



An Old Guys Perspective of Cyber - Journey Through INL Cyber Research

November 2024

Changing the World's Energy Future

Kenneth W Rohde



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

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

An Old Guys Perspective of Cyber - Journey Through INL Cyber Research

Kenneth W Rohde

November 2024

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

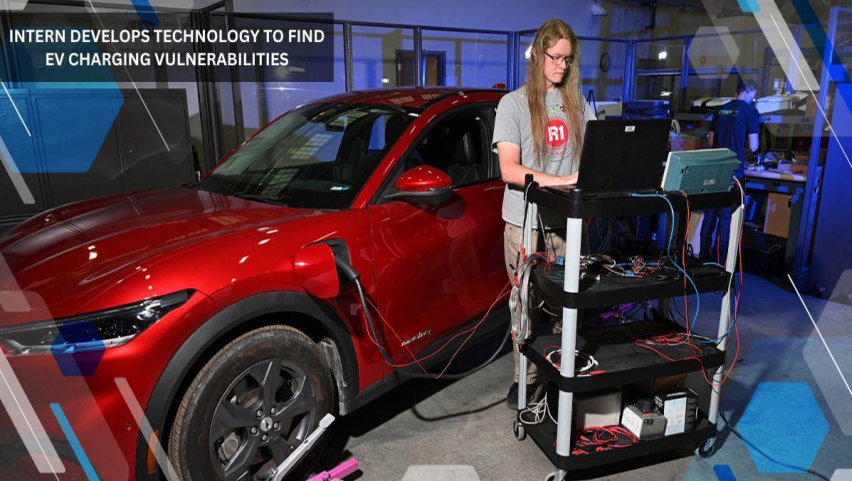
<http://www.inl.gov>

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



November 7-8, 2024

Kenneth Rohde
Cybersecurity Research



INTERN DEVELOPS TECHNOLOGY TO FIND
EV CHARGING VULNERABILITIES

An Old Guys Perspective of Cyber Journey through INL cyber research

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





Overview of INL

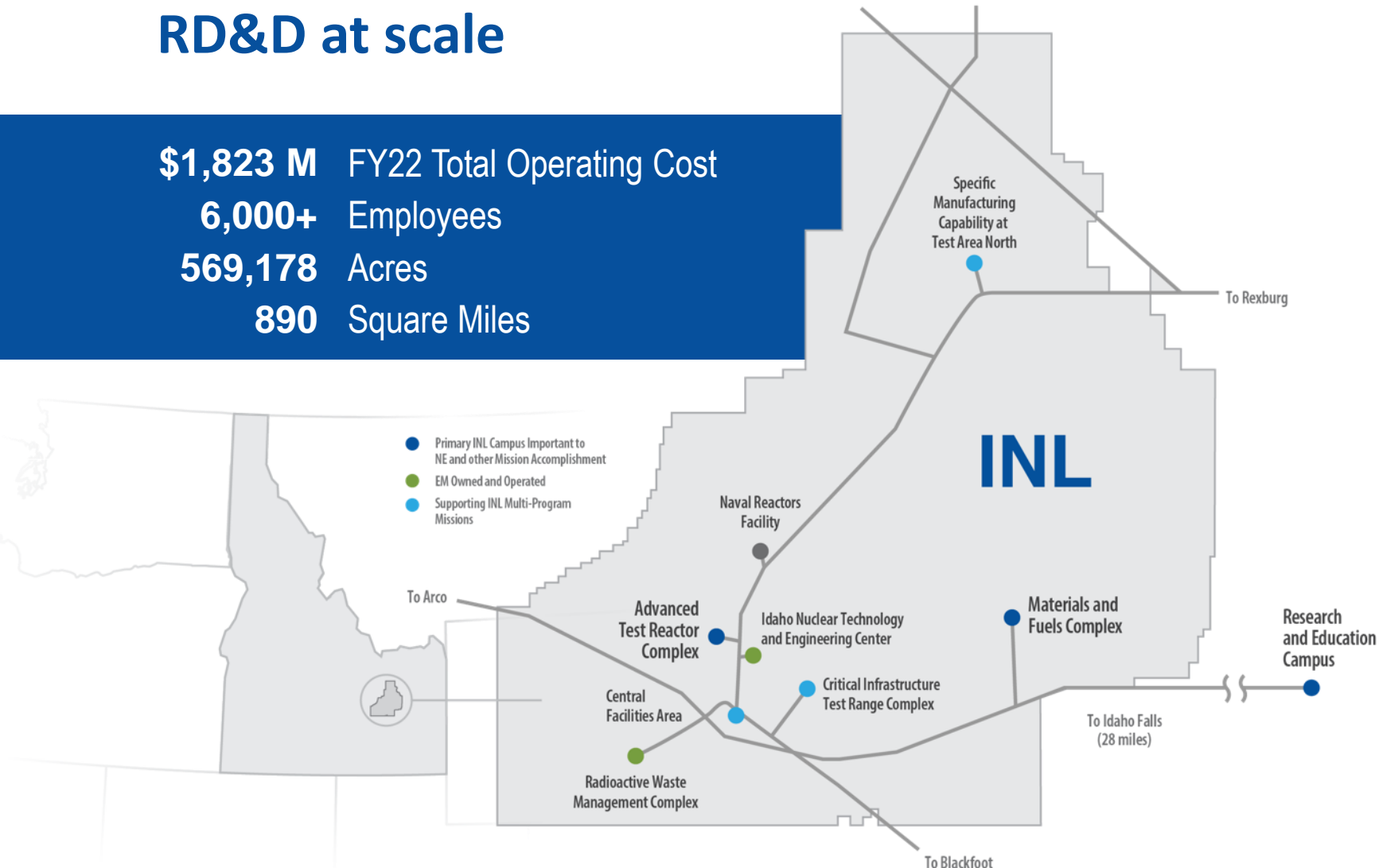
INL' s Position Today – Nationally

- One of 17 DOE multi-program labs
- DOE' s designated lead lab for nuclear energy research, development and demonstration
- A major contributor in national and homeland security, alternate and renewable energy and science and technology
- 890 sq. miles
- ~6000 staff



