INL/MIS-23-75749-Revision-0

S9 Presentations - CELR

November 2023

Timothy Adam Huddleston

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-23-75749-Revision-0

S9 Presentations - CELR

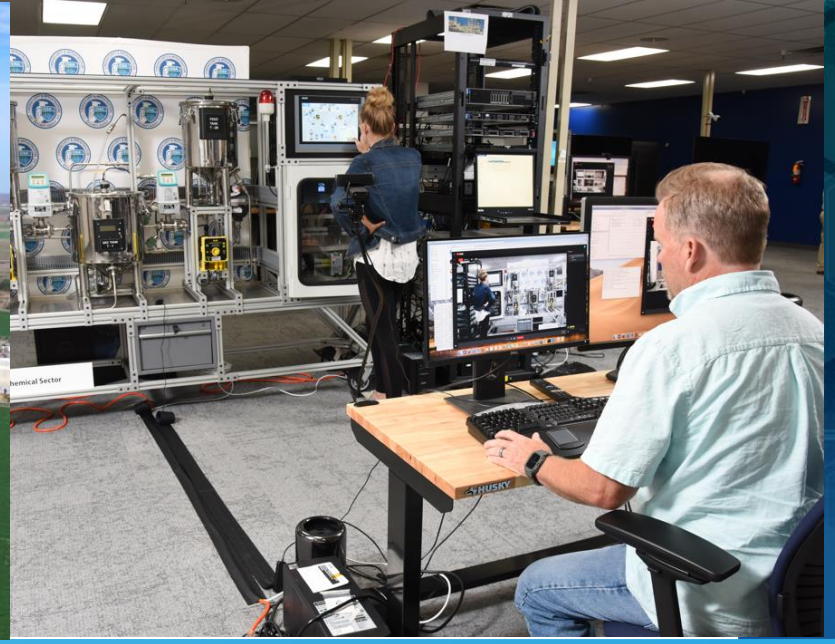
Timothy Adam Huddleston

November 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517



November 7, 2023

Timothy Huddleston
Project Manager

Lynn Pope
Technical Lead

Controls Environment Laboratory Resource (CELR)

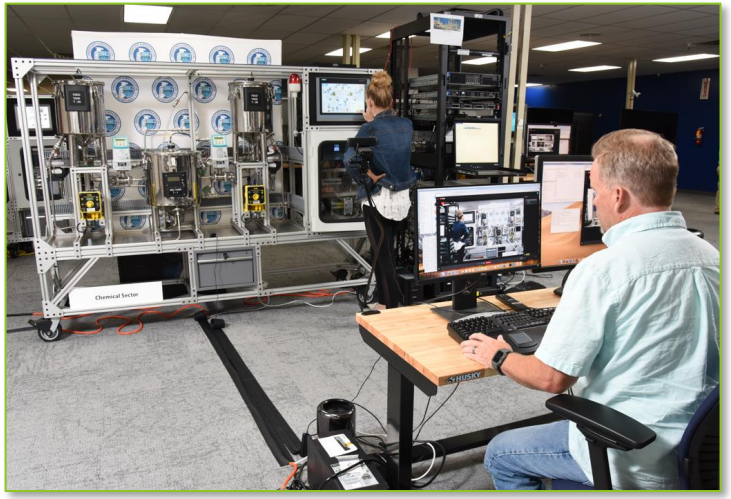
Energy Sector Section 9 Visit

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

Idaho National Laboratory

CELR Overview

- Control Environment Laboratory Resource (CELR) provides sector-specific critical infrastructure environments comprised of operational technology (OT) assets and traditional information technology (IT) systems for research, training, testing and other operational needs of CISA.
- CELR excels in demonstrating cyber-kinetic attacks that leverage Industrial Control System (ICS) elements such as SCADA systems, HMIs, PLCs, OT/IT pivot points, etc.
- Primary Use Cases:
  - ICS/OT Training (Red v. Blue Team Events)
  - OT Capability Evals (DT&E, OT&E, Independent)
  - Vulnerability & Mitigation Measure Research
  - Malware Analysis and Execution



CELR Partners

Idaho National Laboratory

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Pacific Northwest
NATIONAL LABORATORY

