NE-18-16180, NexDefense – Nuclear Cybersecurity Initiative

NexDefense, Inc. (NexDefense) offers a software solution that helps industrial companies monitor their plant networks for malicious cyber activities by providing complete visibility into their networks. This enables industrial companies to protect their plant networks for cybersecurity attacks and focus more time producing and growing their company. NexDefense Integrity™ is an Industrial Network Anomaly Detection solution that passively monitors industrial control system networks for anomalous and malicious cyber activities and provides users with complete network visibility.

This project will enable NexDefense to evaluate their existing software on a production nuclear test bed, hence laying the path for future commercial adoption. All data and experiences will be documented and presented in a use case format. The vision for the use case document is to provide a guide for industrial operators on implementing an industrial monitoring solution and to show how these solutions can be deployed without causing safety and reliability issues.

NexDefense is requesting assistance from Oak Ridge National Laboratory (ORNL) to analyze and address potential cyber vulnerabilities in nuclear reactor cyber-physical systems by using the ORNL High Flux Isotope Reactor for test-bed demonstrations. Combining the expertise of NexDefense and ORNL will allow the development of next generation interrogation methods to establish both normal communication patterns as well as differentiate anomalous noise from potential cyber intrusions on a production network.