Unique INL site, infrastructure, and facilities enable energy and security RD&D at scale

\$1,823 M FY22 Total Operating Cost
6,000+ Employees
569,178 Acres
890 Square Miles



4 Operating reactors

12 Hazard Category II & III non-reactor facilities/ activities

50 Radiological facilities/activities

17.5 Miles railroad for shipping nuclear fuel

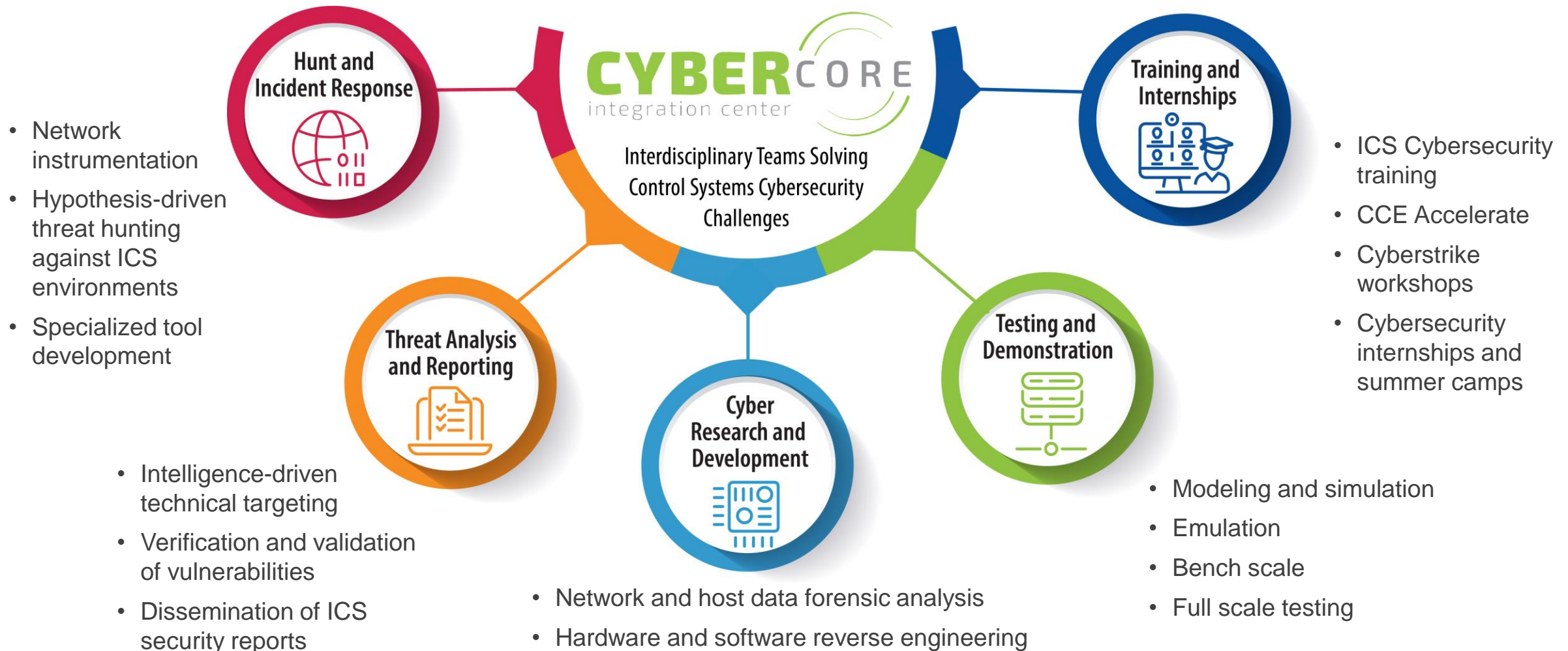
44 Miles primary roads (125 miles total)

9 Substations with interfaces to two power providers

126 Miles high-voltage transmission lines

3 Fire Stations

Cybercore Capabilities

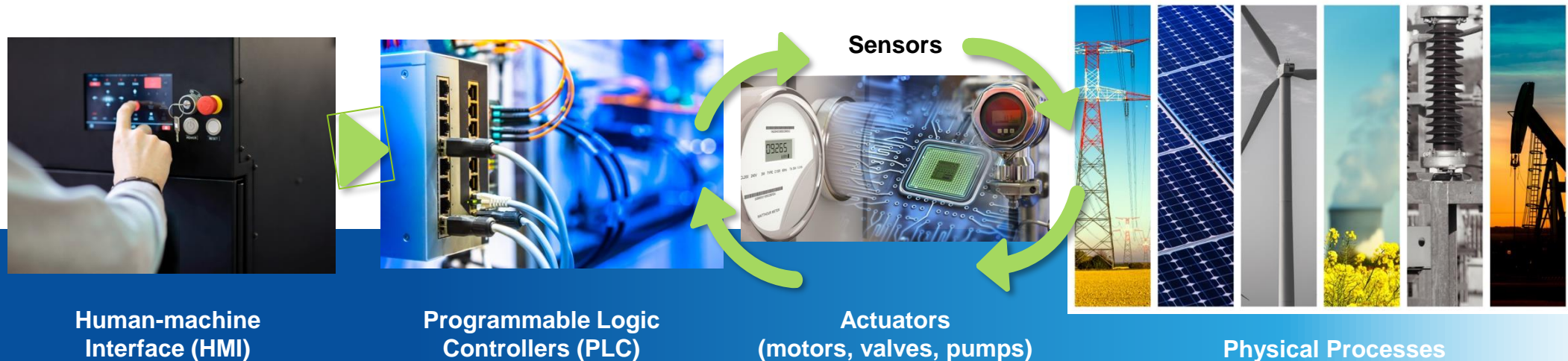


Cybercore's Focus: Critical Function Assurance of Operational Technology (OT)

Digital systems govern and execute complex processes across sectors and infrastructures.

