OPERATIONAL TECHNOLOGY CYBERSECURITY

CAPABILITIES CATALOG

INL Idaho National Laboratory

OVERVIEW

VISION

Secure all critical infrastructure sectors through innovative operational technology cybersecurity solutions.

The Idaho National Laboratory's (INL) Cybercore Integration Center blends technical expertise and one-of-a-kind capabilities to counter cyberattacks that target the operational technology of critical infrastructure. This Center leads efforts to secure OT by bringing together teams of accomplished controls and systems engineers, cybersecurity analysts and cyber research experts. These teams conduct research and development to strengthen the security and resilience of the nation's critical infrastructure against disruption.

MISSION

Address mission critical OT cybersecurity challenges through collaborative, multidisciplinary efforts that:

Drive national research and development (R&D) efforts

Develop partnerships with government, academia, and industry

Accelerate national workforce development

For more info, contact: OTcyber@inl.gov

INL OT CYBERSECURITY HAS EIGHT CORE CAPABILITIES:

1 Critical Function Assurance

2 Hunt and Incident Response

3 Forensics Research and Development

4 Vulnerability Discovery and Mitigation

5 Cybersecurity Threat Analysis

6 Cybersecurity Architecture Risk Evaluation and Mitigation

7 Training Development and Delivery

8 Systems Testing and Demonstration

DISTINCTIVE INL ENABLERS

WORLD-CLASS STAFF

- OT Cyber Threat Analysis
- Control Systems Engineering
- Critical Infrastructure Sector Operations
- Cyber R&D
- Hunt and Incident Response
- Technical Program Management
- Data Analytics – Artificial Intelligence (AI)/Machine Learning (ML)

Multi-disciplinary teams focused on OT cybersecurity research

STATE-OF-THE-ART EQUIPMENT

- Critical Infrastructure Sector Skids
- Critical Infrastructure Specific OT Systems
- Training Platforms
- Hunt & Incident Response Kits
- Skynet R&D Network/Environment
- Real-Time Digital Simulator

OT systems and equipment to further cybersecurity solutions

MISSION-READY FACILITIES & INFRASTRUCTURE

- Class and Unclass Offices & Networks
- Class and Unclass Labs
- Commercial Grade Range Connectivity
- Test Beds/Isolated Systems at Test
- Dedicated Training Facilities
- CIC University Lab

Distinguishing labs, offices, range, and test beds configured to meet multiple research needs and objectives

DIVERSE WORK PORTFOLIO

- Department of Energy
- Department of Homeland Security
- Department of Defense
- Intelligence Community
- Industry

Broad range of sponsors with near- and long-term OT cybersecurity research needs

1 CRITICAL FUNCTION ASSURANCE

INL applies digital engineering principles to build and maintain the cybersecurity of critical infrastructure functions. INL employs advanced infrastructure hardware, software, and system knowledge to manage network defense services and actively remediate unauthorized activities.

Consequence-driven, Cyber-informed Engineering (CCE) is a methodology focused on securing the nation's critical infrastructure systems. CCE begins with the assumption that if a critical infrastructure system is targeted by a skilled and determined adversary, the targeted network can and will be penetrated. This "think like the adversary" approach provides critical infrastructure owners and operators a four-phase process for safeguarding their critical operations.

Cyber-informed Engineering is a strategic initiative to integrate cybersecurity into engineering practices for critical infrastructure. INL leads in implementing the national strategy by developing engineering tools, standards and educational resources that prioritize cybersecurity in infrastructure design and operation.

Cyber defense IT architecture and design uses information technology (IT) automation and systems integration to design stronger cyber-defense infrastructure. INL provides secure design and integration services into cyber-physical testing ranges.

Cyber defense infrastructure research is conducted with special focus on system innovation and resilience integration. This research informs cyber-defense infrastructure design and strengthens testing capabilities.

Cyber systems support is the process of designing systems and networks for testing and research findings. INL uses data warehousing to manage and secure a high volume of cyber-defense infrastructure information from many sources.

RELATED INL TOOLS

CIEMAT Cyber-Informed Engineering Microgrid Analysis Tool (CIEMAT) can inform engineering and traditional cybersecurity mitigations to make microgrid site installation more resilient to the impact of cyberattacks.

CIEBAT Cyber-Informed Engineering Battery Analysis Tool (CIEBAT) can inform engineering and traditional cybersecurity mitigations to make battery energy storage systems (BESS) more resilient to impact of cyberattacks from concept to operations.

