ADROC: EMULATION EXPERIMENTATION PLATFORM FOR ADVANCING RESILIENCE OF CONTROL SYSTEMS

The ADROC project will develop new modeling, analysis, and experimentation capabilities to characterize the resilience of industrial control systems to cyberattacks. This project will facilitate cyber threat analysis, design of effective threat mitigations, and, ultimately, increased cyber resilience for our nation's energy and other critical infrastructure systems.

THE CHALLENGE

Cyberattacks are increasingly targeting industrial control systems (ICS) such as the electric power grid, chemical manufacturing facilities, and shipping ports. As the cyber threat grows, infrastructure operators struggle to prioritize the biggest threats and to understand the potential consequences of crippling attacks.

Cyber resilience modeling and analysis is an active body of research, but some significant technical gaps hinder progress toward understanding the vast spectrum of cyber threats. Modeling approaches frequently do not represent adaptive, dynamic cyber threats in a high-fidelity manner that is scalable and that can be validated. Furthermore, most cyber resilience assessment methodologies rely on qualitative assessments that do not provide quantitative, cyber-specific measures to support the design of effective threat mitigations.

APPROACH

The ADROC project proposes to address these challenges through the development of novel cyber threat modeling techniques and cyber resilience metrics. We will research the development of hybrid cyber threat models that integrate stochastic mathematical modeling techniques with high-fidelity cyber threat emulators. Additionally, we will develop cyber resilience metrics that quantify the

damage cyber threats can have on ICS and how well the systems can operate through and overcome the effects of a cyberattack. We will integrate the threat models and metrics with virtual ICS (emulated with Sandia's SCEPTRE capability) to create a virtual cyber experimentation platform. We expect that this platform will be generally applicable across a broad variety of infrastructure ICS, and the ADROC project will demonstrate the broad applicability on two exemplar infrastructures: a nuclear power plant and a multi-infrastructure shipping port system.

EXPECTED RESULTS

Completion of this project will result in several technical deliverables. Mathematical models and algorithms will provide an abstract framework for representing and analyzing threats. Mathematical data will be used to create customized cyber threat emulators that provide realistic representations of significant cyber risks. New cyber resilience metrics will provide quantitative measures for comparing cyber threats and proposed mitigations.

From a research perspective, these results will be of great interest to both the mathematical modeling and cybersecurity communities and will be documented in research publications. From a practical perspective, the experimentation platform will provide a foundational, hands-on capability that can be used by researchers from other projects and organizations to explore cyber threats and mitigations for ICS.

EXPECTED IMPACT OF THIS RESEARCH

Completion of this project will result in a platform for repeatable, quantitative cyber experimentation in support of cyber risk assessment and resilient design. Researchers will be able to use this platform to sift rapidly through the vast spectrum of cyber threats and identify and prioritize the threats of greatest concern. Furthermore, the platform will provide quantitative evaluations describing the damage that cyberattacks can create and how effectively proposed mitigations can prevent that damage. These evaluations will provide valuable information that can be used to engineer resilient ICS and effective mitigations and to inform cost-benefit decisions.

RESILIENT ENERGY SYSTEMS

Sandia's investment in this project is part of the Resilient Energy Systems portfolio of projects, coordinated R&D that addresses the resilience of the nation's energy systems and other critical infrastructures to threats.

This project directly supports the Resilient Energy Systems Mission Campaign goal to "Discover, characterize, and quantify vulnerabilities and risks." Furthermore, ADROC will support the *Science of Vulnerability* thrust's foci: "Identifying the most pertinent EMP, cyber, physical, and other threats and understanding their potential impacts" and "Development of an Emulytics™ control system model/cyber-security experimentation capability." ADROC represents a foundational capability for the Mission Campaign that could be used on other projects to assess vulnerabilities and proposed defense/mitigation approaches against cyberattacks of interest.

CONTACT:

resilience@sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-13350 O

Sandia National Laboratories