Examples of OT include:

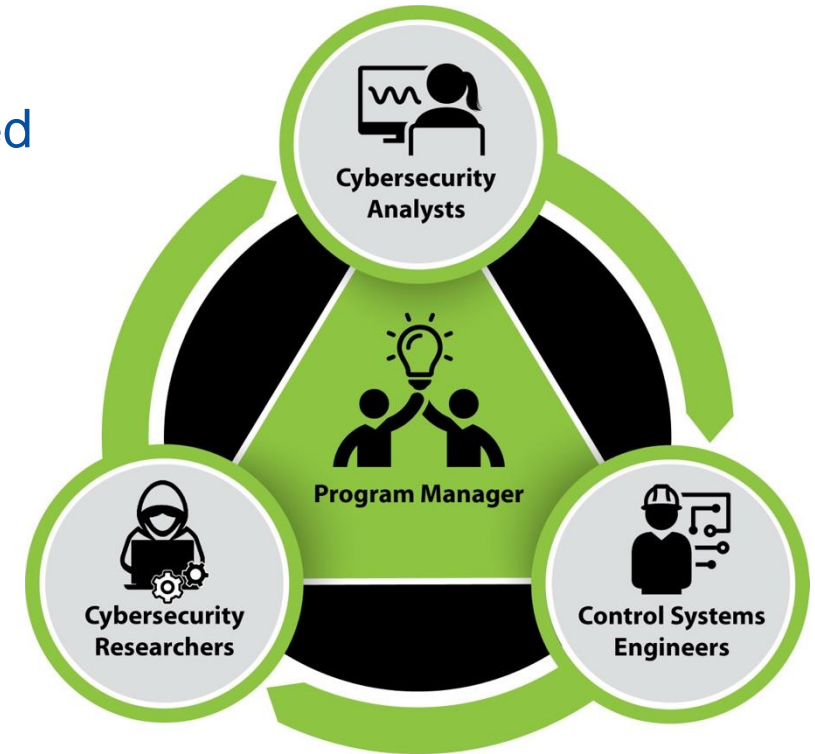
- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)
- Distributed control system (DCS)



The Troika Approach

Interdisciplinary teams that are the integration of specialized expertise which is required to solve our most challenging technical problems.

- **Technical Analysts:** All-source, threat informed technical analysis
- **Control Systems Engineers:** ICS and critical infrastructure subject matter experts
- **Cybersecurity Researchers:** Cutting edge in-depth vulnerability assessments



“Think like the adversary” approach to ensure Critical Function Assurance




Cybersecurity R&D

Origins

- Department was formally created in 2004 after a group of INL employees hacked a Supervisory Control and Data Acquisition (SCADA) system in 2003
- National recognition with the formation of the DOE National SCADA Test Bed and the DHS Control Systems Security Program
- Primarily provided assessments of Industrial Control Systems (ICS) and cyber security awareness trainings





**“Remember kids, the only
difference between Science and
screwing around is writing it
down.”**

- Adam Savage

Aurora Generator Test (2007)

- Put INL and DHS on the map...
- Demonstrated how cyber might cause physical damage



Today

- Continue to support our primary customers
 - DOE CESER and EERE
 - DHS S&T and CISA
- A variety of other customers both in government and the private sector
- Leveraging our 20+ years of experience with ICS to develop unique cyber security solutions
 - Assessments still continue
 - Tool and technology development is exploding
- The scope of our cyber security business has grown into many sectors



How Cyber Has Changed

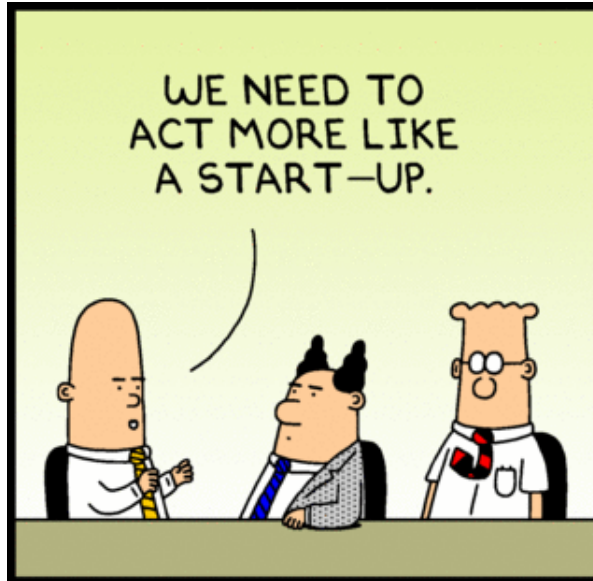
2004

- There were only 3-4 conferences worth attending
- DEF CON 10 – est. 300 people
- I hacked this “SCADA” system (PLC on the table)
- Hacking x86 and x64 services and software
- Focus on SCADA and Industrial Control Systems (usually the servers and software)
- Large systems, big software
- Isolate and disconnect from everything

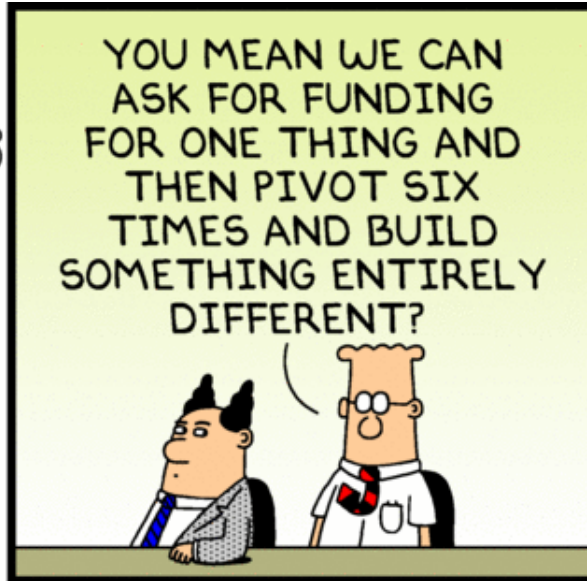
2024

- There are too many conferences to list
- DEF CON 32 – est. 30,000 people
- Here is how I modified the firmware in a VFD
- Unlocking and modifying firmware
- Building automation, HVAC, automobiles, aircraft, traffic signaling, access control systems, medical devices, etc.
- Chip off analysis, embedded devices
- IIOT – yeah, that’s a great idea

An entire industry created and exploded in 20 years!