For more info, contact: OTcyber@inl.gov

OmniTap

OmniTap is a device that protects process control systems with universal capture and translation of both modern and legacy ICS communications. This tool implements hardware circuitry compatible with the signals of all control network protocols instead of relying on transceivers specific to each one.

PARROT

Plug-n-Play Appliance for Resilient Response of Operational Technologies (PARROT) is a device that provides OT cybersecurity without interrupting normal operations. The device can be inserted between the communications and power pins of any controls device, such as programmable logic controllers, for continued operation while monitoring for anomalous behavior.

2 HUNT AND INCIDENT RESPONSE

OT hunt and incident response involves both host and network forensic activities to identify and track threats against critical infrastructure. OT networks instrumentation, OT host memory and disk drive analysis, and user behavior pattern analysis allows INL experts to root out threats against the nation's critical infrastructure and provides methodological guidance to harden each OT environment.

Host and network instrumentation and forensic analysis includes monitoring and analyzing data from computer systems and OT networks to detect and investigate security incidents.

OT targeted malware reverse engineering deconstructs and analyzes malware designed to attack OT systems to understand its behavior and develop countermeasures.

Advanced detection techniques and machine learning for OT network traffic analysis involves using sophisticated algorithms and machine learning methods to identify anomalies and threats within OT network traffic.

Cyber incident response planning and preparedness uses the techniques built during incident response and hunt engagements throughout the last 15-plus years to provide guidance and planning techniques to help partners harden their environments and prepare for potential breaches.

Cyber incident response and threat hunting uses intelligence from adversary tactics, techniques and procedures against critical infrastructure to perform hypotheses-based threat hunting and incident response through network traffic and host forensics. Instruments are deployed to OT partner sites to perform forensic analysis and guide them in what is being observed in their environment.

OT protocol analysis and deep packet inspection involves developing OT protocol parsers through either reverse engineering or translating protocol specifications. These are employed to critical infrastructure locations that rely on these parsers to determine what is occurring within their environment.

RELATED INL TOOLS

Malcolm Malcolm is a hunt and incident response tool that analyzes OT traffic as it flows throughout a network. This tool suite is open source and released to the public to assist the community in further securing their infrastructure and assist incident response teams when arriving with logs and artifacts.

For more info, contact: OTcyber@inl.gov

CyberSentry

CyberSentry is a threat detection and monitoring capability, governed by an agreement between CISA and voluntarily-participating critical infrastructure partners who operate significant systems supporting national critical functions.

Parsnip

Parsnip is a public tool designed to support creation of new Zeek parsers without using the development language (Spicy). The tool features a graphical user interface that makes it simpler for companies without in-house programmers to develop their own parsers.

3 FORENSICS RESEARCH AND DEVELOPMENT

OT forensics research and development focuses on systematically investigating and creating methodologies, tools, and technologies to analyze and understand security incidents within OT environments. Researchers identify vulnerabilities, detect breaches and trace malicious activities in critical infrastructure systems.

By enhancing the ability to respond to and mitigate the impact of cyberattacks on OT systems, these R&D efforts keep experts ahead of emerging threats and improve the security posture of vital operations.

INL RESEARCHER CAPABILITIES AND SKILLS INCLUDE:

- Conducting advanced forensics and malware analysis (unclassified and classified)
- Developing methods and code to detect attack vectors and conduct exploit identification, development and execution
- Identifying unknown and embedded vulnerabilities within systems and applications
- Reverse engineering to identify vulnerabilities within binary and executables files
- Analyzing and developing vulnerability mitigation strategies and concepts
- Developing advanced cybersecurity applications to identify advanced threat actors' indicators of compromise
- Engaging in theory and conceptualization of advanced vulnerability discovery, development and validation for disclosure

RELATED INL TOOLS

@DisCo

Annotated Translated Disassembled Code (@DisCo) translates static compiled code into intermediate languages stored in a graph database for machine learning analysis and visualizations.
https://github.com/idaholab/AtDisCo

For more info, contact: OTcyber@inl.gov

Deep Learning Malware Analysis

Deep learning malware analysis follows the same process as the firmware with additional embeddings for abstract syntax trees, the ability to analyze multiple coding languages in one sample of malware and complete data flows.

FC2

Firmware Command and Control (FC2) is a firmware analysis that translates binaries into an intermediate language stored in a graph database for visualization and analysis using ML.

