

Cybersecurity for
Energy Delivery
Systems
(CEDS) R&D
Program

**FROM
INNOVATION
TO PRACTICE:
RE-DESIGNING
ENERGY DELIVERY
SYSTEMS TO SURVIVE
CYBER ATTACKS**

JULY 2018



U.S. DEPARTMENT OF

ENERGY

OFFICE OF
CYBERSECURITY, ENERGY SECURITY,
AND EMERGENCY RESPONSE

Table of Contents

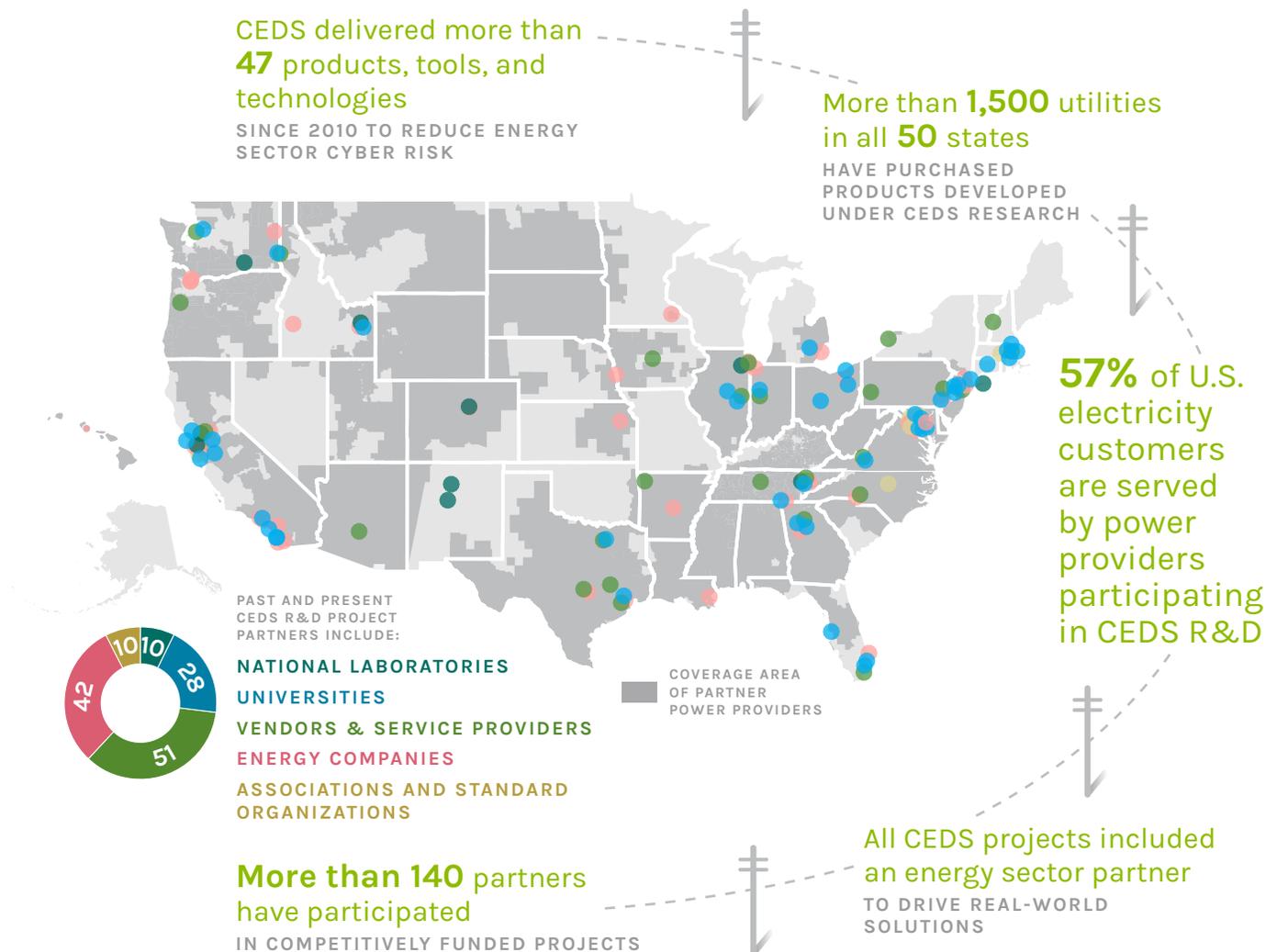
| | |
|-----------------------------------|----|
| Executive Overview | 3 |
| Navigating this Document | 6 |
| Emerging Tools & Technologies | 7 |
| Transitioned Tools & Technologies | 14 |
| Appendix Project Partners | 35 |

Executive Overview

Our Nation's critical energy delivery infrastructure is an engineering masterpiece that has provided power reliably for over a century. Today, advanced computational platforms and communications networks are used to manage, monitor, protect, and control energy delivery. This operational technology (OT) is bringing ever increasing efficiency and reliability to better serve the energy consumer. However, as the world becomes increasingly interconnected, adversaries seek to misuse OT systems with the intent to deliberately misoperate power system equipment and disrupt energy delivery. The intensifying cyber threat landscape has inspired a community of cyber-defenders—in partnership with DOE—to redesign the architecture so that energy delivery systems and devices (both next-generation and legacy equipment) detect adversarial actions, then adapt to survive while sustaining critical functions.

For more than a decade, the Department of Energy (DOE), through its Cybersecurity for Energy Delivery Systems (CEDS) program, has partnered with the energy sector to advance cybersecurity R&D specifically designed to reduce cyber risks to energy delivery infrastructure. The CEDS program cost-shares the earlier-stage, high-risk/high-reward research for which a business case may not be readily apparent but can lead to advanced cyber resilience technologies imperative for national security.

The CEDS program manages a diverse portfolio of competitively funded R&D and risk management initiatives under DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The creation of CESER elevates and intensifies the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to natural and man-made threats.



By partnering with industry, cybersecurity vendors, academia, and National Laboratories, CEDS has been able to deliver more than 47 products, tools, and technologies to help reduce the risk that a cyber attack might disrupt our nation's critical energy delivery infrastructure. Several of these are now being used to reduce energy sector cyber risk in every state across the nation. This report highlights 35 CEDS tools and technologies that have been successfully transitioned to the sector, and are now available for energy companies, vendors, and researchers to use. Also featured are another 12 products that are soon emerging from CEDS R&D after successful demonstrations with industry partners.

CEDS moves innovative research to industry-ready solutions using a strategic mix of R&D. This includes funding for both shorter-term R&D with a high probability of rapid market readiness, and game-changing R&D that supports next-generation cyber system designs. This approach advances today's state of the art, while developing capabilities for future systems to automatically detect, reject, and withstand cyber incidents.

CEDS R&D projects address an urgent industry need, target a clear end use, and engage suppliers and utilities early to develop solutions that can be used today to reduce the risk of energy disruption due to a cyber attack. Research partnerships are used to provide today's advanced capabilities to the energy sector and develop market-ready products. These products are commercialized, released as open source, or adopted into ongoing research to develop new capabilities that help the energy sector achieve its vision of energy delivery systems that can withstand a cyber attack.

What CEDS R&D Delivers

CEDS R&D projects deliver cybersecurity solutions to the energy sector in a number of ways:



VENDOR-COMMERCIALIZED SOLUTIONS

New devices, software, or systems that energy sector suppliers now sell to secure energy delivery operational networks and systems



OPEN-SOURCE PUBLICATION OF SOFTWARE, CODE, OR OTHER SOLUTIONS

New tools and capabilities are often released as open-source code or toolsets that suppliers can build into future products or other existing tools



GUIDES AND EXPERT RESOURCES

Guidance that help energy suppliers and owners and operators better secure, test, and defend critical cyber networks



NOVEL CAPABILITIES AND TOOLS THAT UNDERPIN FUTURE TECHNOLOGY DEVELOPMENT

R&D may demonstrate novel capabilities and testbed tools at laboratories and universities that lay the groundwork for future research and technology designs

Keys to Success: How CEDS R&D Delivers Industry-Ready Solutions

Whether pursuing near-term or long-term solutions, CEDS R&D targets innovations that utilities and suppliers can use to reduce cyber risk. Each CEDS project uses a common strategy:

ADDRESS THE INDUSTRY'S MOST CRITICAL RESEARCH GAPS AND NEEDS TO REDUCE NATIONAL CYBER RISK.

CEDS partners with the energy sector, and coordinates across multiple Federal agencies, to prioritize critical research gaps.

PURSUE STRATEGIC RESEARCH THAT REDUCES CYBER RISK FOR CRITICAL ENERGY INFRASTRUCTURE, BUT IS NOT SUPPORTED BY A BUSINESS CASE FOR PRIVATE INVESTMENT.

As cyber threats advance, truly innovative, first-of-a-kind solutions are needed. CEDS supports promising R&D needed to address the national security imperative of critical energy delivery infrastructure cybersecurity, focusing on projects that lack a strong business case for private sector investment.

ELIMINATE A "RESEARCH VACUUM" THROUGH EXTENSIVE AND EARLY PARTNERSHIP.

Research teams combine the rigor and expertise of National Laboratories and universities with the real-world insight of suppliers and utilities. Diverse project teams engage end users early, ensuring solutions are ready for use and promising solutions don't get stranded.

ACCELERATE TECHNOLOGY ADOPTION BY FOCUSING ON THE COMMERCIAL END USE.

To improve uptake and reduce the time from concept to practice, CEDS research partnerships are designed to strengthen cybersecurity while easing operational and maintenance burdens. Teams keep the end user in mind when developing economical, scalable, interoperable solutions that will work with diverse systems and won't impede critical functions.

INNOVATE, THEN DEMONSTRATE IN REAL-WORLD ENVIRONMENTS.

Nearly all R&D projects conclude with a demonstration at an end-user site under actual operating conditions. This builds confidence that the technology will work well within the real-world operating environment of 24/7 energy delivery systems and helps to accelerate adoption throughout the energy sector.

FOSTER LEAP-AHEAD TECHNOLOGIES BY TEAMING UP SOME OF THE NATION'S BEST MINDS AND RESOURCES.

Multi-disciplinary research teams create an environment that fosters innovation and groundbreaking approaches. CEDS projects are designed to bring together some of the nation's premier cybersecurity knowledge and resources by engaging multi-university R&D centers, National Labs, and industry.

