An INL engineer analyzes the communication on a physical control system network.

Cyber-Informed Engineering for Control Systems

Sector-specific expertise can bolster infrastructure and drive culture change

Control Systems Engineering is a division of Idaho National Laboratory's Cybercore Innovation Center. Our mission is to secure critical infrastructure through innovative control systems cybersecurity solutions.

We drive the national research and development efforts for cyber-physical systems by partnering with government, academia and industry to accelerate workforce development and address mission critical control systems cybersecurity challenges.

INL's unique approach of coordinating efforts between our cybersecurity researchers, analysts and control systems engineers creates unparalleled critical infrastructure engagements and analysis products.

To support this approach, INL builds a team of engineering excellence that incorporates experience and application of controls in critical lifeline sectors and expanded vendor-specific expertise. These control systems engineers develop team cohesiveness and increased collaboration with both cybersecurity analysts and researchers.

SECURING INDUSTRIAL CONTROL SYSTEMS

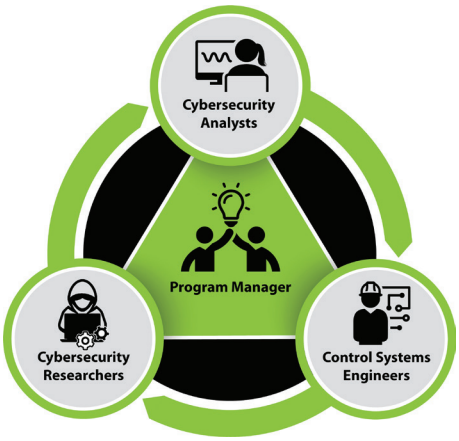
INL researchers secure industrial control systems and digital automation devices commonly found at power and renewable energy utilities, oil and natural gas refineries, water treatment plants, and manufacturing facilities. These systems and devices include:

- Energy management systems
- Process control systems
- Programmable logic controllers
- Supervisory control and data acquisition systems.

These multidisciplinary teams perform cutting-edge analysis, incident response, training, and tool and technology development.

The laboratory's cybersecurity experts combine traditional all-source threat analysis with the technical acumen associated with engineering and systems documentation, operational technology networks, programming languages, and foreign language skills to produce sound analytic products. They have demonstrated

Idaho National Laboratory



proficiency in analytic standards and tradecraft. They also maintain a strategic perspective of the security landscape to analyze evolving cyberthreats targeting the operational technology environment. By maintaining a deep awareness of newly discovered vulnerabilities within industrial control systems, the lab's experts understand adversarial cyber capabilities and the subsequent consequences posed to critical infrastructure.

INL supports and administers large-scale programs for the U.S. Department of Energy, National Nuclear Security Administration, and the Department of Defense.

IMPROVING RESILIENCY

INL also has signature capabilities in infrastructure resiliency, geographical information systems, data visualization, and advanced instrumentation and controls. INL's resiliency research and testing is focused on designing and developing infrastructure components, systems and programs where monitoring, control and human interaction must seamlessly integrate. The laboratory has research facilities and test beds dedicated to sensors, controls and intelligent systems research. These facilities provide complex evaluation of control system designs for cybersecurity, advanced control or operational verification and validation. As a leading provider of research, testing and training services to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the laboratory also supports key activities aimed at protecting and safeguarding the nation's critical assets and capabilities.

LEADING EXPERTISE

INL control systems researchers have diverse industry experience from oil and gas to agriculture, chemical, and water and wastewater, both private and government. They have expertise in areas like pump stations, cabinet layout, wiring diagrams, engine control units, embedded systems programming, protocols, and research and development. Our experience engaging with senior executives in private and public cyber-physical sectors is unmatched, and we have access to cutting-edge testing facilities and digital systems.

Our talent has experience with leading energy-related vendors. These include Schweitzer Engineering Laboratories, Schneider Electric, General Electric, Honeywell, Yokogawa, Siemens, ABB, Allen Bradley, PILZ Safety Systems, Delta V. Wonderwear, and DAQ/ National Instruments, just to name a few.

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy.

CONTROL SYSTEMS ENGINEERING QUICK FACTS

- The Cybercore Integration Center laboratories have more than 150,000 square feet dedicated to industrial control systems cybersecurity, grid and wireless security, and infrastructure resiliency.
- INL's 890-square-mile desert Site includes multiple test ranges, including a power grid test bed, water security test bed, and wireless test bed.
- Our Critical Infrastructure Test Range Complex can perform bench- to full- scale testing of equipment and new technologies from concept to destructive analysis.
- INL's experts have diverse backgrounds and capabilities in cybersecurity, power systems, engineering, system resilience, vulnerability assessments and threat analysis.
- The laboratory is a key contributor, facilitator and advocate for cybersecurity and infrastructure resiliency education and workforce development, providing training to thousands of professionals and students each year.

FOR MORE INFORMATION

Technical contact
Matthew Anderson
208-526-4308
matthew.anderson@inl.gov

General contact
Ethan Huffman
208-526-5015
ethan.huffman@inl.gov

www.inl.gov

A U.S. Department of Energy National Laboratory

22-50537_R3 (Updated: 2023)