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

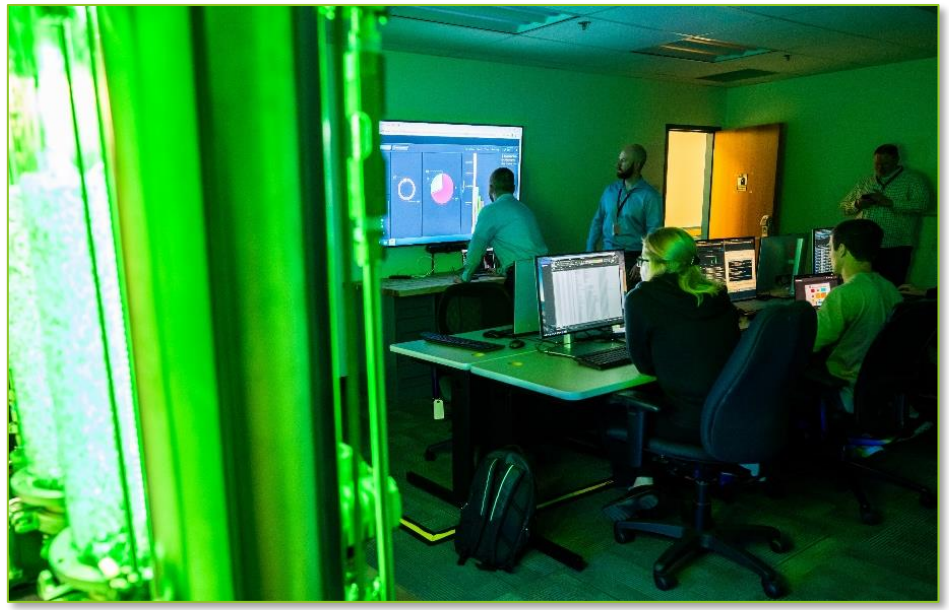
MITRE

CELR
CONTROL ENVIRONMENT LABORATORY RESOURCE

CELR Support

- CELR aims to represent a diverse breadth of critical infrastructure sectors providing opportunities for enhancing the way public and private partners defend ICS networks.

- CELR Supports:
  - CISA's Operational Needs
  - U.S. Critical Infrastructure Owners & Operators
  - Federal Civilian Agencies (e.g., DHS, DOE, DOD)
  - International Partners
  - Academia & Researchers
  - Vendors & Integrators



Current Portfolio of ICS Platforms

Sector Platform	Location	HMI	PLC	OT Protocol(s)
Automotive	INL	N/A	N/A	CAN bus
Building Management System	INL	Web-Based Alerton Ascent Compass on Microsoft Windows Server	Alerton VLCS-1688 configured with Alerton Visual Logic	BACnet
Chemical Processing Plant	INL	Siemens TP1500 Comfort Panel color Touchscreen	Siemens S1516-3 PN/DP	Profibus/Profinet
Electric Distribution	INL	N/A	SEL Axion 2240 w/ SEL-3530 Real-Time Automation Controller	DNP
Electric Transmission	INL	N/A	SEL Axion 2240 w/ SEL-3530 Real-Time Automation Controller	Modbus
Hydroelectric Dam	PNNL	Rockwell Automation RSView SE, Induction Automation Ignition	Allen Bradley ControlLogix 1756, Wago 750, SEL 3505, SEL 851	Modbus TCP, ENIP, DNP3, Profinet
ONG Pipeline Compressor Station	INL	Maple and OASyS HMIs	Emerson Bristol Babcock ControlWave PAC	BSAP
ONG Pipeline Compressor Station	Arlington, VA	Allen Bradley PanelView Plus 7	Allen Bradley ControlLogix 5571	Ethernet IP
Rail Mainline	PNNL	N/A	Hitachi Microlok II	Genisys, EMP (Edge Messaging Protocol)
Wastewater Treatment	PNNL	AVEVA Intouch	AB 1769 CompactLogix	ENIP, Modbus
Water Treatment	PNNL	AVEVA Edge	DirectLogic 205 Koyo D2-068DC1-1	Modbus

