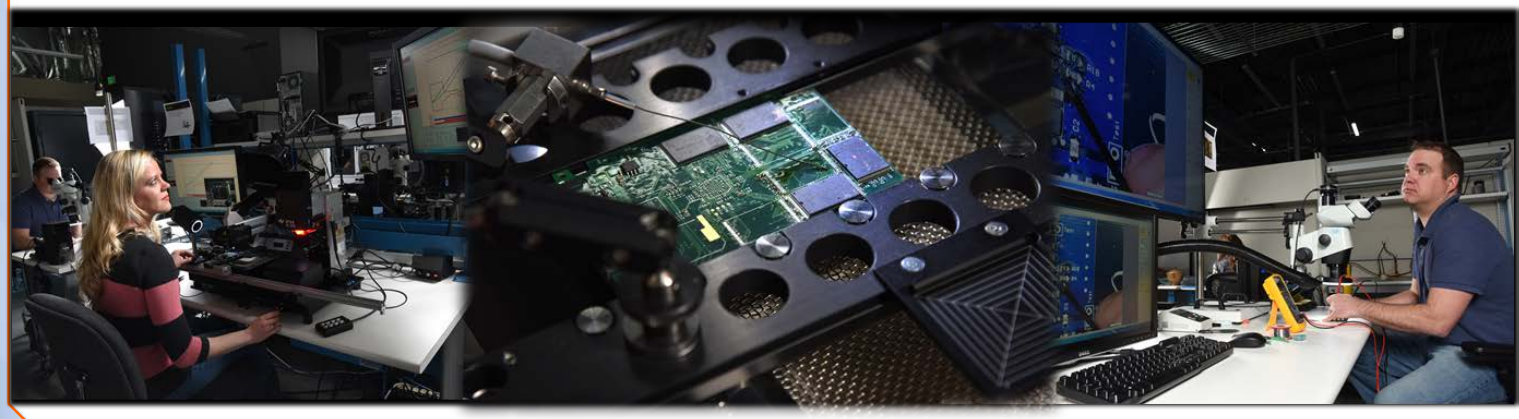
Cybersecurity at the National Laboratories

Wayne Austad
Director, CYBERCORE Integration Center



Teaming for control systems cybersecurity

Idaho National Laboratory

Pacific Northwest NATIONAL LABORATORY

Sandia National Laboratories

Secretary of Energy Advisory Board
June 14, 2016

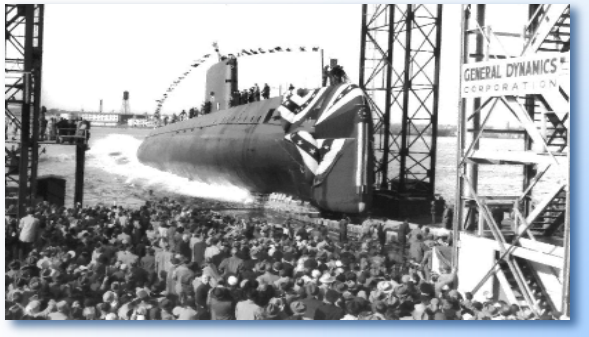
www.inl.gov

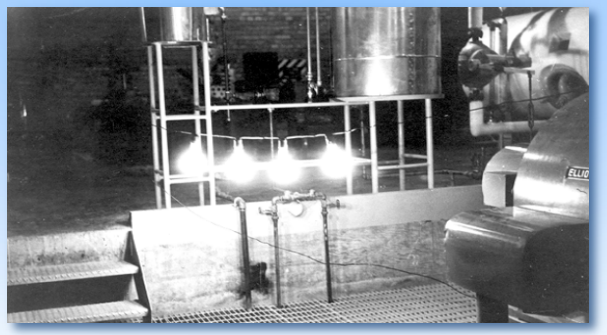
Idaho National Laboratory

INL – A History of Supporting National Security

The Science behind: 1) Core capabilities, 2) Full-scale test & validation, 3) Systematic engineering, 4) Deployment

- Testing naval large caliber guns
- National Reactor Testing Station 1949, INEL 1974, INEEL 1994, INL 2005
- Design, modeling, testing of 52 unique nuclear reactors, Navy prototypes
- Fuel cycle development & demonstration – reprocessing, signatures, protection
- Specific Manufacturing Capability (SMC) – Tank armor and special armor systems
- Critical Infrastructure Test Range Complex

