U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Cybersecure Interconnection of Distributed Energy Resources (DER)

Lawrence Livermore National Laboratory

Jhi-Young Joo, Emma Stewart, Jovana Helms

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

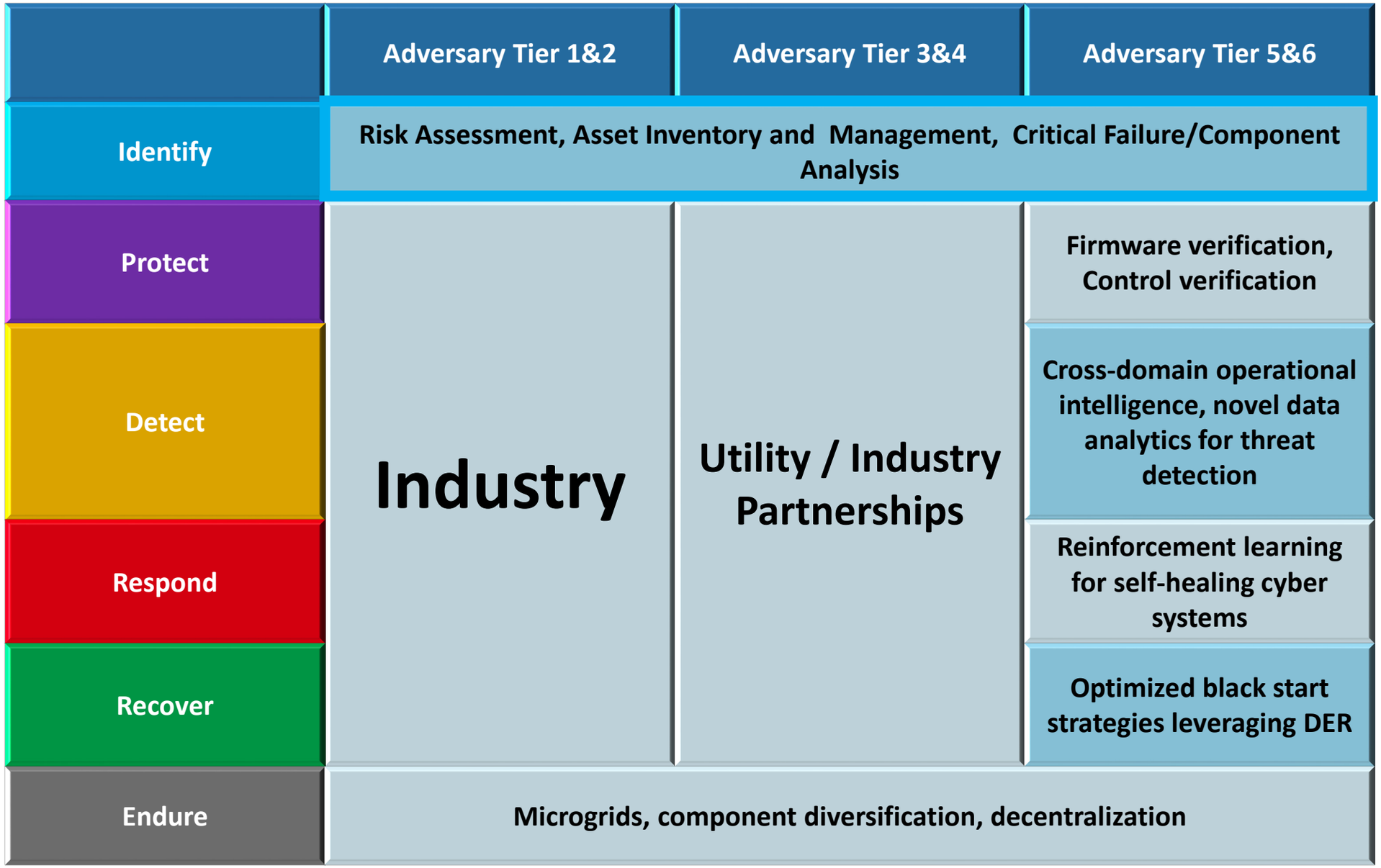
October 6-7, 2020

Layered Defense Strategy for the Electric Grid

NIST	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify			
Protect			
Detect			
Respond	USE vulnerabilities	DISCOVER vulnerabilities	CREATE vulnerabilities
Recover			
Endure			

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Layered Defense Strategy for the Electric Grid