LAY THE GROUNDWORK, AND BUILD ON WHAT WORKS.

Foundational R&D offers advanced capabilities that can be used to accelerate complementary research efforts that lead to additional commercial solutions. CEDS projects may build on one another, use tools from prior projects in new ways, or combine capabilities from several past projects into one new technology.

This summary highlights select CEDS tools and technologies that have transitioned to the energy sector since 2010, or are soon emerging from CEDS R&D. Visit the [CEDS website](#) for more information on the diverse mix of R&D projects that CEDS currently supports.

Navigating this Document

This summary offers a brief overview of successful, industry-ready solutions resulting from CEDS R&D since 2010. The [Emerging Tools & Technologies](#) section includes 12 CEDS R&D solutions that are nearing completion of industry demonstrations or commercialization. The [Transitioned Tools & Technologies](#) section includes more than 35 CEDS R&D products, presented from newest to oldest, that have been successfully commercialized or otherwise transitioned to the energy sector.

CEDS R&D investments result in tools and technologies designed to prevent, detect, mitigate, and survive cyber incidents. These four approaches align with DOE's cybersecurity strategy in the 2018 [Multi-Year Plan for Energy Sector Cybersecurity](#) (MYP), which outlines DOE's two-pronged R&D approach to secure today's energy systems while developing innovative solutions to design next-generation solutions that are inherently secure and resilient to attack. Each summary identifies how the solution supports one or more strategic approach to:

P **PREVENT CYBER INCIDENTS** by decreasing the attack surface or blocking unauthorized access or use of EDS components.

D **DETECT CYBER INCIDENTS** by rapidly identifying anomalous or suspicious behaviors and functions that could potentially damage equipment or destabilize the grid.

M **MITIGATE CYBER INCIDENTS** by distinguishing malicious activity from other operational issues or anomalies, and automatically respond by isolating or eliminating the threats.

S **RE-DESIGN ENERGY DELIVERY SYSTEMS TO SURVIVE CYBER INCIDENTS** by restricting systems from performing functions that cause grid instability and allowing systems to continue operating in the face of an attack.

Each summary includes a short description of CEDS-funded technology, how it works, and how it advanced the state-of-the-art. In addition, each identifies how the product can be used: some of the featured products are market-ready technologies that energy companies can deploy and install today; others are new capabilities that vendors can license and build into their product offerings; and others are novel capabilities or toolsets that interested researchers can build on to develop new technologies. In addition, nearly ¼ of CEDS products build on or incorporate prior CEDS R&D results, and these linkages are highlighted throughout when applicable.

Each product is also categorized based on its core capabilities or functions:

NETWORK ARCHITECTURES

Tools and technologies that design or reconfigure the way devices interconnect or communicate to enhance cybersecurity capabilities. This includes software-defined networking, wireless configurations, and altering the way information flows between EDS components.

ACCESS CONTROL

Tools and technologies that use encryption, authentication, or authorization to make information and devices indecipherable or inaccessible to unauthorized users.

ATTACK IDENTIFICATION AND RESPONSE

Tools and technologies that identify and respond to cyber attacks or intrusions to mitigate potential damage. This includes detecting and mitigating the effects of malicious software, anomalous behavior, abnormal communication, and physical tampering

SITUATIONAL AWARENESS AND OPERATOR SUPPORT

Tools and technologies that assist human operators by providing real-time information on the status of their operational networks to inform decision-making.

GUIDANCE AND PRACTICES

Guides, best practices, or reports that inform owners, operators, regulators, and/or end users of policies or practices that can improve cybersecurity. This includes identifying requirements, challenges, misconceptions, and recommendations for future action.

REDUCED EXPOSURE

Tools and technologies that preemptively identify and assess system risks and potential attack vectors to enhance cybersecurity.

Each project also identifies the project lead and participants of the team funded by CEDS research, though projects often engage additional stakeholders throughout development. A list of current and past CEDS project partners, including three multi-university consortia, is in the [Appendix](#).

Emerging Tools & Technologies

Emerging Tools & Technologies includes 12 CEDS R&D projects that are currently in demonstration or in the process of commercialization. These products give stakeholders insight into emerging capabilities that advance the state-of-the-art for energy delivery system networks and cybersecurity. Some of the products take a fresh approach to securing long-standing cyber vulnerabilities in EDS; others address cybersecurity needs emerging with the growth of distributed energy resources (DERs); while others expand on prior CEDS-funded projects.

Stakeholders may expect to see these products released as commercial products or open-source resources in the near future.

| NAME | NETWORK ARCHITECTURES | ACCESS CONTROL | ATTACK ID AND RESPONSE | SITUATIONAL AWARENESS | REDUCED EXPOSURE | GUIDANCE AND PRACTICES |
|---|---|---|---|-----------------------|------------------|------------------------|
| Alliance: Unified Cyber-Physical Access Control | |  | | | | |
| Anomaly Detection for Securing Communications in Advanced Metering Infrastructure (AMI) | | |  | | | |
| CODEF: Collaborative Defense of Grid Protection and Control Devices | | |  | | | |
| Cyber Attack Resilient High-Voltage, Direct Current (HVDC) Systems | | |  | | | |
| Digital Ants: Bio-inspired Technology for Enhancing Cyber Security in the Energy Sector | | |  | | | |
| Digital Ghost: Cyber Attack Detection and Accommodation | | |  | | | |
| Distribution Edge Security Architecture |  | | | | | |
| Scalable Quantum Key Distribution for Operational Networks | |  | | | | |
| Secure Software-Defined Radio Platform |  | | | | | |
| Chess Master Application Programming Interface |  | | | | | |
| Precise Time Synchronization Platform | | |  | | | |
| TIMER - Time Intrusion Management Ensuring Resiliency | | |  | | | |

Alliance: Unified Cyber-Physical Access Control

Emerging

CATEGORY

 ACCESS CONTROL

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Sandia National Laboratories • Tennessee Valley Authority

SEL developed a proximity card reader and controller that provides a single system for utilities to monitor, track, and control access to physical facilities and their associated cyber infrastructure. Alliance integrates facility access controls into the same authentication system used for cyber access, allowing utilities to specify each employee's physical and cyber access rights under one user account. The card reader can be applied to facilities, cabinets, and panels, allowing operators to restrict physical access to racks of cyber equipment, not just rooms or facilities.

For remote substations in particular, Alliance can better verify that only approved individuals are logging into cyber-connected systems, and can lock down racks of cyber equipment if a physical break-in is detected. This streamlined and scalable solution uses advanced multifactor authentication for physical and electronic access, delivers highly granular cyber-physical and role-based access control settings, and supports NERC CIP reporting and compliance.

The proximity card reader was successfully demonstrated at DistribuTECH 2018. Alliance will be ISO 14443 Type A and B, ISO 15693, and FIPS 140-2 Level 2 compliant, and designed to withstand IEEE-1613 and IEC 61850-3 environmental conditions. Alliance solutions are designed to integrate with existing SEL Exe-Guard security gateways (SEL-3620 and 3622).

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

Anomaly Detection for Securing Communications in Advanced Metering Infrastructure (AMI)

Emerging

CATEGORY

 ATTACK IDENTIFICATION AND RESPONSE

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Cyber Resilient Energy Delivery Consortium (CREDC); project led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

Cisco Systems

The Cyber Resilient Energy Delivery Consortium (CREDC) developed a peer-to-peer method to detect and localize interference, jamming, and other denial-of-service (DoS) attacks in AMI wireless mesh networks. DoS attacks can undermine the ability of AMI devices to communicate with one another and compromise measurements from smart meters. Operators today lack the tools to validate these measurements before using them to make important control decisions. CREDC is designing the code to run inside each smart meter, as well as a central management server, to detect attacks and direct response measures to the right locations. Resulting tools will distinguish true attacks from non-malicious anomalies, reducing false positives.

Cisco is now developing the anomaly detection solution for their own platform using the joint CREDC and Cisco research, which resulted from a CREDC student's summer internship at Cisco. CREDC is developing an open-source version of the solution for release in the next year.

FOR MORE INFORMATION

[CREDC Research Summary](#)

CODEF: Collaborative Defense of Grid Protection and Control Devices

Emerging

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**
 **VENDORS**

PROJECT LEAD

ABB, Inc.

PROJECT PARTNERS

The Information Trust Institute, led by University of Illinois at Urbana-Champaign • Bonneville Power Administration • Ameren Illinois

CODEF is a cybersecurity capability that detects and blocks insider attacks, spoofed power system data, and malicious commands by anticipating their effects on the grid. CODEF works by allowing intelligent electronic devices (IEDs), such as protective relays, to communicate with each other to validate that incoming commands, configuration changes, and data inputs support reliable grid operation. Using CODEF, the devices leverage grid physics, computer science, and power engineering principles to anticipate the effect of actions on grid stability given its current state. These devices can reach consensus in under four milliseconds, allowing the grid to continue delivering energy during a cyber attack.

CODEF was successfully demonstrated at the transmission level at two utilities (Bonneville Power Administration and Ameren Illinois) and is now being developed for further use in ongoing CEDS projects (including Cyber Attack Resilient HVDC Systems).

ABB is currently transferring CODEF from demonstration to a commercially available product. CODEF will be available as both a firmware upgrade to ABB protection and control devices and a vendor-neutral extension for the IEC 61850 communications protocol. In addition, CODEF is currently being considered in ABB's roadmap to enhance cybersecurity in their product line.

FOR MORE INFORMATION
[CEDS Fact Sheet](#)

Cyber Attack-Resilient High-Voltage Direct Current (HVDC) Systems

Emerging

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

PROJECT LEAD

ABB, Inc.

PROJECT PARTNERS

University of Illinois at Urbana-Champaign • Bonneville Power Administration • Argonne National Laboratory • University of Idaho

ABB is designing and testing a system to detect and reject cyber attacks that target HVDC control systems, including spoofed commands and configurations that appear to be valid. By building on ABB's CODEF system for distribution networks, this system uses real-time digital simulators that assess current conditions to determine if a given command or action can destabilize grid operations and automatically rejects those with harmful effects. With growing renewable energy adoption, HVDC systems are becoming the method of choice to reliably interconnect asynchronous alternating current (AC) grids, requiring robust new cybersecurity measures. Unlike conventional network defense, this system enables devices between substations and control centers to rapidly communicate and check commands against the physical grid state. The project team is now testing and validating the defense system in a lab setting. It was demonstrated at DistribuTECH 2018.