4 VULNERABILITY DISCOVERY AND MITIGATION

OT vulnerability discovery and mitigation development identifies known and/or unknown vulnerabilities residing within the OT ecosystems, along with any tangentially connected IT architecture. Using a variety of cybersecurity strategies and reverse engineering techniques and tools allows INL to increase cybersecurity posture, manage assets, and address security vulnerabilities across systems and operations.

Hardware and software enumeration identifies and catalogs the hardware and software systems within a computing environment. It provides a comprehensive inventory to help manage resources and detect unauthorized or malfunctioning components.

Hardware/software bill of materials (H/S BOM) creates a detailed inventory of the components and systems within a computing environment. Using asset management tools or scanning software simplifies the collection process, ensures accuracy, organizes information in a database, and updates as materials change.

Supply chain risk management identifies, assesses, and mitigates risks within the network of suppliers and vendors that provide hardware, software, and services to an organization. INL teams conduct cybersecurity assessments of vendor equipment, implement secure procurement processes, monitor emerging threats and establish contingency plans to address potential disruptions.

Vulnerability assessments (discovery, verification, validation) evaluates a given environment to identify and address potential operational security risks. This three-phase approach involves: discovery mapping all ICS components; verifying and testing identified vulnerabilities; and validating to ensure remediation efforts resolve risks without disrupting functions of the system.

Reverse engineering (hardware, software, firmware) deconstructs and analyzes components to understand their design, functionality, and underlying code. This technique is often used to uncover vulnerabilities, identify malicious code or validate security measures. Cybersecurity experts leverage reverse engineering to enhance defenses, patch vulnerabilities and ensure the integrity of systems against evolving threats. This process incorporates intellectual property rights and uses reverse engineering tools such as:

- **Binary Ninja**
- **IDAPro**
- **Ghidra**
- **Wireshark**

OT vulnerability trend analysis examines patterns and developments in the security weaknesses of OT systems. Analysts use this data to track recurring vulnerabilities, emerging attack vectors and shifts in exploit tactics. By studying these trends, organizations can anticipate potential risks, prioritize security measures and strengthen defenses against dynamic and sophisticated cyber threats and attacks.

Artificial intelligence and machine learning integration is used to enhance cybersecurity vulnerability assessments across hardware, software, and OT networks by streamlining and strengthening detection, analysis, and mitigation processes. AI and ML enables automating repetitive tasks and adapting to evolving cyber threats, empowering organizations to secure complex ecosystems with greater precision and efficiency.

