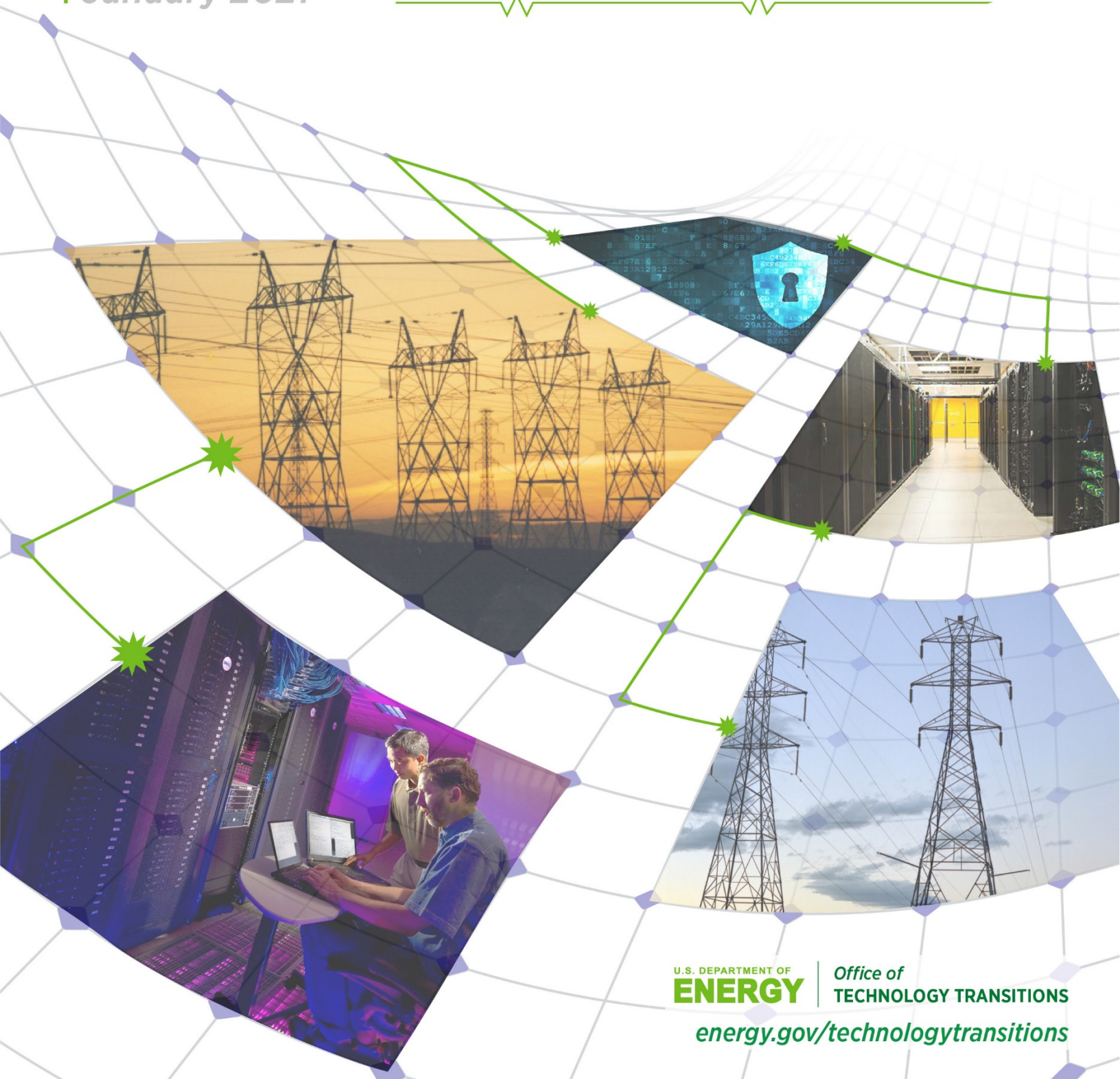
Spotlight

Advancing Cybersecurity to Strengthen the Modern Grid

January 2021



U.S. DEPARTMENT OF ENERGY | Office of TECHNOLOGY TRANSITIONS

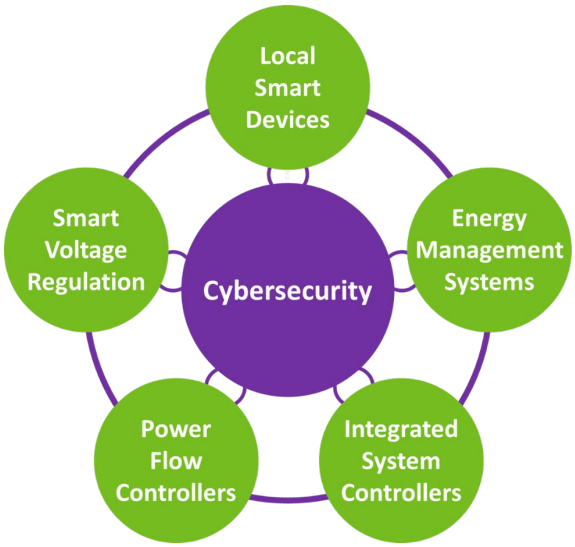
energy.gov/technologytransitions

A Modernizing Grid Is Vulnerable to Cyberattacks

A secure and resilient power grid is vital to national security and a strong and vibrant economy. Much of the current electric grid was designed and built using technologies and organizational principles developed decades ago to serve vertically integrated markets, with large-scale generation sources remotely located from consumers, a one-way flow of power, and centralized control schemes with minimal feedback. A modern grid must be flexible to integrate distributed energy resources, accommodate the two-way flow of electricity and information for better power management, and provide strong protection against physical and cyber risks.

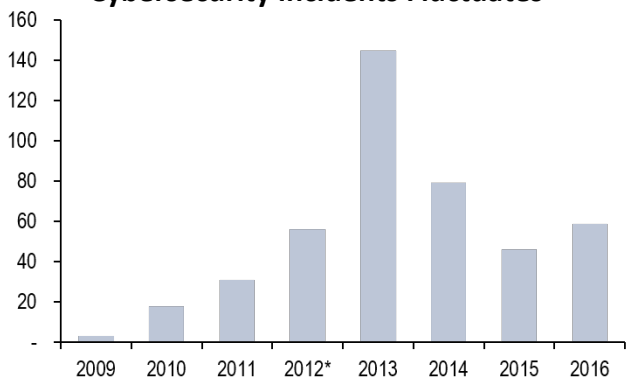
As the electric grid evolves, it is an increasingly attractive target for cyberattacks. Today, cyber incidents have the potential to disrupt the grid, damage highly specialized equipment, and threaten human health and safety. Protecting the Nation's grid and other critical energy infrastructure from cyberattacks is a national priority outlined in the National Cyber Strategy.[1]

Energy-related systems that may be vulnerable to attack include those for fuel processing, power plant control, communications in buildings, pipelines, automated vehicles, and supervisory control and data acquisition (SCADA) for manufacturing. The U.S Department of Energy (DOE) is committed to protecting the Nation's critical infrastructure from all threats, including cyber threats. DOE has addressed cybersecurity in a number of documents, including portions of the *Quadrennial Energy Review*[2] and *Quadrennial Technology Review*.[3] In addition, DOE and the private sector have responded to the critical need for advanced cybersecurity by increasing research and development (R&D) investment in this sector.



Grid modernization has introduced devices and systems that are interconnected and need cybersecurity technologies to remain secure.

The Number of Energy Sector Cybersecurity Incidents Fluctuates



The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) tracks the number of reported cyber incidents in the energy sector. It is assumed that a number of incidents are not reported or detected.

*The 2012 data is an estimate (given data: 40% of 138 total incidents). To view data, please visit ics-cert.us-cert.gov/Other-Reports.

Cover: Power lines image (left) adapted from Pacific Northwest National Laboratory image: flickr.com/photos/pnnl/7404564340. Power lines image (right) adapted from photo by Warren Gretz, NREL 00001

[1] "National Cyber Strategy of the United States of America." The White House. September 2018. whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[2] "The Quadrennial Energy Review." U.S. Department of Energy. January 2017. energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf

[3] "The Quadrennial Technology Review." U.S. Department of Energy. energy.gov/quadrennial-technology-review-0

Challenges Facing Grid Cybersecurity

DOE invests in early-stage R&D of advanced cybersecurity technologies to secure and protect the electric grid, and it works closely with private-sector partners to ensure these technologies are available for industry adoption.