FOR MORE INFORMATION
[CEDS Fact Sheet](#)

Digital Ants: Bio-inspired Technology for Enhancing Cybersecurity in the Energy Sector

Emerging

CATEGORY

 ATTACK IDENTIFICATION AND RESPONSE

MYP GOAL

 PREVENT  DETECT

 MITIGATE  SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Pacific Northwest National Laboratory

PROJECT PARTNERS

Wake Forest University • Argonne National Laboratory • SRI International

Digital Ants are decentralized software sensors that work in concert to identify and resolve potential cyber threats in energy delivery system architectures.

As smart grids grow and require communications among different organizations, the traditional approach of central monitoring is too static and slow to react and adapt to emerging attacks. Inspired by the swarming defense used in ant colonies, Digital Ants wander across the network from device to device and detect and mark the location of suspicious behavior based on their own unique problem indicators. Potential issues attract more Ants, which “swarm” to validate a threat and notify system operators. This agent-based approach rapidly identifies attacks, including zero-day exploits, and reduces the occurrence of false positives. Digital Ants sensors support legacy devices and can scale with emerging smart grid technologies.

Digital Ants is licensed to [Cynash Inc.](#), where it is currently being integrated into a suite of commercial products and services. SRI International is also in the pilot/test phase with this technology, with a commercial release planned for 2018.

To date, industry reception of Digital Ants has been positive: this technology received the 2018 Excellence in Technology Transfer Award from the Federal Laboratory Consortium for Technology Transfer (FLC), and in 2014 was a product in the U.S. Department of Homeland Security (DHS) [Transition to Practice](#) Program.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Digital Ghost: Cyber Attack Detection and Accommodation

Emerging

CATEGORY

 ATTACK IDENTIFICATION AND RESPONSE

MYP GOAL

 PREVENT  DETECT

 MITIGATE  SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

General Electric Global Research

PROJECT PARTNERS

GE Power • Inland Empire Energy Center

With the aid of CEDS funding, General Electric (GE) is designing an automated anomaly detection and accommodation (ADA) system that provides power plant operators with real-time visibility into grid operations and security, and the ability to continue power generation even in the presence of a cyber attack. The technology supplies real-time insight into a generation plant’s cyber posture using algorithms based on data in a high-fidelity model of the power plant’s network. With this model, or “digital twin,” the system can run live operating data from the physical plant through the twin in real time to detect and identify anomalies. The technology will also apply accommodation algorithms that allow power generation systems to quickly mitigate the effects of an attack by reverting to operating data from the digital model in the event of an attack. Digital Ghost aims to minimize the number of false positives received in incident detection, limiting unnecessary mitigation actions.

The team has moved the technology into demonstration using a live gas turbine and power plant running with GE’s [Mark VIe](#) distributed control system hardware.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Distribution Edge Security Architecture

Emerging

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Intel Federal, LLC

PROJECT PARTNERS

Schneider Electric • LiveData Utilities

The Distribution Edge Security architecture reduces the attack surface of the distribution system network by securing network communications among field devices located at the edge of the utility's distribution system (e.g., field devices and customer devices). With increasing deployment of intelligent, interconnected devices on distribution feeders and customer energy systems that connect to distribution networks, operators need greater interoperability and real-time power system situational awareness for equipment on the grid-edge. This network cybersecurity architecture will provide these features in the form of a secure gateway for legacy power system devices, then as an internal field programmable gate array (FPGA) upgrade designed for modern devices.

The cybersecurity gateway, physically separated from the protected devices and acting as a security proxy, will protect legacy devices by creating a security layer on top of the existing operational communications, ensuring secure communications between protected devices and other network devices. The same cyber security controls will be embedded into an FPGA on the power system edge device creating a trusted execution environment that isolates security traffic from energy delivery functions, enhancing security and boosting system performance.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Scalable Quantum Key Distribution for Operational Networks

Emerging

CATEGORY

 ACCESS CONTROL

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Qubitekk, Inc.

PROJECT PARTNERS

Oak Ridge National Laboratory • Schweitzer Engineering Laboratories (SEL) • EPB • University of Tennessee

Qubitekk is developing a commercial quantum key distribution (QKD) system to detect attempted eavesdropping and safely exchange the cryptographic keys used to encrypt operational network communication. Growing networks of grid automation devices create a target for sophisticated attacks that attempt to manipulate or spoof device-to-device communications. QKD uses principles of quantum physics to safeguard cryptographic keys as they are exchanged, using signals that automatically and measurably change if an adversary attempts to intercept the key. It alerts operators in real time of an attempt to steal the key, reducing the risk that data that appears to be secure has actually been compromised. Qubitekk developed low-cost nodes that can integrate into existing devices and communicate with any other nodes on a common QKD channel, unlike the dedicated point-to-point channels required by traditional QKD solutions. The commercial system will offer a scalable, cost-effective QKD solution for energy infrastructure operational networks and integrate with existing commercial hardware.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Secure Software-Defined Radio Platform

Emerging

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

San Diego Gas and Electric •
Pacific Northwest National Laboratory

This flexible and configurable radio platform secures “last-mile” wireless communications out to remote automation devices on distribution lines, while offering superior performance with fast data throughput, low latency, message prioritization, and efficient use of channel bandwidth. This radio platform simplifies wireless communications by connecting multiple applications through one radio, provides precise message timing, and offers advanced security features not found in conventional radios. It enables secure and flexible communication between utilities and the millions of new smart sensors and automation devices on the grid, with security features comparable to wired communications, which can be expensive and impractical for remote networks.

SEL’s versatile radio platform will support strong passwords, event and device access logging, and advanced encryption and authentication, while offering data throughput that is 3-4 times faster than conventional radios. These levels of speed and security grow more important as utilities increasingly use sub-second level data to make real-time automation and control decisions.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Chess Master Application Programming Interface

Emerging

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Ameren Energy Resources •
Sempra • Veracity Security Intelligence

Chess Master offers operators a global view of the operational network, including the services running, network components, and network communication pathways, along with the ability to pre-engineer network policies. The tool automatically enforces preconfigured security controls for system services and network devices by dropping or isolating anomalous, untrusted traffic without impeding legitimate, trusted network traffic. Chess Master is being developed as the application programming interface (API) for SEL’s Software Defined Networking (SDN) Flow Controller, and allows operators to preconfigure automated responses to attacks and reroute critical information and control flows around affected network areas.

Chess Master is currently being demonstrated at utilities and was demonstrated at Fort Belvoir for the Department of Defense. More information on SEL’s SDN technology suite is available [here](#).

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Precise Time Synchronization Platform

Emerging

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Bonneville Power Administration

SEL is developing a customizable platform that protects against attacks that manipulate, jam, or spoof GPS signals used for critical operational data in intelligent electronic devices (IEDs). As IEDs—such as sychrophasors—become increasingly commonplace in smart grids for communicating operational data and time references to and from control systems, adversaries gain more vectors of attack (for example, false or inaccurate time data can compromise or damage equipment, which can cascade into faults or grid instability). This platform uses spoof detection algorithms and inputs from multiple time and frequency sources to root out manipulated or counterfeit signals. Once an attack has been detected, the platform logs the event and falls back to a trusted, reliable time source to ensure that operations continue as normal. The platform also comes with visualization tools that aid with configuration, access control, and situational awareness.

The Precise Time Synchronization Platform was presented at DistribuTECH 2018 and is being field tested with Bonneville Power Administration.

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

TIMER - Time Intrusion Management Ensuring Resiliency

Emerging

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

 **VENDORS**

 **RESEARCHERS**

PROJECT LEAD

Texas A&M Engineering Experiment Station

PROJECT PARTNERS

Idaho Power Company • Pacific Northwest National Laboratory

Time Intrusion Management Ensuring Resiliency (TIMER) is a set of hardware and software tools developed to detect attacks that use compromised or spoofed signals from Global Navigation Satellite Systems (GNSS). Phasor measurement units (PMUs) provide situational awareness of grid operations across wide geographic regions, and rely on precise, synchronized timestamps from GNSS. Consequently, PMUs need to be resilient against attacks aimed at these timing signals. The TIMER toolset deploys layers of intrusion detection modules that identify and locate potential attack vectors, simulate and predict the consequences of spoofed or manipulated data, and inform an appropriate response for operators.

The project team is currently working on commercialized software and hardware solutions that perform these capabilities and help maintain the integrity of critical energy infrastructure.

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

Transitioned Tools & Technologies

Transitioned Tools & Technologies includes 35 CEDS R&D products that have been successfully commercialized or transitioned for wider use in the energy sector since 2010. They are presented from newest to oldest based on the year they were transitioned. Each summary highlights how to access the tool or technology. Some of the earlier products may have since been superseded by newer technology advancements, but helped to advance the state-of-the-art for cybersecurity R&D in energy delivery systems at the time.

