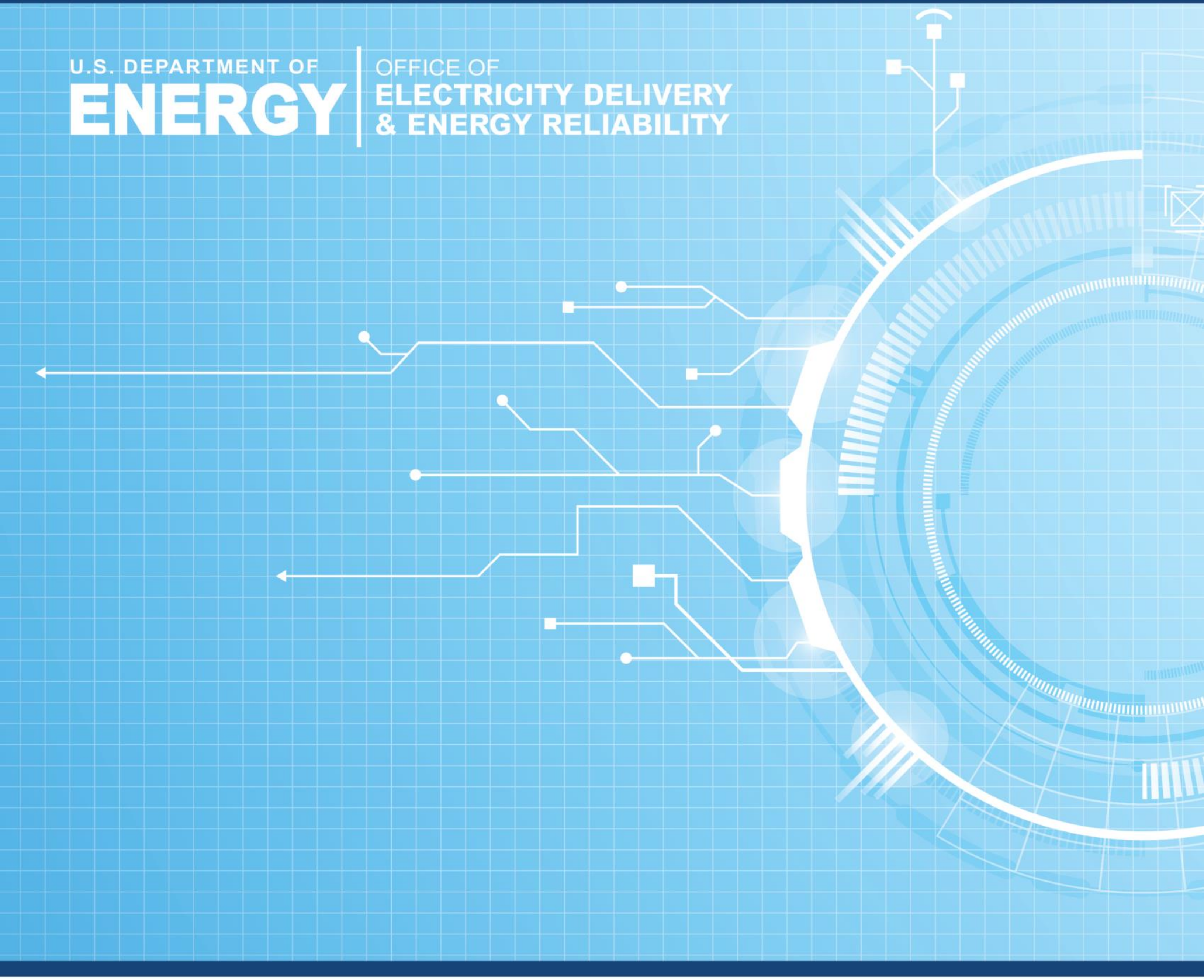
U.S. DEPARTMENT OF
ENERGY
OFFICE OF
ELECTRICITY DELIVERY
& ENERGY RELIABILITY



Multiyear Plan for Energy Sector Cybersecurity

MARCH 2018

Letter from the Assistant Secretary

Protecting America's energy systems from cyber attacks and other risks is a top national priority. Reliable energy and power is the cornerstone of our advanced digital economy and is essential for critical operations in transportation, water, communications, finance, food and agriculture, emergency services, and more. Today, any cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. As nation-states and criminals increasingly target energy networks, the federal government must help reduce cyber risks that could trigger a large-scale or prolonged energy disruption.

