NREL
NATIONAL RENEWABLE ENERGY LABORATORY

Disruptive Ideas for IT/OT Security in Energy Systems

Maurice Martin
2018 FICS Research Cybersecurity Conference
March 1, 2018

NREL/PR-5D00-71223

Cybersecurity at NREL

- The Cyber-Physical Systems Security and Resilience Center (CPSSR) is developing an **innovative way to secure operational technology (OT) networks that provide consistent cybersecurity protection across legacy and modern systems alike.**
- This allows for greater flexibility and adaptability as new technologies emerge, and eliminates a need for forklift upgrades of legacy energy systems to meet new cybersecurity requirements from compliance standards.
- OT networks, or industrial control systems, support command and control functions in any energy system.

Why OT Networks?

- A disruption to the OT network could physically disrupt the energy system it controls.
- Cybersecurity for information technology (IT) networks are more established compared to cybersecurity for OT networks, which directly impact the physical controls of energy systems.
- NREL's approach integrates its layered cybersecurity architecture to protect OT networks alongside IT networks.

Grid Disturbance: Cyberattack of an OT Network

Electricity

Regional power outages; disturbance in medical care, business, and government operations; possible data breach

Water

Water and wastewater treatment; increase in health risks; possible data breach

Gas

Disruptions to heat; equipment damage; gas leakage; possible data breach

Transportation

Public transit infrastructure; safety risks; possible data breach

Cybersecurity on Today's OT Networks

- OT networks have evolved over the past 50 years.
- There are older and newer systems with different communications processing capabilities.
- Today, there's a lot of advocacy around standards, creating a minimum set of requirements for memory processing and networking to support more modern controls.
- Legacy controls can't keep up, and businesses look for workarounds that can leave systems vulnerable.

The NREL Approach

Secure the network at a systemic level rather than solely relying on protocol or end point security. NREL incorporates a nine-layer architecture approach, which addresses network segmentation, role-based access control, intrusion detection, in-line blocking, and end-point security.

The NREL Approach

Key Aspects

1. Good network hygiene
2. Role-based access control
3. Signature-based and context-based intrusion detection
4. In-line blocking tools
5. End-point security using virtualization, hypervisors, virtual machines, and operating systems

All combined = NREL nine-layer architecture for cybersecurity.

