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

From Innovation to Practice:

The CESER RMT Program's Real-World Impact on Energy Sector Cybersecurity

August 2024

The Risk Management Tools and Technologies (RMT) division within DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads research, development, and demonstration (RD&D) projects to improve cybersecurity of the energy sector.

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

Table of Contents

Introduction

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 mis-operate power system equipment and disrupt energy delivery. The intensifying cyber threat landscape has inspired a community of cyber-defenders—in partnership with DOE—to develop solutions to allow energy delivery systems and devices to detect adversarial actions and adapt to survive while sustaining critical functions.

Through the Risk Management Tools and Technologies (RMT) program in the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the Department of Energy (DOE) has partnered with the energy sector for more than a decade to advance cybersecurity RD&D that can reduce cyber risks to energy delivery infrastructure.

Since 2010, RMT has transitioned more than **80 products, tools, and technologies** to reduce the energy sector's cyber risk.

More than half of electricity customers in the U.S. are served by power providers participating in RMT research.

More than 1,500 utilities, in all 50 states, have purchased products developed through RMT research.

All RMT projects included an energy sector partner that can refine requirements and provide a path to demonstration of a tangible product.

By partnering with industry, electric utilities, academia, and national laboratories, RMT has been able to deliver **more than 80 products, tools, and technologies** to help reduce the risk that a cyberattack might disrupt our nation's critical energy delivery infrastructure. This report highlights **50 of them**. **Thirty-two entries describe technologies that have successfully transitioned** to the sector since 2018 and are now available for energy companies, vendors, and researchers to use. The other **18 describe technologies that will soon emerge** from RMT R&D after successful demonstrations with industry partners.

> *This report considers a technology to be **transitioned** if it has been made available as **open-source software**, been integrated into a **commercialized product** available for purchase or license, or otherwise been **deployed in operational technology for the grid**.*

The CESER RMT program delivers a wide range of tools and technologies supporting the identification and mitigation of risk in the energy sector. This report highlights outcomes of the Cybersecurity RD&D performed by RMT, but this is just one piece of a larger portfolio addressing risks to the security and resilience of the energy sector. RMT has developed and continues to support a variety of other tools, including:

- A complementary portfolio of RD&D addressing risks from natural hazards, physical security, and electromagnetic disturbances;
- The Energy Cyber Sense program, a comprehensive effort to address supply chain risk within the energy sector through policies, standards, testing, educational awareness, and more;
- Under the Cyber Sense umbrella, Cyber Testing for Resilient Industrial Control Systems (CyTRICS), which leverages the testing capabilities of the National Laboratories to strengthen the security and resilience of hardware and software in the energy sector;
- Methods for ensuring security through the design process, including the Cyber-Informed Engineering (CIE) and Consequence-driven Cyber-Informed Engineering (CCE) methods, which are gaining acceptance by industry and being incorporated into engineering education programs; and
- A capability maturity model and related guidance to assist energy sector partners in assessing and improving their risk postures.

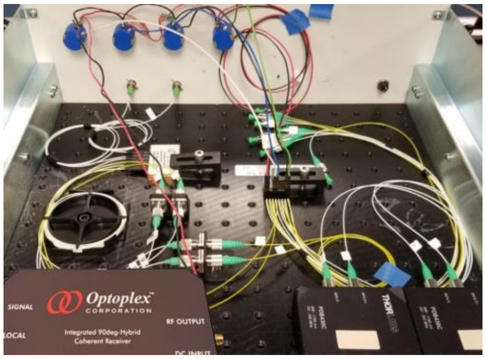
Success Story: Quantum Key Distribution

RMT-Funded Projects Are Elevating Cybersecurity to New Heights

RMT-funded projects have explored the use of Quantum Key Distribution (QKD) to secure critical energy infrastructure on Earth and, potentially, in space. QKD employs quantum mechanics to generate unique numerical “keys” that can be used to encrypt and decrypt data. Doing so protects that data from malicious actors who would steal it or use it to sabotage the grid.

With its quantum-focused project— “Multi-Hop Quantum Networking for Electric Grid Security” —Los Alamos National Laboratory (LANL) developed hardware and software to bolster the security and reduce the cost of quantum communication nodes that enable QKD. As part of DOE’s Quantum & Space Collaboration, LANL plans to provide its quantum random number generator (developed through this project) for integration with a demonstration aboard the International Space Station. This off-world application will demonstrate—in a dramatic way—how random number generation can protect communication between distant devices.

LANL’s random number generator is relevant to a range of energy systems and components, from fuel cells to nuclear power plants. Qrypt, Inc., has licensed the technology’s patent, has executed a cooperative research and development agreement with LANL, and is now providing the technology to NVIDIA for use in its BlueField-3 digital processing units. BlueField-3 was designed to accommodate the rise of artificial intelligence and cloud computing, which bring new vulnerabilities to the grid.



An Optoplex receiver being demonstrated as part of ORNL’s Q-Sens project.

LANL isn’t the only national laboratory that used RMT support to pursue QKD technologies. So, too, did Oak Ridge National Laboratory (ORNL) with its project, “Quantum Physics Secured Communications for the Energy Sector” (Q-Sens). Q-Sens addresses the distance limitations and expense of QKD by providing new quantum protocols for authenticating data. The key management server that resulted from this project makes it possible to combine multiple signals into one, over a shared medium. Keys can be established between any two endpoints that have gained the trust of the key server—even if those end points have not connected with each other before. With the project’s conclusion in 2021, ORNL demonstrated the technology; in the intervening years, Optoplex Corporation has commercialized it.

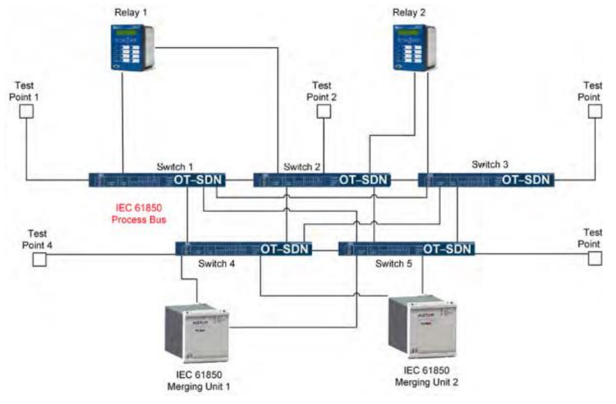
Lastly, Qubitekk developed a QKD system to detect eavesdropping attempts that threaten network encryption on the grid. The technology—which came from the “Scalable Quantum Cryptography Network for Protected Automation Communication” project—safeguards cryptographic keys as they are exchanged, using signals that automatically change if an adversary targets a key. The technology also alerts operators of theft attempts in real time, reducing the risk that data has been compromised despite appearing secure. The technology was successfully installed and tested in a field test network at a partnering utility (EPB of Chattanooga), and the utility is now adding customers to this Qubitekk-powered, quantum-protected network.

Success Story: Software-Defined Networking

Schweitzer Engineering Laboratories (SEL) Pioneers SDN to Secure the Power Grid

Building on the success of multiple RMT-funded projects, SEL now offers cybersecurity tools that have been deployed in electric power systems across—and beyond—the nation. These tools leverage Software-Defined Networking (SDN) to monitor and direct network traffic. RMT-funded SND solutions are now a critical component of products that SEL and other vendors markets for real-world applications.

These RMT-funded projects included one—led by Pacific Northwest National Laboratory—that involved piloting SDN tools at Department of Defense (DOD) sites, such as Ft. Belvoir in Virginia. Since the project ended in 2021, the tools have achieved widespread adoption. The National Nuclear Security Administration deemed them foundational to its Mission-Critical Control Systems. The Itaipu Hydroelectric Dam—on the border between Brazil and Paraguay—relied on them to bring a new ethernet network online, and an electric utility in Belgium used them to integrate a new, offshore wind farm into the European grid.



Sample use case applying PNNL SDN tool for testing or isolation

SEL and its partners are currently preparing to pilot the tools at more DOD sites and in various locations across the Indo-Pacific region. These tools have also formed the basis of products offered by Splunk and Elasticsearch.

Through another project that ended in 2021, SEL worked with Dragos and Juniper Networks to demonstrate a technology that manages data across numerous software applications in a scalable way. The technology—called Ambassador—secures data in near real time, provides continuous monitoring, prioritizes application functions, and visualizes networks' security posture overall. The Ambassador project built on SEL's previous research and was demonstrated on SEL's commercialized Blueframe Application Platform. The team commercialized and published the solution as Converged Industrial Edge, a solutions architecture that safeguards critical infrastructure networks today.

Finally, SEL's Chess Master project brought about an interface that allows software packages from multiple suppliers to securely communicate with each other. This type of interface is important because it enables various suppliers to work together and orchestrate network management and telemetry monitoring. After the project's conclusion in 2020, the technology became part of SEL's SDN Application Suite (SEL-5057), SDN Flow Controller (SEL-5056), and SDN Switch (SEL-2742S)—all of which are in use by utilities, vendors, and other users.

Success Story: AI-supported Patch Delivery

With Artificial Intelligence, the Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS) Makes Patch Delivery Easier and More Secure

SEEDS—an RMT-supported consortium of universities—used artificial intelligence to optimize risk analysis and decision making in patch and vulnerability management. Led by the University of Arkansas, SEEDS developed a technology that automates vulnerability-remediation decisions. It can even recommend specific actions, such as "patch immediately," "mitigate immediately," and "patch-in-cycle." It also compiles vulnerability mitigation information from the National Institute of Standards and Technology's National Vulnerability Database (NVD) to conduct efficient and effective risk assessments. The latter is important because NVD is the federal government's repository of standards-based vulnerability-management data. It is updated regularly, and it comprises databases of security checklist references, security-related software flaws, product names, and impact metrics.

The technology that SEEDS developed—called "Security Patch Automated Remediation Tool Analyzing the National Vulnerability Database" (SPARTAN)—is now a commercialized, cutting-edge solution that Bastazo, Inc., offers for securing operational technology and industrial control systems in the energy sector. Two electric utilities currently use it at their generation facilities. Additionally, Bastazo, Inc., is pursuing a partnership agreement with Network Perception to sell a "combined" product: a network-attack simulation capability for vulnerability management.

SPARTAN was, moreover, the basis for further commercialization funded by another DOE project ("V-INT: Automated Vulnerability Intelligence and Risk Assessment") and by a grant from the Israel-U.S. Binational Industrial Research and Development Foundation.