The U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE OE) has prepared this ***DOE Multiyear Plan for Energy Sector Cybersecurity*** to improve cybersecurity and resilience of the nation's energy system. It lays out an integrated strategy to reduce cyber risks in the U.S. energy sector by pursuing high-priority activities that are coordinated with other DOE offices, and with the strategies, plans, and activities of the federal government and the energy sector.

This includes close alignment with the cybersecurity priorities of the 2017 *National Security Strategy* and with recommendations from private-sector executives in the National Infrastructure Advisory Council's 2017 *Securing Cyber Assets* study—both of which recognize that energy sector cybersecurity is imperative for national security and economic prosperity. The Multiyear Plan framework helps to align the efforts of government at all levels with those of energy owners and operators and key energy stakeholders in the private sector.

DOE OE recognizes that cybersecurity is a shared responsibility between the public and private sectors and has worked with the energy sector to enhance cybersecurity and resilience for more than 15 years. Our Plan priorities are guided by two industry-led efforts: the ***Roadmap to Secure Control Systems in the Energy Sector*** in 2006, and its subsequent update, the ***Roadmap to Achieve Energy Delivery Systems Cybersecurity*** in 2011. Although significant progress has been made toward Roadmap goals, much more needs to be done as new technologies are adopted and as threats to the energy sector become more sophisticated and pervasive.

The Plan identifies the goals, objectives, and activities that DOE will pursue over the next five years to reduce the risk of energy disruptions due to cyber incidents. It describes how DOE will carry out its mandated cybersecurity responsibilities as the Sector-Specific Agency and address the evolving security needs of energy owners and operators.

It establishes the guiding principles and strategic approach needed to drive both near- and long-term national cybersecurity priorities for DOE's support of the energy sector. The Plan supports implementation of Executive Order (EO) 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which directs DOE and other federal agencies to examine how federal authorities and capabilities can support cyber risk management for critical infrastructure owners and operators, and to work with the energy sector in assessing the grid's capabilities to manage and mitigate prolonged power outages resulting from cyber attack.

The Plan will provide a critical foundation to DOE's newly announced **Office of Cybersecurity, Energy Security, and Emergency Response (CESER)**, which will shift OE's cybersecurity and incident response activities to a new, dedicated office. The Plan outlines a game-changing strategy for DOE, informed by the energy industry's highest-priority needs, which can continue to be built upon by CESER leadership.

While the Plan outlines activities specifically for DOE, we look forward to conducting these efforts in close partnership with the energy industry and federal and non-federal partners throughout the nation.

Bruce J. Walker
Assistant Secretary
Office of Electricity Delivery and Energy Reliability
March 2018

Executive Summary

The nation's energy infrastructure has become a major target of cyber attacks over the past decade, with more frequent and sophisticated attacks that are increasingly launched by nation-states and cyber criminals. Despite ever-improving defenses, attackers have shifted their aim from exploitation to disruption and destruction. Today, a cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. This makes energy cybersecurity a top national priority that will require the federal government and the energy sector to work together to reduce cyber risks that could trigger a large-scale or prolonged energy disruption.

To address this priority, the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE OE) has prepared the ***DOE Multiyear Plan for Energy Sector Cybersecurity*** to improve cybersecurity and the resilience of the nation's energy system. The Plan aligns DOE's distinct roles and programs with the efforts of government, energy owners and operators, and key energy stakeholders, at all levels.