| NAME | YEAR | NETWORK ARCHITECTURES | ACCESS CONTROL | ATTACK ID AND RESPONSE | SITUATIONAL AWARENESS | REDUCED EXPOSURE | GUIDANCE AND PRACTICES |
|---|------|---|--|---|---|---|------------------------|
| Hammer: Secure Parsing Tool for EDS Protocols | 2018 | | | | |  | |
| Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) System | 2017 | | |  | | | |
| Patch and Update Management Program (PUMP) | 2017 | | | |  | | |
| Applied Resiliency for More Trustworthy Grid Operation (ARMORE) | 2016 | |  | | | | |
| Cyber-Intrusion Auto-Response Policy and Management System (CAPMS) | 2016 | | |  | | | |
| SecureSmart Wireless Network Intrusion Detection and Monitoring | 2016 | | |  | | | |
| Software-Defined Networking Flow Controller | 2016 |  | | | | | |
| Software-Defined Network Switch | 2016 |  | | | | | |
| Exe-Guard Whitelisting Architecture | 2015 |  | | | | | |
| Amilyzer Software | 2015 | | |  | | | |
| Autoscopy Jr. Intrusion Detection System | 2015 | | |  | | | |
| Hyperion Software | 2015 | | |  | | | |
| NP-View Software | 2015 | | | |  | | |
| Specification-Based Intrusion Detection System for the Distributed Network Protocol | 2015 | | | | |  | |
| Cyber Security Manager Software | 2014 | | | |  | | |
| Cyber-Physical (Hybrid-State) Monitoring to Detect Attacks on Protective Relays | 2014 | | |  | | | |

| NAME | YEAR | NETWORK ARCHITECTURES | ACCESS CONTROL | ATTACK ID AND RESPONSE | SITUATIONAL AWARENESS | REDUCED EXPOSURE | GUIDANCE AND PRACTICES |
|---|------|---|---|---|---|---|---|
| Cybersecurity Procurement Language for Energy Delivery Systems | 2014 | | | | | |  |
| Role-Based Least-Privilege Access Control for ONG Control Systems | 2014 | |  | | | | |
| NESCOR Guide: Penetration Testing for Electric Utilities | 2014 | | | | | |  |
| Sophia: Control System Mapping and Monitoring Tool | 2014 | | | |  | | |
| Api-do Toolset: KillerBee Software Updates and Api-Mote Hardware | 2013 | | | | |  | |
| CodeLock Software | 2013 | |  | | | | |
| Converged Networking for SCADA Systems (CONES) | 2013 |  | | | | | |
| Dynamic Defense and Network Randomization | 2013 |  | | | | | |
| Intrusion Response and Recovery Using Game Theory | 2013 | | |  | | | |
| NESCOR Reports: Electric Sector Failure Scenarios, Impact Analyses, and Mitigations Mapping | 2013 | | | | | |  |
| NESCOR Guide: Cybersecurity for Distributed Energy Resource (DER) Systems | 2013 | | | | | |  |
| Secure Information Exchange Gateway for Electric Grid Operations (SIEGate) | 2013 |  | | | | | |
| Agent-based, Distributed, and Extensible Cybersecurity for the Grid (ADEC-G) | 2013 | | |  | | | |
| Padlock Cyber-Physical Sensor Technology | 2012 |  | | | | | |
| Smart Grid Cryptographic Key Management System | 2012 | |  | | | | |
| Hallmark Secure SCADA Communications Protocol | 2011 |  | | | | | |
| Contribution: ISA Trustworthiness in Wireless Industrial Automation Report | 2011 | | | | | |  |
| Cybersecurity Audit and Attack Detection Toolkit (Bandolier and Portaledge) | 2010 | | | | |  | |
| Lemnos Interoperable Configuration Profiles | 2010 |  | | | | | |

Hammer: Secure Parsing Tool for EDS Protocols

2018

CATEGORY

 REDUCED EXPOSURE

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Cyber Resilient Energy Delivery Consortium (CREDC); project led by Dartmouth College

PROJECT PARTNERS

Upstanding Hackers • General Electric (GE) • SRI International

CREDC developed a secure parsing tool and hardened parsers for EDS protocols to prevent zero-day exploits on vulnerable devices embedded at the edge of OT networks. As modern networks grow, these devices are becoming too numerous and geographically dispersed to continuously patch and effectively manage—particularly over time, when they may no longer receive vendor support.

Hammer is a secure parsing tool that allows CREDC to build parsers based on language-theoretic security (LangSec), which treats device inputs as formal languages with strict grammar rules. LangSec is superior to traditional pattern matching because it has lower false-positive rates and cannot be defeated by slightly tweaked code. The resulting parsers block protocols from using inherently unsafe commands and options. Select parsers also use CREDC's executable and linkable format-based access control (ELFbac) technique, which helps protect sensitive code or data within a process, even if that process is exploited by an attacker.

ACCESS

Parsers for DNP3 and IEEE C37.118 are now available via GitHub, and work continues to support additional protocols. The CREDC research team also built a LangSec parser for GE's Predix time series format, which GE plans to incorporate into future products.

FOR MORE INFORMATION

[CREDC Research Summary](#)

Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) System

2017

CATEGORY

 ATTACK IDENTIFICATION AND RESPONSE

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Georgia Tech Research Institute

PROJECT PARTNERS

Virgin Islands Water and Power Authority • Burbank Water and Power • Open Information Security Foundation

CYMSA uses novel modeling and simulation research to anticipate the physical effect of cyber commands on grid operations, alerting operators to any attempt to destabilize the grid. It uses advanced sensors that work with faster-than-real-time modeling and simulation tools to evaluate “what-if” scenarios and assess how a cyber command could affect grid operations. This allows CYMSA to detect malicious commands that “play by the rules” and often evade traditional intrusion detection tools.

CYMSA uses a distributed dynamic state estimator (DDSE), a modeling and simulation technology that integrates a physics-based grid model with a model of the communications network to provide a complete view of cyber-physical power system health. Distributed sensors work with the DDSE to continuously and rapidly analyze possible cyber-physical contingencies. CYMSA has been designed to co-evolve with the power system over time.

ACCESS

The U.S. Department of Defense is working with the Georgia Tech Research Institute to incorporate CYMSA into DOD installations and energy programs. For more information, contact [Trina Brennan](#) at GTRI.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Patch and Update Management Program (PUMP)

2017

CATEGORY

 SITUATIONAL AWARENESS

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

FoxGuard Solutions, Inc.

PROJECT PARTNERS

TDi Technologies • NRG Energy

The Patch and Update Management Program (PUMP) offers a simplified method to identify, validate, and deploy patches or updates to energy assets, including software, hardware, and firmware. Patches or updates can mitigate known vulnerabilities and so are time-critical to deploy, because once a vulnerability is known, cyber attacks that exploit it rapidly become available. Operators can spend considerable time and resources managing patches and updates and verifying version and model information for a large contingent of devices. PUMP includes an information-gathering tool and an asset analysis tool for identifying and aggregating discrepancies in patch installations. PUMP also includes a usable web interface and validation training to help end users determine that a patch can be deployed safely. It is essential to verify that patches will perform as expected prior to taking energy components offline, as updates can potentially interrupt service, and deploying patches safely and efficiently can reduce downtime. Implementing this program can help utilities meet the NERC CIP-007 standard, which requires utilities to implement a patch management process.

PUMP is now widely used by U.S. investor-owned utilities, electric co-ops, and public utilities, who report it saves time and helps eliminate patching gaps. PUMP integrates the query engine from TDi Technologies' [ConsoleWorks](#) cybersecurity platform.

ACCESS

Program information is available on FoxGuard's [product page](#) or on the TDi Technologies [website](#).

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Applied Resiliency for More Trustworthy Grid Operation (ARMORE)

2016

CATEGORY

 ACCESS CONTROL

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Grid Protection Alliance

PROJECT PARTNERS

University of Illinois at Urbana-Champaign • Pacific Northwest National Laboratory • Ameren • Tennessee Valley Authority • Sempra Energy • National Rural Electric Cooperative Association

ARMORE software comprehensively inspects, analyzes, encapsulates, and encrypts energy delivery system (EDS) network traffic and alerts operators to suspicious activity or commands. Building on the prior [SIEGate](#) solution, an ARMORE node at each end can “wrap” and encrypt communications between legacy devices, which often lack sufficient security and authentication. By leveraging an open-source network analysis platform, ARMORE can also inspect network traffic, collect statistics, and track communication patterns between devices to alert operators to any suspicious behavior. Users can feed results from ARMORE into a security incident and event manager (SIEM) or other decision system to trigger alerts or actions. ARMORE is tailored for traffic that uses the common DNP3 and Modbus protocols, but could support other standard protocols. It provides a cost-effective solution for resilient substation communications without the need to buy new equipment.

This open-source software was demonstrated with more than five utilities. Current CEDS projects continue to advance more secure communications protocols for energy delivery systems.

ACCESS

ARMORE is an open-source [software solution](#) available for download via [GitHub](#).

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Cyber-Intrusion Auto-Response Policy and Management System (CAPMS)

2016

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

PROJECT LEAD

ViaSat

PROJECT PARTNERS

Duke Energy • Southern California Edison

The Cyber-Intrusion Auto-Response Policy and Management System (CAPMS) is a managed security system that integrates data across legacy and modern control systems and applies advanced cybersecurity algorithms to detect and automatically respond to cyber attacks in energy delivery systems. ViaSat's Trusted Network Platform (TNP)—an existing protection and detection system—builds on and enhances CAPMS threat detection capabilities by incorporating behavioral and causal analyses with TNP's information collection. These enhanced insights into system events improve operator situational awareness and increase the likelihood of detecting early-stage attacks.

Using CAPMS, utilities will have a continuous view of a network's cybersecurity posture. CAPMS can be set up as part of a detection system or a detection and response system.

ACCESS

More information on the CAPMS managed security system is available via [ViaSat](#).

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

SecureSmart Wireless Network Intrusion Detection and Monitoring

2016

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

PROJECT LEAD

Perspecta (formerly Vencore Labs)

PROJECT PARTNERS

Sacramento Municipal Utility District • Hawaiian Electric Company

The SecureSmart monitoring and analysis system provides visibility and detects anomalies and intrusions in wireless mesh networks that connect smart grid devices. SecureSmart uses a network of sensors to continuously assess wireless and SCADA networks that connect applications like smart meters and distribution automation systems, where millions of active endpoints make them a prime target for cyber attacks. The tool performs deep packet inspection, analyzes traffic behavior, and feeds analytics into a real-time health monitoring dashboard. The dashboard allows analysts and engineers to diagnose failures, identify misconfigured devices, recognize emerging threats, and shorten the time from threat discovery to remedy.

The SecureSmart managed service is now used by utilities coast-to-coast, where it has led to the discovery and remediation of significant wireless infrastructure vulnerabilities, one which had gone undetected for five years.

ACCESS

Perspecta built this capability into its [SecureSmart](#) managed service for wireless and SCADA network intrusion detection and prevention. The service also integrates [SCADA protocol evaluation capabilities from ADEC-G](#), also developed under CEDS.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Software-Defined Networking Technology Suite: Overview

Schweitzer Engineering Laboratories (SEL) developed the first software-defined networking (SDN) capability for Ethernet-based networks used in energy delivery systems. SDN allows operators to configure the way that communications move across a network and proactively determine pathways that isolate or reroute traffic during a cyber incident with minimal disruptions to grid operations. SEL's solution allows operators to design and configured a software-defined network using a suite of SEL technologies, which build upon a foundational whitelisting (or deny-by-default) capability developed in the [Exe-Guard project](#). The SDN and whitelisting capabilities help utilities strengthen cybersecurity, reduce latency in network communications, and decrease network and operator response time during cyber incidents.