Success Story: Cyber Risk Assessment Tool

The Cyber Resilient Energy Delivery Consortium (CREDC) Developed a New Method for Detecting and Localizing Attacks on Bulk Power Systems

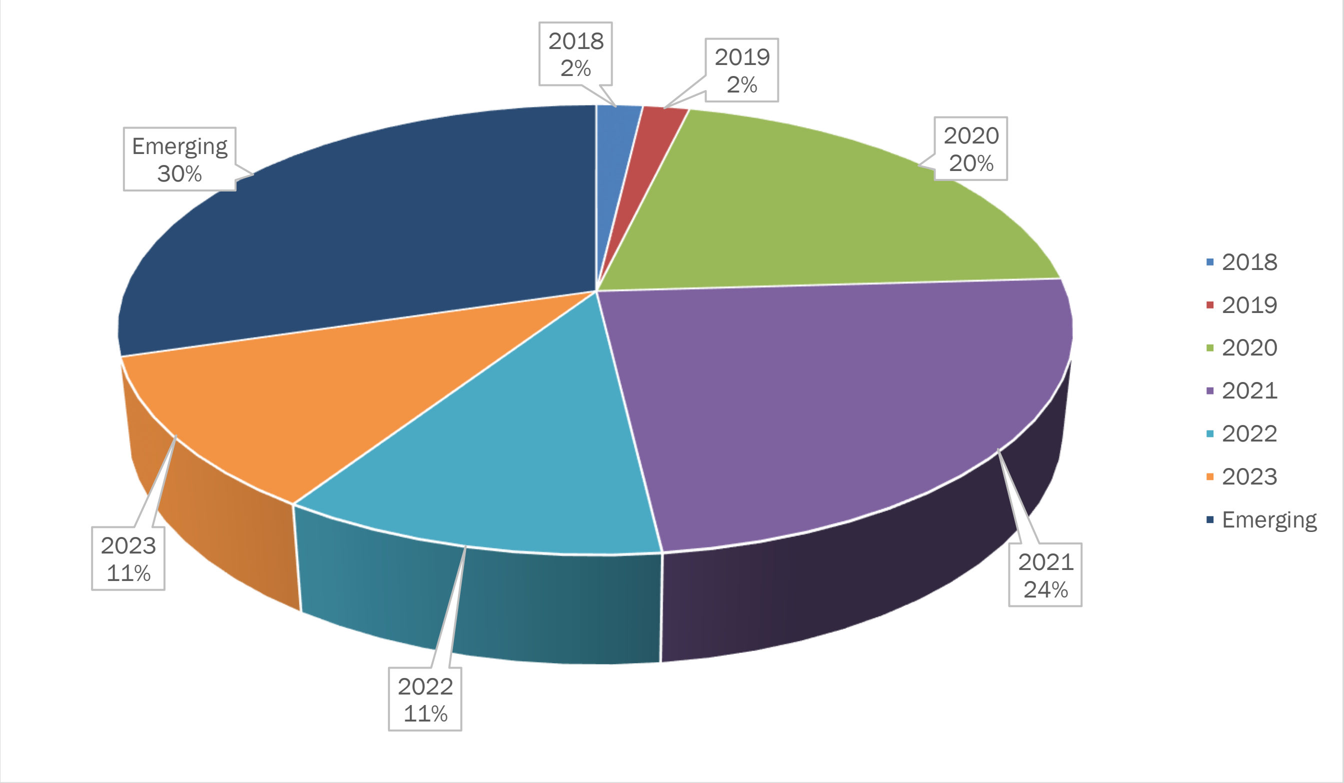
Through an RMT-supported project—called "Cyber Resilient Metrics for Bulk Power Systems"—Old Dominion University and its CREDC partners created a novel risk-assessment tool for bulk power systems, which encompass a vast network of generation and transmission facilities.

To safeguard this network, the project team developed the Cyber Risk Assessment Tool (CRAT) to evaluate how bulk power systems withstand the presence of cyberattacks. Based on a self-assessment, CRAT generates an extensive report that operators can use to identify areas of improvement. The cyber-resilience metrics that CRAT provides can inform the effective management of risks that threaten bulk power systems. The metrics also make it simpler for asset owners to prioritize corrective actions by determining the most resilient system configurations, the most critical vulnerabilities, and the most cost-effective security controls.

ReliabilityFirst, a project partner, now offers CRAT as a web-based tool for entities that wish to benchmark their own cyber-resilience posture. More than 230 utilities in the ReliabilityFirst region currently use this tool, which is based on CREDC's RMT-funded project. Technologies like CRAT are especially important because the sheer scale of bulk power systems increases their exposure to cyberthreats. The North American bulk power system comprises more than 200,000 miles of high-voltage transmission lines, thousands of generation plants, and millions of digital controls. Through projects like "Cyber Resilient Metrics for Bulk Power Systems," RMT's cyber R&D has advanced novel tools for assessing and mitigating the risks that threaten this diverse range of equipment.

Transitioned Tools and Technologies

This section includes 32 RMT products that have been successfully commercialized or transitioned for wider use in the energy sector since 2018. They are presented below with the year they were transitioned indicated in the top bar. Each summary highlights how to access the tool or technology. In some cases, earlier products may have been superseded by newer ones; regardless, they helped to advance the state of the art for cybersecurity R&D in energy delivery systems at the time. The figure below shows the number of technologies transitioned to practice by year.



.

Transitioned in 2022

Ambassador

SEL collaborated with multiple manufacturers to design secure sharing of data between software applications to overcome the interoperability challenges that emerge on the grid.

With its Ambassador project, SEL, Dragos, and Juniper Networks developed and demonstrated a technology that manages trust, data, and resources across numerous software applications in a scalable method with a focus on maintaining this interoperability across products' lifetimes. The technology provides for a secure way to share information between software applications in near real time (e.g., detecting network intrusions, orchestrating responses to cyberthreats). It also provides continuous monitoring, prioritizes application functions, and visualizes networks' security posture overall. The Ambassador project built on SEL's previous research and was demonstrated on SEL's commercialized Blueframe Application Platform. The team commercialized and published the solution as Converged Industrial Edge. Concepts of the Ambassador project are commercialized and being deployed to secure critical infrastructure networks today.

Access: SEL's website provides more information on Converted Industrial Edge, which was the result of the Ambassador project.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Juniper Networks, Dragos, BPA

FOR MORE INFORMATION

Factsheet: Ambassador Project

Product Website: Partnerships and Product Development

Product Website: Converged Industrial Edge

Product Website: Converged Industrial Edge

Product Website: Converged Industrial Edge Network Architecture Solution

News Release: SEL and Dragos Team Up on Utility Cyber Defense

Technical Brief: Juniper Networks and SEL: Providing Reliable IT-OT Convergence

Transitioned in 2021

Chess Master Application Programming Interface (API)

With Chess Master, SEL has given operators a new way to ensure that only approved and expected cyber-activity is allowed on the control systems they oversee through a scalable and standards-based API.

An application programming interface (API) allows software packages from multiple suppliers to securely communicate with each other. This software architecture is important to formalize in OT systems so that software from various suppliers can work together to orchestrate network management and telemetry monitoring.

SEL developed and commercialized the SEL-5057 Software-Defined Networking (SDN) Application Suite.

An SEL-5057 application, Flow Auditor, details what ports and services are operating on a deny-by-default OT SDN network and produces a report showing what devices are allowed to use each port and service and why those ports and services are needed. This provides enhanced situational awareness, simplifies NERC CIP audit preparation and eliminates costly network scanning.

Chess Master is now the API for SEL's SDN Flow Controller.

Access: To access or learn more about these products, see SEL's website, in particular SEL's SDN Flow Controller, SDN Switch, or SDN Application Suite.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Ameren, Sempra, Veracity Security Intelligence

FOR MORE INFORMATION

Factsheet: Chess Master

Transitioned in 2020

Secure Software-Defined Radio Platform

SEL developed an affordable and secure radio platform for securing wireless communications between distribution transformers and the customers they serve.

SEL's configurable radio platform secures last-mile wireless communications out to remote automation devices on distribution lines. By connecting multiple applications through one radio, the platform simplifies wireless communications. It also provides precise message timing, and it offers security features that are comparable to—but less expensive than—those used in wired communications. It supports strong passwords, event and device access logging, and advanced encryption and authentication. It also offers data throughput that is three to four times faster than what conventional radios provide. Such speed and security will only grow in importance as utilities increasingly use sub-second-level data to make real-time automation and control decisions.

Access: SEL's fault and load transmitter and receiver system builds on this platform's success. It uses the 900 MHz license free ISM band.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

San Diego Gas and Electric, Pacific Northwest National Laboratory

FOR MORE INFORMATION

Factsheet: Secure Software-Defined Radio Project

Technical Brief: Secure Software Defined Radio Project: Secure Wireless Systems for the Energy Sector (Briefing 6)

Transitioned in 2023

ConsoleWorks Risk Evaluation and Assessment for Cyber Threats (REACT)

TDI Technologies, Inc., offers robust control over which users can—and, crucially, cannot—access resources that are essential to critical infrastructure operation.

The REACT project led by TDI Technologies, Inc., enables insider-threat detection. It takes a comprehensive approach to cybersecurity by securing remote access to systems, managing passwords, monitoring systems' baseline configurations, and maintaining audit trails to record system configurations and behaviors. It also scores risks and vulnerabilities (including those introduced by system users), secures file movement, and enhances situational awareness. TDI Technologies now markets ConsoleWorks REACT as a cybersecurity tool.

CATEGORY

Reduced Exposure

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

TDI Technologies, Inc.

PROJECT PARTNERS

Oak Ridge National Laboratory

FOR MORE INFORMATION

Product Website: ConsoleWorks REACT: Risk Evaluation and Assessment for Cyber Threats

Transitioned in 2020

Firmware Indicator Translator (FIT)

With its firmware-analysis tool, INL used machine learning, visualization, and big-data analytics to pinpoint and respond to cyberthreats that target firmware.

The techniques and tool suite, known as FIT, discover what firmware is running, identifies what interactions with other applications are needed, compares the firmware to an uncompromised baseline, and responds to cyberthreats by translating findings into structured threats for usability in other security products. The tool suite was tested at INL's power grid testbed and was then integrated into a live exercise conducted on a testbed at an electric utility.

By using four tools to detect firmware vulnerabilities—WiiBin, Annotated Translated Disassembled Code (@DisCo), DISCOverFlow, and B-Graph—FIT provides a complete approach to cybersecurity for firmware in embedded energy delivery systems.

First, WiiBin is an open-source tool for identifying the metadata of an unknown binary. Second, INL's @DisCo creates a graph database that many machine-learning methods can use to identify subsomorphic graph similarities. @DisCo was licensed to NetRise in 2023; that license has been extended for 2024. The winner of an R&D 100 Award in 2023, @DisCo has been shared with five other national laboratories for firmware analysis, and the output has been used by numerous university partners. Third, DISCOverFlow makes it possible to visualize, analyze, and create control-flow graphs for @DisCo output. Finally, INL's patented B-Graph tool is being used (alongside other technologies) to trace and predict code behavior.

Taken together, these four tools—and the FIT suite that comprises them—help computer systems understand and make inferences about the bidirectional flow of traffic on the grid.