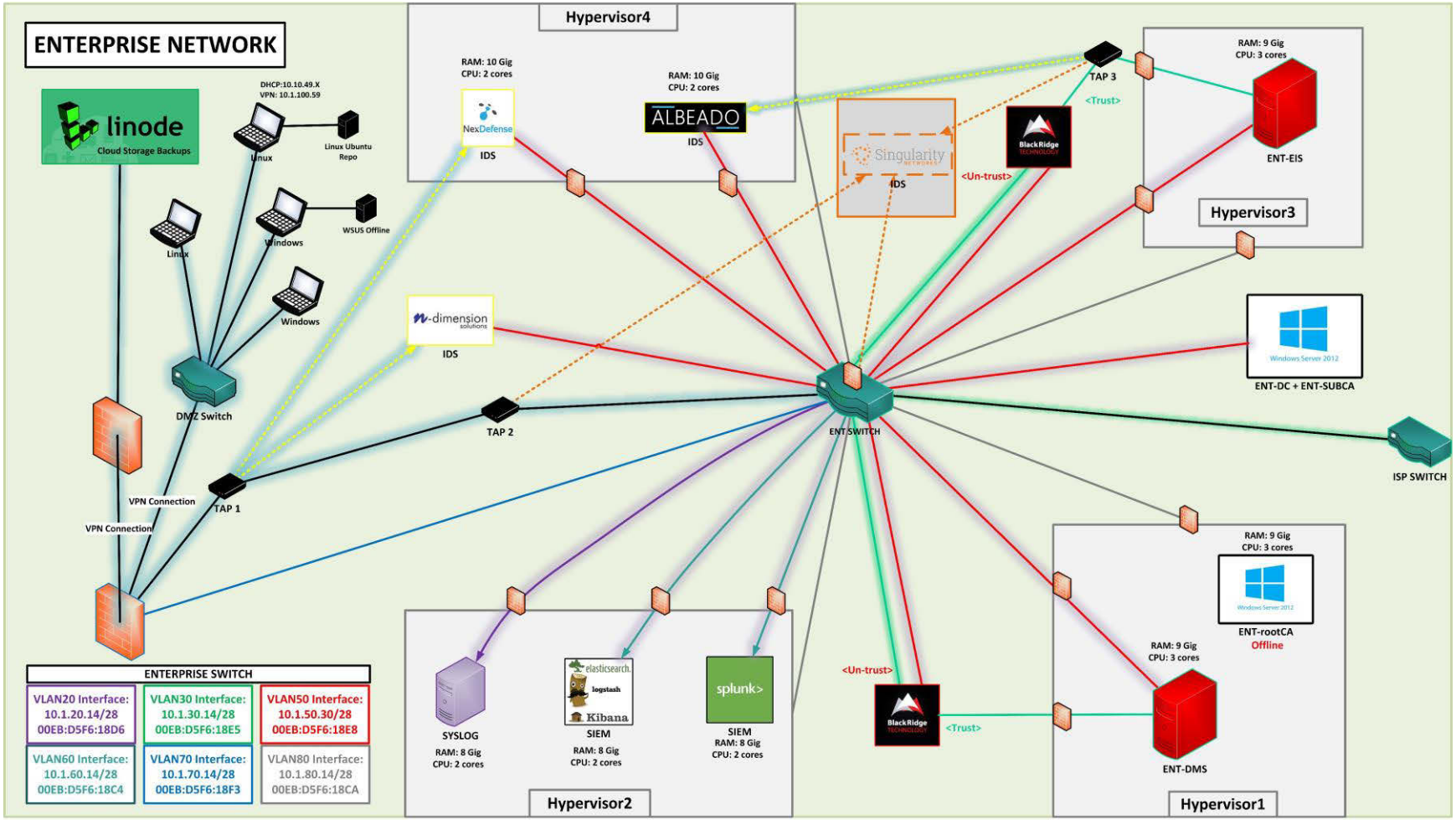

Diagram created by NREL, February 2018

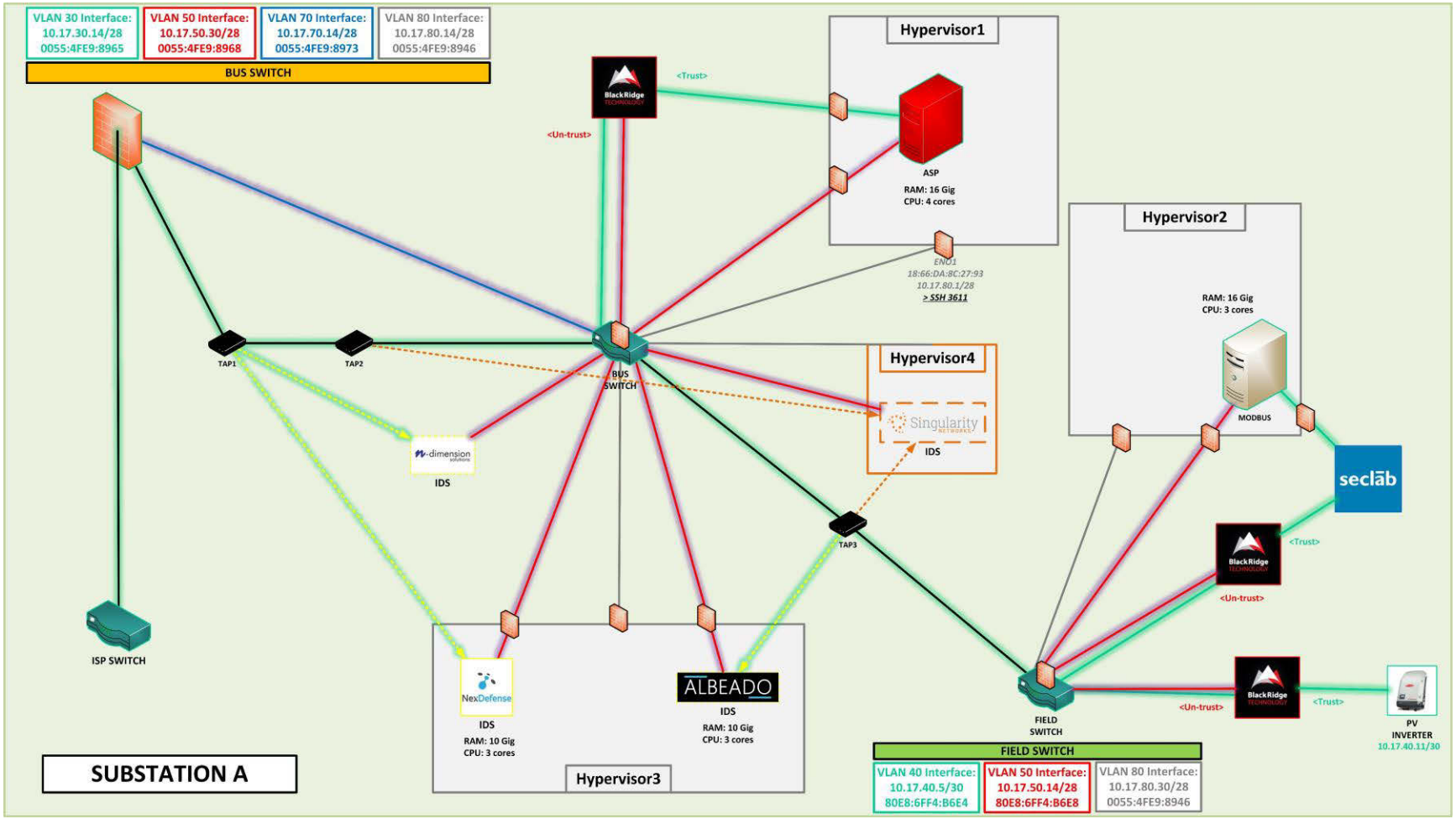

Diagram created by NREL, February 2018

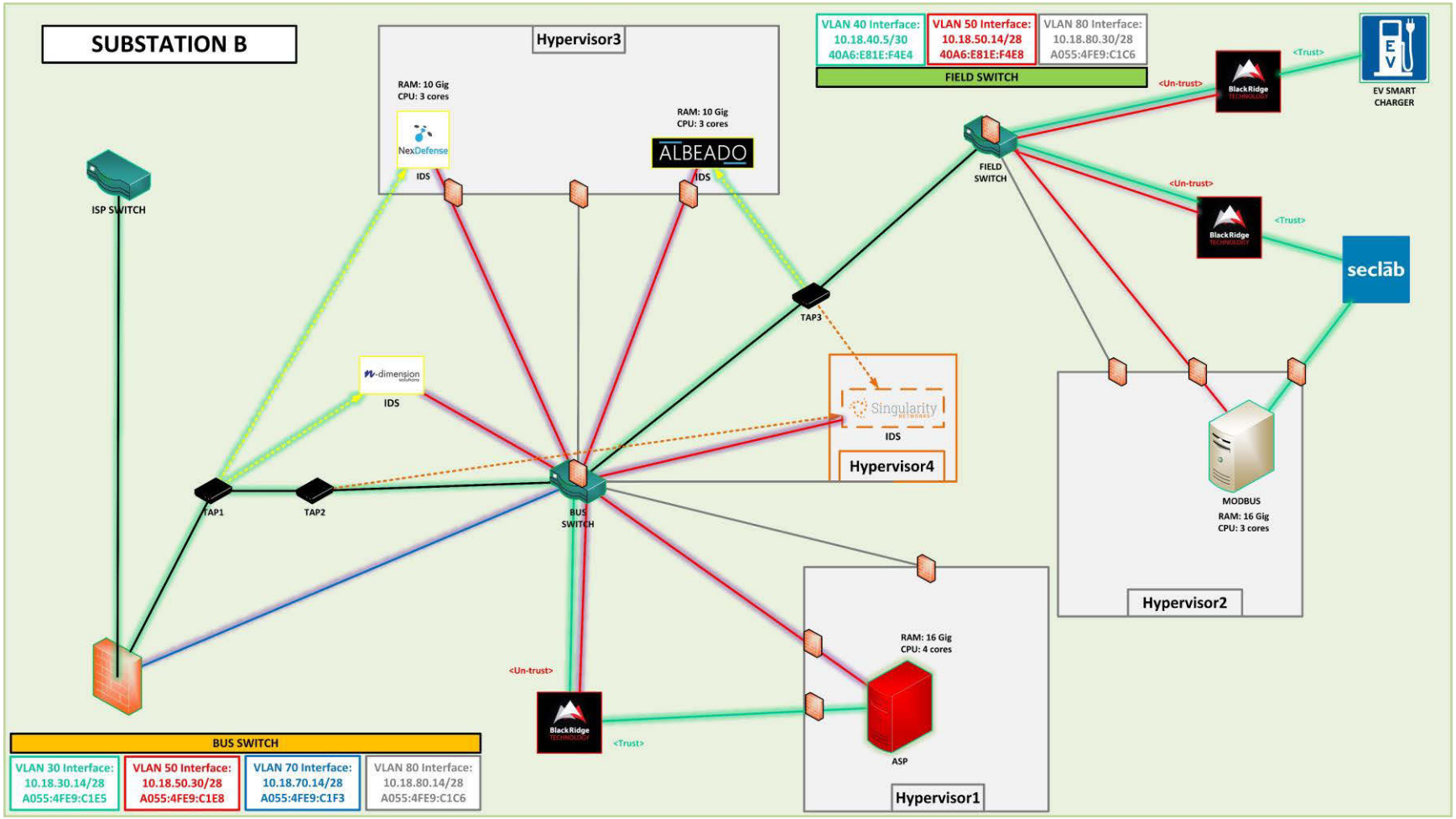

Diagram created by NREL, February 2018

Nine-Layer Security Architecture

Layer \ Security Application	SecLab Denelis	BlackRidge TAC	Cisco Firewall + Switches	NexDefense Integrity	N-Dimension N-Sentinel	Albeado PRISM
GWAC 5-6 Business						■
GWAC 4 Semantic	■			■	■	■
OSI 7 Application	■			■	■	
OSI 6 Presentation	■			■	■	
OSI 5 Session	■			■	■	
OSI 4 Transport	■	■	■	■	■	
OSI 3 Network	■	■	■	■	■	
OSI 2 Data Link	■					
OSI 1 Physical	■					

Flexibility & Resilience

The NREL approach offers:

- Protection of legacy and modern systems
- Flexibility to accommodate technologies of different maturity levels over time
- Ability to be resilient and evolve as hackers identify new entry points in new technologies.

R&D Projects at NREL's CPSSR Center

- Concurrently working with several public power, investor-owned, and co-ops across the United States
  - Approach is scalable **and** agnostic to any energy application
- Offering a 10-step systems engineering approach to help customers protect their IT and OT networks in a methodical way.