Dilbert.com DilbertCartoonist@gmail.com



8-1-14 © 2014 Scott Adams, Inc./Dist. by Universal Uclick



What Does Cyber Security Mean?

- Protection of digital systems from unauthorized or unintended use
- Protection of digital data
- Protection of physical systems connected to digital controls
- Protection of “critical infrastructure”

- Engineering design to mitigate potential impacts of cyber influence
- Analysis and education of how systems should be deployed

A combined team of experts in their field who understand the potential harm that might be caused as a result of successfully exploited vulnerabilities

What Is A Vulnerability?

- A quality or state of being exposed to the ***possibility*** of being attacked or harmed, either physically or emotionally (dictionary)
 - Unencrypted sensitive data
 - Buffer overflows
 - Missing guards on a table saw
 - No GFCI outlet near the pool
 - Disgruntled employees



What Is An Exploit?

- To make use of and derive benefit from a resource (dictionary)
 - Ransomware
 - Code Red
 - Email phishing
 - Loss of power
 - Loss of life

Not all vulnerabilities are exploitable!



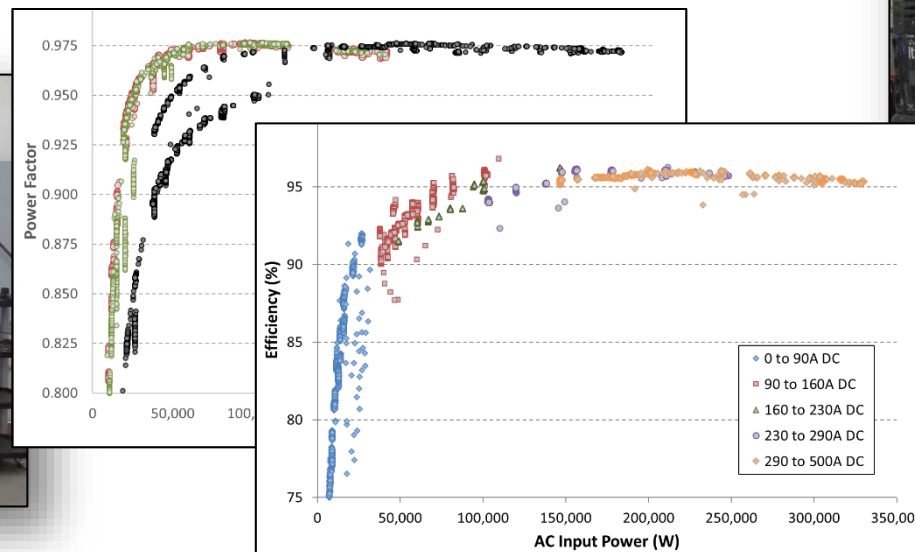
Some Current Research

NIPP Critical Infrastructure Sectors

1. Chemical
2. Commercial facilities
3. Communications
4. Critical manufacturing
5. Dams
6. Defense industrial base
7. Emergency services
8. **Energy**
9. Financial services
10. Food and agriculture
11. Government facilities
12. Healthcare and public health
13. Information technology
14. Nuclear reactors, materials, and waste
15. **Transportation systems**
16. Water and wastewater systems

INL's Electric Vehicle Charging Infrastructure Lab (EVIL)

- Grid integration of high-power EV charging infrastructure
 - Advance charging system characterization
 - Xtreme fast charging (XFC) hardware
 - CCS vehicle charging emulator (400kW)
 - Grid interaction evaluation w/ Power & Energy Systems lab
 - Power hardware-in-the-loop (540 kVA)
 - High fidelity distribution feeder models
 - Virtual tour: EVIL and Power & Energy Systems lab
 - <https://avt.inl.gov/panos/EVLTour/?startscene=pano5141>



EVIL's V2X Cafe

- BorgWarner 60kW V2G with Synop Energy Management system
 - EV emulator: Dana EVCC, CCS-1 inlet, Bitrode battery emulator
- Ford 9.6kW V2H (*Intelligent Back-up Power*)
 - 2024 Ford F150 Lightning
- Fermata 20kW V2G with Fermata Energy Management system
 - 2015 Nissan LEAF



“With great power comes...”