DOE's Multiyear Plan for Energy Sector Cybersecurity sets a strategic course for the future, calling for close DOE collaboration with the private sector to share information, set priorities, and stimulate investment and cost-sharing of new, up-and-coming technologies. The plan identifies three priorities for achieving disruptive and continuous improvement in grid cybersecurity. Each goal faces a number of challenges, as summarized below.[4]

Attack on Ukraine's Utility System in 2015

On December 23, 2015, a cyberattack on three different Ukrainian energy companies disrupted power to about 225,000 customers. The attackers were able to disconnect three substations from the grid for three hours by gaining illegal entry into the victims' SCADA systems. Idaho National Laboratory's Cyber Strike Workshop uses analysis of this event to provide awareness and operations training to prepare utilities for similar attempted attacks.

"Analysis of the Cyber Attack on the Ukrainian Power Grid." E-ISAC and SANS. March 2016. ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Strengthening Preparedness

To protect the grid from cyber risk, utilities must conduct real-time threat monitoring and analysis, which often requires exchanging sensitive data, triggering privacy and liability concerns. Sharing threat information across the sector is also critical; however, the information sharing platforms and processes required to share information

Coordinating Cyber Incident Response and Recovery

Cyber incident response in the energy sector involves a wide range of diverse public and private sector stakeholders. Clearly defined and coordinated roles and responsibilities across the federal government can unify national efforts. In addition, cyber events may affect energy infrastructure across a wide geographic area, with different consequences for each affected system.

Accelerating Game-Changing R&D of Resilient Energy Delivery Systems

New cybersecurity tools and technologies must make the grid easier and less expensive to operate. R&D technologies must anticipate future grid scenarios, integrate with existing systems with diverse legacy and modern devices, and not impede national critical functions.

Image of person at computer adapted from LLNL: llnl.gov/news/laboratory-looks-expand-data-science-pipeline-through-internship-program.

Power lines photo by Dennis Schroeder, NREL 46264.

[4] "Multiyear Plan for Energy Sector Cybersecurity." U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability. March 2018. energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

Toward a More Secure, Reliable, and Resilient Grid

DOE takes a two-pronged approach to advancing cybersecurity capabilities: supporting continuous improvement of cybersecurity systems and funding R&D to enable disruptive change.[5] DOE's Cybersecurity for Energy Delivery Systems (CEDS) program within the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is responsible for developing tools and technologies that can reduce risks to energy systems from cyber threats. CESER's vision and activities align with the Office of Electricity's (OE) mission of ensuring that the Nation's defense-critical energy infrastructure is secure and able to rapidly recover from disruptions.[6] DOE program-directed research supports grid modernization initiatives and helps increase the security, reliability, and resiliency of the grid.[7]

DOE's R&D Focus Areas for Cybersecurity

The following actions comprise DOE's focus areas, which are based on the National Institute of Standards and Technology's Cybersecurity Framework.[8]

Identify. Understand cybersecurity risk to systems, people, assets, data, and capabilities.
Actions: Risk Assessment, Asset Management, Critical Failure/Component Analysis

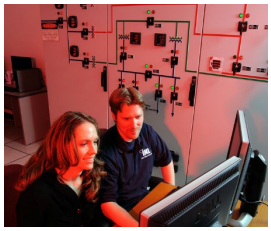
Protect. Install appropriate safeguards to ensure delivery of critical services.
Actions: Encryption, Network Segmentation, Firmware and Control Verification

Detect. Conduct activities to identify the occurrence of a cybersecurity event.
Actions: Data Aggregation, Threat Detection, Data Analytics for Threat Detection

Respond. Take action with appropriate activities related to a cybersecurity incident.
Actions: Orchestration and Remediation, Cyber-physical Fault Isolation, Network Segmentation

Recover. Plan for resilience and restoration of any impaired services due to an incident.
Actions: Cyber Event Reconstruction, Employing Optimized Black Start Strategies

Endure. Continue to operate in the event of a cyberattack through preparation.
Actions: Component Diversification, Utilizing Cyber Safe Modes



INL personnel monitoring grid operations

Grid monitoring at PNNL

Examples of Cyberattacks

Network Probes. Attackers often try to detect and gain access to a weak point in a computer or network system.

Distributed Denial of Service (DDoS). Overwhelming a system with many access attempts may prevent authorized access.

Advanced Persistent Threat (APT). By maintaining ongoing, covert access to a network, hackers can gain access to more and more information over time.

Phishing. These fraudulent emails typically impersonate a business in an attempt to get users to give out personal information or download malicious software.

Spoofing. False messages from what appears to be a trusted host are sent to a computer's specific internet protocol (IP) as a means to gain access to a network.

Brute-force Cracking. Hackers repeatedly guess passwords until they find the correct one and gain entry.

Image of grid monitoring at PNNL: flickr.com/photos/pnnl/3811688057/in/photolist-68sDL5-pTTowk-L7Y4Wt-KmKhaP-6NPU4B-6NPU3Z-6NPU4X

[5] "Multiyear Plan for Energy Sector Cybersecurity." U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability. March 2018. energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

[6] "OE Mission." U.S. Department of Energy, Office of Electricity. Accessed January 7, 2019. energy.gov/oe/mission

[7] "Cybersecurity for Critical Energy Infrastructure." U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure

[8] "Cybersecurity Framework." National Institute of Standards and Technology. nist.gov/cyberframework

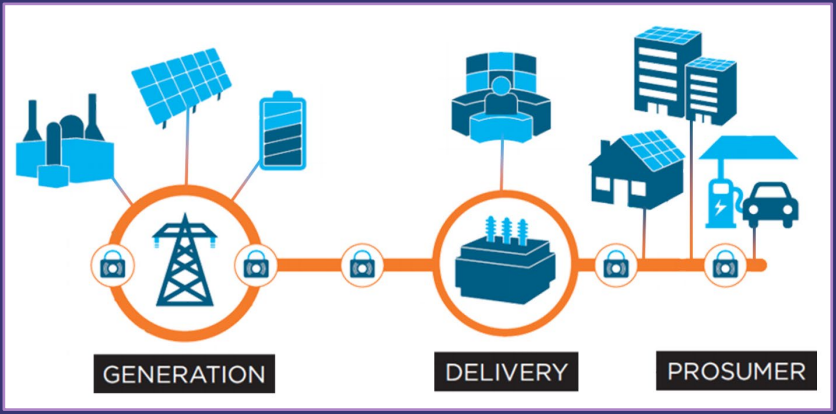


Image Adapted with Permission from Michael Kintner-Meyer, PNNL

DOE Is Modernizing the Grid from Generation to Consumer End Use

DOE supports grid modernization by catalyzing private sector innovation, increasing regional deployment, and bringing disparate organizations together to collaborate. DOE also works through its National Laboratories, industry, and its public partners to support R&D projects in grid modernization.

DOE's Grid Modernization Initiative (GMI) is a collaborative partnership of DOE's five applied offices. The GMI focuses on developing new architectural concepts, tools, and technologies that will better measure, analyze, predict, protect, and control the grid, as well as enable the institutional conditions that allow for development and adoption of these tools and technologies.

GMI's current lab call consists of the following six topic areas that address security challenges of the electric power system:

1. **Resilience Modeling**
2. **Energy Storage and System Flexibility**
3. **Advanced Sensors and Data Analytics**
4. **Institutional Support and Analysis**
5. **Cyber-Physical Security**
6. **Generation**

An Evolving Energy Landscape

- **Changing energy mix** – Driven by technology, market, and policy developments.
- **Changing demand for energy** – Driven by population growth, adoption of energy-efficient technologies, and broader electrification, including more electric vehicle integration.
- **Increasing variability –** On the supply side, more variable renewables are being incorporated. On the demand side, there are more active customers who are being accommodated with technology.
- **Interconnecting systems** – Distributed, automated devices need communications systems to control the grid efficiently.

Challenges Facing Grid Modernization

- **Regional differences**
- **Small number of innovators**
- **Costs**
- **Disjointed grid regulation**
- **Proliferation of Distributed Energy Resources (DER)**

Grid Modernization Lab Consortium

The Grid Modernization Lab Consortium (GMLC) is composed of 13 DOE National Labs. This strategic partnership brings together experts and resources to work collaboratively toward grid modernization goals. The GMLC works with partners in industry, academia, and state and local governments and organizations. These partnerships work to advance the focus areas defined by the GMI. The GMLC manages a comprehensive set of projects that includes tools, platforms, concepts, and technologies that will help to analyze, measure, predict, and control the grid in the future.

For more information on the GMLC, please visit energy.gov/grid-modernization-initiative-0/grid-modernization-lab-consortium.