Access: WiiBin and @Disco are open-source and can be obtained from GitHub. @Disco has export control limitation and can be licensed or use in partnership to non-foreign entities for use in better cyber protections.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Idaho National Laboratory (INL)

PROJECT PARTNERS

Brigham Young University, DTE Energy, Eaton, Hitachi Federal, Idaho State University, New Context Services, Pacific Gas & Electric, Schneider Electric, Southern California Edison, Siemens

FOR MORE INFORMATION

Factsheet: Firmware Indicator Translator

Patent: Systems and Methods for Architecture-Independent Binary Code Analysis (U.S. Patent 11900086)

Transitioned in 2022

Cyber Resilient Flexible AC Transmission Systems (XFACTS)

ABB, Inc., has fortified the cybersecurity of substations by bringing more in-depth cyber defense to the substations themselves.

With XFACTS, developed by ABB, Inc., controllers at flexible AC transmission-system substations can detect and mitigate attempts to depress system voltages, destabilize power flows, trip circuit breakers, and corrupt currents and voltages, even if the malicious commands have the correct syntax.

XFACTS uses the physics of active power electronic systems, control, and protection; electric power engineering principles; and state estimation to deepen the protection of substation devices.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Recover

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

ABB, Inc.

PROJECT PARTNERS

Bonneville Power Administration, University of Illinois Urbana-Champaign, Iowa State University, University of Idaho

FOR MORE INFORMATION

Technical Report: Cyber Resilient Flexible Alternating Current Transmission Systems (XFACTS)

Transitioned in 2020

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

ABB, Inc., has demonstrated cybersecurity measures for the HVDC systems that are increasingly connecting the modern grid.

ABB, Inc. (and its project partners) developed and tested a system to detect and reject cyberattacks that target High-Voltage Direct Current (HVDC) control systems, including spoofed commands. The two major technologies for securing HVDC systems included an intrusion detection system (IDS) and an emergency response mechanism to maintain/restore power control.
The IDS detects suspicious deviations from the system's normal behavior, and specialized algorithms return the system to baseline performance.

The project team demonstrated these technologies at BPA's Celilo HVDC converter station. Subsequently, ABB, Inc., incorporated them into its own product line.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

ABB, Inc.

PROJECT PARTNERS

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

FOR MORE INFORMATION

Factsheet: Cyber Attack Resilient High Voltage Direct Current (HVDC) Systems

Transitioned in 2020

Keyless Infrastructure Security Solution (KISS)

PNNL's blockchain technology addresses the unprecedented challenges for securing energy delivery systems on the grid's edge.

The technology—KISS—provides grid-edge protection by verifying the integrity of data in distributed energy resource (DER) exchanges, using a blockchain-enabled cybersecurity controller. KISS is built on blockchain technology and uses PNNL's VOLTTRON platform to prevent malicious modifications to complex energy exchanges.

KISS autonomously detects data anomalies, normalizes evidence across a unified timeline (for incident analysis), and responds in real time to unauthorized attempts to change critical data, configurations, applications, appliances, and sensors. Guardtime has incorporated KISS into its KeyLess Signature Infrastructure (KSI) platform, GridAware. Additionally, two patents pertaining to KISS have been filed.

Access: KISS is being integrated into Guardtime's KSI platform, GridAware. Guardtime's integration software development kit is available at Github.

Patents: US 11727120 B2 (Granted), US-20210014065-A1 (In progress)

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

Guardtime, Washington State University

FOR MORE INFORMATION

Factsheet: KISS: Keyless Infrastructure Security Solution

News Release: Building Trust in Blockchain for the Electric Grid

Publication: Enabling Secure Grid Information Sharing through Hash Calendar-based Blockchain Infrastructures

Publication: Digital Data Provenance for the Power Grid Based on a Keyless Infrastructure Security Solution

Patent: Sri Nikhil Gupta Gourisetti et al., "Blockchain Cybersecurity Solutions," U.S. Patent #11,727,120 B2, awarded August 15, 2023.

Transitioned in 2021

Quantum Physics Secured Communications for the Energy Sector (Q-Sens)

By developing new protocols for authenticating data, ORNL has worked to overcome the distance and cost limitations of Quantum Key Distribution (QKD)—an exciting but currently expensive method for enhancing cybersecurity.

ORNL's new technology—Q-Sens—addresses the distance limitations and expense of QKD by providing new quantum protocols for authentication and data integrity. The key management server that resulted from this project makes multiplexing possible. More specifically, keys can be established between any two endpoints that have established trust with the key server—even if those end points have not connected with each other before. The team tested the photonic integrated circuits to reduce their cost and to improve how well they couple to the integrated optics chip. The chip was then integrated into the passive continuous variable (CV) QKD setup for demonstration. Optoplex now offers the technology for high-performance balanced photodetectors.

ACCESS: The technology can be accessed through the Optoplex website by searching for "quantum" or "demodulator."

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Oak Ridge National Laboratory (ORNL)

PROJECT PARTNERS

EPB of Chattanooga, Los Alamos National Laboratory, Brigham Young University, Optoplex

FOR MORE INFORMATION

Factsheet: Quantum Physics Secured Communications for the Energy Sector

Peer Review: Quantum Physics Secured Communications for the Energy Sector

Transitioned in 2021

Anomaly Detection for Securing Communications in Advanced Metering Infrastructure

CREDC developed a method to detect and localize cyberattacks that jeopardize smart meters' communication networks.

Denial-of-service attacks—and other types of cyberattacks—can undermine the ability of advanced-metering-infrastructure devices to communicate with one another. They can also compromise measurements from smart meters. Operators lack the tools to validate these measurements before using them to make important control decisions. CREDC's method is designed to run the code inside each smart meter, as well as in a central management server, to detect attacks and direct response measures to the right locations.

This project has contributed to patents with IBM. Cisco Systems has incorporated the approach into an anomaly detection solution for its own platform.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

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

PROJECT PARTNERS

IBM, Cisco Systems, Schneider Electric

FOR MORE INFORMATION

Factsheet: Anomaly Detection for Securing Communication in Advanced Metering Infrastructure

Transitioned in 2018

Detecting Differences Between Micro-Synchrophasor Measurements and Cyber-Reported Supervisory Control and Data Acquisition (SCADA)

LBNL's innovation pinpoints cyberattacks by detecting the inconsistencies they cause between SCADA values and micro-phasor measurement units (µPMUs).

This technology identifies and diagnoses attacks on the distribution grid using µPMUs, which measure the physical state of the distribution network in real time. To do this, µPMUs are compared to SCADA values at various locations, and if there is a significant inconsistency between the two, operators receive an alert. This approach is robust, can verify existing cybersecurity systems on the grid, can detect potential cyber and physical attacks, and can be inexpensively and rapidly deployed at existing utility facilities.

ACCESS: This technology is available through Stream-Processing Architecture for Real-Time Cyber-Physical Security, open-source software, on GitHub. It is also sold by PowerSide.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Lawrence Berkley National Laboratory

PROJECT PARTNERS

Electric Power Research Institute; EnerNex; University of California, Davis

FOR MORE INFORMATION

Factsheet: Cyber Security of Power Distribution Systems by Detecting Differences Between Real-time Micro-Synchrophasor Measurements and Cyber-Reported SCADA

Publication: Cyber Defense Tool is an Early Warning System for Grid Attacks

Transitioned in 2019

Artificial Diversity and Defense Security (ADDSec)

SNL's technology leverages machine learning algorithms and software-defined networking (SDN) to detect and address threats to energy infrastructure.

With ADDSec, SNL developed a defense against the reconnaissance phase of attacks. When SNL demonstrated ADDSec, the technology automatically detected and responded to a computer worm in real time (with less than 0.01 second of latency) during red-team testing in a microgrid environment.

By exploiting the programmability of SDN, ADDSec advances the techniques SNL developed during an earlier RMT project, called "Dynamic Defense and Network Randomization."

ADDSec has now undergone testing and evaluation with over 300 end devices. It received a patent in 2018 and is compatible with SNL's commercial SDN Switch (SEL-2740). In 2018, the Department of Homeland Security deemed ADDSec a Transition to Practice technology, and in 2019, it won a prestigious R&D 100 award.

In 2018, the Department of Homeland Security deemed ADDSec a Transition to Practice technology, and in 2019, it won a prestigious R&D 100 award.

ACCESS: SNL demonstrated ADDSec using the Ryu and POX SDN controllers, which are open-source tools available for download at GitHub. The ADDSec technologies are available for licensing through Sandia's Licensing and Technology Transfer website.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Sandia National Laboratories (SNL)

PROJECT PARTNERS

Chevron, U.S. Army Night Vision and Electronic Sensors Directorate, GRIMM Cyber, Lawrence Livermore National Laboratory, Schweitzer Engineering Laboratories

FOR MORE INFORMATION

Factsheet: Artificial Diversity and Defense Security (ADDSec)

Project Website: ADDSec: Artificial Diversity & Defense Security

Patent: U.S. Patent No. 9,985,984

Transitioned in 2021

Design for Resilient Energy Delivery and Control System Networks

LANL has produced a modeling language that is five times faster—and up to 60 times more memory-efficient—that its conventional counterparts.

The new language—called Gravity—is an open-source, scalable modeling language for solving mathematical models in optimization and machine learning. Its extensible interface lets users specify the accuracy of variables and parameters. It also accommodates distributed algorithms, iterative model solving, and other approaches. Gravity helps to safeguard Alternating Current (AC) Optimal Power Flow against cyberattacks; it can play a critical role in optimizing distributed power systems inexpensively, making secure microgrids or quantum grids cost competitive with other distribution systems. Gravity models the grid's reaction to damage (line failure, loss of generation, etc.), supporting rapid reconfiguration of the grid, helping recovery from outages. It is leveraged by Operations & Design Optimization for Networked Microgrids—open-source software that Los Alamos National Laboratory has released.

Access: Operations & Design Optimization for Networked Microgrids is available at lanl-a nsi / odo; Gravity can be accessed through the GravityOpt website.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Respond, Recover

FOR ADOPTION BY

Vendors

Researchers

PROJECT LEAD

Los Alamos National Laboratory (LANL)

PROJECT PARTNERS

Virginia Tech

FOR MORE INFORMATION

Peer Review: LANL Optimal Grid Design for Cyber-physical Resiliency

Project Website: Gravity

Product Website: lanl-a nsi / odo

Technical Report: Gravity: A Mathematical Modeling Language for Optimization and Machine Learning

Transitioned in 2020

Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

BNL's technology ensures the integrity of sophisticated forecast data, on which energy delivery systems have grown increasingly dependent.

The technology—AIERCI—is an online cybersecurity tool that addresses threats to forecasting data in real time. If an attack succeeds in compromising the data, AIERCI mitigates its harmful effects. Using mathematical models, AIECRI compares forecasts with grid operations to identify and provide insight into vulnerabilities and exposures in data flows. It also identifies ways data could be compromised, determines how cyberattacks could feed tampered data to forecasting models, and determines the actions needed to correct compromised forecasts and resume normal grid operations.

BNL and its project partners deployed AIERCI in a controlled environment to demonstrate performance using real utility data sets. In addition, the North Carolina Electric Membership Corporation now uses the model-based anomaly detection module of the AIERCI tool.