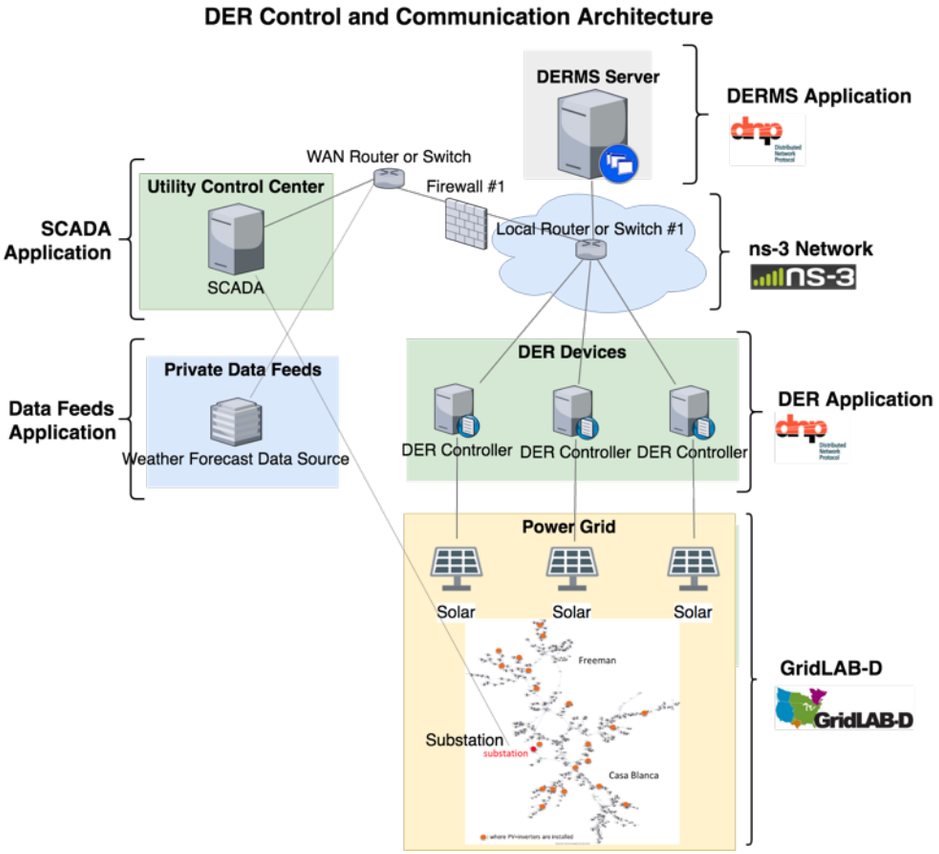
Cybersecure Interconnection of Distributed Energy Resources (DER)

Objective

- Develop a tool that can evaluate the cybersecurity risk of various DER integration architectures, and design remediation strategies for a grid with high-penetration of DER to become more resilient and better able to survive a cyberattack

Schedule

- October 2017 – December 2020
- Key deliverables
  : Report on attack strategies and 10 cybersecurity scenarios (Oct 2018); models and methods for remediation and prevention of attack consequences (Mar 2019); 2 conference papers on framework and scenarios (Oct 2020)
- Expected capability
  : streamlined analyses for utilities and product vendors to use best practices for cybersecurity protection during DER interconnection, without increasing cost or time



Total Value of Award:	**$ 2.5M** (no cost share)
Funds Expended to Date:	**95.2%**
Performer:	**Lawrence Livermore National Laboratory**
Partners:	**Smarter Grid Solutions; Revolutionary Security, Part of Accenture Security; Riverside Public Utilities**

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Advancing the State of the Art (SOA)

Current state of the art

- **Interconnection tools and scenario analysis** developed through numerous EERE funded projects
- Numerous publications on the **impact of high penetration of PV** on the distribution and bulk systems
- **Cybersecurity plans** often specific to interconnecting technology
  → no analysis on a wide-scale impact and multiple threat areas with a significant number of controllable inverters
- **Inadequate tools** for cybersecurity analysis
  → tools used by power engineers focus only on grid, no models of communication network and/or flow

Advancing the SOA

Our approach

- Leverage co-simulation work at LLNL to develop a tool to give **a broad picture of impact of cybersecurity in the DER space**
  → prioritization of remediation strategy based on impact and attack vector analysis

- **Utility and vendor interaction** for sanity checks and rapid transition of research results
  → no increase in time and cost for cybersecurity analysis of DERs