Building Management System

- Alerton Equipment
- BACnet Protocol

- Physical Effect:
  - Electric Power
  - HVAC Operations
  - Lab Fume Hood

Idaho National Laboratory

Chemical Processing Plant

- Siemens Equipment
- Profibus/Profinet, S7Comm Protocol

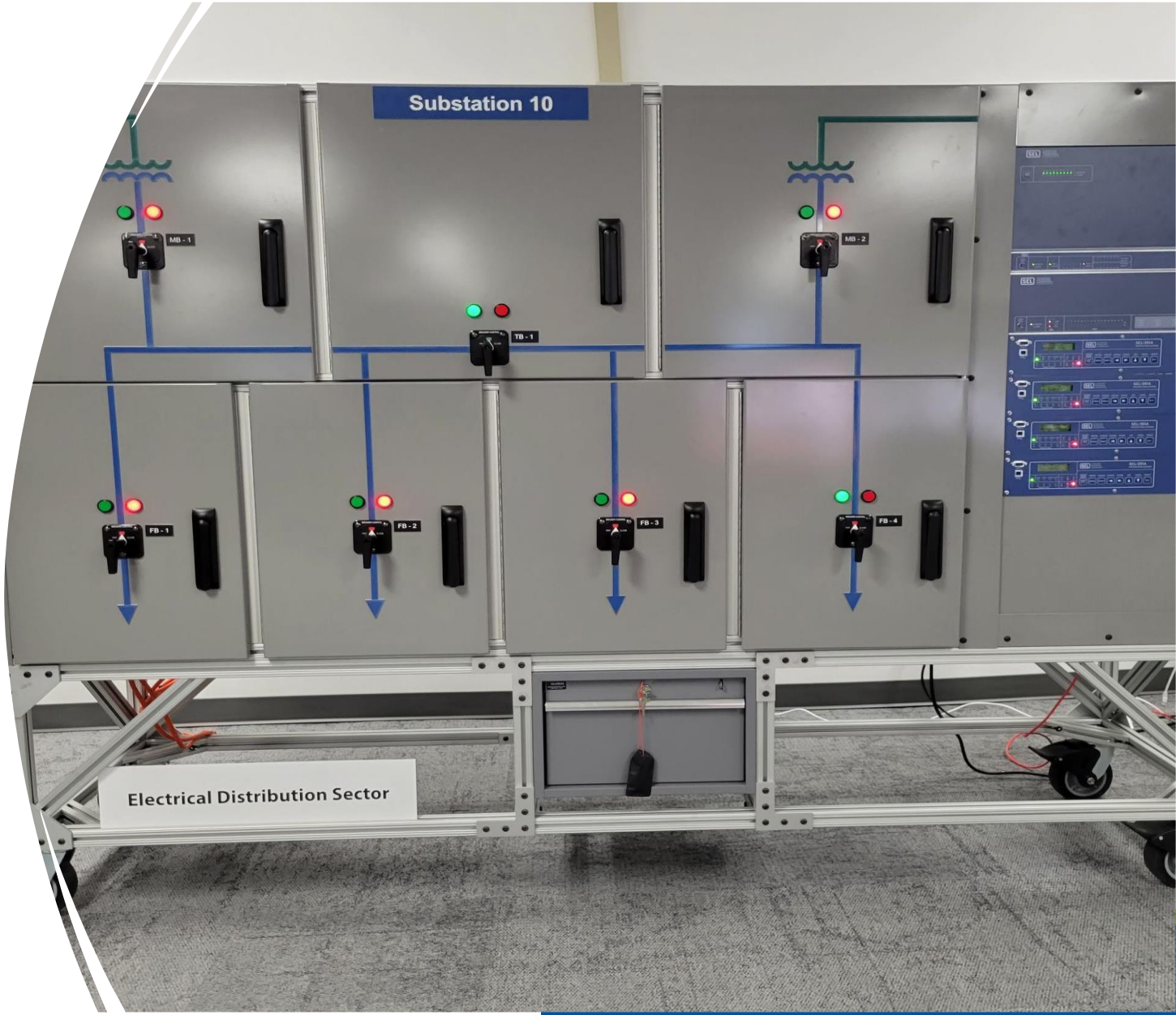
- Physical Effect:
  - Mixing Operations
  - Improper Ratio
  - Overflow Mixing Tank

Idaho National Laboratory

Electric Distribution Substation

- SEL Equipment
- DNP3 Protocol

- Physical Effect:
  - Circuits & Breakers



Idaho National Laboratory

Electric Transmission Substation

- SEL Equipment
- Modbus Protocol

- Physical Effect:
  - Circuits & Breakers
  - Switch (Arcing)

Idaho National Laboratory

Hydroelectric Dam

- Allen Bradley, Prosoft, and SEL Equipment
- Modbus TCP, Ethernet/IP, DNP3, and Profinet Protocols

- Physical Effect:
  - Electric Turbine
  - Spill Gates
  - Navigation Locks
  - Forebay Level Control

Pacific Northwest
NATIONAL LABORATORY

Oil & Natural Gas Compressor Station

- Emerson Bristol Babcock ControlWave (INL), Allen Bradley (Glebe) Equipment
- BSAP (INL), Ethernet/IP (Glebe) Protocol

- Physical Effect:
  - Compressor Operations
  - Vent Flare

Idaho National Laboratory

Rail Mainline

- Hitachi Equipment
- Genisis, EMP Protocols

- Physical Effect:
  - Centralized Traffic Control (CTC) communications
  - Positive Train Control (PTC) communications