Access: AIERCI is hosted in a GitHub repository; CESER must approve access to it.

CATEGORY

Situational Awareness and Operator Support

NIST CYBERSECURITY FRAMEWORK

Identify, Detect, Respond

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Brookhaven National Laboratory (BNL)

PROJECT PARTNERS

Argonne National Laboratory, Idaho National Laboratory, Orange and Rockland Utilities, University of Connecticut, University of North Carolina at Charlotte

FOR MORE INFORMATION

Factsheet: Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

Peer Review: Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

Transitioned in 2022

Cyber Resilient Metrics for Bulk Power Systems

CREDC has improved the cybersecurity posture of bulk power systems by creating better risk assessment tools.

The technology—called the Cyber Risk Assessment Tool (CRAT)—gives users a qualitative approach for assessing the security posture of cyber systems and networks in bulk power systems. CRAT captures cyber resilience from technical, organizational, and physical perspectives. From each of these three perspectives, CRAT computes cyber resilience metrics based on robustness, rapidity, redundancy, and resourcefulness. CREDC developed a web-based application to realize CRAT. The team evaluated the tool with two utility companies and provided the software to RF (a project partner) for further evaluation. Since then, RF has developed its own self-assessment tool based on its work with CREDC, and more than 230 utilities in the RF region now use the tool.

Access: To learn more about or request access to CRAT, interested users may visit the RF website.

CATEGORY

Guidance and Practices

NIST CYBERSECURITY FRAMEWORK

Protect, Respond, Recover

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Cyber Resilient Energy Delivery Consortium (CREDC), led by Old Dominion University

PROJECT PARTNERS

ReliabilityFirst (RF), University of Illinois Urbana-Champaign

FOR MORE INFORMATION

Factsheet: Cyber Resilient Metrics for Bulk Power Systems

Product Website: Cyber Resilience Assessment Tool (CRAT)

Transitioned in 2021

Autonomous Tools for Attack Surface Reduction

ISU delivered algorithms, metrics, and tools for analyzing and shrinking the attack surface of critical energy infrastructure.

ISU and its project partners developed, evaluated, and demonstrated a suite of attack-surface-reduction tools. The tools encompass numerous capabilities: an open-source Attack Surface Host Analysis tool that was transitioned to practice, moving-target defense for electric-distribution-system networks, a field-tested SIEM-based anomaly detection system for SCADA, and anomaly-detection algorithms for phasor-measurement-unit data. These tools continually and autonomously reduce the attack surface of the power grid's control environment. They also lower the risk that cyber threats pose to substations, control centers, and our nation's increasingly complex and interconnected grid. ISU also developed testbed-based cybersecurity training modules and hosted over a dozen hands-on training sessions that benefitted several utilities across our nation.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Iowa State University (ISU)

PROJECT PARTNERS

Argonne National Laboratory, Pacific Northwest National Laboratory, Washington State University, GE Global Research, Cedar Falls Utilities

FOR MORE INFORMATION

Factsheet: Autonomous Tools for Attack Surface Reduction (energy.gov)

Technical Report: Autonomous Tools for Attack Surface Reduction (Final Report)

Transitioned in 2023

Cybersecurity via Inverter-Grid Automatic Reconfiguration (CIGAR)

LBNL used reinforcement learning to counter cyber-physical attacks on solar photovoltaic systems.

The technology, CIGAR, monitors energy systems and allows distribution grids to automatically reconfigure themselves to thwart cyberattacks. LBNL and its team designed reinforcement-learning algorithms that reconfigure the settings of uncompromised systems to actively fight a variety of attacks. These algorithms were integrated into NRECA's Open Modeling Framework (OMF).

CIGAR has been incorporated into two RMT projects—Supervisory Parameter Adjustment for Distribution Energy Storage, and Mitigation via Analytics for Grid-Inverter Cybersecurity—as well as the Python-based software tool PyCigar.

Access:
Users can download OMF, an open-source software package that incorporates CIGAR technology, or access CIGAR directly from GitHub.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Lawrence Berkeley National Laboratory

PROJECT PARTNERS

Arizona State University, National Rural Electric Cooperative Association (NRECA), Siemens

FOR MORE INFORMATION

Factsheet: Cybersecurity via Inverter-Grid Automatic Reconfiguration

Project Website: Cybersecurity via Inverter-Grid Automatic Reconfiguration (CIGAR)

Transitioned in 2020

DOD Installation Energy Resiliency Pilot Program

Through a strategic partnership between DOE and DOD, PNNL advanced the cybersecurity of DOD's energy infrastructure and worked to improve military responsiveness.

The project team piloted cybersecurity tools to establish an ongoing coalition with DOE and reduce DOD's energy sector cybersecurity risk. This pilot redesigned DOD operational technology network architecture, advanced DOD's ability to survive a cyberattack, and validated RMT technologies to energy providers that support DOD installations. At each SDN pilot location, lessons learned were captured to improve efficiency in the SDN deployment process; the end result being a labor cost reduction of 50% between the first and last pilot engagements. The success of the pilot program has been shared across the globe. For example, not only has DOD's Ft. Belvoir site (in Virginia) incorporated the technology, so too have a hydroelectric dam on the border of Brazil and Paraguay and a windfarm in Belgium. The importance of SDN for Zero Trust network access control and Facility-Related Control System security by multiple DOD organizations is a direct result of the pilot program.

Additionally, SDN-enabled content has been incorporated into both Splunk and Elasticsearch to highlight the new data types available with SDN, illustrate new types of analysis, and demonstrate security improvements provided by SDN.

Splunk provides a tool for situational awareness of operational technology with the MITRE ATT&CK System as a reference.

Access:
SEL provides more information about its portfolio of products on their website. Similarly, more information about Splunk's and Elasticsearch's security related content can be found on their respective websites.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

Naval Facilities Engineering Command; Fort Belvoir Night Vision and Electronic Sensors Directorate; Spectrum Solutions

FOR MORE INFORMATION

Factsheet: DOD Installation Energy Resiliency Pilot Program

Publication: Enabling Situational Awareness in Operational Technology Environments Through Software Defined Networking

Publication: Software-Defined Networking Traffic Engineering Process for Operational Technology Networks

Publication: Software Defined Networking for Energy Delivery Systems Blueprint

Transitioned in 2020

Robust and Secure Global Positioning System (GPS) Timing for Power Systems

CREDC produced simulated datasets that integrate both GPS and phasor measurement units (PMUs) and are suitable for testing GPS spoofing attacks.

Conducting GPS spoofing tests is illegal without approval from the U.S. government. It is also costly to carry out experiments on the real power grid instrumented with PMUs. Additionally, current spoofing datasets are for GPS only and lack integrated GPS-PMU datasets. To address this issue, CREDC developed simulated datasets that can prove essential to assessing how a GPS spoofing attack could affect the power grid's state estimation. The data—produced by hardware-in-the-loop simulations with a GPS, two physical PMUs, and six virtual PMUs—was based on the IEEE-14 test bus case and made available online.

Access: The University of Illinois Urbana-Champaign, which led the project, has made the relevant datasets available for download.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Cyber Resilient Energy Delivery Consortium (CREDC), led by the University of Illinois Urbana-Champaign

FOR MORE INFORMATION

Product Website: Robust and Secure GPS-Based Timing for Power Systems

Transitioned in 2021

Scalable Quantum Cryptography Network for Protected Automation Communication

Qubitekk used quantum technology to address the cybersecurity vulnerabilities of our nation's growing networks of grid-automation devices.

Qubitekk developed a QKD system to detect eavesdropping attempts and to safely exchange the cryptographic keys used for encrypting network communication. This technology uses principles of quantum physics to safeguard cryptographic keys as they are exchanged, using signals that automatically change if an adversary attempts to steal the key. It alerts operators of theft attempts in real time, reducing the risk that data has been compromised despite appearing secure. The resulting system represents a scalable, commercial, and cost-effective QKD solution that can integrate with existing hardware. The developed quantum technology was successfully installed and tested in a field test network at a partnering utility (EPB of Chattanooga). EPB Quantum NetworkSM is adding customers to its Qubitekk powered network.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Qubitekk

PROJECT PARTNERS

EPB of Chattanooga; Oak Ridge National Laboratory; Schweitzer Engineering Laboratories; University of Tennessee, Knoxville

FOR MORE INFORMATION

Factsheet: Scalable Quantum Cryptography Network for Protected Automation Communication

Product Website: Qubitekk

Transitioned in 2021

Trusted Relay Node Networking

LANL extended quantum communications over distances that are unfeasible for current technologies.

Existing quantum links have a limited range of about 100 miles, which has impeded quantum communication's widespread adoption. Nationwide deployment of quantum technologies also requires interoperable systems from multiple vendors.

In response to these issues, LANL developed hardware and software to integrate quantum-communication transceivers with one another and with legacy network hardware to overcome distance limitations of quantum communications. The project implemented a secure relay node that allowed for unattended, reliable, and secure operations, and it increased the distance that a single system could handle. The technology performed well during preliminary testing on the site electric grid, sustaining operations over 13 days (including a weather event that involved a 40-inch snowfall). This technology is a novel capability for future scale-up of secure quantum networks.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Los Alamos National Laboratory (LANL)

PROJECT PARTNERS

Oak Ridge National Laboratory

FOR MORE INFORMATION

Factsheet: Trusted Relay Node Networking

Patent: U.S. Patent No. 9,887,976

Patent: U.S. Patent No. 10,291,399

Transitioned in 2020

Mitigation of External-Exposure of Energy Delivery System Equipment (MEEDS)

PNNL leveraged vulnerability database search engines to detect, identify, and mitigate the risk of cyberthreats to energy delivery systems.

PNNL's technology—MEEDS—provides a cost-effective way to quickly identify and protect energy delivery systems that are externally exposed to cyberthreats. Built on the technology of Shodan, MEEDS continuously monitors and identifies exposed devices, scans OT, and quantifies risks and mitigation actions. A working, stable version of this technology has been developed and tested in the laboratory. Field testing was conducted at several energy utility pilot sites. MEEDS was demonstrated to SANS Institute instructors and to various industry organizations interested in licensing and distributing it. Moreover, the Federal Energy Management Program (FEMP) has adopted MEEDS for Federal facility deployment and expanded on its capabilities by adding Censys and BinaryEdge as available services.

Access: A partner's version of this technology can be accessed through project partner Shodan's website.

CATEGORY

Situational Awareness and Operator Support

NIST CYBERSECURITY FRAMEWORK

Identify, Protect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

Hawaiian Electric Company, National Rural Electric Cooperative Association, Shodan

FOR MORE INFORMATION

Factsheet: Mitigation of External-Exposure of Energy Delivery System Equipment

News Release: New Cyber Technologies Protect Utility Energy Delivery Systems

Patent Application: Michael E. Mylrea and Sri Nikhil Gupta Gourisetti, "Mitigation of External Exposure of Energy Delivery Systems," U.S. Patent #2021/0173940 A1, filed June 10, 2021.