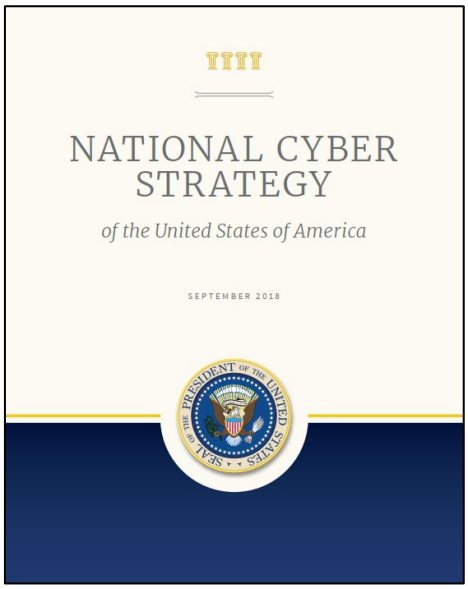
GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Cybersecurity Is an Executive Priority Supported by DOE and CESER

Several recent executive orders and strategies stress the importance of cybersecurity for critical infrastructure. DOE and CESER are pursuing initiatives and actions to address these high priorities in the energy sector.

National Cyber Strategy (NCS) From the White House[9]

The release of the President's NCS reflects the Administration's commitment to protecting America from cyber threats. DOE plays an active role in supporting the security of our Nation's critical energy infrastructure in implementing the NCS.



These efforts reflect a concerted response to the emergence of energy cybersecurity and resilience as one of the Nation's most important security challenges. DOE must work with other federal agencies and its industry partners to share information, define roles, and speed coordination across multiple stakeholders—this work is presently being accomplished through CESER's programs, DOE's world-class National Laboratory network, and advanced education and training exercises across the country.

Executive Order on Securing the United States Bulk-Power System (BPS)[10]

This order restricts the supply of bulk-power system electric equipment from foreign entities to ensure the integrity, reliability, and security of the country's electric grid. Exploitation of cybersecurity vulnerabilities in this equipment would impact our economy, health, and safety by rendering the country unable to act fully to defend itself and its allies.

Executive Order on Electromagnetic Pulses (EMPs)[11]

An EMP can be created by non-nuclear events and by the high-altitude detonation of a nuclear weapon, which have the potential to damage power delivery assets and impact BPS reliability over a wide area. In alignment with this Executive Order, CESER works closely with the private sector, as well as federal and state, local, tribal, and territorial (SLTT) government partners, to enable more coordinated preparedness for and response to disruptions caused by EMPs and geomagnetic disturbances.

[9] "National Cyber Strategy of the United States of America." The White House. September 2018. whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[10] "Executive Order on Securing the United States Bulk-Power System." The White House. May 1, 2020. whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system
[11] "Executive Order on Coordinating National Resilience to Electromagnetic Pulses." The White House. March 26, 2019. whitehouse.gov/presidential-actions/executive-order-coordinating-national-resilience-electromagnetic-pulses

Executive Order on Maintaining American Leadership in Artificial Intelligence (AI)[12]

CESER works with DOE's AI program to surface new ways AI can advance our Nation's energy security. One example of CESER's work in this area is the Cyber Attack Detection and Accommodation for Energy Delivery Project, which uses feature-based machine learning and control and estimation algorithms to detect, localize, and mitigate attacks in real-time with very low false positive rates with multiple heterogeneous data streams.

Executive Order on Securing Information and Communications Technology (ICT) and Services Supply Chain[13]

This order prohibits U.S. transactions involving ICT services designed or developed by foreign adversaries that might compromise the security of U.S. critical infrastructure or put U.S. national security and citizens' safety at risk reinforcing initiatives CESER has underway in the energy sector, including efforts to develop a collective understanding of systemic and supply chain risks and vulnerabilities.

Executive Order on America's Cybersecurity Workforce[14]

The national priority of growing the Nation's cyber workforce is outlined in the President's NCS and further reinforced by this Executive Order. CESER's state, local, tribal, and territorial workforce development efforts through organizations like the National Association of State Energy Officials constitute a multifaceted approach of online trainings, playbooks, workshops, and guidance. CESER also hosts its annual collegiate-level CyberForce Competition™ to help train the next generation of cybersecurity professionals to help secure the nation's critical energy infrastructure.

DOE Cybersecurity Strategy 2018–2020[1]

The DOE Cybersecurity Strategy addresses challenges associated with an increasingly complex cyber landscape and will help to modernize DOE information technology (IT) infrastructure to deliver effective services to support smart, efficient cybersecurity and enhance DOE's cybersecurity risk management across the enterprise.

The strategy identifies four crosscutting principles: "One Team, One Fight"; employment of risk management methodology; prioritized planning and resourcing; and enterprise-wide collaboration. DOE will apply these principles across four IT strategy goals:

1. Deliver high-quality IT and cybersecurity solutions;
2. Continually improve cybersecurity posture;
3. Transition from IT owner to IT broker for better customer focus;
4. Excel as stewards of taxpayer dollars.

[12] "Executive Order on Maintaining American Leadership in Artificial Intelligence." The White House. February 11, 2019. whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence

[13] "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." The White House. May 15, 2019. whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain

[14] "Executive Order on America's Cybersecurity Workforce." The White House. May 2, 2019. whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce

DOE Leverages Unique Cybersecurity Capabilities

DOE's scientific and technical capabilities are rooted in its system of National Laboratories—world-class institutions that constitute the most comprehensive R&D network of its kind.

The DOE National Laboratories possess a unique collection of scientific expertise and highly specialized facilities. Collectively, these assets play a vital role in helping the United States maintain the science and technology leadership needed to sustain economic superiority in a dynamic and innovative global economy.

Researchers at the National Labs and other DOE-funded facilities actively collaborate with partners in industry, academia, and government to develop transformational technologies essential to grid cybersecurity.

Core Capabilities in Cybersecurity

Our National Laboratory System uses its world-class expertise and facilities to lead basic discovery research, technology development, and demonstrations. The following laboratories hold core capabilities in cybersecurity R&D:

- Argonne National Laboratory
- Brookhaven National Laboratory
- Idaho National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- National Energy Technology Laboratory
- National Renewable Energy Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories
- Savannah River National Laboratory
- Stanford Linear Accelerator Laboratory

Learn more at energy.gov/downloads/annual-report-state-doe-national-laboratories

Partnership Agreements With DOE National Laboratories

Industry, academia, and other entities can access the specialized expertise and facilities of the National Labs through collaborative research agreements. A variety of partnership mechanisms are available to suit the diverse needs of the U.S. research community:

- Agreements for Commercializing Technology (ACT)
- Cooperative Research & Development Agreements (CRADA)
- Material Transfer Agreements
- Strategic Partnership Projects (SPP)
- Technical Support Agreements
- Technology Licensing Agreements
- User Agreements

In fiscal year 2017, 21 unique nonfederal partner organizations worked on 21 active cybersecurity research projects using the ACT, CRADA, or SPP mechanisms. These partners contributed $2.8 million to this work covered by agreements which included 8 CRADAs, to which DOE contributed nearly $1 million.

For more information on how to work with the National Laboratories, please refer to the 2016 *Guide to Partnering with DOE's National Laboratories* at inl.gov/wp-content/uploads/2016/05/Revised-Guide-Partnering-with-National-Labs-Final.pdf

DOE's National Laboratories are dedicated to accelerating the development of the next generation of cybersecurity technologies.

The Labs are home to multiple facilities and collaborative research groups that solve cybersecurity problems through multidisciplinary research.

Left image from Idaho National Laboratory: flickr.com/photos/inl/7895742584

National Labs are Proactively Preparing for Cyber Threats

A widespread cyberattack in the northeast United States could cause hundreds of billions of dollars in damage.[1] The National Labs have a number of test beds that are working to model and anticipate events to prevent cyberattacks from ever happening.

[1] "Business Blackout." Lloyd's. Published July 6, 2015. lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

INL Critical Infrastructure Test Range Complex (CITRC)

An Electric Grid Test Bed and a Cyber Security Test Bed provide industry-scale infrastructure systems for testing the performance of physical and cybersecurity strategies. Understanding the interconnection of wireless devices and communications pathways enables innovation.

LLNL Skyfall Laboratory

This laboratory allows LLNL to create highly complex simulations of the power grid and associated control systems. This setup is used to conduct detailed and realistic simulations of cyberattacks on the power grid, including executing real cyberattacks on actual physical devices.

NREL Energy Systems Integration Facility (ESIF)

The facility's simulation capabilities, high-performance computing and 3-D visualization, parallel AC and DC power buses, and integrated cybersecurity architectures, offer a unique platform for the evaluation of cybersecurity and emerging energy technologies.

PNNL CyberNet Test Bed

The cybersecurity sector is often unable to deploy engineered solutions with consistent results. This test bed was developed to emulate enterprise network environments so scientists can conduct research. The data from this test bed will lead to the development of consistent, reliable cybersecurity products.

Modeling and Information Sharing Boosts Grid Cybersecurity for All Stakeholders

DOE is setting up comprehensive models and facilitating data sharing to strengthen the grid's cybersecurity.