The following products are the result of several CEDS R&D projects transitioned to commercial use, and can be used in conjunction to build a secure and highly configurable Ethernet-based network for energy delivery systems.

- Secure Software-Defined Radio Platform (currently in demonstration)
- Chess Master Application Programming Interface (currently in demonstration)
- SDN Flow Controller (transitioned in 2016)
- SDN Network Switch (transitioned in 2016)
- Exe-Guard Whitelisting Architecture (transitioned in 2015)

Software-Defined Networking Flow Controller

2016

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Ameren • Pacific Northwest National Laboratory • University of Illinois at Urbana-Champaign

The Software Defined Networking (SDN) Flow Controller (SEL-5056) offers a highly customizable and adaptable solution for managing complex energy delivery system (EDS) networks and devices by allowing users to define communication routes among devices on Ethernet-based local area networks.

The software enables operators to configure and monitor communications traffic as a single asset, and serves as a proactive solution to rerouting traffic during network faults and failures. SEL-5056 is designed to work in conjunction with the SEL-2740S Network Switch, which establishes secure baseline network communications using the whitelisting (or deny-by-default) capability.

ACCESS

The SDN Flow Controller was released in 2016 as [SEL-5056](#); the full suite of software-defined networking technology is available [here](#).

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Software-Defined Network Switch

2016

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

CenterPoint Electric • Pacific Northwest National Laboratory

The SEL-2740S Network Switch hardware protects devices on an Ethernet-based local area network (LAN) by denying all network traffic from devices that are not authorized or recognized as part of the network. The whitelisting (or deny-by-default) technology used in the software-defined networking (SDN) suite restricts network traffic to a defined set of known and trusted devices, denying any unknown traffic, whether malicious or not. The switch examines all traffic using deep packet inspection to either allow each bit of information to continue to its approved destination or safely quarantine it while isolating the untrusted device.

This product builds on the whitelisting capability of Exe-Guard and integrates with Padlock, another SEL product that merges cyber and physical security for remote devices. The switch also works together with SEL's SDN Flow Controller software, which allows operators to configure and monitor network traffic.

ACCESS

The SDN Network Switch was released in 2016 as **SEL-2740S**; the full suite of software-defined networking technology is available [here](#).

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

Exe-Guard Whitelisting Architecture

2015

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Sandia National Laboratories • Dominion Virginia Power • Dartmouth College

Exe-Guard offers a broad security framework that denies all untrusted communication, applications, and system responses, which helps protect against past, present, and future malware. Approved, trusted communications are secured through techniques including cryptographic protocols and secure auditing. Whitelisting, the deny-by-default architecture, eliminates the need for antivirus signature updates and is better suited to OT systems, since traditional blacklisting antivirus techniques require regular decommissioning for updates and cannot detect previously unseen malware. The Exe-Guard capability does not require any downtime for patches and updates.

Exe-Guard's capability was originally commercialized in SEL's Ethernet Security Gateway devices (SEL-3620 and SEL-3622), and subsequently built into the SDN Flow Controller and the SDN Network Switch; the capability is now standard in SEL products produced after 2014.

ACCESS

Exe-Guard was commercialized through CEDs as part of SEL's Ethernet Security Gateways (**SEL-3620** and **SEL-3622**) and **SEL-2740S** Network Switches. The full suite of software-defined networking technology is available [here](#).

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

Amilyzer Software

2015

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

PROJECT LEAD

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) consortium, led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

Electric Power Research Institute • Sandia National Laboratories • University of Texas at Dallas • Various industry partners: one utility, two vendors

Amilyzer is an intrusion detection system that monitors advanced metering infrastructure (AMI) traffic and alerts operators to any deviations from expected behavior.

Since 2007, the number of U.S. smart meters has grown from 2.5 million to over 70 million, creating a need for security advances catered specifically to AMI networks. Amilyzer defines a security policy that places constraints on communication traffic using the standard AMI protocol and raises the alarm when the protocol is used in an unexpected way. The security policy was defined based on the set of failure scenarios identified in the [NESCOR Electric Sector Failure Scenarios Report](#), which was also developed under the CEDS program.

In December 2012, a utility partner successfully deployed Amilyzer; the system is currently monitoring a 100,000-meter deployment.

ACCESS

Amilyzer was transitioned in 2015 and is available upon request. For more information, visit the Amilyzer [product page](#) or contact [Tim Yardley](#) at the Information Trust Institute at the University of Illinois Urbana-Champaign.

FOR MORE INFORMATION

[TCIPG Fact Sheet](#)

Autoscopy Jr. Intrusion Detection System

2015

CATEGORY

 **ATTACK IDENTIFICATION AND RESPONSE**

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 **ENERGY COMPANIES**

 **VENDORS**

 **RESEARCHERS**

PROJECT LEAD

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) consortium, led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

Dartmouth College • Schweitzer Engineering Laboratories (SEL)

Autoscopy Jr. is an intrusion detection system (IDS) designed specifically to integrate with and protect remotely deployed smart grid devices. Typical signature-based IDS solutions can be impractical for these embedded devices, which often lack the necessary computing power or are too widely dispersed to constantly update with new malware signatures. Autoscopy Jr. instead integrates threat detection into the device's operating system, allowing it to identify abnormal behavior and verify that commands are coming from a trusted source—all without unacceptably increasing latency on these time-critical devices.

Autoscopy Jr. was licensed by SEL, which leveraged elements of the IDS for the [Exe-Guard](#) whitelisting capability developed under CEDS.

ACCESS

Autoscopy Jr. is available from Dartmouth upon request ([contact](#)) and provided under version 2 of the GNU General Public License.

FOR MORE INFORMATION

[TCIPG Fact Sheet](#)

Hyperion

2015

CATEGORY



ATTACK IDENTIFICATION AND RESPONSE

MYP GOAL



FOR ADOPTION BY



ENERGY COMPANIES

PROJECT LEAD

Oak Ridge National Laboratory (ORNL)

PROJECT PARTNERS

EnerNex • Sensus

Hyperion distinguishes between malicious and healthy executable software by evaluating the compiled binary code to predict how a program will operate before it is deployed in an energy delivery system. Hyperion leverages ORNL's Function Extraction (FX) technology to analyze software, irrespective of the language, and determine whether a program includes hidden malware that may have been inserted at an earlier stage in the supply chain. Traditional malware detection methods for compiled code rely on searching for patterns of bytes that match existing malware (i.e., signature detection), but do not have the ability to detect malicious intent associated with unknown malware. Hyperion offers proactive malware detection and software assurance, providing users with new insight into compiled software behavior without requiring its source code.

Hyperion is a 2015 winner of the prestigious [R&D 100 Award](#) as an advanced technology for cyber security, and has been used in malware pilot projects at US-CERT and in the U.S. intelligence community. In 2013, the U.S. Department of Homeland Security (DHS) also selected Hyperion for its [Transition to Practice Program](#).

ACCESS

ORNL exclusively licensed Hyperion to [R&K Cyber Solutions](#) and partner company [Lenvio, Inc.](#), which redeveloped the prototype into a set of commercial products.

FOR MORE INFORMATION

[ORNL Fact Sheet](#)

NP-View Software

2015

CATEGORY



SITUATIONAL AWARENESS AND OPERATOR SUPPORT

MYP GOAL



FOR ADOPTION BY



ENERGY COMPANIES

PROJECT LEAD

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) consortium, led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

Network Perception • University of Illinois at Urbana-Champaign

The NP-View software tool performs a comprehensive network scan of firewall and router configurations, allowing system analysts to review the system's security controls, ensure proper functioning, and prepare for NERC Critical Infrastructure Protection (CIP) audits. Scan results are presented graphically, and can be filtered to show any deviations from the network's security policies and standards. This can help identify device misconfiguration, which could create vulnerabilities. NP-View also helps operators solve practical problems (such as network connectivity issues) while offering security experts and auditors a streamlined tool to assess and verify NERC CIP compliance. One utility used NP-View to perform a review of over 10,000 lines of firewall configuration in less than a week—a daunting task that otherwise would not have been feasible in the same time.

NP-View was commercialized in 2015 and has been deployed in over 20 utilities since its transition. The product also received a one-year DHS commercialization grant.

ACCESS

To access NP-View, visit the Network Perception [product page](#).

FOR MORE INFORMATION

[TCIPG Fact Sheet](#)

Specification-Based Intrusion Detection System for the Distributed Network Protocol

2015

CATEGORY

 REDUCED EXPOSURE

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 VENDORS

PROJECT LEAD

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) consortium, led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

The Information Trust Institute, led by University of Illinois at Urbana-Champaign

TCIPG developed a specification-based intrusion detection algorithm to provide high visibility of semantic data (information that allows machines to understand communications) carried by the DNP3—a network protocol widely used in SCADA systems—for use in network traffic monitoring tools.

Traditional anomaly-based detection technologies lack sufficient capabilities to investigate network traffic based on the unique proprietary protocols found in SCADA systems, while signature-based detection systems are unable to detect unknown or zero-day attacks. A specification-based system provides added benefit to OT system operators through its ability to detect unknown threats while providing detailed information on malicious activities detected.

The project team adapted Bro, a real-time open-source intrusion detection system, to integrate the detection algorithms for DNP3. Bro uses that algorithm to evaluate the SCADA system network events to detect defined security policy violations. Such abnormal patterns may indicate malicious operations that could destabilize control environments.

ACCESS

The specification-based DNP3 analyzer tool was released as open source in 2015 and is available with [Bro](#), an open-source intrusion detection system. The DNP3 analyzer algorithms are also built into [Amilyzer](#), a CEDS software tool that identifies real-time security threats for AMI devices.

FOR MORE INFORMATION

[TCIPG Fact Sheet](#)

Cyber Security Manager Software

2014

CATEGORY

 SITUATIONAL AWARENESS AND OPERATOR SUPPORT

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Siemens Energy

PROJECT PARTNERS

Pacific Northwest National Laboratory • Sacramento Municipal Utility District

The Cyber Security Manager (CSM) is a centralized software component that helps operators assess and address cyber threats to their supervisory control and data acquisition (SCADA), energy management, and distribution management systems. The manager helps operators make decisions by gathering and presenting data in a visual and meaningful way, providing actionable advice, and training operators with simulations and replays of real-life scenarios. It provides operators with the information and tools to recognize and respond quickly to cyber incidents, without requiring operators to have in-depth cybersecurity training.