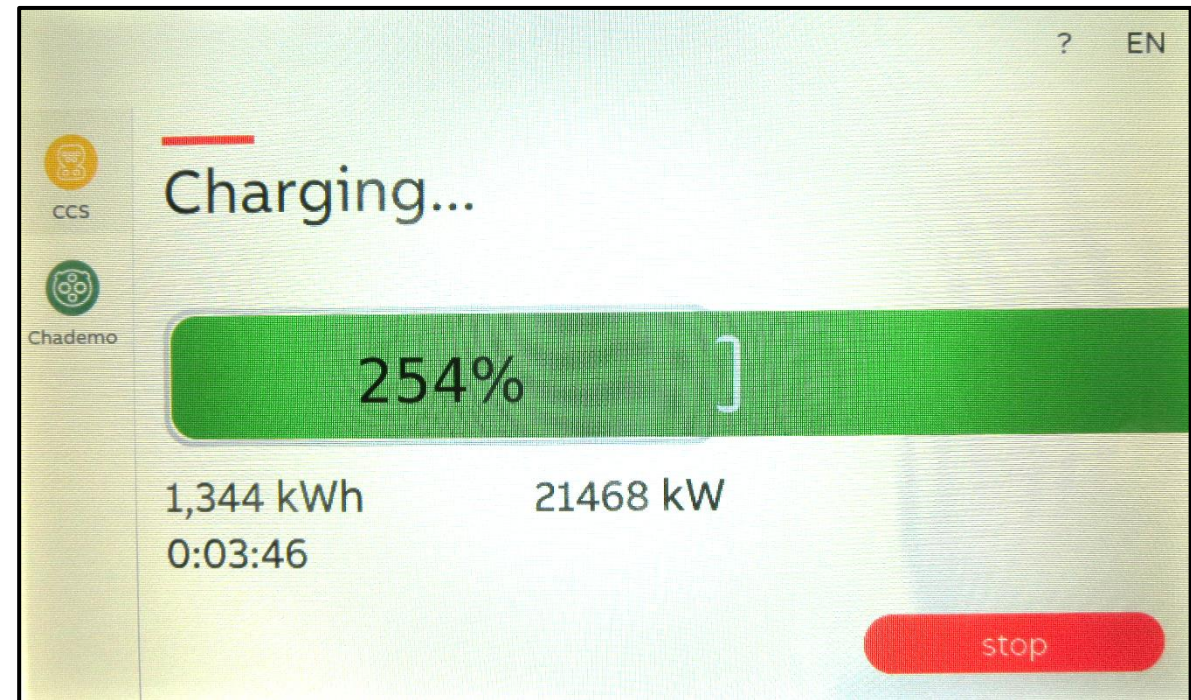
- With higher complexity comes more vulnerabilities
- Electric and autonomous vehicles raise the bar significantly
 - F-22 Raptor – 2 million
 - Boeing 787 – 7 million
 - 2006 Ford GT – 10 million
 - 2016 Ford F150 – 150 million
 - Autonomous/Electric Vehicles – a plethora!
- A more complex infrastructure is also required



When things go wrong...

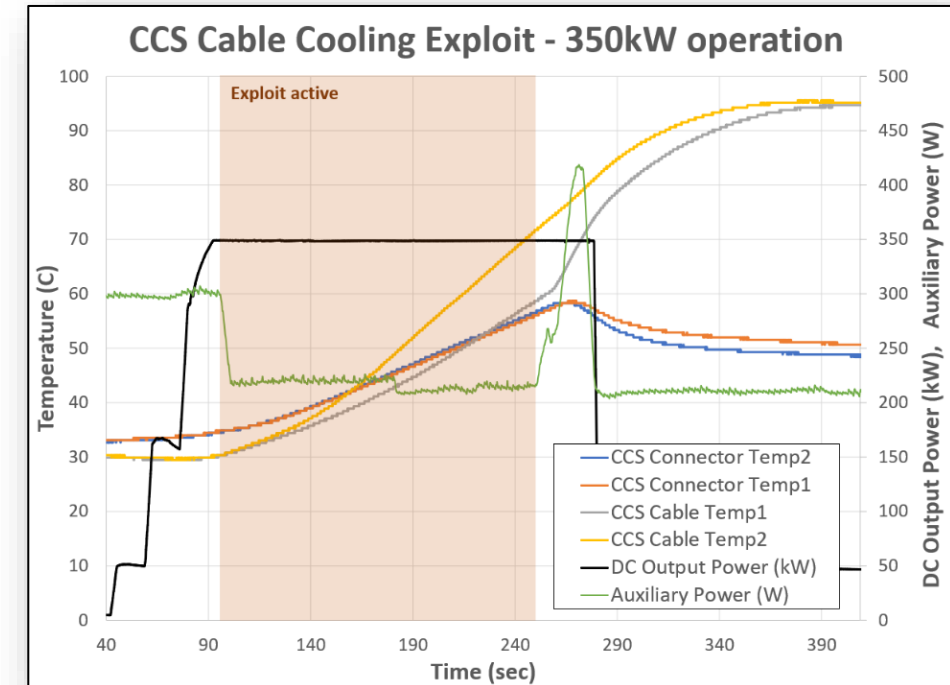
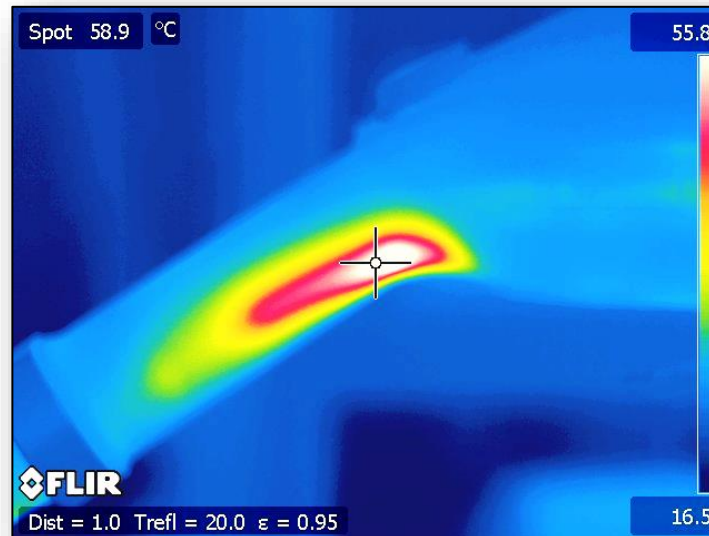
Charging Station Exploit - HMI

- Spoofed SOC%, DC current, & DC voltage
 - 254% SOC, 6554A, 3277V (21.5 MW)
- Impacts:
 - Displayed values seen by customer
 - Reported kWh delivered *may* impact actual cost \$\$ of charge session
(1,344kWh * \$0.42 = \$564.48)
- Does NOT impact:
 - Safety, hardware, grid stability, charge resiliency (no physical impact)



Charging Station Exploit - Liquid Cooled Charge Cable

- Manipulation of XFC cable liquid chiller system
 - Temperature measurement
 - Coolant pump control
- Exploit shown to be successful at 350kW



