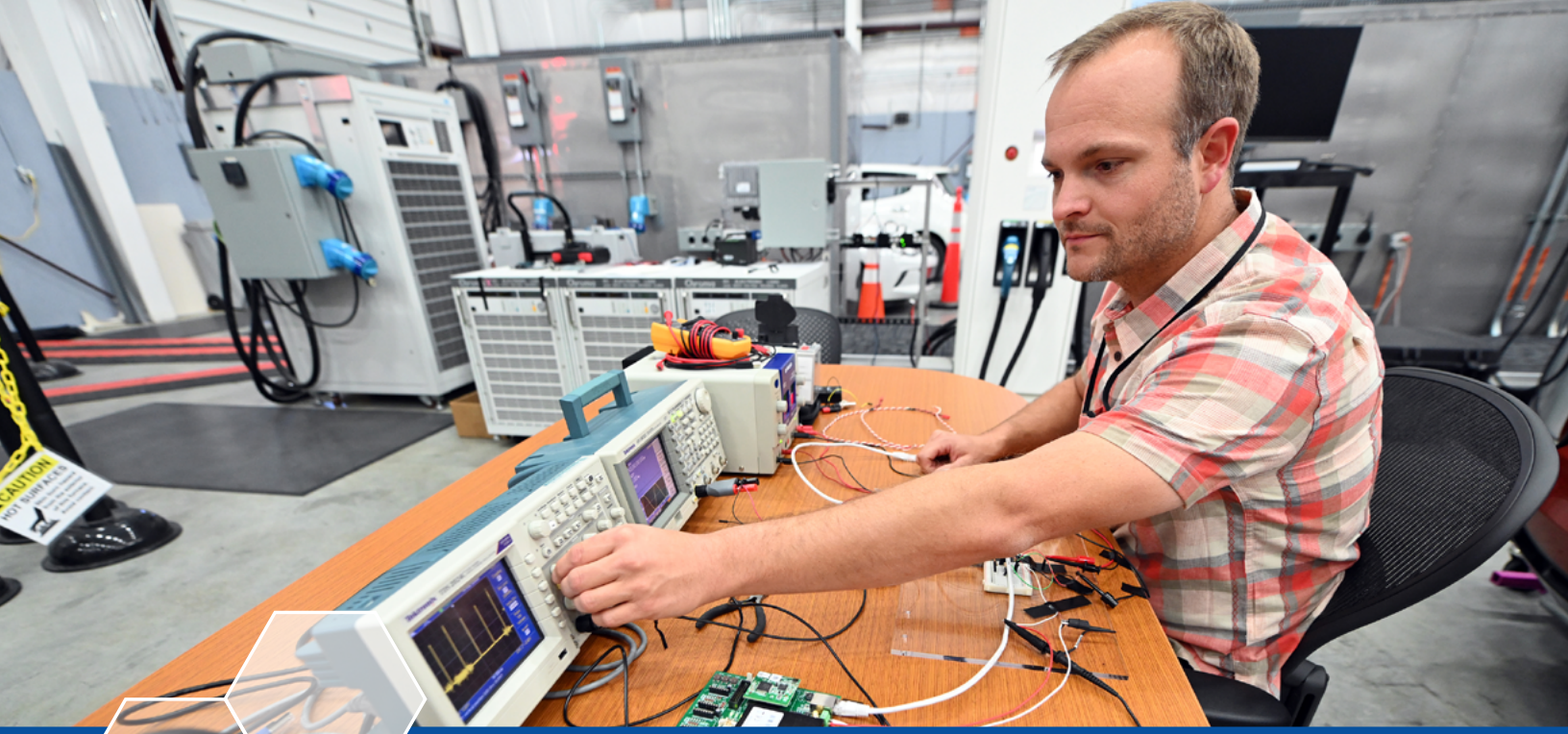


Cybersecurity Research and Assessment

Identifying vulnerabilities and improving operational efficiency and reliability.

INL cyber researchers use cutting-edge techniques and tools to help reduce critical infrastructure vulnerabilities.

Idaho National Laboratory's Cybercore Integration Center employs an elite team of cyber and control systems researchers and engineers who conduct in-depth vulnerability assessments of equipment common across all critical infrastructure sectors. Our work helps identify vulnerabilities and provides analysis and assessments so utility owners, operators and vendors can improve their defenses, operational efficiency, network reliability and security.

Cybercore's unique approach of coordinating efforts between our cybersecurity researchers, analysts and control systems engineers creates unparalleled critical infrastructure engagements and assessment solutions.

Our dynamic team of cybersecurity researchers perform vulnerability assessments that illuminate and alert both the manufacturers and end users to equipment weaknesses, need for added protections, mitigation research or patch development.

Our researchers work with a broad range of industries, manufacturers and government organizations to develop techniques and tools that help reduce the cyber vulnerabilities found in many of the nation's critical infrastructures. To protect proprietary information, the laboratory has established cooperative research agreements and nondisclosure agreements with dozens of companies and maintains relationships with other stakeholders interested in the lab's capabilities.