For more info, contact: OTcyber@inl.gov

RELATED INL TOOL

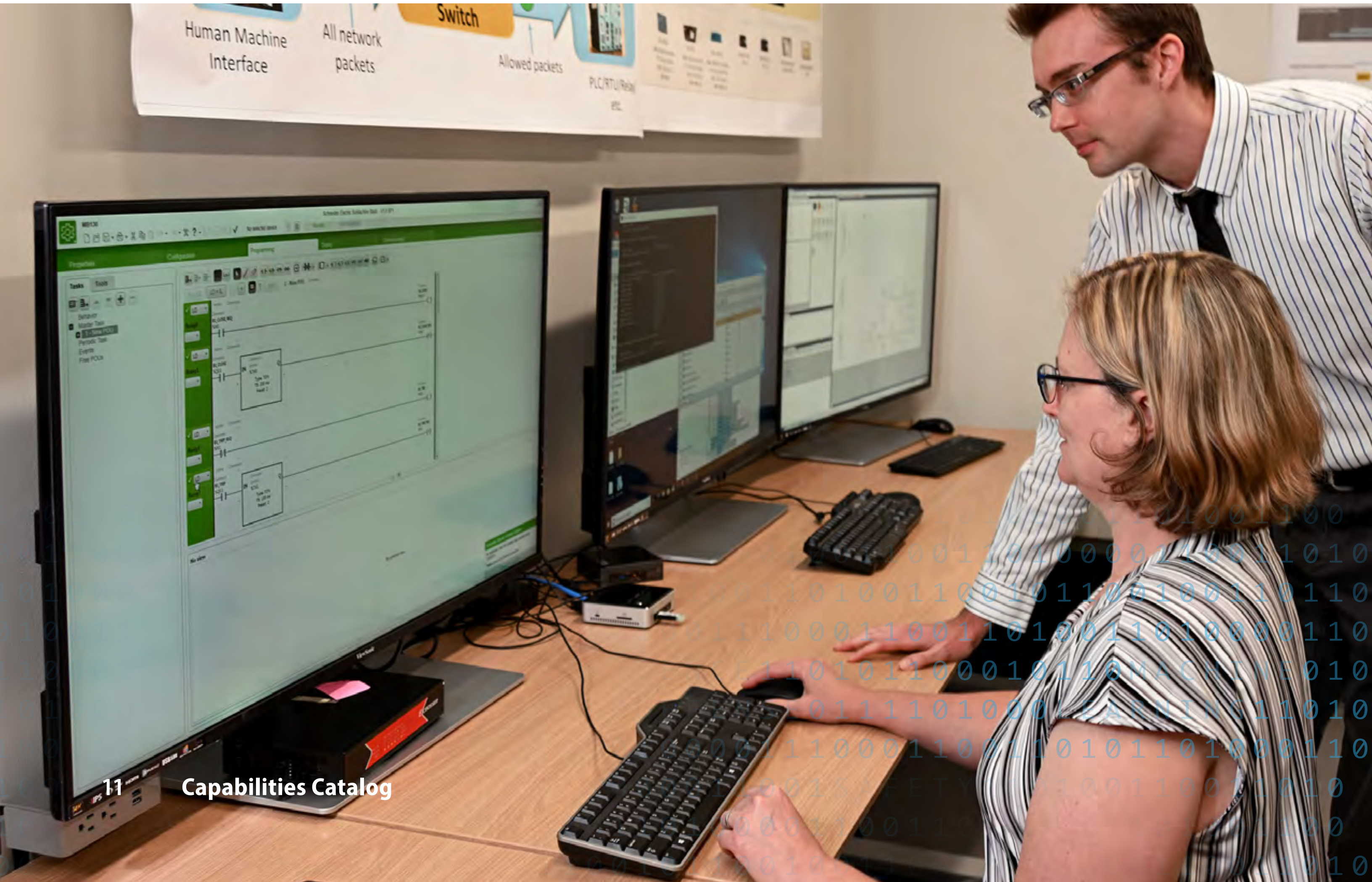
OpDefender

OpDefender is an INL-engineered technology that can protect utilities and other users of computer-controlled industrial systems from cyberattacks.

5 CYBERSECURITY THREAT ANALYSIS

OT cybersecurity threat analysis improves stakeholder understanding of infrastructure vulnerabilities by collecting and analyzing data from a wide variety of sources. This information is used to formulate sector-related assessments to inform stakeholder decisions and planning for cyber and all-hazard threats to OT environments.

- Technical prioritization involves working within a risk management framework, identifying critical operations that must not fail and then gathering information to identify pathways and interdependencies between critical processes, defense systems, and components to recommend the most effective mitigation strategies.
- OT cyber report development and dissemination involves assessing OT cyber events, technical findings of research and summaries/insights into emerging threats.



TYPES OF APPLIED ANALYSIS USED:

Supply chain analysis and optimization increases stakeholder knowledge of supply chain system behavior through modeling, simulation, and decomposition, while securing reliable materials, transportation, and backups.

Risk and decision analysis helps stakeholders make decisions that support emergency response, hazard preparation, infrastructure resilience, and cyber-physical security through applying advanced simulation and modeling capabilities and expertise to mitigate risk and enhance infrastructure resilience.

Comprehensive resiliency analysis applies advanced analytic techniques and development to better understand interdependencies, improve partnerships between owners and operators, and enhance regional resilience. These efforts inform decisions that characterize cyber and physical systems and supply chains.

Infrastructure systems characterization develops infrastructure dependency profiles and groups systems through engineering design principles to help identify relationships between systems. This reveals guides for analysts or ML algorithms to evaluate dependency relationships within infrastructure systems.

Emergency management planning, response and recovery uses continuity planning that involves staff deployment for data collection and infrastructure stabilization, dependency analysis, and all-hazards analysis integration. Subject matter experts create mission decomposition analyses and support, mitigation evaluations, and mission assurance reports to increase stakeholder knowledge of planning and response best practices.

For more info, contact: OTcyber@inl.gov

RELATED INL TOOLS

STIG

Structured Threat Intelligence Graph (STIG) is a database for advanced graph theoretics to create, edit, query, analyze and visualize threat intelligence. It uses Structured Threat Information eXpression (STIX v2) and international standards for threat sharing.