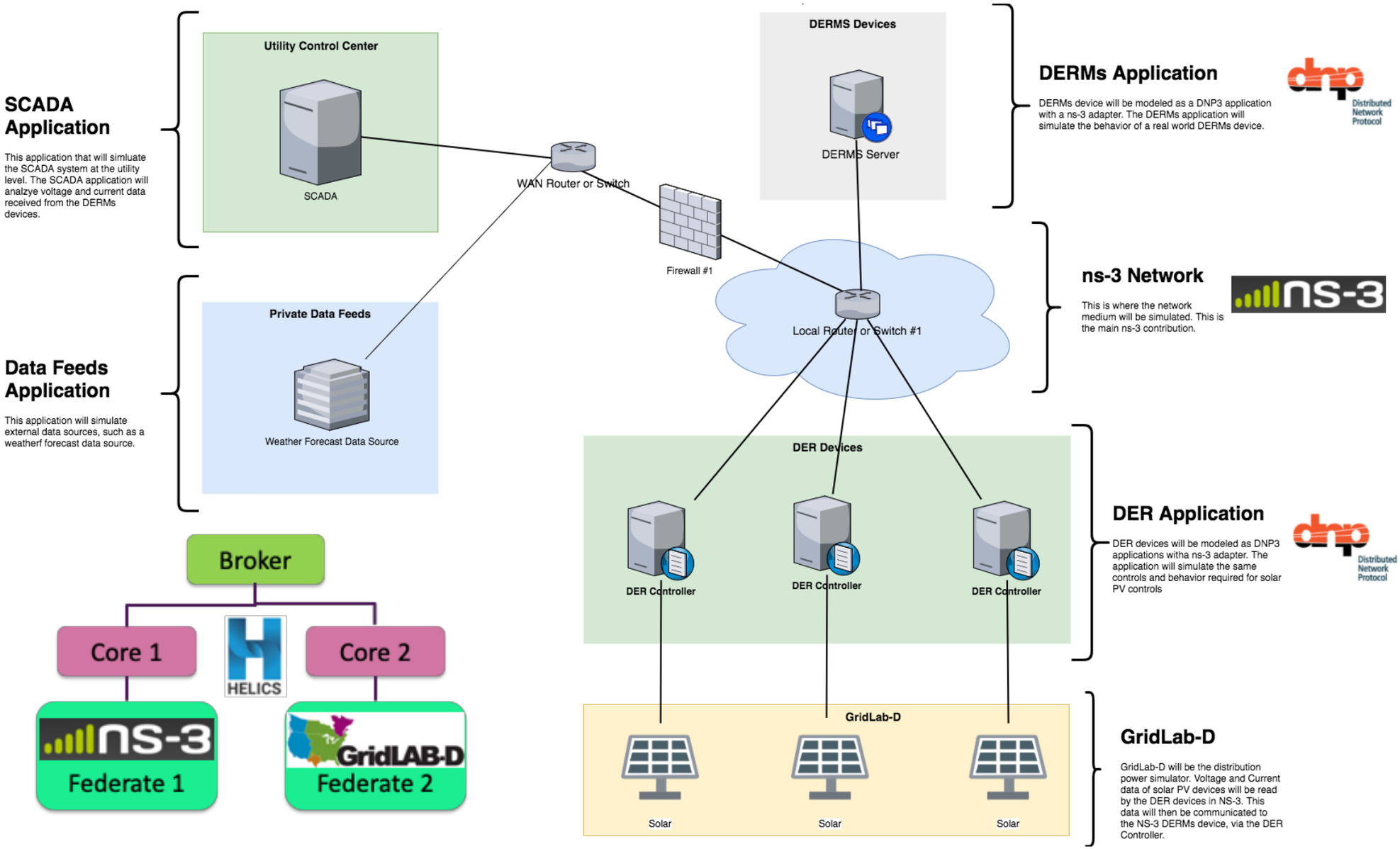
- Coupling of **power grid and cyber expertise** for a full range of potential scenarios and solutions
  → leverage LLNL's core capabilities in power system and cybersecurity research

Progress to Date

Major Accomplishments

- Cybersecurity scenarios
  - Scenarios by attack vector and severity of impacts
- Mitigation strategies
  - Preventative and corrective actions simulated
- Co-simulation demonstration on CINDER project
  - North Las Vegas Veterans Affairs Medical Center (April 2019)
  - Second demo at Hurlburt AF for future microgrid deployment for load and water management
  - Third deployment planned at Camp Parks
- Outreach of CINDER project
  - 2019 AEE World, 2020 PES General Meeting, Stanford Professionals in Energy (SPIE)
  - Regional FLC Award FY19 for Outstanding Partnership

Overall Architecture



Cybersecure Interconnection of DERs (CINDER)

- **DOE Ask: Rapid deployment of CEDS technologies to DoD sites in partnership with industry**

- **CINDER Goal**: Enhance the resilience of energy delivery systems by proactively addressing potential threats introduced by highly dispersed controllable generation.

- **Execution**: Combine LLNL's DER deployment cyber risk analysis and network mapping tools with Foxguard patching platform to deploy comprehensive DER focused cybersecurity measures and capabilities.