Current Situation

- Energy owners and operators have integrated advanced digital technologies to automate and control physical functions to improve performance and adjust to a rapidly changing generation mix. This has created a larger cyber attack surface and new opportunities for malicious cyber threats.

- The frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. Nation-states, criminals, and terrorists regularly probe energy systems to actively exploit cyber vulnerabilities in order to compromise, disrupt, or destroy energy systems. Growing interdependence among the nation's energy systems increases the risk that disruptions might cascade across organizational and geographic boundaries.

- In response, the government and private sector continue to increase their spending on cybersecurity operations and maintenance. Despite improving defenses, it has become increasingly difficult for energy companies to keep up with growing and aggressive cyber attacks.

Critical Importance of Energy Sector Partnerships

- The public and private sectors share the responsibility to secure energy systems from cyber threats. Energy owners and operators have the primary responsibility to protect their systems from all types of risk. The federal government complements private-sector efforts to help reduce the risk that a cyber event could trigger a large-scale or prolonged energy disruption that impacts national and economic security.

- As nation-states and criminals increasingly target energy networks, the federal government provides leadership, guidance, technical expertise, and specialized information and resources to help the private sector protect its energy systems.

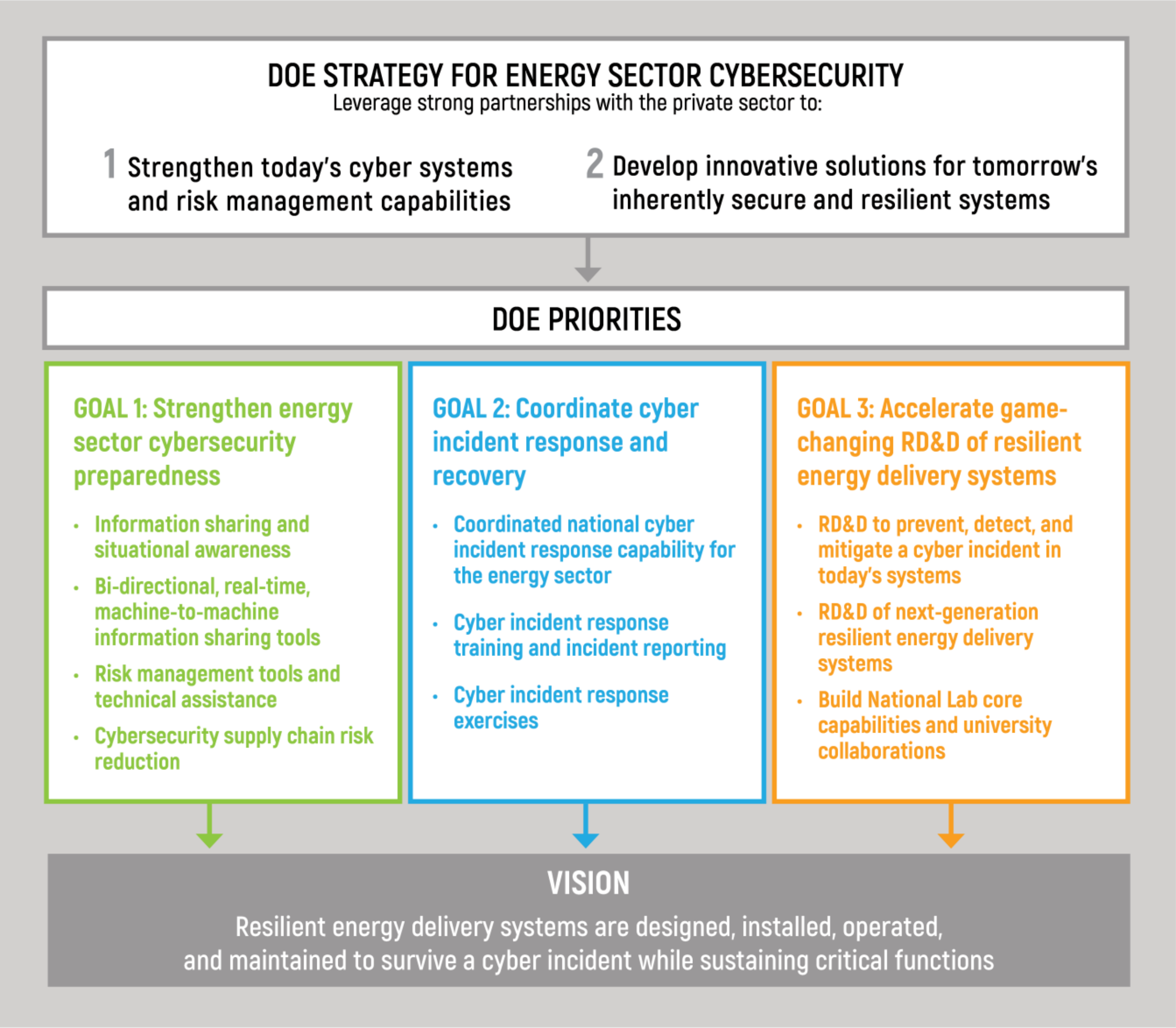
DOE's Strategy to Change the Game

- Anticipating and reacting to the latest cyber threat is a ceaseless endeavor that requires ever more resources and manpower. This approach to cybersecurity is not efficient, effective, nor sustainable in light of escalating cyber threat capabilities. We must recognize today's realities: resources are limited, and cyber threats continue to outpace our best defenses. To gain the upper hand, we need to pursue disruptive changes in cyber risk management practices.

- DOE’s cyber strategy is two-fold: **strengthen today’s energy delivery systems** by working with our partners to address growing threats and promote continuous improvement, and **develop game-changing solutions** that will create inherently secure, resilient, and self-defending energy systems for tomorrow.