WiFIRE

Wireless Radio Frequency Signal Identification and Protocol Reverse Engineering (WiFIRE) is a monitoring and analytic tool for protecting the cybersecurity of wireless systems. The capability captures and analyzes radio frequency traffic, identifying the protocols in use, and locating the approved and rogue devices emitting the signals.

Cyber-Physical Consequence

Cyber-physical consequence and interdependency analysis identifies risk reduction measures, trains national and homeland security workforces, and provides a new framework for examining vulnerabilities in OT. This service complements INL cybersecurity and electric test bed capabilities, bridging the gap between cyber- and physical-interdependency analysis. Services for this capability are funded by the Cybersecurity and Infrastructure Security Agency (CISA).

CyPhStAR

Cyber Physical State Awareness for Resilience (CyPhStAR) is a novel strategy of integrating the physical, cyber and resilience components of the distribution power grid. This INL technology provides an integrated cyber-physical root cause and resilience analysis, and visualization approach that could be integrated into current power systems.

6 CYBERSECURITY ARCHITECTURE RISK EVALUATION AND MITIGATION

INL conducts cyber risk evaluations to understand system and network vulnerabilities and determine risk levels through on-site analysis, recurring system scanning, and vulnerability analysis. INL develops recommendations by analyzing exploitable vulnerabilities to help organizations apply the appropriate mitigation measures.

Architecture design review involves expert-level engagement with critical infrastructure cybersecurity engineers (CICSEs) and subject matter experts using federal and industry standards, guidelines and best practices for analysis. This engagement is not intended to be an audit but rather an in-depth cybersecurity design review of an asset owner's OT architectures that directly supports critical and enabling functions.

Network architecture validation and verification evaluates against industry best practices like CISA's Recommended Secure Architecture (based on the Purdue model), NIST 800-82 and NIST 800-53. Asset owner's subject matter experts and CICSEs identify weaknesses that affect critical functions. CICSEs validate current architecture against captured network traffic and identify possible unverified trust using discussion-based interviews and open-source tools (INL-developed and other).

Critical infrastructure cyber assessments and risk analysis analyzes critical infrastructure assets to identify system threats and vulnerabilities. INL assessments of cyber maturity, OT and IT, regional resiliency, and macro- and microsystems help asset owners mitigate risk and formulate policy and research priorities.

Assessment methodology development enhances tools and methods to improve assessments of system and network vulnerabilities. The tools and methods are developed using research, known vulnerabilities and cybersecurity analysis to support this analysis.

Cybersecurity Risk Management Framework (RMF) development uses INL programs, policy development tools, and industry best practices to help asset owners build and manage a strong cybersecurity foundation.

RELATED INL TOOLS

CSET Cyber Security Evaluation Tool (CSET) is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate ICS and IT network security practices.

For more info, contact: OTcyber@inl.gov

IGHTY·P

7 TRAINING DEVELOPMENT AND DELIVERY

INL uses instructional systems design models to develop and deliver cybersecurity educational products and experiences for today's workforce. INL develops curriculum for infrastructure owners and operators related to topics such as cyber and physical security, infrastructure dependencies and interdependencies, resilience, and risk.

INL experts also help organizations create a cybersecurity workforce development and education pipeline. This pipeline combines identifying and adopting educational IT and OT cybersecurity standards for academia.

INL offers virtual, in person (Idaho Falls) and mobile training locations. The trainings take place in immersive laboratory settings based on real-world industry job roles.

Sponsor-specific ICS cybersecurity training (virtual and in person) designed to help industry professionals and all levels of government with cybersecurity defense. INL leverages investments in resources and expertise to accelerate the sharing of discoveries and emerging threats.

The Cybersecurity Analysis Center (CSAC) provides a full-size processing, distribution and supply control systems environment. The facility includes electrical distribution and supply CS and wireless access points throughout. The CSAC facility is used for 301L (red/blue) and 401L cyber self-evaluation courses. Courses can be tailored to sector-specific training requirements.

ICScape Rooms use ICS cybersecurity-focused escape room puzzles. The rooms are designed to test teams of ICS experts against OT and IT problems, evaluating their teamwork, communication and technical skills against a ticking clock.

aCCElerate Training provides critical infrastructure companies with a self-guided approach to conducting their own Consequence-driven Cyber-informed Engineering (CCE) effort. The course is two days (16 hours) and includes CCE methodology plus a detailed guide and templates participants can use to facilitate a CCE effort within their organization. The course offers continuing educations units/credits.