Pacific Northwest
NATIONAL LABORATORY

Wastewater Treatment

- Allen Bradley Equipment
- Ethernet/IP Protocol

- Physical Effect:
  - Anaerobic Digester
  - Particulate Membrane
  - Barscreen

Pacific Northwest
NATIONAL LABORATORY

Water Treatment

- Direct Logic Equipment
- Modbus TCP Protocol

- Physical Effect:
  - Ultraviolet (UV) Treatment
  - Water Supply
  - Ozonation

Pacific Northwest
NATIONAL LABORATORY

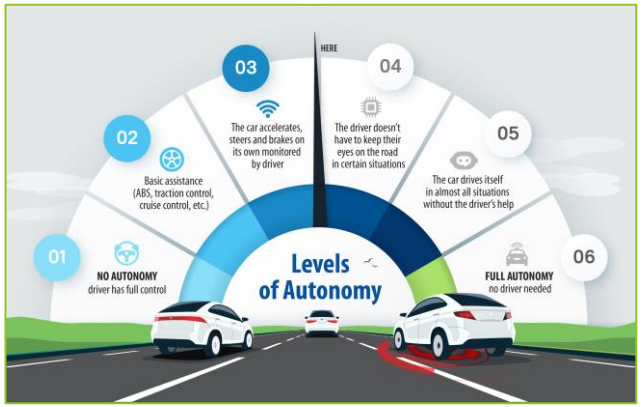
Portable Demonstration Units

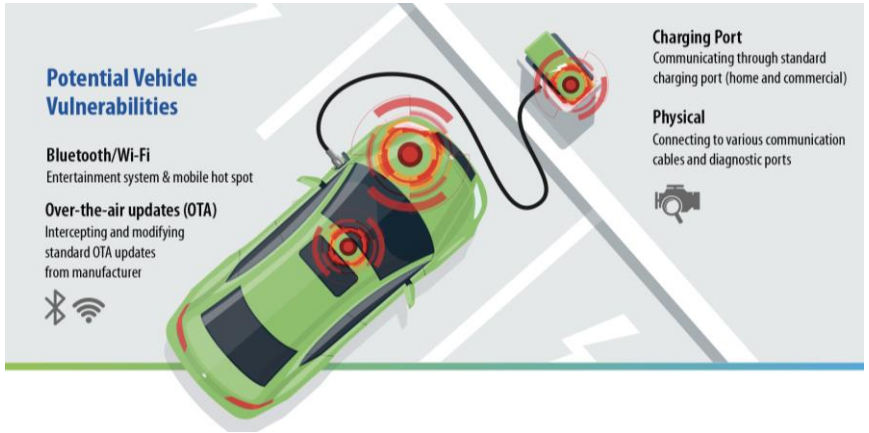
- Communications
- Electrical Grid
- Food & Agriculture
- Healthcare
- ONG Separator
- Transportation
- Water/Wastewater

Idaho National Laboratory

Automotive Cyber Research

- Research on communications networks, pathways, and protocols (CANbus)
- Focus on leading edge Electric Vehicles (EV) with Semi-Autonomous Capabilities
- Attack vectors include EV charging stations, over-the-air communications, Bluetooth

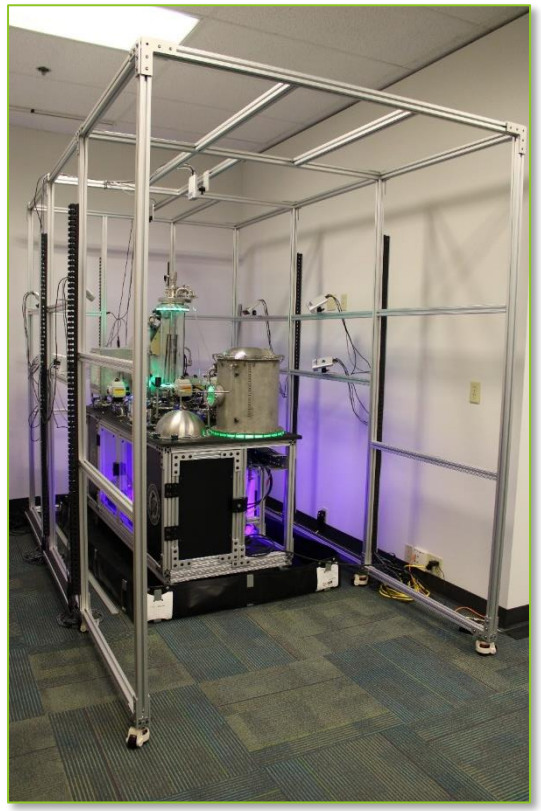




Idaho National Laboratory

Mixed Reality / Virtual Reality

- Microsoft and Scatter Equipment
- Creates 3D recordings and renders of CELR platforms for community outreach



Questions?

For more information:

www.inl.gov/ics-celr/

Questions?

Email: timothy.huddleston@inl.gov

Email: cisa_celr@cisa.dhs.gov

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.