



Cybersecurity for Nuclear Facilities

INL cybersecurity researchers lead international efforts to secure nuclear facilities from cyberthreats.



Instrumentation and control (I&C) within nuclear facilities are continuously connected with information technology and wireless communications in facilities and operations to address efficiencies, cost savings and convenience. In this digital command and control environment, the use of physical boundaries alone is inadequate to secure nuclear technology and facilities. An integrated cyber physical security approach is essential to address the resiliency of the facility and continuity of operations.

Idaho National Laboratory employs the foremost cyber and industrial control systems security experts in the world. The lab has worked with more than 40 countries to assist them in understanding cyber and physical security risks and to

develop mitigation strategies and techniques to meet the unique requirements of network and operation environments. The lab works with the international nuclear community to assist them in understanding cyber and physical security risks and to develop mitigation strategies and techniques to meet the unique requirements of network and operational environments.

Cybersecurity assistance is provided by understanding the capabilities of malicious actors and developing customized mitigation technologies and tactics to meet the configuration requirements of installations at nuclear facilities and the protection of radioactive materials in and out of regulatory control. This enables the nuclear industry to address a sustainable long-term approach to nuclear

cybersecurity that increases the security posture and manages the evolving and emerging threats of nuclear proliferation and terrorism.

INL's unique capabilities in nuclear and cybersecurity include:

- Internationally recognized nonproliferation experts with real-world experience and backgrounds in nuclear facility inspection, physical protection, modeling and simulation, materials science, physics, and engineering.
- Comprehensive instrumentation and control, cyber and nuclear nonproliferation capabilities with similar nuclear infrastructure, and examination equipment found worldwide.



- Replication of typical control system network for architecture reviews and system hygiene to support asset owners in securing their systems.
- Protocol analysis, reverse engineering and forensics to advance persistent threat mitigations for the nuclear industry.

- Cyber-informed risk methods and unique engineering designed tools and methodologies to anticipate cyber and physical security risk and investment strategies.
- Frameworks for prioritization of investments and threat indicators for high-consequence activities.

with embedded security; secure industrial control systems can reduce the threat of cyberattack; and physical devices and barriers are part of the overall security posture.

INL's nuclear security programs are fundamentally changing how the nation and world approach analysis of threats to the complex myriad cyber-physical systems.

INL is an internationally recognized thought leader on industrial control systems cybersecurity across multiple domains: vulnerability assessments, mitigation research and development, future architectures, policies, and processes.

INL has proven that intelligent sensors and wireless communications can be integrated effectively

FOR MORE INFORMATION

Point of Contact

Tommie Burks

(208) 526-2512

tommie.burks@inl.gov

Media Relations

Ethan Huffman

208-526-5015

ethan.huffman@inl.gov

www.inl.gov

A U.S. Department of Energy
National Laboratory



Students participate in hands-on exercises and classroom instruction.