METHODOLOGY

Cybercore researchers use a rigorous methodology to analyze and test control system components including:

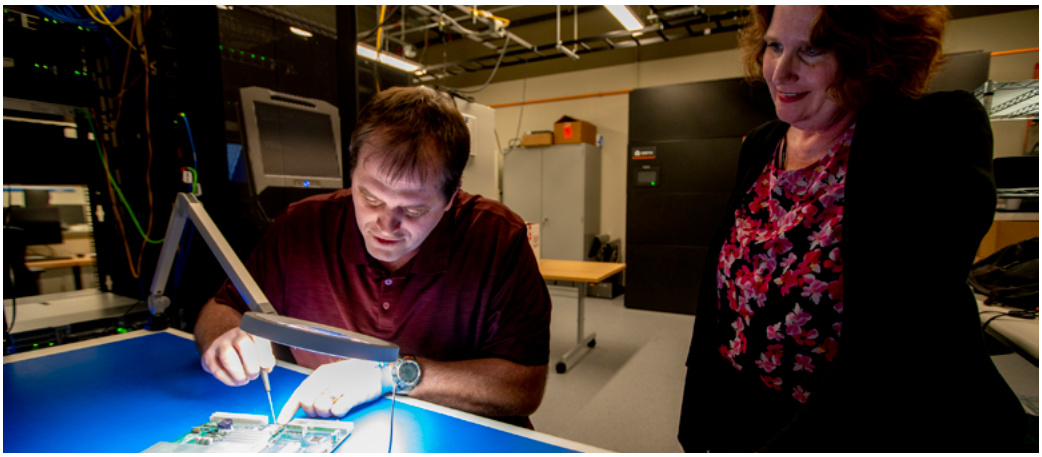
Setup Equipment

Upon receipt of equipment from a manufacturer, the assessment team will set it up to operate as intended in the field. This includes acquiring configuration, management and monitoring software, as well as use and setup documentation.

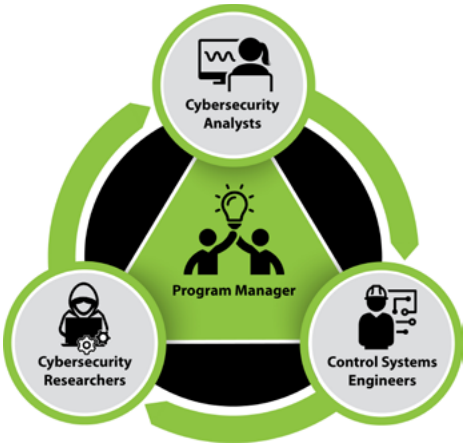
Conduct Teardown

During this step, INL researchers disassemble equipment to the board level,

INL
Idaho National Laboratory



Cyber researchers and control systems engineers collaborate to provide a multidisciplinary approach to cyber vulnerability assessments.



exposing and removing all circuit boards from the unit. Researchers photograph progress to thoroughly document their activities, pull datasheets for all identified components, and confirm all communication ports.

Pull Firmware

Nonvolatile memory integrated circuits (ICs) and microcontrollers are of special interest during teardown. From these components, researchers attempt to pull the unit's firmware via on-board, in-circuit programming headers, pulling ICs from the board, or by observing a firmware update, and note any observed protections or encryptions.

Reverse Engineer Circuit Boards

Researchers generate schematics detailing the connections between the microcontroller(s)/processor and other circuit components. These traceouts help the firmware team understand how the microcontrollers' hardware peripherals and inputs/outputs are utilized in the system. Communication links between components or other circuit boards are of special interest and are often observed to determine the bus and communication protocol type.

Analyze Firmware

Researchers assess firmware for vulnerabilities by either reviewing vendor-provided source code or pulling binaries from the system. Then, they analyze buffer overflow vulnerabilities, password or key encryption, coding practices, open ports or unused peripherals, undisclosed wireless interfaces, software backdoors, and potential use of the device as an access point.

Black Box Approach

Simultaneous to the teardown and firmware analysis, researchers conduct a parallel effort to determine vulnerabilities by treating equipment as a black box. In other words, assuming no physical access, what information can be ascertained about this system, and can it possibly be compromised? This analysis primarily includes equipment that is connected to a network via wired or wireless means.

Report Findings

Finally, researchers report device and network vulnerabilities discovered during the firmware analysis and black box assessment to the manufacturer. Security assessments of equipment are kept confidential. Reports generated in cooperation with industry or government agencies are provided only to the sponsoring organization or manufacturer. These assessments play a vital role in identifying and correcting potential vulnerabilities that could be exploited by adversaries.

FOR MORE INFORMATION

Technical contact
Darren Stephens
208-526-1569
darren.stephens@inl.gov

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

www.inl.gov

A U.S. Department of Energy National Laboratory

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