Cybersecurity Capability Maturity Model (C2M2)
This model helps private sector owners and operators evaluate their cybersecurity capabilities to guide efforts in prioritizing and improving cybersecurity activities.

Cybersecurity for the OT Environment (CyOTE™)
CyOTE™ pilot programs are demonstrating the challenges of collecting data on OT networks. These programs will determine what to monitor, how to collect and process data, and how to share sensitive data.

Cyber Analytics Tools and Techniques (CATT™ 2.0)
This program is working with industry to support discovery and mitigation of advanced cyber threats to critical energy infrastructure through automated analysis of voluntarily provided energy sector data.

ESIF Photo by Dennis Schroeder, NREL 23401

Multi-University Collaborations Strengthen the Innovation Ecosystem

DOE and its National Laboratories and facilities have a rich history of collaborating with universities. Several of DOE's National Laboratories are run by or are affiliated with universities. These include Ames Laboratory (run by Iowa State University), Los Alamos National Laboratory (affiliated with Texas A&M University), and Lawrence Berkeley National Laboratory (run by the University of California), among others. DOE also directs funding toward universities to work specifically toward R&D and strategic goals. This funding currently supports two multi-university collaborations working to advance the cybersecurity of the U.S. electric grid.

The Cyber Resilient Energy Delivery Consortium (CREDC)

CREDC involves 10 university partners as well as two National Laboratory partners (Argonne National Laboratory [ANL] and Pacific Northwest National Laboratory [PNNL]) and is funded by DOE and the DHS Science and Technology Directorate. The University of Illinois at Urbana-Champaign serves as CREDC's base of operations. CREDC has a bevy of research technology areas that focus on mid-term and long-term goals. Some of the research priorities for this group include cyber protection technologies, risk assessment of electricity delivery systems, cyber monitoring, data analytics for cyber event detection, and resilient electricity delivery system architectures and networks.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

CREDC University Involvement:

Dartmouth College
Rutgers University
University of Houston
Massachusetts Institute of Technology
Arizona State University
Washington State University
Oregon State University
University of Illinois
Tennessee State University
Old Dominion University

For additional information, visit cred-c.org

In addition to the numerous R&D activities undertaken by CREDC, 10 different cybersecurity technologies have been generated by the group so far. The organization also hosts workshops for universities and education activities for students and stakeholders in the cybersecurity field.

The Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)

SEEDS' goal is to conduct R&D on innovative cybersecurity technologies that help the energy sector survive cyber incidents while maintaining functionality. The University of Arkansas serves as the SEEDS' base of operations, and the group has five other university partners. SEEDS was first funded by CEDS in 2015 and currently has 21 active projects and 9 completed projects related to grid cybersecurity. The organization maintains its funding through industry members that make contributions, as well as from funding from CEDS. SEEDS works within a framework of five technical objectives and a 3-phase roadmap that guides its R&D activities and projects.[15]

SEEDS CYBERSECURITY CENTER

SEEDS University Involvement:

University of Arkansas
University of Arkansas Little Rock
Lehigh University
Massachusetts Institute of Technology
Carnegie Mellon University
Florida International University

For additional information, visit seeds.thepower.group

[15] "Research." SEEDS Cybersecurity Center. seeds.thepower.group/research.

National Winners of the Nov. 2019 CyberForce Competition™ from University of Maryland, Baltimore County. (Image: CyberForce Competition™)

DOE Working with Academia to Grow the Grid Cybersecurity Workforce

Academic projects engage undergraduate and graduate students and develop their skills for a career in cybersecurity. DOE is striving to increase the number of cybersecurity professionals through programs and competitions.

U.S. DEPARTMENT OF ENERGY'S CYBERFORCE™ COMPETITION
DEFENDING U.S. ENERGY INFRASTRUCTURE

DOE's CyberForce Competition™ for college and university students is developing the next generation of cybersecurity professionals to help defend and bolster our Nation's critical energy infrastructure. The competition's interactive, energy-focused scenario challenges students to protect their servers and virtual machines, as well as their physical, simulated industrial control system.

DOE's CyberForce Competition™ provides students with a unique look at critical energy infrastructure and incorporates cyber-physical elements that help them develop a better understanding of the real-world consequences of cyber events.

For more information, please visit cyberforcecompetition.com

Academic Partnerships Drive Workforce Development

80 Trained Cybersecurity Professionals

370 Cybersecurity Research Publications

600 Industry-Relevant Presentations

The CREDC Summer Symposium (formerly Summer School) is a weeklong program focusing on cybersecurity and cyber-resiliency of energy delivery systems for electric power and oil and gas industries. The symposium caters to energy industry professionals, academic researchers, and college students.

This program allows participants to network, learn about R&D activities, and explore collaborative research initiatives. The symposium complements other activities at CREDC, which is partially funded by DOE's Office of Electricity and DHS's Science & Technology Directorate.

For symposium dates and information, please visit cred-c.org/events/summer-symposium-formerly-school

59% OF ORGANIZATIONS have unfilled cybersecurity positions

54% of Organizations take **3 MONTHS OR MORE** to fill open positions

State of Cybersecurity 2018: Contours of the Skills Gap, ISACA © 2018. All rights reserved. Used with permission

Partners Advance Cybersecurity With DOE

DOE invests in cybersecurity R&D to protect and defend America's energy systems and bolster U.S. competitiveness in global markets. Primarily run through the CEDS program within CESER, DOE cybersecurity R&D has led to significant technological progress over the past several decades.

U.S. DEPARTMENT OF ENERGY

Office of ELECTRICITY

Office of CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Office of TECHNOLOGY TRANSITIONS

GRID MODERNIZATION LABORATORY CONSORTIUM

DOE supports de-risking cybersecurity technology through R&D partnerships with the National Laboratories, industry, academia, federal and state agencies, and a range of public-private consortia. Industry and federal partners also assist DOE by developing frameworks and coordinating security efforts. The activities conducted among these partners include data collection, software sharing, and incident management.

Industry Partners

ESCC Electricity Subsector Coordinating Council

Coordinates efforts by the federal government and electric power sector to protect the grid from national security and public safety threats.

GRID PROTECTION ALLIANCE *open source solutions for electric utilities*

Nonprofit that develops and supports software solutions for the electric industry.

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Collects and analyzes security data provided by members. Manages sharing and exchange of data and coordinates incident management.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Conducts R&D on diverse energy and environmental issues. Collaborates with sector stakeholders with a focus on electricity generation, delivery, and use.

Federal Government Partners

U.S. Department of Homeland Security

Works with DOE on cybersecurity via its Science & Technology Office; National Cybersecurity and Communications Integration Center; CISA; and ICS-CERT.

DARPA

Invests in technologies that can provide breakthroughs to improve national security.

Additionally, the Department of Defense pursues a cybersecurity strategy to defend its own networks, prevent significant cyberattacks against the U.S., and provide cyber capabilities to the military.

Office of Technology Transitions' Programs Strengthen the Innovation Ecosystem

Energy I-Corps: Relevant Project Teams

Volttron: Pacific Northwest National Laboratory (Cohort 2). Open-source platform for distributed sensing and control. Allows for development and deployment of smart building's solutions by allowing applications to communicate with physical devices. Cybersecurity is a prioritized consideration for this system.

4CS: Idaho National Laboratory (Cohort 6). Technology that enables automation in monitoring valve positions with retrofitted wireless controllers/sensors. The technology is modular and is based on 4CS: communication, connectivity, co-existence, and cybersecurity. These characteristics allows for easy integration with legacy systems at nuclear power plants.

DCAT: Pacific Northwest National Laboratory (Cohort 6). Dynamic Contingency Analysis Tool (DCAT) that evaluates power grid cascading outages due to extreme events. Therefore, possible to adapt tool to evaluate outages due to a large cyberattack. DCAT can improve power system planning by allowing engineers to model serious failures.

For additional and up-to-date Energy I-Corps project teams and more information, visit energyicorps.energy.gov

Technology Commercialization Fund

The Technology Commercialization Fund (TCF) leverages the Energy Department's annual R&D funding in the areas of Applied Energy Research, Development, Demonstration, and Commercial Application to mature promising energy technologies with the potential for high impact.

The TCF is implemented by OTT and helps businesses move promising technologies from DOE's National Laboratories to the marketplace. TCF projects receive at least an equal amount of nonfederal funds to match the federal investment.

Energy I-Corps

Energy I-Corps (EIC) pairs teams of researchers with industry mentors for an intensive two-month training where the researchers define technology value propositions, conduct customer discovery interviews, and develop viable market pathways for their technologies.