Transitioned in 2021

Structured Threat Intelligence Graph (STIG)

INL has linked geographical information with predicted cyberthreats to give system operators a greater awareness of grid vulnerabilities.

This STIG technology—developed through the Geo Threat Observables project—provides situational awareness by displaying predicted threats linked to geographical-information-system layers. STIG uses machine-learning techniques and graph theory to define the structure of cyber threats and convey that structure in a meaningful way. The software makes it easier to create, manage, and query data related to cyber threats, and it helps users visualize the underlying objects and how they relate to each other. The result is a common operating picture that can be applied with higher fidelity in a local environment. This project leveraged the existing FIT project and automated threat feeds from DOE, the Department of Homeland Security, and others.

Access: As an open-source software tool, STIG is available for download on GitHub, along with documentation and usage instructions.

CATEGORY

Situational Awareness and Operator Support

NIST CYBERSECURITY FRAMEWORK

Identify

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Idaho National Laboratory (INL)

PROJECT PARTNERS

New Context Services, Splunk, Eaton, Hitachi, Southern California Edison, Argonne National Laboratory

FOR MORE INFORMATION

Product Website: idaholab / STIG

Transitioned in 2022

Enhanced Security for the Power System Edge

By using the cloud for advanced analytics, Intel Federal advanced cybersecurity for grid-edge devices.

The technology—Enhanced Security for the Power System Edge—involves a security-architecture model that improves system integrity, makes systems faster, and applies to existing brownfield and greenfield deployments. After researching, developing, and implementing an enhanced cybersecurity gateway and a security-management channel (for use with existing devices), Intel Federal developed technology that can embed security into a field-programmable gate array on the endpoint itself. This configuration protects legacy devices by creating a security layer on top of the existing operational communications. The project team successfully demonstrated the technology—using commercial-off-the-shelf network devices—and Intel Federal has since commercialized the product through internal channels.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Intel Federal

PROJECT PARTNERS

LiveData Utilities, Schneider Electric

FOR MORE INFORMATION

Factsheet: Enhanced Security for the Power System Edge

Peer Review: Enhanced Power Edge Security

Transitioned in 2021

Timing Authentication Secured by Quantum Correlations (TASQC)

ORNL produced a wireless hybrid of quantum and classical technology that authenticates timing signals so they can be sent securely to remote energy sector devices.

The technology—TASQC—is composed of ground-based timing and communication beacons that use quantum key distribution (QKD). Unlike GPS-based timing schemes, this new system features transmitted timing signals that appear truly random to eavesdroppers and are difficult to spoof. Using quantum correlations, the system also provides several avenues for authenticating timing signals, power systems data, and other variables. Since the project's conclusion, lessons from TASQC have informed the development of other DOE-funded technologies, notably the "Multi-Hop Quantum Networking for Electric Grid Security."

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

Vendors

National Laboratories

PROJECT LEAD

Oak Ridge National Laboratory

PROJECT PARTNERS

EPB of Chattanooga, Pacific Northwest National Laboratory, Qubitekk, RedWire Technologies, Sandia National Laboratories, University of Texas Austin

FOR MORE INFORMATION

Factsheet: Timing Authentication Secured by Quantum Correlations (TASQC)

Transitioned in 2021

Modular Security Apparatus for Managing Distributed Cryptography for Command and Control Messages on OT Networks (MODULE-OT)

NREL has developed a lightweight, cryptographic module that cost-effectively secures DER systems.

The technology—Module-OT—evaluates the integrity of command-and-control messages in transit to and from DERs. It represents an advancement beyond the status quo because current standards do not include cybersecurity requirements for DERs, leaving them lacking robust cyber-protection. Module-OT addresses this by including voluntary standards that improve data privacy for user applications through a reduction of cyberattack vectors. It controls user access, manages certificates, and encrypts and authenticates data. It is also vendor-agnostic, making it easy to integrate with (and retrofit onto) devices.

NREL has released Module-OT as an open-source technology that energy companies can use as a low-cost, all-in-one solution for protecting energy-infrastructure information.

Access: Module-OT is an open-source technology that the project team has made available for download on GitHub.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

National Renewable Energy Laboratory (NREL)

PROJECT PARTNERS

Public Utility of New Mexico, Sandia National Laboratories, Yaskawa – Solectria Solar

FOR MORE INFORMATION

Factsheet: Module-OT: Modular Security Apparatus for Managing Distributed Cryptography for Command and Control Messages on Operational Technology Networks

Publication: Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources

Publication: Module OT Laboratory Test Procedure

Transitioned in 2020

Secure Policy-Based Configuration Framework (PBCONF)

With PBCONF, EPRI has created an open-source framework that supports the secure configuration of—and remote access to—modern and legacy devices from a variety of vendors.

PBCONF offers utilities a single, organization-wide view of power-delivery security configuration. By combining policy and translation engines, it addresses the interoperability challenges that can arise from remote-access control. By building PBCONF in a modular way, EPRI gave it the flexibility and adaptability to accommodate both legacy and new devices. This modularity is particularly important for the electricity sector, which features legacy devices that may be 40 years old. The system leverages distributed-architecture concepts to enable centralized and peer-based configuration of devices, which—in turn—supports scalability and resiliency.

Access: PBCONF is an open-source software solution available for download on GitHub.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Electric Power Research Institute (EPRI)

PROJECT PARTNERS

University of Illinois at Urbana-Champaign, Duke Energy

FOR MORE INFORMATION

Factsheet: Secure Policy-Based Configuration Framework

Technical Report: Secure Policy-Based Configuration Framework (PBCONF)

Product Website: PBCONF: Secure Policy Based Configuration Framework

Transitioned in 2023

Multi-Hop Quantum Networking for Electric Grid Security

LANL has developed a technology that can help to secure quantum communications across the nation's electric grid and that may even be deployed on the International Space Station.

LANL developed hardware and software to bolster the security and reduce the cost of quantum communication nodes. The team also implemented quantum systems on the links between these nodes. By implementing quantum-safe key switching protocols, the team managed the distribution of quantum-generated secret keys to utility sites. As part of DOE's Quantum & Space Collaboration, LANL will provide its Quantum Random Number Generator (developed under this project) in key applications. Moreover, LANL is in discussions to integrate the project's key-switching technology into the server as well. This technology is a novel capability for further scaling up of secure quantum networks.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

National Laboratories

PROJECT LEAD

Los Alamos National Laboratory (LANL)

FOR MORE INFORMATION

Factsheet: Multi-Hop Quantum Networking for Electric Grid Security

News Release: U.S. Department of Energy Announces First of Its Kind Collaboration for Quantum Technology Demonstrations in Space

Transitioned in 2023

Security Patch Automated Remediation Tool Analyzing the National Vulnerability Database (SPARTAN)

SEEDS used artificial intelligence to automate and optimize risk analysis and decision making in patch and vulnerability management.

The technology—SPARTAN— automates operational technology vulnerability remediation decisions, and it can even recommend specific actions (such as "patch immediately," "mitigate immediately," and "patch-in-cycle"). The technology—which is applicable to OT in the energy sector—compiles vulnerability mitigation information from the National Vulnerability Database to conduct efficient and effective risk assessments. The technology was licensed to Bastazo, Inc., for commercialization. It was, moreover, the basis for further commercialization funded by another DOE project ("V-INT: Automated Vulnerability Intelligence and Risk Assessment") and by a grant from the Israel-U.S. Binational Industrial Research and Development Foundation.

Access: Licenses for SPARTAN can be obtained through the Bastazo, Inc., website.

CATEGORY

Situational Awareness and Operator Support

NIST CYBERSECURITY FRAMEWORK

Identify, Respond

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS), led by the University of Arkansas

PROJECT PARTNERS

University of Arkansas at Little Rock

FOR MORE INFORMATION

Factsheet: Security Patch Automated Remediation Tool Analyzing the NVD (SPARTAN)

Transitioned in 2021

Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems (SSASS-E)

PNNL delivered a tool that combines passive network analysis with active scanning techniques to protect critical energy infrastructure.

The tool—SSASS-E—scans energy delivery systems for vulnerabilities. If it detects any, it reports them to users (through a web-based interface) and recommends mitigation strategies. Because it continuously monitors infrastructure, SSASS-E minimizes the frequency of probes necessary to identify potential vulnerabilities. PNNL now offers SSASS-E as open-source software. SSASS-E scanning capabilities were integrated into the Mitigation of External-Exposure of Energy Delivery System Equipment (MEEDS) tool in support of the Federal Emergency Management Program for deployment at federal facilities, and project partner Tenable has incorporated the tool's passive signatures and scan mechanisms into its products, including its industry-leading Nessus Professional and Nessus Network Monitor.

Access: As open-source software, SSASS-E is available for download from GitHub.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

Tenable; University of Illinois Urbana-Champaign; National Rural Electric Cooperative Association; Siemens; Public Utility District of Chelan County, WA

FOR MORE INFORMATION

Factsheet: Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems

Publication: Safer and Optimised Vulnerability Scanning for Operational Technology Through Integrated and Automated Passive Monitoring and Active Scanning

Transitioned in 2021

Containerized Application Security for Industrial Control Systems (CAPSec)

SNL employed "containers" to isolate applications from the systems surrounding them and to keep the effects of cyberattacks from spreading systemwide.

With its CAPSec technology, SNL allows critical operational technology software to be patched and secured immediately, without downtime, rather than delaying the actions until scheduled maintenance periods. CAPSec sequesters applications in software containers, which are lightweight processing environments that include everything needed to run an application but are isolated from the rest of the system. If malware is successful in reaching contained software, it still cannot broach the container or harm anything on the system beyond it. SNL demonstrated CAPSec in October 2021—together with the Survivable ICS project—and CAPSec will be incorporated into another RMT project, "Energy Storage Security Microservices technology."

CATEGORY

Reduced Exposure

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Sandia National Laboratories (SNL)

PROJECT PARTNERS

Chevron, U.S. Army Night Vision and Electronic Solutions Directorate, GRIMM Cyber, Pacific Northwest National Laboratory, Schweitzer Engineering Laboratories

FOR MORE INFORMATION

Factsheet: Containerized Application Security for Industrial Control Systems

Transitioned in 2023

Precise Time Synchronization Platform

SEL provided a customizable way for energy companies to protect intelligent electronic devices (IEDs) against cyberattacks.

SEL's Precise Time Synchronization platform safeguards against attacks that would manipulate, jam, or spoof GPS signals used for critical operational data in IEDs. IEDs (such as synchrophasors) communicate operational data and time references to and from control systems. As they have become more common on smart grids, they have introduced more attack vectors that adversaries can exploit. To address this vulnerability, the Precise Time Synchronization 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. SEL built and tested prototypes of the technology. Now, they are offering products that stem from it (including, for example, their line of satellite clocks).