Our goal: to make sure that all enterprises across the United States adopt this type of process for current technologies, as well as new purchases.

10-Step Systems Engineering Approach to Securing Energy Technologies

1. Assess cyber-governance	Security controls in place, prioritized action items for gaps in security controls.
2. Evaluate gaps	Implement technical plan to address gaps identified in cyber-governance assessment
3. Validate technologies	Perform due diligence on cutting-edge technologies for energy systems identified in the technical plan
4. Identify language	Develop procurement language for secure, reliable, and resilient energy systems
5. Review architecture	Review energy system cybersecurity architecture and benchmark against NREL 9-layer cybersecurity model, including vulnerability assessment and risk mitigation
6. Identify risks	Scan energy system software code and binary executables to identify malware and cyber risks, in addition to techniques for mitigation
7. Evaluate data fuzzing	Validate data fuzzing vulnerabilities of energy system application with appropriate risk mitigations
8. Pen-test SCADA systems	Perform cybersecurity pen-tests of energy system in NREL's cybersecurity research platform and identify residual risks and provide mitigations
9. Analyze failure scenarios	Develop failure scenarios with mitigations to build incremental resilience
10. Train staff	Offer training on cybersecurity awareness for corporate staff and IT/OT audiences to reduce cyber risks from social engineering and phishing schemes from advanced, persistent threats

NREL's Cybersecurity Research Platform

- Ability to run realistic cybersecurity use cases and work the kinks out
- With a multi-site internet protocol (IP) network, ability to drop anything into the platform and create a unique environment
- Flexibility in level of evaluation
- Knowledge and expertise to help customers reduce risk before a technology is deployed.

A Utility Model of the Future

Through our work with a variety of industry partners, we're constantly researching the latest tools, capabilities, and systems that can be integrated into NREL's nine-layer architecture. Our approach enables a viable, long-term solution for the secure integration of emerging energy technologies.

Thank you

www.nrel.gov

maurice.martin@nrel.gov

NREL is a national laboratory of the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, operated by the Alliance for Sustainable Energy, LLC.