EIC is managed for the Office of Technology Transitions (OTT) by DOE's National Renewable Energy Laboratory, which leads curriculum development and execution, recruits program instructors and industry mentors, and assembles teams from the following national labs:

Argonne National Laboratory; Berkeley Lab; Fermilab; Idaho National Laboratory; Lawrence Livermore National Laboratory; Los Alamos National Laboratory; NREL; Oak Ridge National Laboratory; Pacific Northwest National Laboratory; Sandia National Laboratories

Select TCF Projects Relevant to Cybersecurity

Quantum Key Distribution System
Oak Ridge National Laboratory

Prototype a quantum secure communication (QSC) operational network. Allows trustworthy relays to extend distance and decrease cost for critical energy infrastructure.

Event Model Risk Assessment using Linked Diagrams (EMRALD)
Idaho National Laboratory

Software tool that can perform probabilistic risk assessments (PRAs) of discrete events. Can be used to support electrical system modeling such as deployment of small modular reactors. System security is one parameter that can be analyzed.

Implementing Coupled Transmission and Distribution Simulation
Lawrence Livermore National Laboratory

This project is working to commercialize a mod/sim capability that can do co-simulation of transmission and distribution so that the system can be accurately captured.

For more information, please visit energy.gov/technologytransitions/services/technology-commercialization-fund

Cybersecurity Patents Available for Licensing

The DOE National Labs create numerous technologies in a variety of fields thanks to funding from the DOE. These technologies are often patented and then made available for use through licensing. The following grid cybersecurity technologies are available for licensing. Contact the applicable National Lab directly if interested.

Laboratory Partnering Service (LPS)

LPS is an online platform managed by OTT to provide public access to world-class DOE energy experts, facilities, and licensing opportunities at the National Laboratories.

For additional and up-to-date information on all available DOE technologies, please visit labpartnering.org

Grid Cybersecurity Patents

Encryption

Obfuscated Authentication Systems, Devices, and Methods
US8566579, Sandia National Laboratories

Quantum Key Distribution Using Card, Base Station and Trusted Authority
US9002009, Los Alamos National Laboratory

Quantum Key Management
US9509506, Los Alamos National Laboratory

Multi-Factor Authentication Using Quantum Communication
US9887976, Los Alamos National Laboratory

Quantum Random Number Generators
US10019235, Los Alamos National Laboratory

Apparatus, System, and Method for Providing Cryptographic Key Information with Physically Unclonable Function Circuitry
US9208355, Sandia National Laboratories

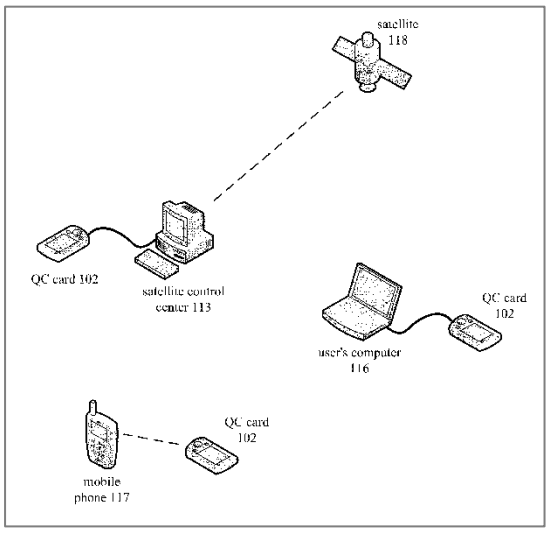
System and Method for Key Generation in Security Tokens
US9172698, Oak Ridge National Laboratory

Operational Technology

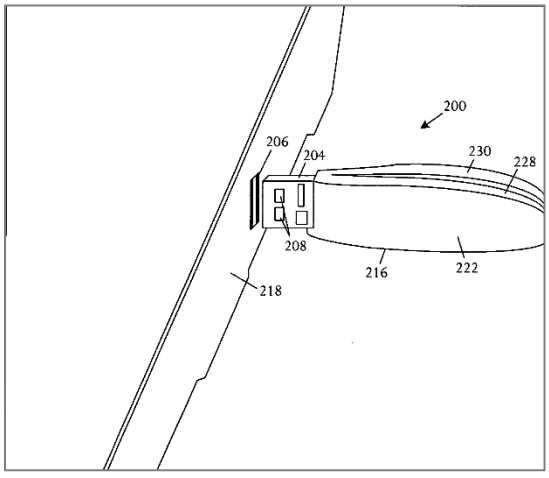
Data Port Security Lock
US7390201, Sandia National Laboratories

Communication

Secure Multi-Party Communication with Quantum Key Distribution Managed by Trusted Authority
US8483394 and US9680640, Los Alamos National Laboratory



Patent Number: US9002009



Patent Number: US7390201

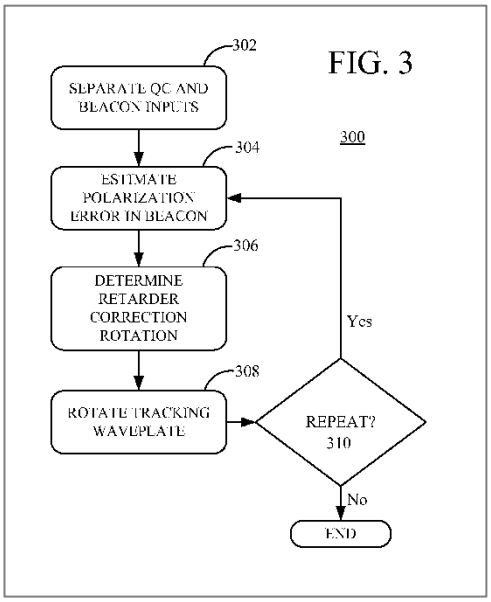
Quantum Communications System with Integrated Photonic Devices
US9819418, Los Alamos National Laboratory

Long-Haul High Rate Quantum Key Distribution
US10044504, Los Alamos National Laboratory

Increasing Security in Inter-chip Communication
US9722796, Sandia National Laboratories

Great Circle Solution to Polarization-based Quantum Communication in Optical Fiber
US9287994, Los Alamos National Laboratory

Polarization Tracking System for Free-Space Optical Communication, Including Quantum Communication
US9866379, Los Alamos National Laboratory



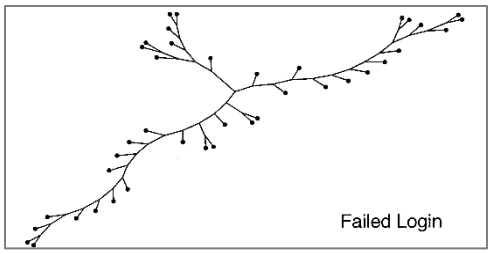
Patent Number: US9866379

Information Technology

Method for Detecting Sophisticated Cyber Attacks
US7454790, Oak Ridge National Laboratory

Computer-Implemented Security Evaluation Methods, Security Evaluation Systems, and Articles of Manufacture
US9092631, Pacific Northwest National Laboratory

Cyberspace Security System
US8762188, Oak Ridge National Laboratory



Patent Number: US7454790

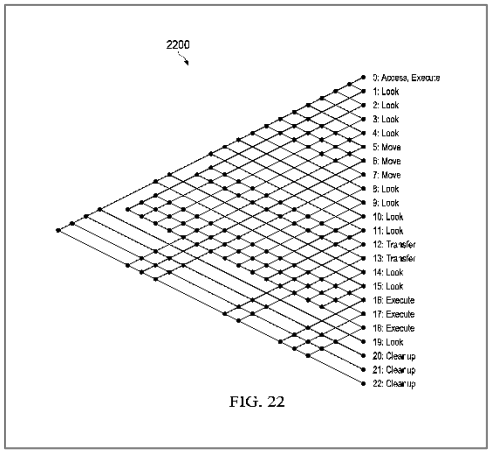
Multiple Operating System Rotation Environment Moving Target Defense
US9294504, Argonne National Laboratory

Method and Tool for Network Vulnerability Analysis
US7013395, Sandia National Laboratories

Computer Network Defense System
US9742804, Sandia National Laboratories

Method and Apparatus for Distributed Intrusion Protection System for Ultra High Bandwidth Networks
US8561189, Pacific Northwest National Laboratory

Network Protection System using Linkographs
US10027698, Sandia National Laboratories



Patent Number: US10027698

Real-time Software Upgrade
US10037203 – Sandia National Laboratories

Dynamic Defense and Network Randomization for Computer Systems
US9985984 – Sandia National Laboratories

Learn More

Organizations may use several mechanisms to partner with the DOE National Laboratories in collaborative research and access the specialized capabilities of their facilities and experts.

OTT engages with stakeholders, collects partnership data, and extends awareness about the impact of DOE's partnering efforts. OTT works to enhance public-private partnership outcomes that expand the commercial impact of the DOE R&D investment portfolio.

Contact OTT to learn how to access technical experts, acquire the latest reports, identify promising energy projects, and locate DOE-funded technologies.