ACCESS

Siemens offers the Spectrum Power [Cyber Security Manager](#) for use with their Spectrum Power Energy Management System.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Cyber-Physical (Hybrid-State) Monitoring to Detect Attacks on Protective Relays

2014

CATEGORY



MYP GOAL



FOR ADOPTION BY



PROJECT LEAD

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) consortium, led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

Lawrence Berkeley National Laboratory • University of California at Davis

Protective relays are programmed to take safety measures when physical conditions (e.g., voltage, power flows) reach levels that could potentially destabilize the grid. This intrusion detection tool uses the same parameters that relays use to determine if an attacker has manipulated the device or its communications. The tool verifies that monitoring information is consistent with physical grid conditions and flags abnormal commands or behavior that could indicate either insider error or a cyber attack. It then displays an alert in the control room where the operator can act upon the information without needing specialized cybersecurity knowledge to understand the issue.

ACCESS

This tool is available as an open source script. Contact [TCIPG](#) for more information.

FOR MORE INFORMATION

[TCIPG Product Page](#)

Cybersecurity Procurement Language for Energy Delivery Systems

2014

CATEGORY



MYP GOAL



FOR ADOPTION BY



PROJECT LEAD

Pacific Northwest National Laboratory

PROJECT PARTNERS

Electric Power Research Institute (EPRI) • Various researchers, National Laboratories, and academic partners

This guide provides reference language that energy companies can use to more precisely specify their cybersecurity requirements to vendors when purchasing energy delivery systems and components. Vendors need to see a business case that supports designing advanced cybersecurity features into new systems, which is strengthened when customers specifically request these features. The guide's reference language provides utilities with a starting point to request best-practice cybersecurity features during procurement, ensuring cybersecurity is considered in system design, testing, installation, and support.

The guide provides sample procurement language pertaining to general cybersecurity considerations, product life cycle, intrusion detection systems, physical and wireless security, and cryptographic technology for EDS. The Department of Defense now uses, trains on, and is building upon this language as a template for its contractual agreements with renewable energy generation and microgrid providers across the nation.

ACCESS

[Cybersecurity Procurement Language for Energy Delivery Systems](#), 2014

Role-Based Least-Privilege Access Control for ONG Control Systems

2014

CATEGORY

 ACCESS CONTROL

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Honeywell International

PROJECT PARTNERS

The Information Trust Institute, led by University of Illinois at Urbana-Champaign
• Idaho National Laboratory

Role-based, least-privilege access control limits each user's access permissions to the data, device, or equipment necessary for performing a specific task or role. This effectively reduces the potential for insider threats and limits what an attacker could achieve using stolen credentials in OT systems.

Honeywell built on the role-based access capability by incorporating least-privilege rights, which limit users' access privileges to the least amount necessary based on their specific role in an energy organization. Roles and permissions are defined based on the common needs and functions specific to energy delivery systems.

ACCESS

This capability is found in Honeywell's **Experion Process Knowledge System** (PKS), a control system platform widely used in oil and natural gas delivery systems, and has been built into various other Honeywell products.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

NESCOR Guide: Penetration Testing for Electric Utilities

2014

CATEGORY

 GUIDANCE AND PRACTICES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

National Electric Sector Cybersecurity Organization Resource (NESCOR)

PROJECT PARTNERS

Electric Power Research Institute

The Guide to Penetration Testing for Electric Utilities provides guidance on how to perform penetration tests on smart grid systems, with specific information regarding testing for vulnerabilities in advanced metering infrastructure; wide-area monitoring, protection, and control; and home-area networks. The penetration testing process is a complex hands-on assessment that network operators use to find and exploit vulnerabilities in OT and IT devices and systems and locate gaps in their security.

The guide helps security experts plan their penetration testing activities with a better understanding of the effort required for each test. It can also be used as a template for procurement language for smaller organizations that do not have a large in-house security team.

ACCESS

Guide to Penetration Testing for Electric Utilities was first released in 2014; version 3.0 is available on the [EPRI Website](#).

FOR MORE INFORMATION

[NESCOR Homepage](#)

Sophia: Control System Mapping and Monitoring Tool

2014

CATEGORY

 SITUATIONAL AWARENESS AND OPERATOR SUPPORT

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Idaho National Laboratory

PROJECT PARTNERS

Idaho Falls Power • NexDefense • University of Illinois at Urbana-Champaign

The Sophia software tool automatically maps and monitors IP-based SCADA networks, giving operators a better view of how devices communicate in order to quickly identify anomalous behavior. As more digital sensors and controls are added and networks grow in piecemeal fashion, it is an increasingly difficult task to oversee real-time communications among hundreds or thousands of components. Sophia simplifies this network complexity by mapping out all devices and expected communication patterns, passively monitoring networks, and alerting operators when anything deviates from the norm. The reduced human oversight needed for monitoring activities means a week's worth of work can be cut down to only four man-hours. The tool provides a 3-D visual interface, allowing operators to drill down and analyze messages between control system components, evaluate alerts, and make informed decisions.

ACCESS

NexDefense exclusively licensed the Sophia software, which has evolved into the [Integrity](#) product suite.

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

Api-do Toolset: KillerBee Software Updates and Api-Mote Hardware

2013

CATEGORY

 REDUCED EXPOSURE

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) consortium, led by University of Illinois at Urbana-Champaign

PROJECT PARTNERS

Dartmouth College • River Loop Security

Api-do is a collection of tools that enable utilities to identify and mitigate potential attack points in wireless radio networks commonly used for smart meter communication. Wireless networks (ZigBee and IEEE 802.15.4) can be used to communicate between critical SCADA systems and remote field devices, making it important to strengthen the security of these networks. Api-do includes major updates to KillerBee—an open-source software tool that uses “active fingerprinting” to locate digital radio devices in short-range networks—and Api-Mote, a hardware tool custom-designed to support self-assessment of utility networks. Together, these tools help utilities find and fix vulnerabilities in wireless networks that attackers could otherwise exploit. The tools are both faster and more accurate than passive techniques traditionally used to self-assess wireless network security.

ACCESS

[KillerBee open-source tools](#) and [Api-Mote hardware design files](#) are available on GitHub and through [River Loop Security](#) (founded by TCIPG alumni), which continues to maintain and update the toolset.

FOR MORE INFORMATION

[TCIPG Project Page](#)

CodeLock Software

2013

CATEGORY

 ACCESS CONTROL

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Sandia National
Laboratories

CodeLock protects critical applications by obfuscating code on network devices that make up energy delivery control systems. Obfuscation makes it difficult for an adversary to reverse-engineer and maliciously alter executable files, and so counters attempts to make the executable file untrustworthy.

This product was also developed as part of the U.S. Department of Homeland Security's Office of Science and Technology (S&T) Transition to Practice program.

ACCESS

CodeLock is available to utilities as software-as-a-service. It has been embedded in GridSTAR's Vir2us Security Suite ([Citadel](#)). CodeLock 2.0 is currently in testing and evaluation with [Dark](#)³.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Converged Networking for SCADA Systems (CONES)

2013

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 VENDORS

 RESEARCHERS

PROJECT LEAD

Trustworthy Cyber
Infrastructure for the Power
Grid (TCIPG) consortium, led by
University of Illinois at Urbana-
Champaign

PROJECT PARTNERS

Grid Protection Alliance

The Converged Networking for SCADA Systems (CONES) architecture provides a secure and efficient way to exchange large amounts of information at high speeds by integrating multiple SCADA networks and devices. As new sensors and smart devices add new communication pathways to power system networks, SCADA systems are beginning to merge multiple separate communication channels, many with different requirements for timing and security. CONES leveraged off-the-shelf hardware and software where possible, augmenting them as needed, to create a toolkit for converged SCADA networks that coordinates communication traffic based on the priority, latency, and protection requirements of each data type. This network convergence framework greatly improves the efficiency of SCADA systems while keeping applications isolated, optimizing resources, and guaranteeing data delivery in the time required.

ACCESS

CONES provided the foundational research base that led to the successful development of the [Secure Information Exchange Gateway](#) (SIEGate). Access information about CONES through the [research page](#) or learn more about [SIEGate](#).

FOR MORE INFORMATION

[TCIPG Fact Sheet](#)

Dynamic Defense and Network Randomization

2013

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 VENDORS

 RESEARCHERS

PROJECT LEAD

Sandia National
Laboratories

PROJECT PARTNERS

Tennessee Valley Authority

Dynamic defense and network randomization techniques can thwart attackers by 1) recognizing and responding to attack patterns in near real time, and 2) making network communications unpredictable so that intruders cannot effectively map the system or plan attack pathways. Sandia's proof-of-concept uses machine learning algorithms to detect network traffic that is either abnormal or resembles previous attacks. A detected threat then triggers network randomization, which turns computer systems into moving targets by automatically randomizing IP addresses, application port numbers, and communication pathways. These techniques can quickly detect and interrupt an attack, and eliminate static configurations that give adversaries a predictable target.

After the CEDS project, Sandia continued testing its solution under the DHS Transition to Practice program in 2015, improving the accuracy, speed, and scalability to large infrastructure networks.

ACCESS

Sandia incorporated network randomization into its open-source POX SDN controller, available on [GitHub](#). Sandia is now building on and advancing these techniques through the CEDS AddSec project.

FOR MORE INFORMATION

[DHS Transition to Practice Guide](#); [Sandia Technical Report](#)

Intrusion Response and Recovery Using Game Theory

2013

CATEGORY

 ATTACK IDENTIFICATION
AND RESPONSE

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Trustworthy Cyber
Infrastructure for the Power
Grid (TCIPG) consortium, led
by University of Illinois at
Urbana-Champaign

PROJECT PARTNERS

Schweitzer Engineering
Laboratories (SEL)

The Response and Recovery Engine (RRE) compiles data on broad system behaviors, network architecture configurations, and measurements from system-level sensors and uses this data to develop algorithms that identify system threats and suggest an effective response to these threats. The RRE algorithms help human operators verify the safety and feasibility of executing a response to a system threat or anomaly, and allows them to do so quickly. It also helps to reduce the number of false positives and help operators quickly identify valid threats. This method integrates with the CEDS [Amilyzer](#) tool, which identifies security threats on advanced metering infrastructure (AMI) using distributed network protocol (DNP3) communications.