Highest Level: What is CINDER

Network Scanning & Data Discovery

NeMS & N2N

Co-Simulation framework

HELICS

System Modeling

ns-3
Gridlab-d
cymdist
GridDyn
PSLF

Scenarios & Cyber Attack

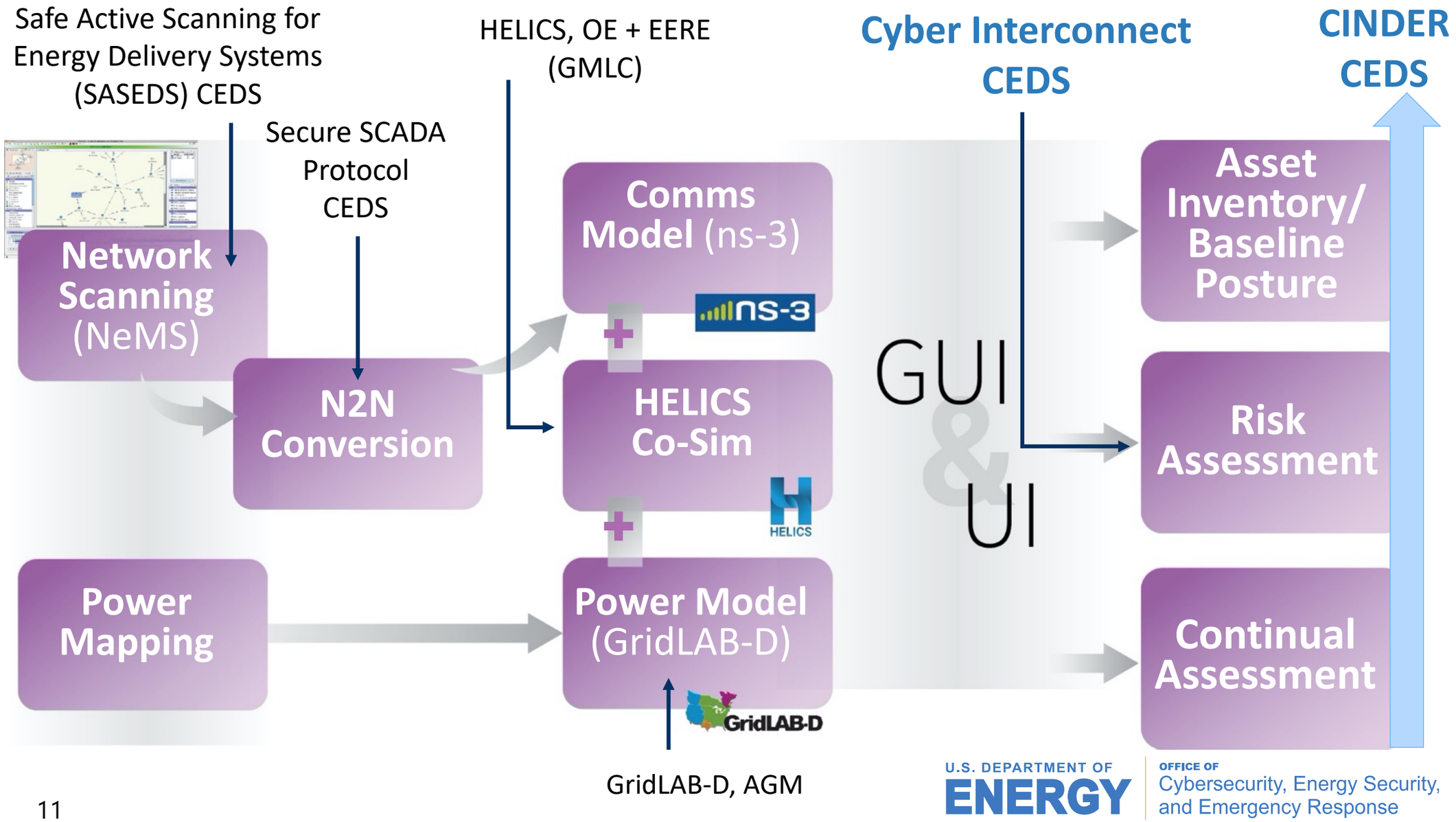
Digital Twin of Network

Goal
Automated Scenario & System Level Risk Analysis

CINDER Innovation is in the ability to analyze multiple scenarios in a synchronized and methodological way, assessing both the physical behavior and cyber risk in one environment, with practical outputs for all levels of the interconnection process

CINDER Evolution

For comprehensive evaluation of impacts and mitigation strategies



Cybersecurity Scenarios

Combined or singular events categorized by severity of impacts, attack vector, and simulation timescale