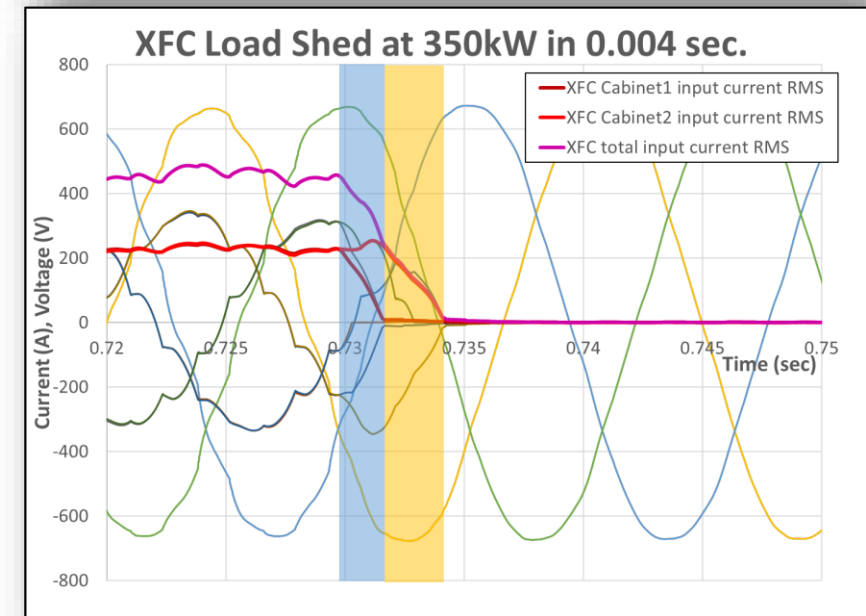
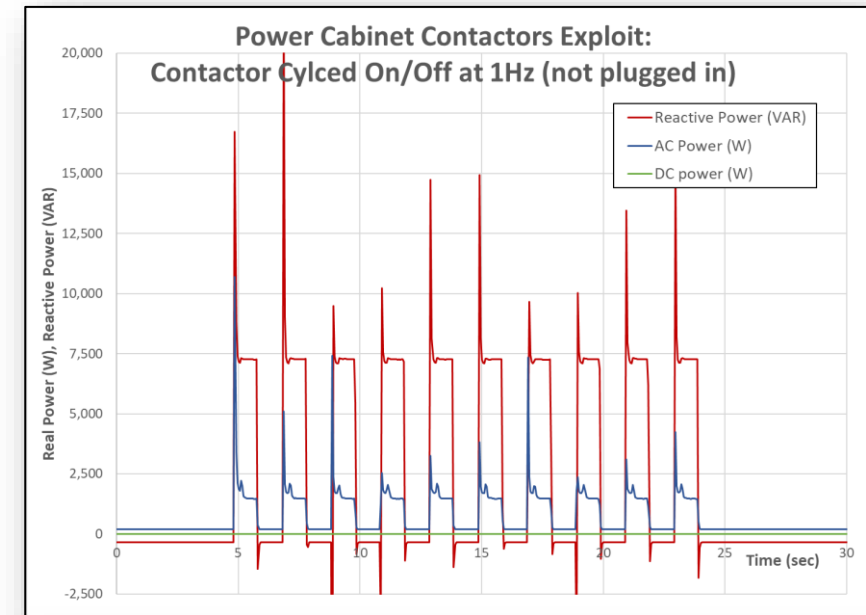
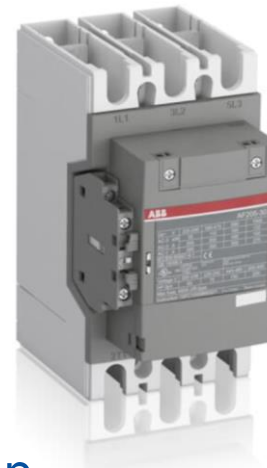
Charging Station Exploit - High Voltage Present at CCS Connector

- note: DC voltage should only be present at the CCS connector AFTER
 - Connection to EV is verified
 - Ground-fault safety check completed
- Spoofing internal controls communication for:
 - AC/DC inverter control
 - Contactor control between inverter systems and the CCS cable
- Result: 826V DC present on CCS connector while not plugged into an EV



Charging Station Exploit – Hardware Manipulation

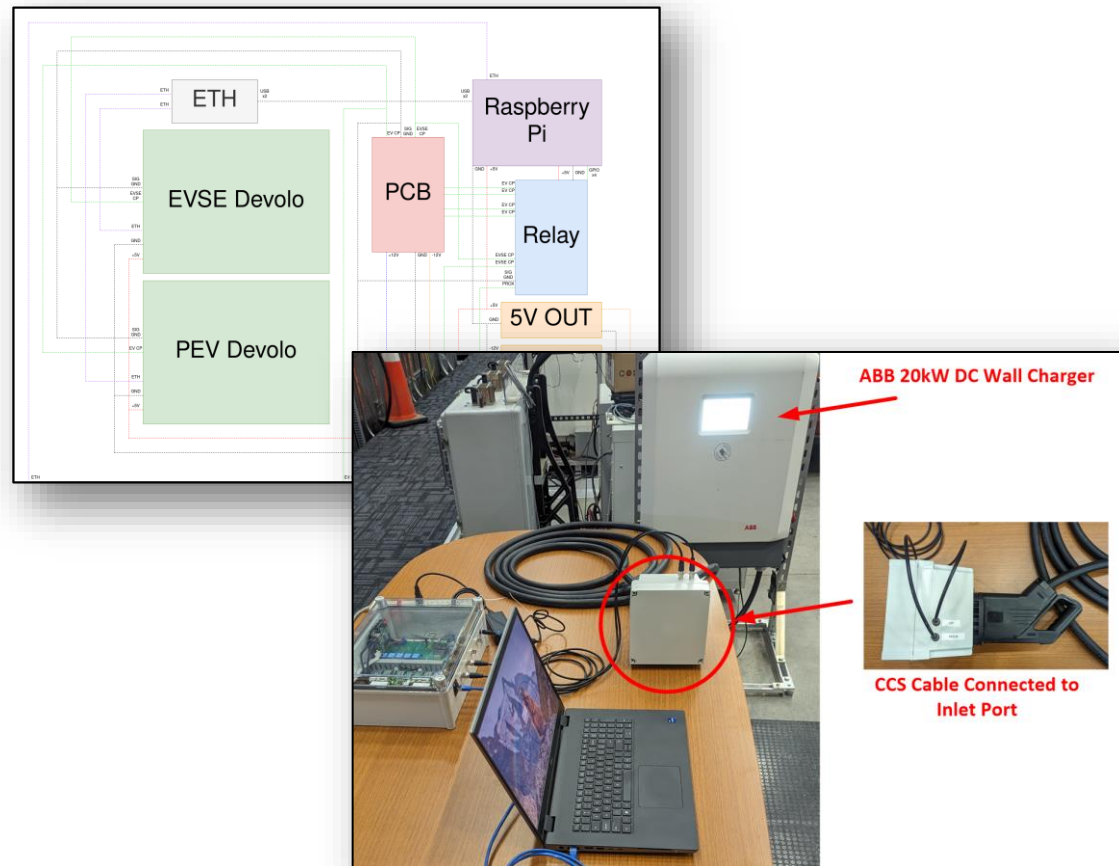
- Power cabinet main AC contactor control
 - Contactor control was accomplished
 - Turn ON contactors while not plugged in to EV
 - Turn OFF while charging, opening the contactors ends the charge event
 - Rated for:
 - 5 million switching cycles
 - 3,500A max. breaking capacity
 - 15x than 350kW operation
 - 300 cycles / hour (12 second period)
 - **Yet, another method for load shed**
 - Opened contactors during 350kW operation
 - 0.004 second load shed