ACCESS

The RRE method transitioned to an open-source product designed for deployment in utility intrusion detection systems (IDS). It is integrated into [Snort 2.7](#) (an open-source IDS) and was partially implemented in SEL OpenFlow devices in 2013.

FOR MORE INFORMATION

[TCIPG Fact Sheet](#)

NESCOR Reports: Electric Sector Failure Scenarios, Impact Analyses, and Mitigations Mapping

2015 (Mitigations Mapping)

2013 (Scenarios)

CATEGORY

 GUIDANCE AND PRACTICES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

National Electric Sector
Cybersecurity Organization
Resource (NESCOR)

PROJECT PARTNERS

Electric Power Research
Institute • International
Electrotechnical
Commission • Smart Grid
Interoperability Panel

This set of reports identifies 127 realistic cybersecurity failure scenarios and mitigation strategies that could impact electricity delivery, business operations, or customers. These reports aid utilities in identifying system vulnerabilities, potential impacts from exploitation of these vulnerabilities, and mitigation solutions that can be used to prevent adverse events. Each scenario includes a list of potential system vulnerabilities that could be exploited by an attacker and a list of associated impacts and mitigations.

The *Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping* report builds on *Electric Sector Failure Scenarios* by grouping common vulnerabilities and mitigations into NISTIR 7628 Vulnerability Classes and Mitigation Classes, and mapping individual scenario mitigations to common mitigations.

These reports can be used by many different organizations. In addition to providing utilities with a better understanding of their vulnerabilities, vendors use the information provided as part of their development/upgrade process, and researchers have used them to inform their research on control systems security. While these reports do not contain tabletop exercises, the scenarios included in each can be used in developing a tabletop.

ACCESS

Originally released in 2013, the *Electric Failure Scenarios and Impact Analysis* report version 3.0 was released in 2015. Version 2.0 of the *Common Vulnerabilities and Mitigations Mapping* was released in 2015.

FOR MORE INFORMATION

[NESCOR Resource Center](#)

NESCOR Guide: Cybersecurity for Distributed Energy Resource (DER) Systems

2013

CATEGORY

 GUIDANCE AND PRACTICES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

 RESEARCHERS

PROJECT LEAD

National Electric Sector
Cybersecurity Organization
Resource (NESCOR)

PROJECT PARTNERS

Electric Power Research
Institute • International
Electrotechnical
Commission • Smart Grid
Interoperability Panel

The **Cybersecurity for Distributed Energy Resource (DER) Systems** guide identifies baseline cybersecurity requirements for DER systems, addressing the complex mix of protocols and standards that may be used across multiple DER system architectures. DERs are geographically dispersed devices that meet the supply and demand needs of the distribution grid through energy generation (e.g., solar panels), storage, or a variety of demand response options. These devices are often in customer-owned or remote locations, making security a greater challenge, particularly in light of increased adoption since 2013.

The guide maps DER systems engineering schemes to the framework used in the National Institute of Standards and Technology (NIST) Interagency Report 7628: *Guidelines for Smart Grid Cyber Security*, the industry's landmark cybersecurity requirements for the smart grid. It defines cybersecurity guidelines for five different levels of DER system architectures:

1. Autonomous cyber-physical DER systems
2. Facilities DER energy management systems
3. Information and communications technologies for utility and retail energy providers
4. Distribution utility DER operational analyses
5. Interactions with ISOs/RTOs and energy markets

ACCESS

[Cybersecurity for Distributed Energy Resource \(DER\) Systems](#) (Version 1.0), 2013

FOR MORE INFORMATION

[NESCOR Homepage](#)

Secure Information Exchange Gateway for Electric Grid Operations (SIEGate)

2013

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Grid Protection Alliance

PROJECT PARTNERS

Alstom Grid • Pacific Northwest National Laboratory • PJM Interconnection • University of Illinois at Urbana-Champaign

SIEGate is a software tool that maintains the integrity of large volumes of time-sensitive data moving between control centers and transmission organizations (e.g., synchrophasor data) while maintaining low-latency, high-throughput communications. SIEGate functions as a secure gateway directing traffic at the edge of a SCADA system, while also combining data-sharing tasks across multiple systems into a single, coherent platform. SIEGate strengthens cybersecurity while reducing the administrative burden and cost of exchanging grid data among control rooms. The software is currently in use in at least three utilities and has been downloaded more than 3,000 times as of 2017. Current CEDS projects continue to advance more secure communications protocols for energy delivery systems.

ACCESS

SIEGate is on the Grid Protection Alliance [website](#) and available for download via [GitHub](#). The software is also an integrated feature in the [e-terrplatform](#) Energy Management System by Alstom Grid, which was later purchased by GE.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Agent-based, Distributed, and Extensible Cybersecurity for the Grid (ADEC-G)

2013

CATEGORY

 ATTACK IDENTIFICATION AND RESPONSE

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Perspecta (formerly Vencore Labs)

PROJECT PARTNERS

DTE Energy • Electric Power Research Institute, Inc. • University of Illinois at Urbana-Champaign • Sacramento Municipal Utility District • Hawaiian Electric Company

ADEC-G monitors commonly used protocols in SCADA systems to detect and alert operators to anomalies, ongoing attacks, and even zero-day attacks. SCADA systems may use a wide range of protocols for network traffic, and each protocol has a unique set of vulnerabilities and design flaws that can be exploited. ADEC-G employs behavior model checkers to detect communication anomalies and can alert operators through a user-friendly dashboard or perform predetermined actions to stop an attack. The software has been designed to accommodate multiple different protocols and allow operators flexibility in choosing which protocol to monitor and protect.

This SCADA system protocol evaluation software developed as part of this CEDS project provides a foundational capability to Perspecta's SecureSmart Managed Security Service (MSS), which is a comprehensive and continuous monitoring solution for advanced metering infrastructure (AMI) and SCADA systems.

ACCESS

Perspecta incorporated ADEC-G into its [SecureSmart](#) Managed Security Service, which is used by multiple utilities.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Padlock Cyber-Physical Sensor Technology

2012

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Sandia National Laboratories (SNL) •
Dominion Virginia Power •
Dartmouth College

Because of the remote nature of many components of smart grid infrastructure, it can be difficult for operators to determine if a field control cabinet has been compromised. Padlock is a device with sensors that automatically warns operators of potential tampering by detecting sudden movement in field cabinets, abrupt changes in visible light, opening of cabinet doors, and the connection and disconnection of Ethernet cables. Padlock technology is the first hardware and software product to merge physical tamper detection with advanced cybersecurity capabilities.

ACCESS

Padlock is fully commercialized as a standalone dongle and is integrated in the [SEL-3622](#) Security Gateway.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Smart Grid Cryptographic Key Management System

2012

CATEGORY

 ACCESS CONTROL

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

PROJECT LEAD

Sypris Electronics, LLC

PROJECT PARTNERS

Purdue University Center for Education and Research in Information Assurance and Security • Oak Ridge National Laboratory • Electric Power Research Institute • Valicore Technologies

Sypris Electronics developed a Cryptographic Key Management System (CKMS) for the secure management and distribution of network security keys (unique and specific identifiers for pieces of network traffic), which are difficult to manage and verify at a large scale in IT networks. CKMS separates network traffic into segments and assigns different keys to each segment, ensuring that a compromised segment does not affect the security of the remaining segments. This key management process is also able to recover the compromised segment by reauthorizing the approved devices. CKMS leverages the best practices of existing Department of Defense (DoD) key management systems to protect high-value data, while also enabling the system to quickly recover from and/or fend off cyber attacks. While this project has been transitioned to commercialization for IT systems, researchers and vendors are actively working to develop a key management system for OT networks (Module-OT, in partnership with the National Renewable Energy Laboratory [NREL]).

ACCESS

Learn more on the Sypris [product page](#). The product was originally sold by Sypris, and later purchased by Analog Devices, Inc.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Hallmark Secure SCADA Communications Protocol

2011

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Pacific Northwest National Laboratory

PROJECT PARTNERS

Schweitzer Engineering Laboratories (SEL) • CenterPoint Energy • Siemens

The Secure SCADA Communications Protocol (SSCP) safeguards serial communications between remote devices and control centers using message authentication and optional encryption. SCADA systems require a common method to authenticate device-to-device communications and verify the information comes from a trusted source. SSCP works with both new and legacy system designs, marks all messages with a unique sending device identifier, and optionally encrypts the message with a Federal Information Processing Standard (FIPS) encryption. Vendors could use the protocol to build more secure communications into new systems and components.

SEL designed two hardware devices that help build the SSCP into existing legacy equipment—one for vendors, and one plug-and-play device for utilities. The cryptographic card (SEL-3045) is an electronic hardware card that runs the SSCP, and that manufacturers can embed into their own equipment. The serial shield (SEL-3025) is a “bump-in-the-wire” device (a device placed on the serial communication link between legacy devices) that adds only minimal latency while securing serial communications using SSCP. Additionally, current CEDS projects continue to advance more secure communications protocols for energy delivery systems.

ACCESS

SSCP is being considered as a component of the Universal Utility Data Exchange project, funded through CEDS and lead by Pacific Northwest National Laboratory. Contact [Mark Hadley](#) at PNNL for more information.

FOR MORE INFORMATION

[CEDS Fact Sheet](#)

Contribution: ISA Trustworthiness in Wireless Industrial Automation Report

2011

CATEGORY

 GUIDANCE AND PRACTICES

MYP GOAL

P PREVENT **D** DETECT
M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

International Society of Automation

PROJECT PARTNERS

Argonne National Laboratory • Oak Ridge National Laboratory

This technical report identified requirements, metrics, use cases, and assessment criteria that vendors can use to build trustworthy wireless networks for critical automation systems in energy delivery infrastructure.

The requirements in this report were instrumental in helping design and build secure wireless network technologies, which were in growing demand by 2011 as industry-wide adoption of smart grid technologies began to rise.