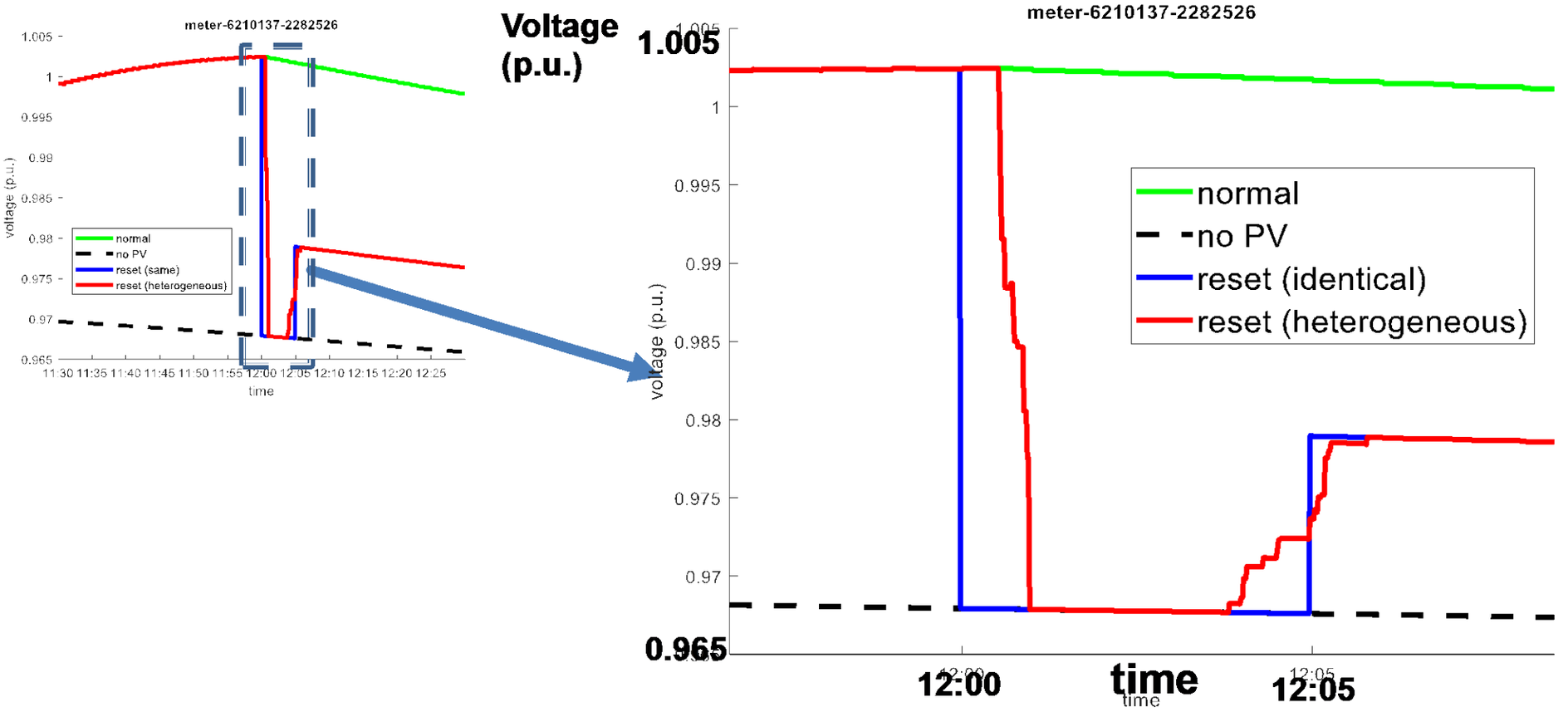
	Impact (from low to high)	**Incorrect dispatch of DER** (unnecessary usage, financial loss)	**Instability at customer sites** (DER/generation/ loads)	**Distribution impacts** (transformer overload via sudden increase in loads)	**Transmission impacts** (under/over-frequency load shedding to large scale outage)	**Safety hazard** (anti-islanding by unintended desynch or resynch)
Cyberattack Vector						
		Severity of impact →				
Configuration/operational setting Change			7	9	1, 3, 5	9
Firmware/software Change			6	9	4, 5	
Compromised communications		10	7		10	8
Timing attack			9		10	8
Improper verification of messages		10	8			
Data feed change		10			10	
Time scale		Steady state (DERMS dispatch interval; 5-60 minutes)	Dynamic (seconds)	Steady state (SCADA interval; ~15 minutes)	Dynamic/steady state (seconds to minutes)	Dynamic/steady state (seconds to minutes)

Which scenarios + attack vectors + penetration levels/resource mixes result in these issues

Simulation of Physical Impacts

DER controller modeling accuracy

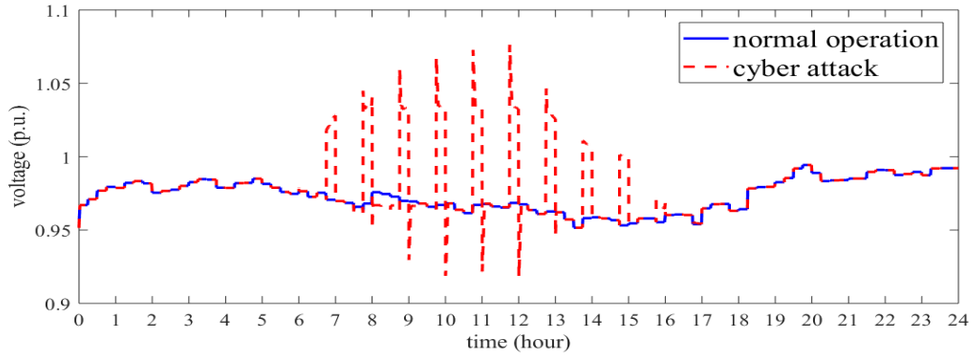
- But if all inverters had the same communication and control settings…