Access: SEL's precise-timing devices that rely on the Precise Time Synchronization platform are available for purchase on SEL's website.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Recover

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Schweitzer Engineering Laboratories (SEL)

PROJECT PARTNERS

Bonneville Power Administration

FOR MORE INFORMATION

Factsheet: Tempus Project

Emerging Tools and Technologies

This section includes 18 RMT projects that are in demonstration or otherwise being finalized prior to transition to practice. These products give stakeholders insight into emerging capabilities that advance the state of the art for energy delivery systems' networks and cybersecurity. Some of the products take a fresh approach to addressing long-standing vulnerabilities in the cybersecurity of energy delivery systems; others address cybersecurity needs that the adoption of DERs (and other grid-modernizing technologies) have given rise to.

Stakeholders may expect to see these products released as commercial products, open-source resources or novel capabilities soon.

Emerging

Metrics and Tools for Measuring Cyber Resiliency of Electrical Grids

Integrating multiple grid factors into a single metric, CREDC improved how energy delivery systems can ward off and withstand cyberattacks.

The technology that CREDC developed incorporates grid factors from both the cyber and physical domains—and at the device and systems levels—into one understandable metric that operators can use to anticipate, prepare for, resist, and recover from cyberattacks. Using machine learning and real-time system analysis, CREDC and its project partners developed programmable-logic-controller code to measure the resilience of controller devices and take measures to increase that resilience. Looking ahead, Siemens is developing the technology further and integrating it into its own product line.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Respond, Recover

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Cyber Resilient Energy Delivery Consortium (CREDC), project led by Rutgers University

PROJECT PARTNERS

Siemens, Washington State University

FOR MORE INFORMATION

CREDC Factsheet: Metrics and Tools for Measuring Cyber Resiliency of Electric Grids

Emerging

Cyber-Secure Power Router

SEEDS pursued a cybersecure router that stays in operation as firmware is updated, patches are installed, or cyberattacks are launched.

By introducing security into the hardware-development phase, SEEDS ensured that the router is cyber-hardened by design. The router comprises multiple layers of security: a communication layer, a control layer, and a hardware layer. Taken together, these layers provide holistic protection for DER devices at the grid's edge. The router safeguards devices by encrypting their communication and storing their encryption algorithms. When SEEDS tested the router, it enabled secure communication for a combined solar inverter, a battery management system, and a grid-tied inverter. The results of this testing informed SEEDS' design of a preproduction router prototype.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS), led by the University of Arkansas

FOR MORE INFORMATION

Factsheet: Cyber-Secure Power Router

Project Website: Cyber-Secure Power Router

Emerging

Scalable Quantum Cybersecurity for Energy Storage Systems (SEQCESS)

ORNL provided a quantum communication interface that can interact with distributed-energy-storage devices to protect them from the malicious—and potentially dangerous—commands an adversary might send.

This interface—called SEQCESS—leverages the advancements ORNL achieved with its Q-Sens project. SEQCESS uses QKD to secure point-to-point communications for both current and future hardware. Its associated quantum techniques can both authenticate data and reveal the presence of adversaries upon intrusion. Along with its project partners, ORNL conducted a test demonstration of SEQCESS, using distributed-energy-storage communications system.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Oak Ridge National Laboratory (ORNL)

PROJECT PARTNERS

EPB of Chattanooga, Los Alamos National Laboratory, Qubitekk

FOR MORE INFORMATION

Factsheet: Scalable Quantum Cybersecurity for Energy Storage Systems (SEQCESS)

Patent Application: M. Alshowkan et al., "Authentication of smart grid communications using quantum key distribution," U.S. Patent Application #18/478,376, filed September 30, 2023.

Emerging

Grid Graph Signal Processing (Grid-GSP)

CREDC established how to apply graph signal processing to voltage phasors—a capability that makes it possible to detect grid anomalies that characterize cyberattacks.

The result of CREDC's efforts, Grid-GSP is a novel method for detecting when false data has been injected into the grid. Leveraging machine and Fourier analysis, it removes "noise" from data by compressing and reconstructing it. Using a graph structure of the grid, the technology estimates the grid's state and compares that estimate to expected norms. In this way it can detect anomalies that indicate false data injections have occurred.

Building on this project, OSIsoft provides compression of phasor-measurement-unit measurements, and Siemens is developing graph convolutional neural networks for its communications products.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect

FOR ADOPTION BY

Energy Companies

Vendors

Researchers

PROJECT LEAD

Cyber Resilient Energy Delivery Consortium (CREDC), project led by Arizona State University

PROJECT PARTNERS

Cordova Electric, OSIsoft, Siemens

FOR MORE INFORMATION

Project Website: Attack Graph Based Metrics for Identifying Critical Cyber Assets in Electric Grid Infrastructure

Publication: Detection of False Data Injection Attacks in Smart Grids based on Graph Signal Processing

Risk-Informed Verification and Validation Recommendation (RIVVR)

By developing RIVVR, PNNL created a web-based tool that identifies, scores, and analyzes risks in energy delivery systems—allowing utility operators to make better-informed decisions regarding how they should mitigate critical vulnerabilities.

With RIVVR, organizations can drive the secure design and development of a product, formalize the verification and validation (V&V) testing process, and make the V&V testing process more consistent across different products, all while making room for tailored testing. RIVVR is a one-stop shop for guiding risk-informed V&V testing.

An overview of the Verification and Validation Assuring Reliability and Security (VARS) framework and a demonstration of RIVVR was provided to the leadership of Fortress Information Security, which serves energy utility concerns. In addition, the North American Transmission Forum (NATF) has shown interest in integrating NATF's supply-chain security criteria into RIVVR to extend its capabilities for use by NATF and its member utilities.

CATEGORY

Reduced Exposure

NIST CYBERSECURITY FRAMEWORK

Identify

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

ABB, Inc.; Argonne National Laboratory; National Rural Electric Cooperative Association

FOR MORE INFORMATION

Factsheet: Verification and Validation Assuring Reliability and Security (VARS)

Project Website: Risk-Informed Verification and Validation Recommendation Tool

Risk Reduction Tool (RRT)

With RRT, PNNL gives utilities a novel way to determine how they can most effectively use their limited resources to reduce cyber risks, based on a defined set of proposed countermeasures.

RRT builds on the Risk Management Tool. It provides users with the ability to explore network diagrams representing their system of interest and presents scenarios generated by an associated attack tree. Users are presented with the relative change in risk that results from addressing subsets of scenarios, enabling them to prioritize effort and resources. PNNL's objective was to automate this tool, make it customizable, and ensure its scalability. New research was needed to make the generation of custom models possible. To that end, PNNL pursued automation and limited the custom models' computational scale.

PNNL leveraged the attack tree API and the Architecture Generation Tool (ArcGen) to allow users to build a custom architecture and build an associated attack tree on the fly. Updates to RRT allow the user interface to ingest the customized architectures and attack trees for exploration. The team also undertook the research challenge of developing a method to reduce attack tree complexity. The outcomes from this effort support partner interest in representing multiple stations across a geographic region.

After RRT's development, the tool was piloted across five electric utilities, a cybersecurity firm, and oil and natural gas utilities to positive reception. PNNL presented the tool at the 15th Annual API Cybersecurity Conference and the 2023 American Gas Association Fall Security Conference. This has led to a continued relationship with the American Gas Association to expand capabilities and evaluate usability within the oil and natural gas industry. PNNL has continued to pursue commercialization efforts for RRT and identify associated challenges.

CATEGORY

Reduced Exposure

NIST CYBERSECURITY FRAMEWORK

Identify

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

Great River Energy, Western Area Power Administration, Bonneville Power Administration, New York Power Authority, Dominion Energy, Omaha Public Power District, American Gas Association

FOR MORE INFORMATION

Factsheet: Method to Quantify Relative Cyber Risk Reduction

Emerging

Sequence Hopping Algorithm for Securing IEC 61850 Layer 2 Generic Object-Oriented Substation Event (GOOSE) Messages

FIU advanced how utilities can safeguard GOOSE messages, which are sent among intelligent electronic devices (IEDs) and are crucial for communications within substations.

As a SEEDS member, FIU developed a lightweight algorithm for authenticating and ensuring the integrity of GOOSE-messaging data. The tool employs pseudo random number generators (PRNGs). After generating a publisher sequence hopping number, a PRNG attaches the number to a message and sends the message to a subscriber IED. The IED then confirms the message's validity by comparing its attached number to a subscriber sequence hopping number that the subscriber PRNG generated. Version 1.0 of the algorithm underwent alpha testing at FIU's smart grid testbed and beta testing at the Electric Power Research Institute. A patent has been granted for the technology.

CATEGORY

Network Architectures

NIST CYBERSECURITY FRAMEWORK

Protect, Detect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS), led by Florida International University (FIU)

FOR MORE INFORMATION

Factsheet: Sequence Hopping Algorithm for Securing IEC 61850 Layer 2 Generic Object Oriented Substation Event

Patent: U.S. Patent No. 9,894,080

Emerging

Watching Grid Infrastructure Stealthily Through Proxies (WISP)

With WISP, RTRC leveraged an unconventional type of data to thwart cyberattacks: publicly available, real-time pricing mechanisms.

WISP is an advanced attack-detection and energy-market monitoring platform that RTRC developed for utilities, regional transmission organizations, and independent system operators to deploy. It exploits locational marginal prices—in conjunction with bids, weather, outages, load data, and other information—to analyze anomalous deviations in pricing. WISP can then correlate those observations to specific regions of interest and identify potential cyber events. RTRC and its partners have constructed a two-settlement electricity-market simulator for WISP. In addition, the team has published about false data injection attacks in professional journals. The team tested the software on the Texas and the ISO New England systems and evaluated the detection performance.

CATEGORY

Situational Awareness and Operator Support

NIST CYBERSECURITY FRAMEWORK

Detect, Respond, Recover

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

RTX Technology Research Center (RTRC)

PROJECT PARTNERS

Pacific Northwest National Laboratory; Southern California Edison; University of Tennessee, Knoxville

FOR MORE INFORMATION

Factsheet: Watching Grid Infrastructure Stealthily Through Proxies

Publication: Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations

Product Website: RTX Technology Research Center

Emerging

Scalable Identity and Key Management Scheme for Message Queuing Telemetry Transport (MQTT)

CREDC adapted the MQTT messaging protocol to secure cloud communications for Internet of Things (IoT) devices, which are proliferating on the grid.

To keep cloud communications secure, utilities and vendors use public key infrastructure (PKI) as a framework for securing the gateway to cloud communications. PKI issues, maintains, and revokes certificates for systems, processes, and users. Its heavyweight nature, however, leads to poor usability and unacceptable latencies on the smart grid. In contrast, MQTT is a lightweight messaging protocol for the IoT. MQTT has achieved widespread use, successfully managing generators, sensors, and the range of smart grid devices between them.