Developed by a working group of more than 50 researchers, vendors, and owners and operators, the report provided a strong foundation to other ISA standards work on wireless sensors, systems, instrumentation, and integration. It led to substantive improvements in the ISA100/IEC62734 worldwide standard for industrial wireless sensors and systems, which major technology vendors such as Honeywell, Schneider, and Yokogawa have used to design their products. The report can also be used by energy companies and regulators to inform secure wireless system design.

Note: CEDS funding was used by Argonne National Laboratory and Oak Ridge National Laboratory as participants in the development of the report; the International Society of Automation (ISA) led the work in developing this standard.

ACCESS

Trustworthiness in Wireless Industrial Automation (ISA-TR100.14) can be [purchased from ISA](#). More than 500 companies have purchased the report as of 2018.

Cybersecurity Audit and Attack Detection Toolkit (Bandolier and Portaledge)

2010

CATEGORY

 REDUCED EXPOSURE

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 ENERGY COMPANIES

 VENDORS

PROJECT LEAD

Digital Bond

PROJECT PARTNERS

OSIsoft • Tennessee Valley Authority • PacifiCorp • Tenable Network Security

By building configuration audit and attack detection capabilities into tools already used by the energy sector, Bandolier and Portaledge offer energy-asset owners low-cost and easily integrated control systems security solutions. Bandolier's assessment capabilities help energy system operators to audit and detect the control system's security configurations and compare these configurations against industry best practices. Portaledge captures production and process data stored within the OSIsoft PI Server¹ to analyze and correlate operational patterns with malware indicators or security events. The development and release of Bandolier and Portaledge in 2010 paved the way for today's technologies that continue to anticipate and meet the rapidly evolving needs of energy delivery systems.

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

Lemnos Interoperable Configuration Profiles

2010

CATEGORY

 NETWORK ARCHITECTURES

MYP GOAL

P PREVENT **D** DETECT

M MITIGATE **S** SURVIVE

FOR ADOPTION BY

 VENDORS

PROJECT LEAD

EnerNex • Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Sandia National Laboratories • Tennessee Valley Authority

Interoperable configuration profiles (ICPs) are an agreed-upon set of capability and operational requirements for vendor products that allow utilities to purchase the devices and software necessary for their unique system architecture. The Lemnos ICP was developed to increase the availability and accessibility of cost-effective security solutions for control systems. Using Lemnos, utilities have more freedom to use software or devices from different vendors without significant service interruptions or costly replacement of incompatible devices. While the open-source and interoperable solutions presented through Lemnos help researchers develop technical capabilities that are deployable across different power systems, several commercialized products, such as the [SEL-3620 Exe-Guard Ethernet Security Gateway](#), used Lemnos standards to enable the device to integrate with other vendor's energy system components.

The profiles are also available for vendors who wish to incorporate interoperability guidelines into their energy delivery system components. To date, more than 10 vendors have demonstrated interoperability using these profiles. Lemnos is referenced, maintained, and updated as part of the [Institute of Electrical and Electronics Engineers \(IEEE\) 1547 Standard](#), and vendors that implement IEEE P2030.102.X are using results based on this CEDs project.

FOR MORE INFORMATION

[CEDs Fact Sheet](#)

1. The OSIsoft PI Server aggregates and correlates process data. In Portaledge, Digital Bond has created modules to aggregate security events and correlate these events to detect cyber attacks. There are a variety of modules including modules that meet the NERC CIP monitoring requirements.

Appendix Project Partners

CEDS research projects have engaged more than 140 energy companies, vendors and service providers, universities, National Laboratories, industry associations, standards organizations, and other federal partners.

Energy Companies

| | |
|---|--|
| Ameren | Inland Empire Energy Center |
| Arkansas Electric Cooperative Corporation | New York Power Authority |
| Avista | Northern Indiana Public Service Company |
| Bonneville Power Administration | NRG |
| Burbank Water and Power | Omaha Public Power District |
| CenterPoint Energy | Orange and Rockland Utilities |
| Chevron | Pacific Gas and Electric |
| Commonwealth Edison | PacifiCorp |
| Dominion | Peak RC |
| DTE Energy | PJM Interconnection |
| Duke Energy | Rochester Public Utilities |
| Electric Reliability Council of Texas (ERCOT) | Sacramento Municipal Utility District |
| Energy | San Diego Gas and Electric |
| EPB | Sempra |
| FirstEnergy | Southern California Edison |
| Florida Power & Light | Southern Company |
| Ft. Belvoir | Tennessee Valley Authority |
| Hawaiian Electric Company | Virgin Islands Water and Power Authority |
| Idaho Falls Power | Washington Gas Energy Systems |
| Idaho Power Company | Westar Energy |
| Independent Electricity System Operator (IESO) Ontario | Western Area Power Administration (WAPA) |

Vendor and Service Providers

- ABB, Inc.

- Alstom Grid

- Applied Control Solutions

- ArcSight

- Cigital, Inc.

- Cisco Systems

- Critical Intelligence

- Cybati

- Digital Bond

- Digital Management, Inc.

- Eaton

- EnerNex Corporation

- FoxGuard Solutions, Inc.

- Fujitsu

- General Electric

- Grid Protection Alliance

- Grimm

- Honeywell

- ID Quantique

- Intel

- Invensys

- Kenexis Consulting

- LiveData Utilities

- Network Perception

- NexDefense

- ViaSat

- OPAL_RT Technologies

- Open Information Security Foundation

- Opus Consulting

- OSIsoft

- Parsons

- Perspecta (formerly Vencore Labs)

- Power Standards Laboratory

- Qubitekk, Inc.

- River Loop Security

- RTDS Technologies

- Schneider Electric

- Schweitzer Engineering Laboratories

- Sensus

- Siemens

- SRI International

- Sypris Electronics

- TDi Technologies

- Telvent

- Tenable Network Security

- United Technologies Research Center (UTRC)

- Upstanding Hackers

- Utility Advisors

- Utility Integration Solutions

- Valicore Technologies

- Veracity Security Intelligence

University Partners and Consortia

| | |
|---------------------------------------|--|
| Arizona State University | Tennessee State University |
| Carnegie Mellon University | Texas A&M Engineering Experiment Station |
| Dartmouth College | University of Arkansas |
| Florida International University | University of California at Davis |
| Georgia Tech Research Institute | University of Houston |
| Illinois Institute of Technology | University of Idaho |
| Iowa State University | University of Illinois at Urbana-Champaign |
| Lehigh University | University of North Carolina at Charlotte |
| Massachusetts Institute of Technology | University of Tennessee |
| Old Dominion University | University of Texas at Austin |
| Oregon State University | University of Texas at Dallas |
| Purdue University | Virginia Tech |
| Rutgers University | Wake Forest University |
| SUNY-Buffalo | Washington State University |

Many academic partners are part of three multi-university collaborations (one past and two active) that CEDS has funded together with the DHS Science and Technology Directorate. Each university team tackles high-priority cybersecurity needs to develop novel solutions, while actively engaging with a team of industry asset owners and solution providers in each effort. These academic partnerships also help develop and train the next generation of cybersecurity professionals for the energy sector.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID (TCIPG) was the first collaborative RD&D center funded by CEDS from 2010-2015, with co-funding from the Department of Homeland Security. It included four universities that worked with industry, National Labs, and academia to conduct breakthrough research on control systems and design tools that embed security into grid operations. It was the successor of an earlier project established in 2005 with funding from the National Science Foundation. Partners went on to expand the partnership in forming CREDC.

- Partner universities include: University of Illinois at Urbana-Champaign (lead), Arizona State University, Dartmouth College, Washington State University

THE CYBER RESILIENT ENERGY DELIVERY CONSORTIUM (CREDC) is led by the University of Illinois at Urbana-Champaign, in partnership with nine other universities and two National Laboratories. CREDC research engages an industry advisory board that helps identify research priorities, facilitating the transition of new, needed cybersecurity technologies into real-world energy delivery systems. CREDC research themes include real-time cyber event detection and situational awareness, protective and cyber-resilient architectures and technologies, and designing cyber resilience into emerging power system devices for the future grid, and oil and natural gas infrastructure.

- Partner universities include: University of Illinois at Urbana-Champaign (lead), Arizona State University, Dartmouth College, Massachusetts Institute of Technology, Old Dominion University, Oregon State University, Rutgers University, Tennessee State University, University of Houston, and Washington State University
- Partner National Laboratories include: Argonne National Laboratory and Pacific Northwest National Laboratory

THE CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS (SEEDS) is a partnership of six universities and one electric cooperative that is advancing cybersecurity for electricity and oil and natural gas infrastructure. SEEDS research engages an industry advisory board to help determine research priorities, provide input toward ongoing research, and ensure that activities are likely to be useful and used by the energy sector. SEEDS research themes include detecting malicious data input to power system applications such as automatic generation control, moving target defense, detecting supply chain cybersecurity compromise of smart grid devices, optimization of cybersecurity resources, and cybersecurity for time-critical communications necessary for energy delivery system operations.

- Partner universities include: University of Arkansas (lead) Carnegie Mellon University, Florida International University, Lehigh University, Massachusetts Institute of Technology, and the University of Arkansas at Little Rock
- Partner electric cooperative: Arkansas Electric Cooperative Corporation

National Laboratory Partners

| | |
|--|---------------------------------------|
| Argonne National Laboratory | Los Alamos National Laboratory |
| Brookhaven National Laboratory | National Renewable Energy Laboratory |
| Idaho National Laboratory | Oak Ridge National Laboratory |
| Lawrence Berkeley National Laboratory | Pacific Northwest National Laboratory |
| Lawrence Livermore National Laboratory | Sandia National Laboratories |

Associations and Standards Organizations

| | |
|---|---|
| American Public Power Association (APPA) | International Society of Automation |
| Edison Electric Institute (EEI) | National Electric Sector Cybersecurity Organization Resource (NESCOR) |
| Electric Power Research Institute (EPRI) | National Rural Electric Cooperative Association (NRECA) |
| Energy Sector Control Systems Working Group | Smart Grid Interoperability Panel |
| International Electrotechnical Commission | Utilities Telecom Council |

Federal Partners

DHS ICS-CERT



U.S. DEPARTMENT OF
ENERGY

OFFICE OF
**CYBERSECURITY, ENERGY SECURITY,
AND EMERGENCY RESPONSE**