Some Research Outcomes

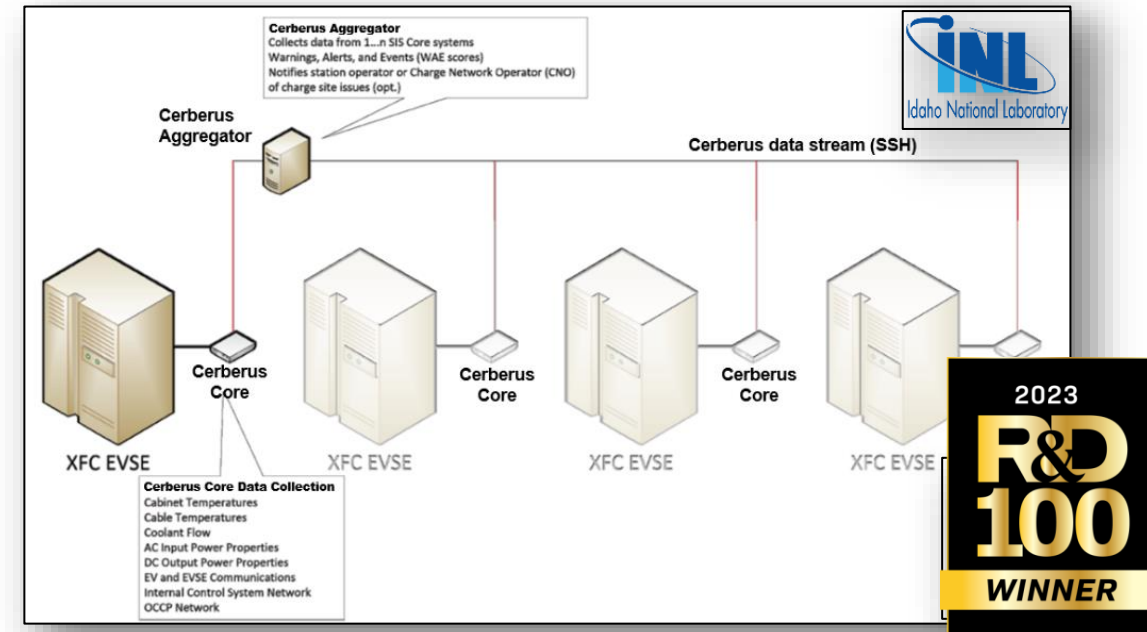
Access Capabilities for CCS (AcCCS)

– <https://github.com/IdahoLabResearch/AcCCS>



CERBERUS

– Detect, Respond Recover





Current Research Needs

How is this still happening?!?

Remember the phrase “with great power comes great responsibility?”



“With great complexity comes a plethora of vulnerabilities!!”

Cybersecurity is Difficult to Scale

- Many different systems are available in each sector
- Intelligent, experienced humans are always required
- Tools are needed to make the humans job faster and easier
 - Machine learning will help
- It will always be an arms race between attackers and defenders
- Stop creating the problem
 - Better “education” (schools and workplace)
 - Too often we add complexity in the name of convenience

"Hey Siri, protect my EV charger"