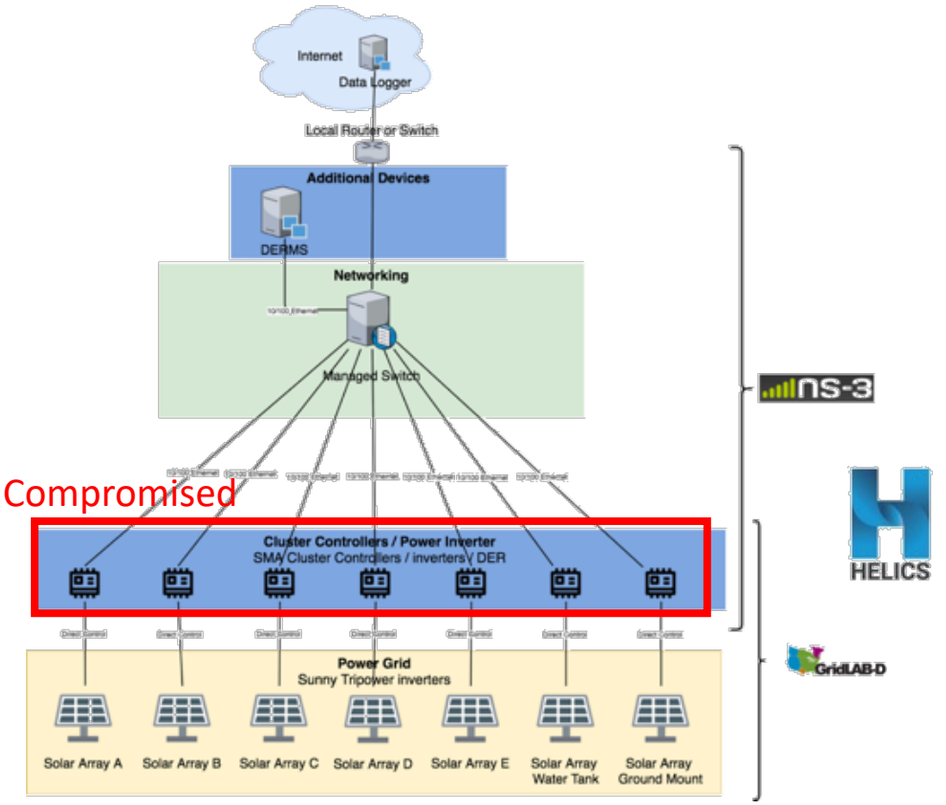


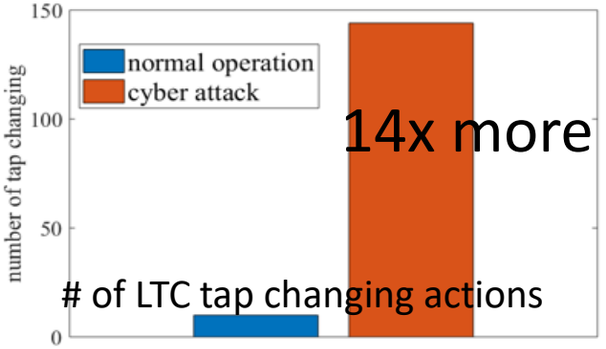
Distribution Cybersecurity Scenario #1

Malicious control of PV inverters causes power equipment deterioration

- Adversary plants a malware on the firmware of the cluster controllers
- Malicious control command from the firmware
  : all PV inverters turning on and off every 30 mins