By employing a key management scheme and macaroons (a type of token that authorizes and authenticates users), the project team made key management easier for smart grid applications. In particular, the team led by Dartmouth built a solution to use MQTT to protect devices from active server compromises and man-in-the-middle attacks.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

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

FOR MORE INFORMATION

Product Website: Scalable Identity and Key Management Scheme for MQTT

Emerging

Integration of Green Renewable Energy Sources Securely with Buildings and Electric Power (INGRESS)

The INGRESS platform—developed by RTRC—automatically detect anomalies using physical measurement data and prevents malicious control commands from impacting DER operations in real time.

By comparing the actual traffic of control systems against traffic models, INGRESS can pinpoint suspicious discrepancies that indicate attacks and make DER more resilient to those attacks. INGRESS secures communication among different systems and utilities, and it accommodates legacy and emerging infrastructure alike. The INGRESS prototype helps to secure VOLTTRON—DOE's reference platform for transactional energy applications—by extracting meaningful information from data to identify anomalous behaviors. The prototype consists of multiple types of algorithms: data-driven and physics-based algorithms that detect anomalous device behaviors, and state-based deterministic algorithms that detect syntactically valid but malicious control commands.

CATEGORY

Attack Identification and Response/

NIST CYBERSECURITY FRAMEWORK

Protect, Detect, Respond

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

RTX Technology Research Center (RTRC) (formerly UTRC)

PROJECT PARTNERS

Pacific Northwest National Laboratory, University of Illinois Urbana-Champaign

FOR MORE INFORMATION

Factsheet: Integration of Green Renewable Energy Sources Securely with Buildings and Electric Power (INGRESS)

Project Website: RTX Technology Research Center

Emerging

Survivable Industrial Control Systems (ICS)

SNL's Survivable ICS reduces the risk of potential attacks on industrial control systems, whose static nature makes them particularly vulnerable.

Survivable ICS integrates two results from RMT: Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) and Artificial Diversity and Defense Security (ADDSec). CYMSA enables real-time monitoring of host-based events; ADDSec provides monitoring for both host- and network-based events. The integration of these projects makes it possible to automatically detect and respond to cyber threats as well as physical ones. By combining CYMSA and ADDSec, the Survivable ICS project met the Risk Management Framework requirements for deployment across DOD. The technology also completes NIST's cybersecurity framework for the energy, oil, and natural-gas sectors' critical infrastructure. SNL successfully demonstrated Survivable ICS—along with CAPSec—at Ft. Belvoir, where Survivable ICS has since been integrated into a 2.5-megawatt microgrid environment. Additionally, Survivable ICS and ADDSec—building off one another—are compatible with SNL's commercial SDN Switch (SEL-2740).

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond, Recover

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Sandia National Laboratories (SNL)

PROJECT PARTNERS

Chevron, Georgia Tech Research Institute, GRIMM Cyber, Ft. Belvoir Night Vision and Electronic Sensors Directorate, Pacific Northwest National Laboratory, Schweitzer Engineering Laboratories, Sempra Energy

FOR MORE INFORMATION

Factsheet: Survivable Industrial Control Systems

Peer Review: Survivable Industrial Control Systems

Emerging

Energy Delivery Systems with Verifiable Trustworthiness

ORNL's technology protects energy delivery systems against "fileless malware," which commandeers a system's legitimate tools to launch a codeless—and traceless—attack against it.

Fileless malware resides in a device's memory and leaves no persistent forensic evidence in permanent storage. In this way, it can bypass detection (even on deny-by-default systems) and avoid making its presence known. It can enter a system by exploiting compromised firmware, among other weaknesses. For this reason, ORNL developed the Energy Delivery Systems with Verifiable Trustworthiness technology to rapidly and remotely verify the integrity of firmware used in energy delivery systems. The technology supports automated verification and does not require that devices be taken offline first. Comparing the firmware in memory from devices in service against a "gold standard" makes it possible to identify vulnerabilities. Without sacrificing device performance or network bandwidth, the technology can detect fileless-malware threats and assess the content of executable memory on demand.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect

FOR ADOPTION BY

Vendors

PROJECT LEAD

Oak Ridge National Laboratory (ORNL)

PROJECT PARTNERS

EPB of Chattanooga, Schneider Electric, National Rural Electric Cooperative Association, ISASecure, Tennessee Valley Authority, General Electric

FOR MORE INFORMATION

Factsheet: Energy Delivery Systems with Verifiable Trustworthiness

Peer Review: Energy Delivery Systems with Verifiable Trustworthiness

Emerging

Energy Storage Security (ESSec) Using Microservices

SNL developed a suite of applications that can upgrade an energy storage system's software in real time, making it possible to launch new applications quickly, manage them as needed, and detect when applications have crashed or been compromised.

The technology—ESSec—uses containerization to isolate power system applications and reduce the cyberattack surface. If malware compromises these containerized processes, they can be identified and replaced without disrupting operation. The project team validated emerging containerization services with open-source software packages and will expand out to microservice architecture. Recent technical advances include integrating custom containers into SEL's Blueframe application platform (SEL-3355). Additionally, project partner OES has containerized the Open Field Message Bus reference implementation with a testbed, using a battery management system. FoxBMS software has been obtained and will serve as a representative energy storage environment.

CATEGORY

Reduced Exposure

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Sandia National Laboratories (SNL)

PROJECT PARTNERS

Duke Energy, Entergy, Schweitzer Engineering Laboratories, DTE Energy, Open Energy Solutions (OES), GRIMM Cyber

FOR MORE INFORMATION

Factsheet: Storage Security (ESSec) Using Microservices

Emerging

A Prototype for Ultimate Secure Transmission and Analysis of Smart Grid Data on the Wire

Bringing together two types of cryptography—classical, which is based on mathematical computation, and quantum, which is based on quantum mechanics—BNL developed a prototype that provides hack-proof encryption for data flowing between locations.

The prototype combines quantum-protected key exchange with real-time (or nearly real-time) computations of streaming data in transit. It ensures that intermediate smart network nodes can access the encrypted data as needed while also enabling the remote control of quantum devices over a classical network. The prototype represents an experimental configuration of a quantum network. It uses ultra-precise optical clocks to synchronize quantum nodes and post-quantum-protected key sharing to analyze encrypted data.

After integrating the prototype's components into a testbed at SBU, BNL and its partners achieved the full operation of this hybrid technology. Now the researchers are pursuing a test deployment of the prototype in a real power grid that extends beyond SBU's campus.

CATEGORY

Access Control

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

Researchers

PROJECT LEAD

Brookhaven National Laboratory (BNL)

PROJECT PARTNERS

Stony Brook University (SBU), Oak Ridge National Laboratory, Los Alamos National Laboratory

FOR MORE INFORMATION

Factsheet: A Prototype for Ultimate Secure Transmission and Analysis of Smart Grid Data on the Wire

Quantum Integrated Chip Scale Security (QuICSS)

With QuICSS, ORNL developed an original, secure communications technology that bases cybersecurity in a quantum trust anchor.

By bringing QKD technology to bear on the grid, this technology—QuICSS—delivers major implementation advantages for bulk optical fiber infrastructures. It can be manufactured on photonic chips at a large scale (and for a low cost), which enables the seamless integration of quantum-secured communications across the energy sector. With QuICSS, the project team expanded on its previous work to develop, implement, and demonstrate elements crucial to new continuous variable quantum key distribution (CV-QKD) protocols that can be transitioned to an on-chip system. The resulting technology makes possible the economical manufacturing and widespread adoption of quantum communications cybersecurity solutions.

CATEGORY

Reduced Exposure

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Oak Ridge National Laboratory (ORNL)

PROJECT PARTNERS

Brigham Young University

FOR MORE INFORMATION

Factsheet: Quantum Integrated Chip Scale Security (QuICSS)

Patent Application: B. Williams, “High Speed Removal of Bias of a Homodyne Detector Using a Clone Local Oscillator,”
U.S. Patent Application 18/437,706, filed February 9, 2024.

Universal Utility Data Exchange (UUDEX)

By taking a dynamic, model-driven approach to data exchange, PNNL has developed UUDEX to update the standard for sharing data and information between organizations.

Currently, the Inter-Control Center Communications Protocol (ICCP) enables the sharing of power system measurement data between utility control centers. ICCP is more than 20 years old, however. Unlike UUDEX, it lacks flexibility, is difficult to configure, and does not prioritize security. UUDEX replaces ICCP's information-sharing component. Leveraging up-to-date methods of security, data transport, information modeling, and configuration, UUDEX uses secure-by-default transport and authentication methodologies. As a result, energy-sector workers can more easily exchange measurement and operational data, disturbance reports, and threat information in near real time. PNNL now offers UUDEX as an open-source implementation, which has relevance across energy subsectors.

UUDEX is being standardized as IEEE Standard P2030.103, and a project has been announced for GE Vernova to develop a commercial version of UUDEX, field test it at the Midcontinent Independent System Operator (MISO), provide updates to the IEEE standardization efforts, and update the GitHub source to match the commercial version and IEEE standard.

Access: As open-source software, UUDEX is available for download from GitHub.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Protect, Detect

FOR ADOPTION BY

Energy Companies

PROJECT LEAD

Pacific Northwest National Laboratory (PNNL)

PROJECT PARTNERS

OATI, MITRE

FOR MORE INFORMATION

Factsheet: UUDEX: Universal Utility Data Exchange

Technical Report: Universal Utility Data Exchange (UUDEX) Functional Design Requirements – Rev 1

Emerging

Digital Ghost: Cyber Attack Detection and Accommodation

With Digital Ghost, GE Vernova Advanced Research Center enables power plants to detect, localize, and survive cyberattacks, while also minimizing the number of mitigation actions that are necessary.

By autonomously detecting and localizing system anomalies, Digital Ghost gives power plant operators real-time visibility into plant operations and security. It also has demonstrated the ability to allow continuous power generation even in the presence of a cyberattack. The technology provides insight into a generation plant's cyber posture, using algorithms based on data from a model of the plant's physical process. With this model, or "digital twin," the system can run live operating data from the physical plant through AI-based algorithms trained using the twin in real time to detect and identify anomalies. Digital Ghost's neutralization algorithms will allow power generation systems to quickly mitigate the effects of an attack by reverting to synthetic data generated from the Digital Ghost. Digital Ghost aims to minimize the number of false positives received in incident detection and can be integrated as stand-alone or in conjunction with other third-party tools, such as security information and event management systems (SIEMs). GE Vernova is working to productize Detection and Localization and continuing research on the Neutralization algorithms.

CATEGORY

Attack Identification and Response

NIST CYBERSECURITY FRAMEWORK

Detect, Respond, Recover

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

GE Vernova Advanced Research Center

PROJECT PARTNERS

GE Gas Power

FOR MORE INFORMATION

Factsheet: Cyber Attack Detection and Accommodation for Energy Delivery Systems

Emerging

A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

To manage the cybersecurity risks that cloud-based applications can introduce to the grid, ANL developed a security framework for cloud-computing and outsourcing that suits the modern energy sector.