INL- and DOE-supported CCE engagement (Tier 1) provides specific engineering (cyber and non-cyber controls) solutions to design out cyber risk from critical operations.

Self-driven CCE engagement (Tier 2) is team-based training for Tier 1 individuals. This 16-hour training (in person or virtual format) offers an overview of CCE concepts and steps for implementation. The target audience is system operators, CS engineers, process experts, functional and operational managers, cybersecurity analysts (IT and OT), risk management analysts, and emergency management system support.

CCE Workforce Development is team-based training for select individuals who will help Tier 1 partners execute a CCE engagement. This weeklong intensive training is a combination of classroom instruction, team exercises, quizzes and a full-day exercise to simulate a complete CCE effort.

Mobile Trainings

Instructor-led courses and workshops can be scheduled at venues across the United States and around the world.

- Introductory and intermediate instructor-led ICS cybersecurity training (101, 201, 202 courses)
- Wireless cybersecurity training course
- CyberStrike (Lights Out, Nemesis — review of top 10 cyber threats and mitigation strategies, various sector workshops)
- Cyber escape rooms

Send requests to schedule an event in your area to: icstraining@inl.gov.

For more info, contact: OTcyber@inl.gov

INL OFFERS 13 ONLINE OT-RELATED TRAINING COURSES VIA THE CISA TRAINING VIRTUAL LEARNING PORTAL (VLP)

101 Introduction to ICS Cybersecurity is an introduction to ICS cybersecurity basics. It includes a comparative analysis of IT and ICS architecture, and basic cyber-risk mitigation strategies.

201 Intermediate Cybersecurity for ICS: Part 1 builds on concepts learned in 101, providing technical instruction on ICS protection using offensive and defensive methods.

201 Intermediate Cybersecurity for ICS: Part 2 hands-on course split into five sessions:

301V/L ICS Cybersecurity Virtual and Lab

1. *ICS overview*
2. *Network discovery and mapping*
3. *Exploitation and using metasploit*
4. *Network attacks and exploits*
5. *Network defense, detection and analysis*

Training – virtual and in-person training that includes a red-blue exercise in a CS environment, hands-on experience with open-source OS and security tools, and ICS cyber escape rooms.