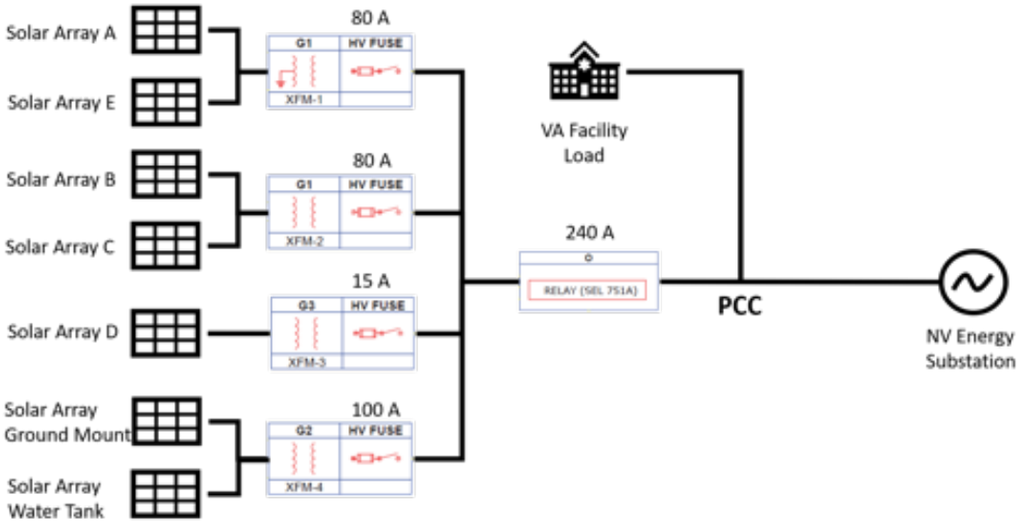


Distribution Cybersecurity Scenario #2

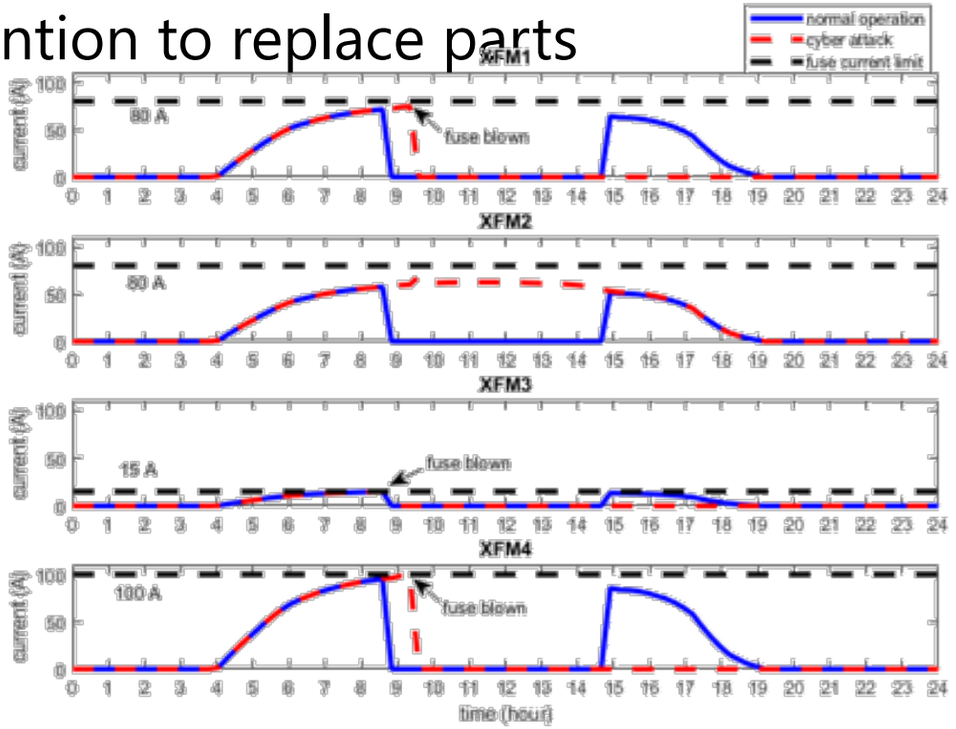
Relay misconfiguration + inverter ramp up

: 3 out of the 4 fuses connected to the transformers blew

- Solar PV arrays disconnected, discontinued DER service
  : 76% of capacity out of service
- Requires field maintenance crew attention to replace parts
  : increase in O&M costs



Connection of PV arrays, transformers, and relay



Currents at all four transformers

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Challenges to Success

Challenge 1

- Data and model acquisition
  - Multiple sources for grid models and data

Challenge 2

- Co-simulation and integration of tools
  - Leverage existing platform from previous efforts

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Targeted end users: utilities, power system planning tool vendors, DERMS vendors, utility/energy managers
- Plans for industry acceptance
  - Project partnership includes targeted end users
  - Outreach to potential users
  - Dissemination of results to industry workshops and conferences
  - Presentation to utility/energy managers at demonstration sites