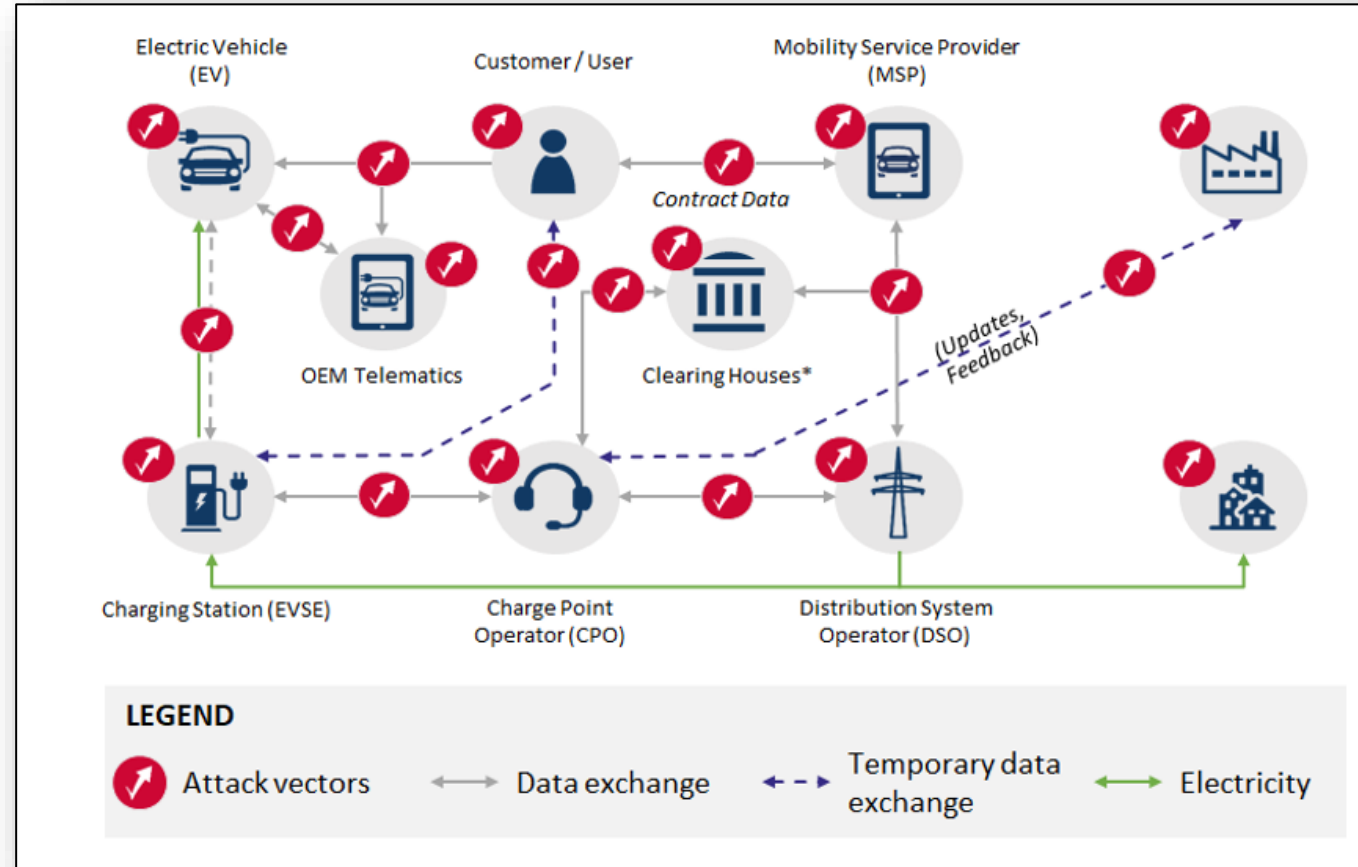
"Sure! Now playing Stevie Wonder on Apple Music"

Reference Architectures are Rarely Used

- Excellent secure by design systems are published and available
- Integration and configuration is still too difficult
- Overall, the expense is too high for production devices

A new approach is needed, but this will require a major technology change.

Large Distributed Systems are Still Difficult



Large Distributed Systems are Still Difficult



But, but...

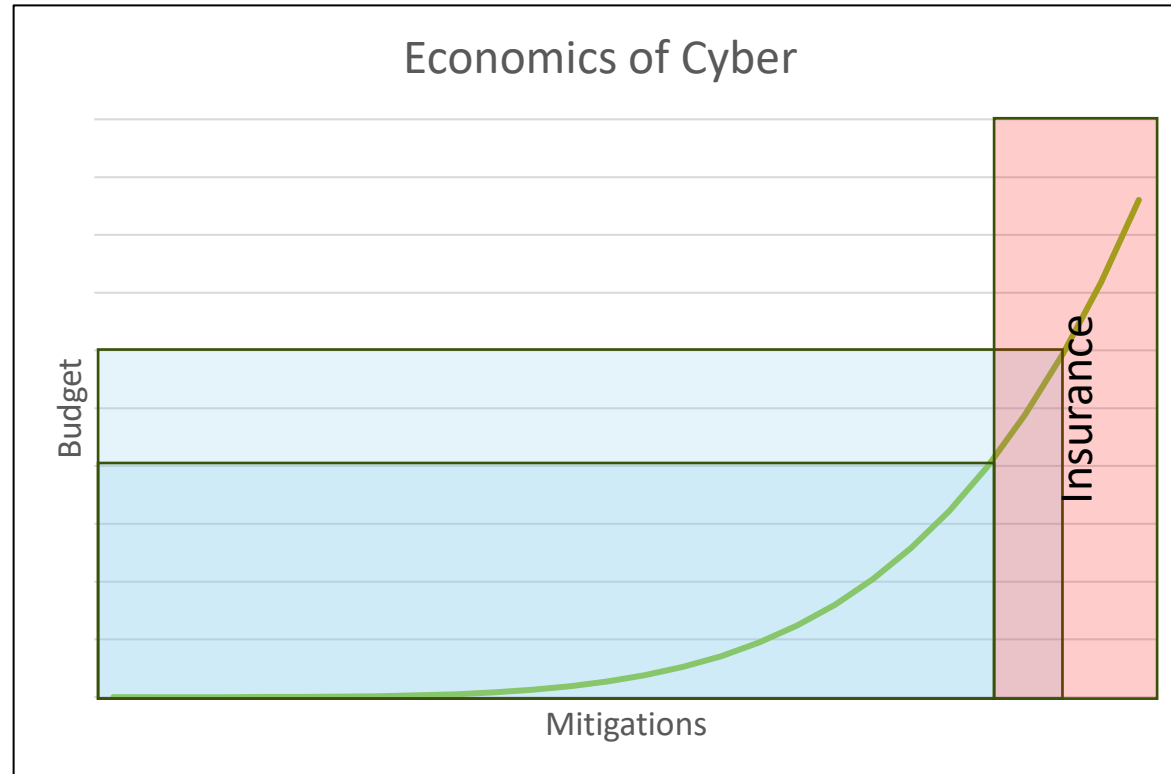


"OK, boomer"



A Word on Economics

A War We Cannot Win...



***“You’ve fell victim to one of the classic blunders!
The most famous is never get involved in a land war in Asia,
but only slightly less well known is this...”***

IDAHO NATIONAL
LABORATORY



TH
ANNIVERSARY

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.



Idaho National Laboratory

www.inl.gov

Kenneth Rohde
kenneth.rohde@inl.gov