, or emulate basic nuclear power plant cyber security systems, states, performance, and operations

3. Capability to integrate power plant systems and cyber systems representations into a composite system representation suitable for research, testing, and evaluation of cyber-attacks and the consequences of the attacks on plant systems
4. Capability to represent, simulate, or emulate cyber-attacks on the composite system representation and measure/evaluate the consequences of the attacks on the composite system
5. Capability to develop and implement AI/ML technologies and approaches related to the capture and modeling of composite system states and the detection/identification of abnormal system states, e.g., states resulting from cyber attacks
6. Capability to collect, analyze, and visualize composite system state information and identify normal and abnormal states, especially those states that may result from a cyber-attack.
7. Capability to complete the research effort within 16 months of a contract award

The vendor must provide a team of key personnel that as a whole possess the following qualifications:

1. Understanding of nuclear power plant operational domain including reactor systems, instrumentation and controls, normal and abnormal operating conditions, and other common commercial nuclear power plant structures, systems, and components
2. Expertise in nuclear power plant cyber security programs, postures, requirements, and controls
3. Expertise in nuclear power plant simulation
4. Expertise in AI/ML approaches and technologies
5. Experience integrating and researching the applications of AI/ML to cyber-physical systems

If the vendor cannot demonstrate the level of formal training or experience specified above, they may submit a plan for how they will acquire the required training and experience.