Next Steps for this Project

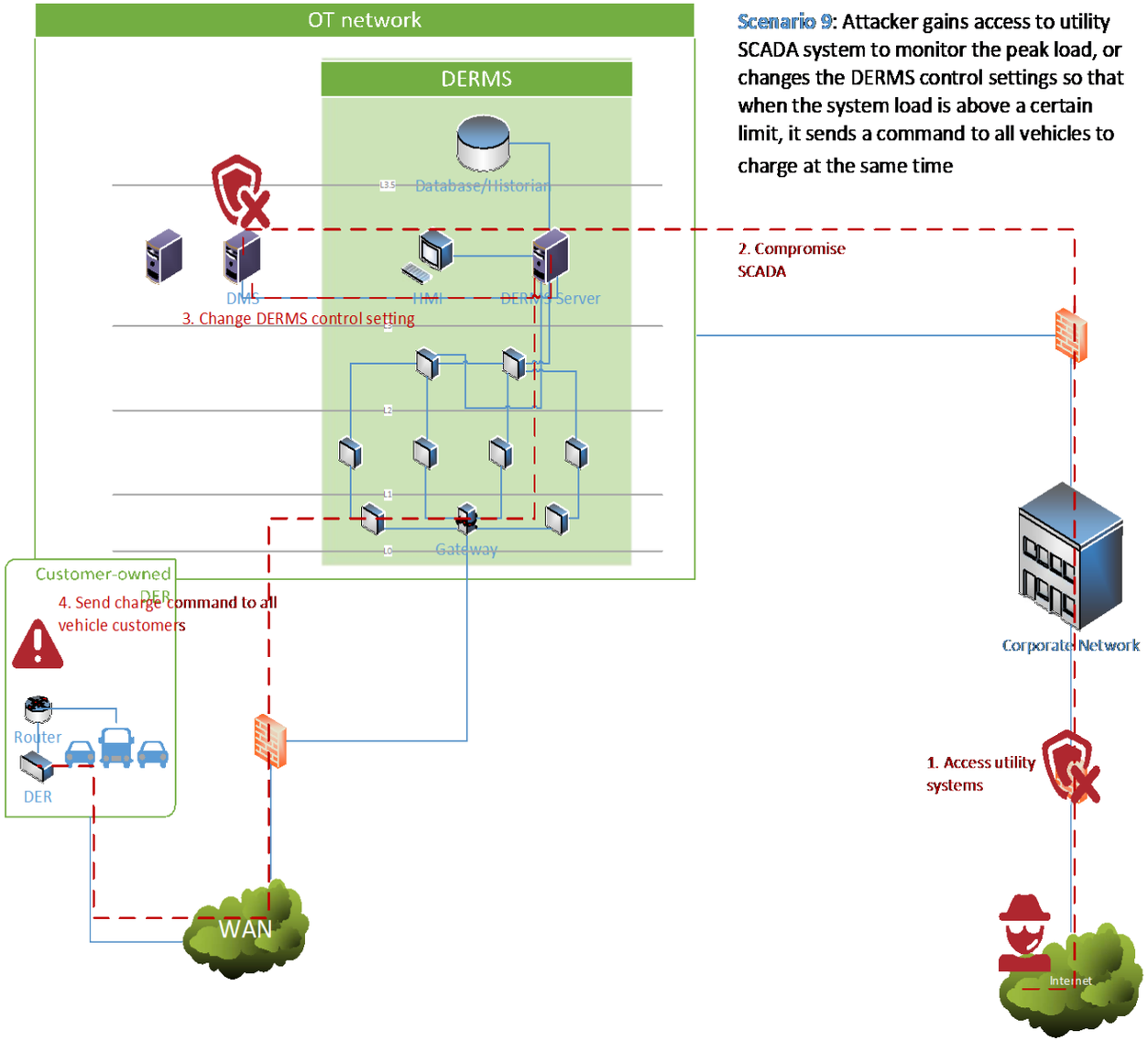
Approach to the end of project

- Second feeder demonstration
  - Differing levels of penetration and effects on cyberattack impacts
  - DERMS integration into co-simulation platform
  - Demonstration of co-simulation on a second site

- Third site demonstration (CINDER)
  - Continued funding by DoD for deployment and improvement on Risk Management Framework
  - Developing user interface for CINDER tool to be transferred DoD partner sites

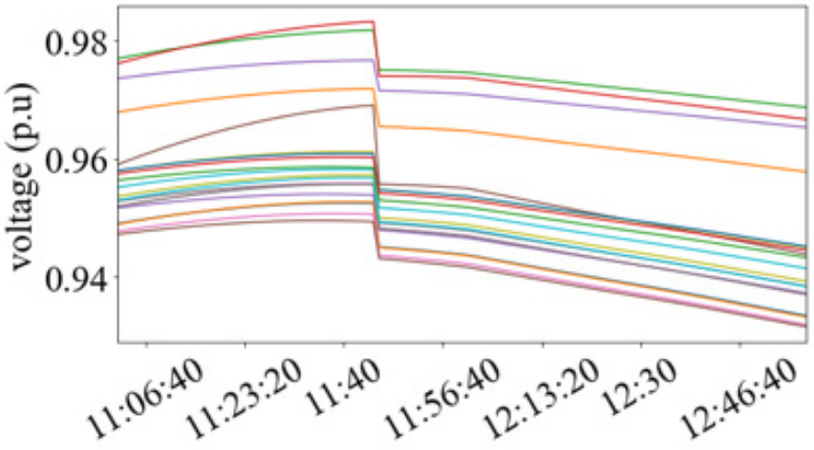
Thank you

Remediation Strategies



Scenario 9: Attacker gains access to utility SCADA system to monitor the peak load, or changes the DERMS control settings so that when the system load is above a certain limit, it sends a command to all vehicles to charge at the same time

Preventative Action	Corrective Action
When a change affecting a significant percentage of the DER population is issued, an additional approval is needed before change commands are sent.	Ensure that an auditable log of all DERMS commands exists and can be referenced to back out specific changes.



Voltage magnitudes after preventative action