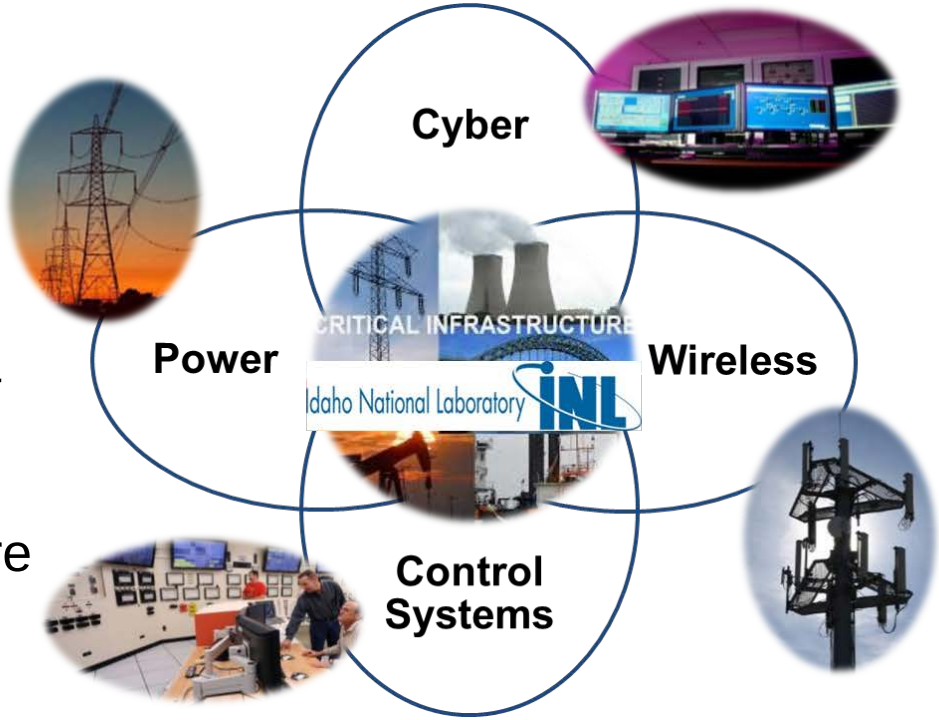




Research – Development – **Demonstration** – Deployment

INL's Cybersecurity Focus

- International leader in control systems cybersecurity
- Full-scale test & validation infrastructure
- Innovation to identify and prevent cyber-physical failures
- Research, Development, Demo & Deployment (RDD&D), modeled and validated at large scale
- Interdependencies of infrastructure and technology
- DOE, DHS, DOD, and Industry partnerships



We resemble a "well-characterized, reconfigurable city/region" enabling holistic solutions and mitigations of technology and infrastructure interdependencies.

Daunting Cybersecurity Challenge

Enterprise IT

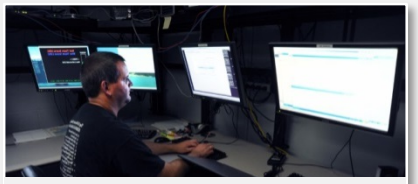
- OPM 2015
  - 21.5M individuals affected
  - $133M for ID theft protection
- Sony Pictures 2014
  - 47,000 unique Social Security numbers stolen
  - $8M employee settlement
  - $35M investigation, remediation, and restoration
- Target 2013
  - 70 million shoppers affected
  - $309M cost to Target (attack and security upgrades)
  - $200M cost of attack to financial institutions

Control Systems (Infrastructure)

- Aurora Demonstration 2007
  - DHS demonstration, conducted by INL, that proved a cyber attack could cause physical damage
- Ukraine 2015
  - 225,000 customers affected
  - 1st destructive attack against operational technology systems in a nation's civilian critical infrastructure

Control Systems Cyber: Different from IT

Control systems are the components that govern and execute complex processes within chemical, critical manufacturing, energy, nuclear, transportation, defense, water and wastewater sectors



Human-machine Interface (HMI)

Programmable Logic Controllers (PLC)

Networks of Networks (Business & Suppliers)

Sensors

Actuators (motors, valves, pumps)

Maintenance & Service (calibration, diagnostics)

Physical Processes

Critical National Challenges in Control Systems

National measure/ countermeasure approach is not sustainable, scalable, or anticipatory

Fundamental science & engineering of cyber challenges are inadequately advanced

R&D and complex solutions require expensive systems and large-scale proving grounds

Technical expertise is in limited supply and mostly consumed in operations

Diverse Missions Have Common R&D Challenges

		Common Control System R&D Needs
DOD	Military forces (base & platform security)	Operating in contested cyber space
Sector Specific Agencies, DHS, Asset Owners	Defend critical infrastructure functions	ICS situational awareness in operational technologies
DOE	Energy and national security R&D	Protecting high impact common systems across domains
		Cyber-physical fundamentals and complex interdependencies

Focus Key Resources on Common & Critical National Security Challenges

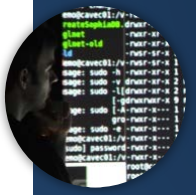
Lab Capabilities and R&D Portfolio Approach

Idaho National Laboratory

Control Systems Cyber & Nuclear Energy

Cyber-Physical Science & Disruption Zones

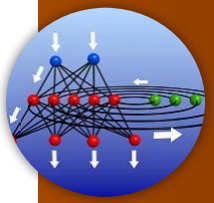
Consequence- & Cyber-Informed Engineering



Operational Technologies: Monitoring & Defense

Pacific Northwest National Laboratory

Energy Infrastructure & Big Data Visualization



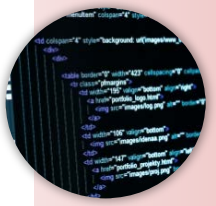
Data Analytics & Visualization

Cyber Situational Awareness

Power Systems Engineering & Analysis

Sandia National Laboratories

Military Systems & Combined Cyber Hardware/Software



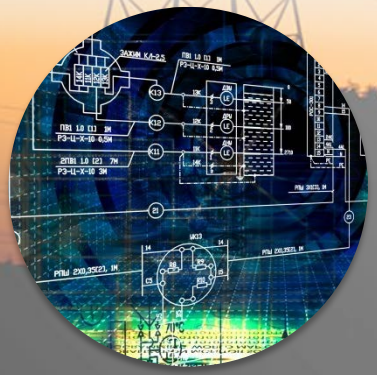
Advanced Cyber HW/SW Research

HW/SW Virtualization & Emulytics™

DOD Systems, Embedded Supply Chain

Long-Term National Benefit of Integrated Approach

- **Science of New Cyber-Informed Control Theories and Engineering Practices**
- **Enhance the Security of Embedded Systems, Nuclear Facilities, and Energy Infrastructure**
- **Establish a Dedicated R&D National Workforce**
- **Effectively Integrate Control Systems Cyber Investments**



Idaho National Laboratory