Email:
OfficeofTechnologyTransitions@hq.doe.gov

Website:
energy.gov/technologytransitions

InnovationXLab[SM] Summits

DOE invests more than $10 billion per year in the 17 National Labs. The InnovationXLab[SM] series is designed to expand the commercial impact of this substantial investment in the Labs.

These summits facilitate a two-way exchange of information and ideas between industry and investors and National Lab researchers and DOE program managers with the following objectives:

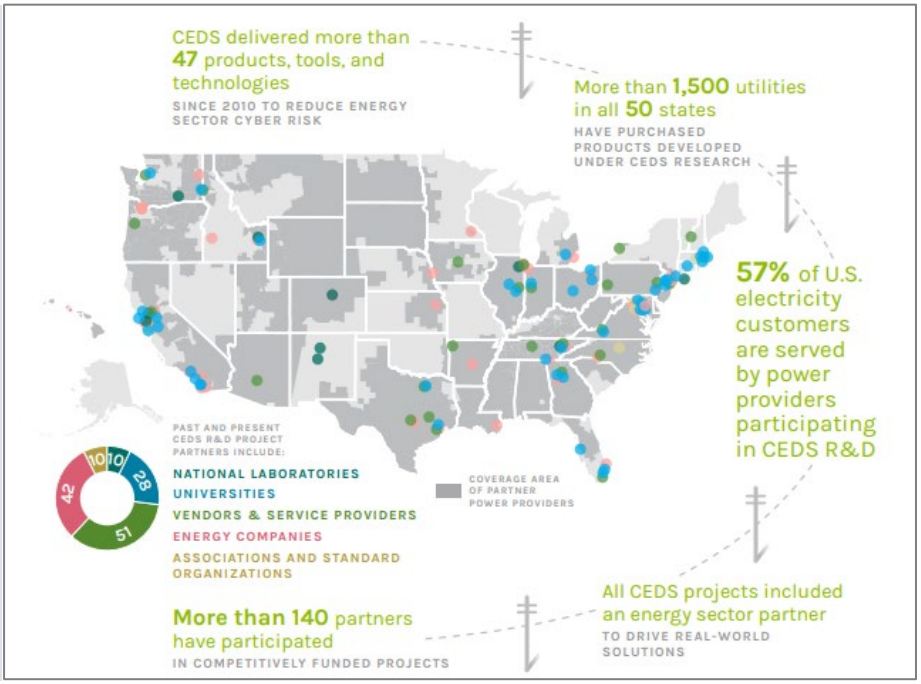
1) **Catalyze** public-private partnerships and commercial hand-offs utilizing DOE's extensive Lab assets: technology, intellectual property, facilities, and world-leading scientists and researchers;
2) **Engage** the private sector to ensure DOE understands industry's technical needs, risk appetite, and investment criteria, thereby incorporating "market pull" into DOE's portfolio planning; and
3) **Inform** DOE R&D planning to increase commercialization possibilities.

InnovationXLab[SM] events are not technical workshops. They enable connections and commercialization opportunities at the decision-maker level.

From Innovation to Practice: Re-Designing Energy Delivery Systems to Survive Cyber Attacks

CEDS summarized cybersecurity R&D projects resulting from their partnerships with industry, vendors, academia, and the National Labs in a July 2018 document with the above title. The report contains descriptions of 47 total projects. Some of these projects are market-ready technologies that can be deployed and installed now. Other technologies can be licensed by industry or built on by researchers to develop new technologies.

Read the document at:
energy.gov/sites/prod/files/2018/09/f55/CEDS%20From%20Innovation%20to%20Practice%20FINAL_0.pdf



Cybersecurity for the Modern Grid Success Stories

U.S. Department of Energy

Contents

U.S. DEPARTMENT OF ENERGY

Office of Technology Transitions

The Office of Technology Transitions develops DOE's policy and vision for expanding the commercial impacts of its research investments and streamlines information and access to DOE's National Labs, sites, and facilities to foster partnerships that will move innovations from the labs into the marketplace.

Cybersecurity for Distributed Energy Resources

Sandia National Laboratories in conjunction with the Department of Energy Solar Energy Technologies Office, SunSpec Alliance, Electric Power Research Institute, National Renewable Energy Laboratory, and industry participants

Creating cybersecurity standards and best practices for interoperable distributed energy resources

Innovation

Distributed energy resources (DER) – energy generation and storage technologies that provide electricity which can include fuel cells, energy storage, solar, and wind systems – are being adopted by both utilities and the public. These systems require proven industry regulations to ensure security and attack-resilient structures to protect against future cyber threats. The U.S. Department of Energy's Solar Energy Technologies Office asked Sandia to create a roadmap to improve cybersecurity for solar DER. The roadmap includes needs for cybersecurity research and development, standards development, and industry best practices.[1] As part of that effort, Sandia, in conjunction with the SunSpec Alliance and partners, is conducting a DER cybersecurity workgroup to create standards in cybersecurity for DER.

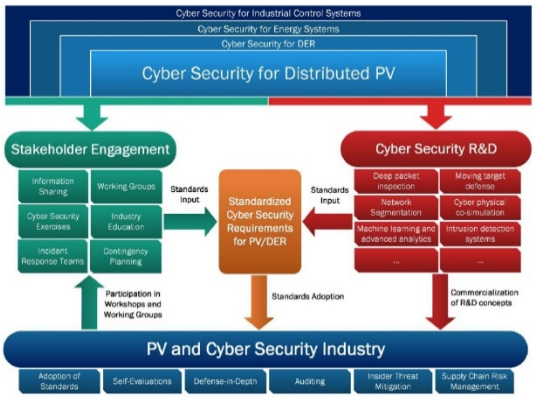
Outcomes

Technology Advancement

The SunSpec Alliance DER Cyber Security Workgroup is actively defining standardized certification procedures for DER and server vulnerability assessments, creating DER control network topology requirements and interface rules, and defining DER boundaries and requirements for transmitting data. Future projects will include classifying data types and permissions, defining protection mechanisms, establishing requirements for patching DER equipment, and creating recommended auditing practices for DER networks.[2]

Impact

The roadmap and the SunSpec Alliance Cyber Security Workgroup are creating a path for improving cybersecurity for DER systems, including communication-enabled photovoltaic (PV) systems, in which there are clear roles and responsibilities for government, standards development organizations, vendors, and grid operators.



Process for achieving cybersecurity of PV systems.
[Image: Sandia, Roadmap for Photovoltaic Cyber Security][1]

"Interoperable Distributed Energy Resources are rapidly becoming a large portion of the Nation's power generation portfolio. These devices have the ability to provide grid services but also pose a risk to critical infrastructure if not properly secured. We established the DER Cybersecurity Workgroup to provide guidance, best practices, and cybersecurity standards for secure DER communications and control."

—Jay Johnson, Principal Member of Technical Staff, Sandia National Laboratories[1]

Timeline

2017: Sandia and SunSpec Alliance launched the DER Cyber Security Workgroup.

2017: Roadmap for Photovoltaic Cyber Security released.

2018: U.S. DER Interconnection Standard, IEEE 1547, is updated to require DER communications.

[1] J. Johnson, "Roadmap for Photovoltaic Cyber Security," Sandia Technical Report, SAND2017-13262, Dec 2017.

[2] sunspec.org/wp-content/uploads/2018/10/5.SandiaDERCyber security-Gridvolution-9-12-2018.pdf

Cybersecurity for Energy Delivery Systems

Sandia National Laboratories, in partnership with Lawrence Livermore National Laboratories, Washington Gas Energy Systems, Fort Belvoir, Chevron, Grimm, and Schweitzer Engineering Laboratories

Ensuring resiliency in energy and utility infrastructure through unpredictability and enhanced situational awareness in energy delivery system networks

Innovation

As critical infrastructure networks and control systems are upgraded and increasingly connected, system security is increasingly at risk. Energy delivery control systems traditionally have predictable communication paths and static configurations. Sandia's Artificial Diversity and Defense Security (ADDSec) project is developing solutions to introduce unpredictability and enhance situational awareness for vulnerable static energy delivery control systems, protecting them against cyberattack.