For more info, visit: https://ics-training.inl.gov/learn

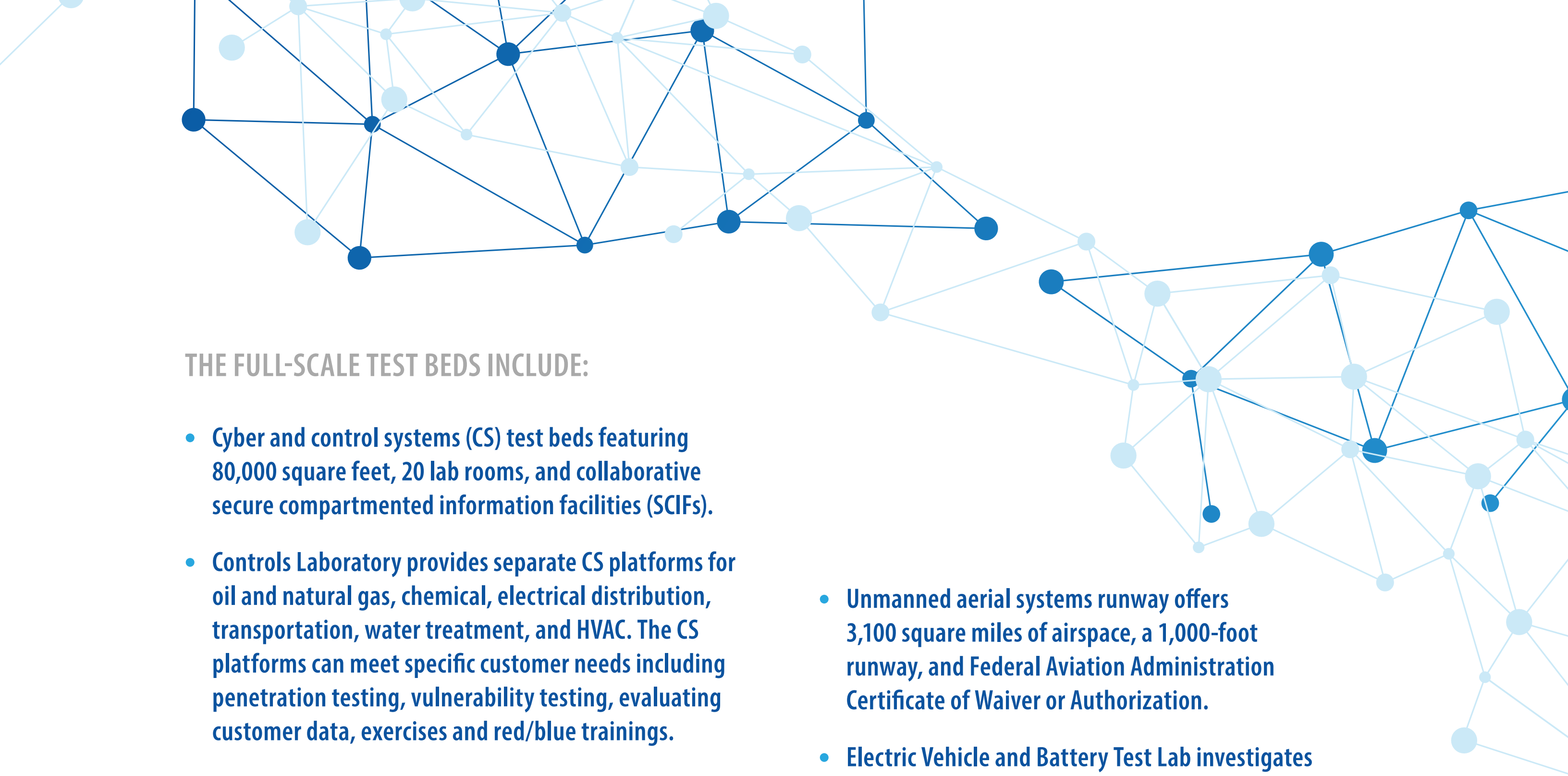
8 SYSTEMS TESTING AND DEMONSTRATION

INL has a broad capability to research, develop, test, evaluate, and demonstrate a wide variety of products and services in the cyber-physical domain. Multisector cybersecurity labs offer modeling and simulation, benchtop, model-scale, and full-scale environments. INL also features an isolated, configurable, 890-square-mile site for dynamic cyber-resilience-focused, full-scale critical infrastructure testing and demonstration.

Bench-scale, sector-specific cyber physical process modeling to laboratory-scale, high-fidelity simulations or experiments of industrial processes for evaluating materials and methods, and determining if a process can safely create the desired product.

Full-scale, industry-grade development, testing, and demonstration provides comprehensive evaluation of structures, components, or systems in a realistic, full-sized environment to verify their performance and integrity under real-world conditions.

INL's Critical Infrastructure Test Range is a collection of specialized capabilities that creates a centralized location where government agencies, utility companies and equipment manufacturers work together to find solutions to many of the nation's most pressing security issues. This capability allows for testing cross-sector cyber and physical scenarios and associated technologies.



THE FULL-SCALE TEST BEDS INCLUDE:

- Cyber and control systems (CS) test beds featuring 80,000 square feet, 20 lab rooms, and collaborative secure compartmented information facilities (SCIFs).
- Controls Laboratory provides separate CS platforms for oil and natural gas, chemical, electrical distribution, transportation, water treatment, and HVAC. The CS platforms can meet specific customer needs including penetration testing, vulnerability testing, evaluating customer data, exercises and red/blue trainings.
- Electric Power Grid Test Bed features over 60 miles of 138 kV, 13.8 kV transmission lines and multiple substations.
- Wireless Test Bed features 2G–5G cellular, high frequency, microwave, satellite and fiber-optic backhaul.
- Water Security Test Bed features pressurized pipelines, household systems and automated controls.
- Unmanned aerial systems runway offers 3,100 square miles of airspace, a 1,000-foot runway, and Federal Aviation Administration Certificate of Waiver or Authorization.
- Electric Vehicle and Battery Test Lab investigates the resilience of charging technologies and software solutions that support electric transportation.
- Nuclear test reactors include the world-leading Advanced Test Reactor.
- Large nuclear materials and post-irradiation examination hot cells.

For more info, contact: OTcyber@inl.gov

FOR MORE INFO, CONTACT:
OTCYBER@INL.GOV

INL.GOV

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

INL Idaho National Laboratory