Data privacy and security is the top priority for grid operators as they gradually move grid applications to cloud. Cloud or other third-party infrastructures inevitably have security vulnerability that out of grid operators' control, especially during computing. To protect time-critical grid computing and data on the cloud with minimal latency, ANL and its project partners modeled different types of cyberattacks while considering the time criticality of various power grid applications. The framework they developed as a result of these efforts underwent validation in three case studies: in a standard IEEE bus configuration, in a ComEd subregion of the PJM Interconnection, and on a model of the PJM grid. With its associated algorithms and software tools, the framework makes it easier and safer for power grid computing applications to run on cloud or other third-party IT infrastructures.

CATEGORY

Guidance and Practices

NIST CYBERSECURITY FRAMEWORK

Protect

FOR ADOPTION BY

Energy Companies

Vendors

PROJECT LEAD

Argonne National Laboratory (ANL)

PROJECT PARTNERS

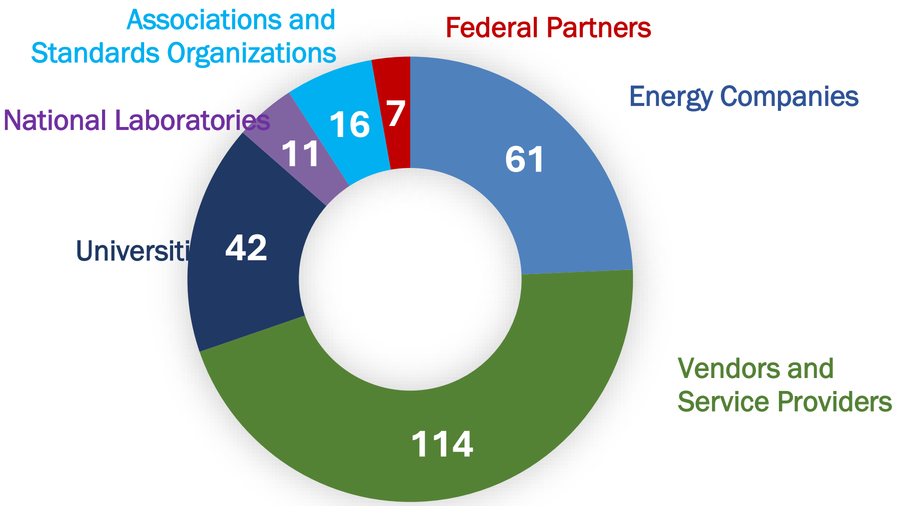
ISO New England, Newton Energy Group, Commonwealth Edison (ComEd), PJM, University at Buffalo, Illinois Institute of Technology

FOR MORE INFORMATION

Factsheet: A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

Project Partners

RMT research projects have engaged more than 250 energy companies, vendors, service providers, universities, National Laboratories, industry associations, standards organizations, and other federal entities as either project leads or partners.



Energy Companies

- Ameren
- Arizona Public Service Company
- Arkansas Electric Cooperatives Corporation
- Avista
- Bonneville Power Administration
- Burbank Water and Power
- California Energy Commission
- California Independent System Operator
- Cedar Falls Utilities
- CenterPoint Energy
- Chelan County Public Utility District
- Chevron
- Commonwealth Edison
- Cordova Electric
- Dominion Energy
- DTE Energy
- Duke Energy
- EPB of Chattanooga
- Entergy
- Electric Reliability Council of Texas
- Eversource Energy
- Exxon Mobil
- FirstEnergy
- Florida Power & Light
- Great River Energy
- Hawaiian Electric Company
- Idaho Falls Power
- Idaho Power Company
- Independent Electricity System Operator – Ontario
- Inland Empire Energy Center

- ISO New England
- Lincoln Electric Systems
- Nebraska Public Power District
- New York Power Authority
- Northern Indiana Public Service Company
- NRG
- Omaha Public Power District
- Orange and Rockland Utilities
- Pacific Gas & Electric
- PacifiCorp
- Peak Reliability
- PJM Interconnection
- Portland General Electric (PGE)
- Public Utility of New Mexico (PNM)
- Riverside Public Utilities
- Rochester Public Utilities
- Sacramento Municipal Utility District
- San Diego Gas and Electric
- Sempra
- Southern California Edison
- Southern Company
- Southwest Power Pool
- Tennessee Valley Authority
- US Indo-Pacific Command
- Virgin Islands Water and Power Authority
- Vistra Energy
- Wake Electric Membership Corporation
- Washington Gas Energy Services
- Washington Gas Energy Systems
- Westar Energy
- Western Area Power Administration (WAPA)

Vendors and Service Providers

- ABB, Inc.
- Alstom Grid
- ANG Consulting
- Applied Control Solutions
- ArcSight
- Automatak
- Axio Global
- Baker Hughes
- Battelle Memorial Institute
- BlackByte Cyber Security, LLC
- Burns & McDonnell Engineering Company, Inc.
- CableLabs
- Cigital, Inc.
- Cisco Systems
- ConnectCR
- Critical Intelligence
- Cybati
- Cyber Phantom
- Digital Bond
- Digital Management, Inc.
- Dispersive Technologies
- Dragos, Inc.
- Eaton Corporation

Emerson Electric

Energetics Incorporated

Energy Blockchain Consortium

Energy Sector Control Systems Working Group

EnerNex Corporation

ForeScout Technologies

Fortinet

FoxGuard Solutions, Inc.

Fujitsu

GE Grid Software Solutions

GE Power

GE Renewable Energy

General Electric (GE)

Grid Cloud Systems

Grid Protection Alliance

GridBridge

GRIMM Cyber

Guardtime USA

Hitachi ABB Power Grids, Inc.

Honeywell

ID Quantique

Increase Technologies

Intel

Invensys

Joe Weiss/Applied Control Systems, LLC

Juniper Networks

Kenexis Consulting

Kevala Analytics, Inc.

LiveData Utilities

LMI Development

Milsoft Utility Systems, Inc.

MITRE

Navigant Consulting, LLC

NCC Group

N-Dimension Solutions USA, Inc.

Network Perception

New Context Services

Newton Energy Group

NexDefense

OATI

OPAL_RT Technologies

Open Access Technology International, Inc.

Open Energy Solutions Inc.

Opus Consulting

OSIsoft

Parsons

Perspecta

Power Standards Laboratory

Qubitekk, Inc.

Rajant Corporation

Raytheon Technologies

Readiness Resource Group (RRG)

Red Trident

Redwire Technologies

Resilient Grid, Inc.

Respond Software, Inc.

Revolutionary Security

River Loop Security

Rocky Mountain Institute

RTDS Technologies

Sayers

Schneider Electric

Schweitzer Engineering Laboratories

SecurityMatters, LLC

Sekurity

Sensus

Shodan LLC

Siemens

Smarter Grid Solutions

Solectria Solar

Southwest Research Institute

Spectrum Solutions

Splunk

SRI International

Sunpower

Synopsys, Inc.

Sypris Electronics

TDi Technologies

Telvent

Tenable Network Security

Total Reliability Solutions

United Technologies Research Center

Upstanding Hackers

Utility Advisors

Utility Integration Solutions

Valicore Technologies

Vencore Labs, Inc.

Veracity Security Intelligence

ViaSat

Witt O'Brien's

Yaskawa - Solectria Solar

University Partners and Consortia

Arizona State University

Brigham Young University

Carnegie Mellon University

Dartmouth College

Florida International University

Florida State University

Georgia Institute of Technology

Georgia Tech Research Institute

Idaho State University

Illinois Institute of Technology

Iowa State University

Lehigh University

Massachusetts Institute of Technology

Ohio State University

Old Dominion University

Oregon State University

Purdue University

Rutgers University

Southern Methodist University

Stony Brook University

SUNY-Buffalo

Tennessee State University

- Texas A&M Engineering Experiment Station
- University at Buffalo
- University of Arkansas
- University of Arkansas at Little Rock
- University of California, Davis
- University of Connecticut
- University of Houston
- University of Idaho
- University of Illinois at Chicago
- University of Illinois Urbana-Champaign
- University of Nebraska
- University of New Mexico
- University of North Carolina at Charlotte
- University of South Florida
- University of Tennessee
- University of Texas at Austin
- University of Texas at Dallas
- Virginia Tech
- Wake Forest University
- Washington State University

Many academic partners have collaborated in multi-university consortia that RMT funded (together with the DHS Science and Technology Directorate). Those consortia include the Cyber Resilient Energy Delivery Consortium (CREDC) and the Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS), discussed below. Every university team—in both consortia—took on the challenge of addressing high-priority cybersecurity needs. In each team's efforts, they pursued novel solutions while actively engaging with industry asset owners and solution providers. These academic partnerships have also helped to develop and train the next generation of cybersecurity professionals for the energy sector.

CREDC

The University of Illinois Urbana-Champaign leads CREDC in partnership with nine other universities and two National Laboratories. The consortium engages an industry advisory board that helps identify research priorities, facilitating the transition of new, needed cybersecurity technologies into real-world contexts. CREDC research themes include real-time cyber event detection and situational awareness; protective and cyber-resilient architectures and technologies; and the design of cyber resilience into emerging power system devices for the grid, oil, and natural gas infrastructure of the future.

- **Partner Universities:** 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, Washington State University
- **Partner National Laboratories:** Argonne National Laboratory, Pacific Northwest National Laboratory

SEEDS

A partnership of six universities and one electric cooperative, SEEDS is advancing cybersecurity for electricity, oil, and natural gas infrastructure. An industry advisory board guides the prioritization of the consortium's research, provides input into ongoing research, and ensures that activities are likely to be useful to (and used by) the energy sector. The consortium's research themes include detecting malicious data input to power system applications (such as automatic generation control), pursuing moving target defense, detecting supply-chain cybersecurity compromise of smart grid devices, optimizing cybersecurity resources, and improving cybersecurity for time-critical communications necessary for the operation of electricity distribution systems.

- **Partner Universities:** University of Arkansas (lead), Carnegie Mellon University, Florida International University, Lehigh University, Massachusetts Institute of Technology, University of Arkansas at Little Rock
- **Partner Electric Cooperative:** Arkansas Electric Cooperative Corporation

National Laboratories

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

Associations and Standards Organizations

- American Public Power Association
- Blockchain Engineering Council
- Edison Electric Institute
- Electric Power Research Institute
- Energy Information Administration
- IEEE Standards Association
- International Electrotechnical Commission
- ISASecure
- Nation Rural Electric Cooperative Association
- National Electric Sector Cybersecurity Organization Resource
- National Institute of Standards and Technology
- National Rural Telecommunications Cooperative
- North American Electric Reliability Corporation
- Open Information Security Foundation
- Protect Our Power
- Utilities Telecom Council

Federal Partners

- Department of Defense Homeland Defense & Security Information Analysis Center
- Department of Homeland Security Industrial Control System Cyber Emergency Response Team
- Department of Veteran Affairs
- Ft. Belvoir Night Vision and Electrical Sensors Directorate
- Naval Facilities Engineering Command
- Veterans Administration Medical Facility - Las Vegas
- White Sands Missile Range