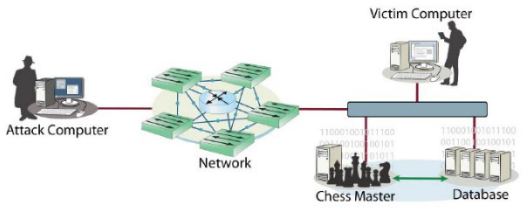
Outcomes

Technology Advancement

The ADDSec program has leveraged software-defined networking to introduce random unpredictability into control system networks through three main components: network randomization, application library randomization, and machine learning based dynamic defense. Machine learning dynamic defense detects active attacks by recognizing patterns, providing situational awareness, and taking appropriate action when necessary.[1]

Impact

Research has resulted in a verified means for a resilient mechanism to support modern grid operation through creating complexity for adversarial attackers and detection capabilities for those attacks. Sandia, in conjunction with partner Schweitzer Engineering Laboratories, successfully employed testing at Fort Belvoir for ADDSec in which the technology defended Fort Belvoir's microgrid control system, detected abnormal behavior, and triggered a mitigation response. The demonstration has proven that the ADDSec technology can interoperate with commercially available products and be retrofitted into operating systems.[2]



Process demonstrating the security of legacy and modern systems by improving overall situational awareness and converting static systems into moving targets.
[Image: Vicente Garcia. Sandia National Laboratories][3]

"The detection and response capability of ADDSec provides a framework for utility operators to proactively defend their networks against active threats in an automated fashion."
—Adrian Chavez, Principal Member of Technical Staff/ADDSec Principal Investigator, Sandia National Laboratories[1]

Timeline[3]

October 2015: Project commences.
July 2016: Initial Fort Belvoir microgrid scenario developed.
October 2016: Completed proof-of-concept demonstration.
July 2018: Demonstration at Fort Belvoir microgrid for ADDSec certification.

[1] DOE. energy.gov/sites/prod/files/2016/09/f33/SNL%20ADD%20Sec%20Fact%20Sheet%20September%202016.pdf
[2] Sandia National Laboratories (SNL). content.govdelivery.com/accounts/USDOESNLEC/bulletins/1ea8c62
[3] SNL. energy.gov/sites/prod/files/2017/02/f34/SNL_ADDSec_Peer_Review_2016.pdf

Cybersecurity for Virtual Power Plants and DER Management Networks

Sandia National Laboratories

Creating secure control networks for distributed energy resources

Innovation

Virtual power plants (VPPs) and other distributed energy resource management systems (DERMS) require secure communications to decentralized power-generating units for reliable grid operations. Sandia National Laboratories is researching cybersecurity solutions for distributed energy resource (DER) control networks which provide these services while maximizing the security of the power system.

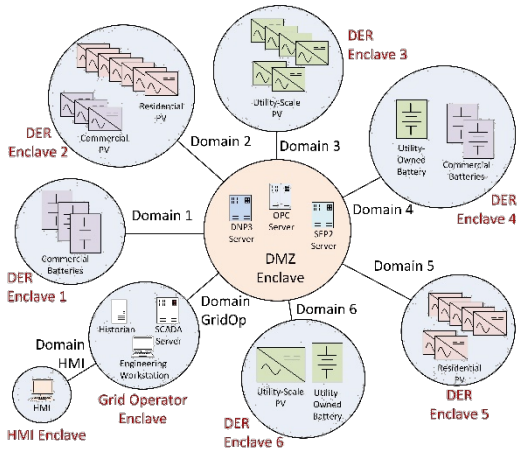
Outcomes

Technology Advancement

Sandia National Laboratories designed multiple network architectures to maximize security for grid services and then evaluated these architectures using an adversary-based assessment methodology. SCEPTRE – a virtual power system and network platform developed at Sandia – is used to conduct red team assessments of these solutions in an isolated, safe environment where the team can study and quantify the tradeoffs between power system performance and cyber resilience.[1]

Impact

To date, Sandia has determined communication requirements for distribution and transmission grid services and deployed SCEPTRE to evaluate cyber resiliency. Three possible approaches to securing DER networks (i.e., enclaving, encryption, and moving target defense) have been assessed using red team methodology to advise the solar industry on the best cybersecurity practices.



Enclaved security reference architecture
[Image: Sandia National Laboratories]

"There are currently a lot of open questions in the DER industry about how to securely design communication networks. Sandia's secure architectures and red team assessments are laying the technical foundation for a secure smart grid of the future."

—Jay Johnson, Principal Member of Technical Staff, Sandia National Laboratories

Timeline

2017: Completed 3-year Secure Virtual Power Plant Research Project.

2017: Developed cybersecurity reference architecture.

2018: Compared control/communications complexity for different approaches.

[1] DOE. energy.gov/sites/prod/files/2018/09/f55/__security_resilience_posters.pdf

Exe-Guard Whitelist Malware Protection Solution

DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Sandia National Labs, in partnership with Schweitzer Engineering Laboratories (SEL) and Dominion Virginia Power

A whitelist malware protection solution called exe-Guard protects the integrity of embedded devices in U.S. power control systems while minimizing the need for updating, security patching, and decommissioning.

Innovation

Instead of blocking device access to an ever-growing list of blacklisted malware, the exe-Guard system approves or whitelists a limited set of trusted programs or code. Using digital signatures and hash functions, this approach affords critical infrastructure protection (CIP) for control systems and lowers costs for administrative and operational management.[1]

Outcomes

Technology Advancement

Whitelist antivirus methods establish a security baseline and deny any code that deviates from that baseline state. The introduction of whitelist protection is particularly important for power systems, which rely on an embedded control system and monitoring devices that are difficult to access remotely.

While blacklist systems require frequent patches and signature updates to remain effective in stopping constantly emerging malware attacks, whitelisting allows less frequent security patching so that system decommissioning can be scheduled and planned.[1]

Impact

SEL was able to expand the original scope of this project and incorporate the exe-Guard technology into six separate products instead of the single product originally planned. This exe-Guard technology advanced the state of technology and is actively protecting America's power systems today.[1]

The SEL-3610 Port Server is one of multiple products embedded with exe-GUARD antivirus technology.
[Copyright: Schweitzer Engineering Laboratories]

"The exe-GUARD project has provided SNL with the unique opportunity of technically contributing to a commercial product that improves the security of energy delivery systems, that addresses CIP compliance standards, and that meets the operational needs of a major energy provider."[3]
—Adrian Chavez,
Cybersecurity Scientist, SNL

Timeline[3]

December 2010: Exe-Guard project starts.

November 2013: Commercial product development completed and field verification started.

January 2016: Technology used in at least six commercial products from Schweitzer Engineering Laboratories. The products are widely deployed and now protect thousands of devices used in power control systems nationwide. [3]

[1] OSTI, Exe-Guard Project: Final Technical Report, Jan. 30, 2016. osti.gov/servlets/purl/1254473

[2] Image provided by SEL

[3] Quote. cdn.selinc.com/assets/Literature/Media/News/SEL_Embedded_exe-GUARD_Anti-Malware.pdf?v=20150812-080416

Interoperable Communication for Control Systems

Sandia National Laboratories and CESER, in partnership with EnerNex Corporation, Schweitzer Engineering Laboratories (SEL), and Tennessee Valley Authority

Producing an open and interoperable security solution for utility control systems through metrics, network security tools, and testing.

Innovation

Among the major issues facing network security for critical infrastructure systems is interoperability for systems from different vendors. When purchasing network security products, control systems users have difficulty comparing products from different vendors due to the lack of an industry-wide mechanism to evaluate functionality, performance, and interoperability. Lemnos creates a universal way to describe and evaluate numerous control system security functions through identifying basic cybersecurity functions needed within industrial control systems, selecting solutions, and producing interoperable configuration profiles through comprehensive testing for cybersecurity functions.[1]

Outcomes

Technology Advancement

Sandia created an interoperable security architecture for common process control system add-on security devices and developed a reference implementation using open-source software and standardized hardware. In conjunction with SEL, Sandia transitioned the reference implementation to a commercial product using open-source software and connected the devices among nine other vendors to demonstrate security interoperability. Sandia provided technical expertise, prototype architecture, and design input.[2]

Impact

Lemnos provides a method to demonstrate interoperability through independently manufactured security product prototypes and has made it possible for vendors to develop interoperable solutions and create more reliable, clearly defined, and interoperable security devices by following an agreed-upon set of vocabulary and metrics.[3] The interoperable devices created by SEL and other vendors are now in use nationwide.

Schweitzer Engineering Laboratories' SEL-3620 Ethernet Security Gateway was developed as part of the Lemnos project.
[Copyright: Schweitzer Engineering Laboratories]

"This serves not only as the basis for secure field device critical infrastructure, but also serves as a shining example of the value that standards-based interoperability can bring to the industry in general."

—Erich Gunther, EnerNex Chairman and Chief Technology Officer[4]

Timeline

2006: Open Process Control Systems Security Architecture for Interoperable Design (OPSAID) program commences at Sandia in which SEL's security gateway is created.

2009: SEL-3620 Ethernet Security Gateway created by SEL.

2010: Lemnos program begins.

[1] researchgate.net/publication/291305786_Cyber_security_interoperability_The_Lemnos_project
[2] energy.gov/sites/prod/files/oeprod/DocumentsandMedia/5-Lemnos.pdf
[3] energy.sandia.gov/wp-content/gallery/uploads/OPSAID-Lemnos-Final-SAND-2012-0557Pno-marks.pdf
[4] securitytoday.com/articles/2011/05/26/cybersecurity-interoperability-project-reaches-milestone.aspx

Legacy Communication Monitoring (SerialTap™)

DHS Science and Technology Directorate (DHS-ST) and Pacific Northwest National Lab, in partnership with Cynash Inc.

SerialTap™ brings a new layer of security to older industrial control systems. As its name suggests, this patented sensor passively taps directly into serial communication systems, monitoring network traffic and watching for control signal anomalies that could indicate a cyberattack.

Innovation

SerialTap™ is a low-cost, compact, embedded device for passively tapping serial line communication and transmitting it over an Ethernet network for comprehensive control system situational awareness. Cost-effective and nonintrusive, SerialTap™ integrates easily with common IT enterprise security solutions.[1]

Outcomes

Technology Advancement

SerialTap™ connects legacy technologies to a computer network and commercial advanced cybersecurity software to monitor older systems. Without interrupting system operations, it "translates" the data from the control system for network cybersecurity software analysis, allowing the identification of anomalies like cyberattacks, speeding their resolution and potentially saving millions of dollars in downtime.[2]

Impact

Large portions of industrial control systems continue to be operated with legacy serial communications and have largely been ignored by the cybersecurity community. This has led to one of the biggest challenges for ICS operators—retrofitting cybersecurity solutions to legacy systems. The ability to monitor traffic in these environments is necessary to provide complete situational awareness of ICS security states.

The Cynash SerialTap™ brings a new layer of security to older industrial control systems.
[Image: Cynash Inc.][3]

"The vast majority of our critical energy, transportation, and industrial infrastructure still runs on control networks that rely on serial communications. These networks have absolutely no intrinsic resistance to cyberattacks. SerialTap provides a deeper level of communications transparency and process verification to these legacy control systems."[4]

—Richard Robinson
CEO, Cynash

Timeline

2010: PNNL develops initial prototype.

2013–2015: SerialTap™ technology matured and promoted through DHS Transition to Practice (TTP) program.

2017: R&D 100 award winner.

2019: Cynash Inc. commercially releases SerialTap™ technology.

[1] TTP Technology Guide. dhs.gov/sites/default/files/publications/CSD_TTP_Guide_2018_webversion_06262018_508%20Final.pdf

[2] rdworldonline.com/rd-100-archive/?YEAR=2017

[3] Image and Quote. cynash.com/#our-technology

[4] Cynash Press Release.

Link Module With Secure SCADA Communications Protocol (Hallmark)

Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Pacific Northwest National Lab, in partnership with Schweitzer Engineering Laboratories (SEL) and CenterPoint Energy Houston Electric

A Secure SCADA Communications Protocol (SSCP) uses authentication and optional encryption to protect communications between remote devices and central control centers.

Innovation

This technology ensures that all SCADA systems' device-to-device communication comes from an authorized and trusted source. Works with both existing and new devices by sending messages between devices with a device identifier. Can also encrypt the data to provide more security to the grid.

Outcomes

Technology Advancement

SEL designed a serial shield (SEL-3025) that plugs into a serial communication link between a legacy device and the system. This device adds a small amount of latency while securing serial communications with SSCP. Another device produced from this project, the SEL-3045, is a cryptographic card that is a hardware card that runs the SCCP within a device.

Impact

The devices developed as part of the Hallmark project will be able to establish secure SCADA connections for both new and legacy devices. In addition, these systems incorporate easily into the new system designs. Encryption of SCADA data secures the serial communications between devices.

The SEL-3025 Serial Shield device is placed next to equipment that transmits data so the signal can be encrypted.[1]
[Copyright: Schweitzer Engineering Laboratories][2]

"Encryption provides confidentiality and integrity for remote monitoring and interactive remote access and locks out malicious intruders from your critical assets. With its remote management functionality and wide range of application support, the SEL-3025 is flexible and easy to use."
—SEL-3025 Product Brochure

Timeline[3]

October 2007: Start of project period.

June 2010: Link module and cryptographic card released.

March 2012: End of project period.

[1] Image provided by SEL

[2] SEL Brochure: cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/3025_PF00246.pdf?v=20180418-133153

[3] OSTI: osti.gov/servlets/purl/1087721

Micro-Synchrophasor Measurements to Secure Power Distribution Systems

Lawrence Berkeley National Laboratory and the Office of Cybersecurity, Energy Security, and Emergency Response, in partnership with ARPA-E, Power Standards Lab, EnerNex, EPRI, Riverside Public Utilities, and Southern Company

Micro phasor measurement units (μPMUs) capture data about the state of the power grid and combine that data with supervisory control and data acquisition (SCADA) information to provide real-time data on system performance.[1]

Innovation

Allows utilities to detect a physical or cyber grid disruption using μPMUs. Synchophasors are able to provide data much faster than SCADA systems and are especially useful when installed at facilities such as substations. The collected data from μPMUs is combined and sent to SCADA systems to provide real-time feedback on the state of the grid. Abnormal behavior on the grid such as a cyberattack can therefore be detected by this system.

Outcomes

Technology Advancement

Increases the amount of data provided by field sensors by using μPMUs, which take measurements 120 times per second, roughly four times more than current phasor measurement units (PMUs). In addition, μPMUs are smaller and less expensive than traditional PMUs, which allows more to be used and more data to be collected. The team at Berkeley also modified an existing machine-learning algorithm to detect abnormal behavior in the power grid by examining differences between SCADA and μPMU data.[2]

Impact

This technology increases grid reliability and resiliency by allowing for faster detection of a cyber or physical disruption of the grid. The increase in local devices and associated communications infrastructure is also an advance for Internet of Things (IoT) technologies. Future μPMU devices should secure distributed energy resources (DERs) such as rooftop solar panels and make it easier to incorporate higher penetrations of DERs.

A μPMU installation on a utility distribution pole. There is a GPS antenna on top of box and a high-resolution power quality monitor.
[Image: ARPA-E] [3]

"The idea is if we could leverage the physical behavior of components within the electrical grid, we could have better insight in terms of whether there was a cyberattack that sought to manipulate those components. These devices provide a redundant set of measurements that give us a high-fidelity way of tracking what is going on in the power distribution grid."[4]

—Sean Peisert,
Computer Scientist, LBNL

Timeline

2015: LBNL cybersecurity project starts.

2018: LBNL project moves to tech transfer phase.

[1] Other. dst.lbl.gov/security/project/ceds-upmu

[2] GCN. gcn.com/articles/2018/09/21/grid-cybersecurity.aspx?m=1

[3] Image. arpa-e.energy.gov/impact-sheet/university-california-berkeley-open-2012

[4] Quote. crd.lbl.gov/news-and-publications/news/2018/combination-of-old-and-new-yields-novel-power-grid-cybersecurity-tool/

Secure Information Exchange Gateway for Electric Grid Operations (SIEGate)

Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Pacific Northwest National Lab, in partnership with Grid Protection Alliance and others

An open source software tool that maintains the integrity of large data sets sent between transmission organizations and control centers.

Innovation

A secure and flexible program that improves the security of electrical utility control centers while minimizing their external exposure to cyberattacks. The system allows for SCADA data, synchrophasor data, alarms, and notifications to be exchanged at low latency. SIEGate strengthens cybersecurity and relieves administrative burdens and costs of data sharing between control centers.

Outcomes

Technology Advancement

SIEGate is capable of exchanging 5 million measurement data points per second among control centers and devices. The SIEGate project introduces an appliance that serves as a gateway to exchange multiple types of data required for real-time electric system operations. SIEGate allows legacy systems to send secure and reliable data to control centers. Making the software open source lowers the cost of the product and makes it widely accessible.

Impact

This software will improve security for control centers by replacing the need for a multitude of devices to exchange power system data and introducing a single, secure gateway appliance. SIEGate also reduces management and overhead costs associated with more complex systems.

SIEGate

Logo for SIEGate open source software. The code is open source and available on GitHub.
[Grid Protection Alliance][1]

"SIEGate is capable of moving a large and continuously varying set of data at low latency … A single instance of SIEGate on common hardware can exchange about 5 million measurements points per second"
—Grid Protection Alliance Product Page[1]

Timeline[2]

2010: Work begins on SIEGate.
2013: Initial version published.
2017: Program has been downloaded more than 3,000 times.

[1] Image: gridprotectionalliance.org/products.asp
[2] GitHub: github.com/GridProtectionAlliance/SIEGate

Office of Technology Transitions • U.S. Department of Energy

The Office of Technology Transitions develops DOE's policy and vision for expanding the commercial impacts of its research investments and streamlines information and access to DOE's National Labs, sites, and facilities to foster partnerships that will move innovations from the labs into the marketplace.

U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

January 2021

U.S. DEPARTMENT OF ENERGY | Office of TECHNOLOGY TRANSITIONS

energy.gov/technologytransitions