- Meaningful public-private partnership is foundational to DOE’s strategy. Facing an ever-evolving threat landscape requires a coordinated approach to improving risk management capabilities, information sharing, and incident response. The federal government has also historically funded innovative research, development, and demonstration (RD&D) that cannot be economically justified in private-sector markets. Today, this includes game-changing RD&D that will build cyber resilience into energy systems for tomorrow.

The ***DOE Multiyear Plan for Energy Sector Cybersecurity*** lays out this integrated strategy (see Figure 1) to reduce cyber risks in the U.S. energy sector. DOE’s strategy aligns with Executive Order 13800, which directs federal agencies to use their authorities and capabilities to support the cyber risk management of critical infrastructure owners and operators.

Figure 1. DOE Multiyear Plan for Energy Sector Cybersecurity



DOE STRATEGY FOR ENERGY SECTOR CYBERSECURITY

Leverage strong partnerships with the private sector to:

1 Strengthen today’s cyber systems and risk management capabilities

2 Develop innovative solutions for tomorrow’s inherently secure and resilient systems

DOE PRIORITIES

GOAL 1: Strengthen energy sector cybersecurity preparedness

- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2: Coordinate cyber incident response and recovery

- Coordinated national cyber incident response capability for the energy sector
- Cyber incident response training and incident reporting
- Cyber incident response exercises

GOAL 3: Accelerate game-changing RD&D of resilient energy delivery systems

- RD&D to prevent, detect, and mitigate a cyber incident in today’s systems
- RD&D of next-generation resilient energy delivery systems
- Build National Lab core capabilities and university collaborations

VISION

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions

The Plan is guided by the energy sector vision contained in the 2011 ***Roadmap to Achieve Energy Delivery Systems Cybersecurity***: *Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions*. It complements the Roadmap by articulating DOE's distinct role and actions to enhance energy sector cybersecurity, working in partnership with the sector. DOE will implement the Plan in coordination with other federal agencies, state and local governments, and the private sector to unify the nation's efforts to achieve our shared vision.

OE will carry out DOE's mandated cybersecurity responsibilities and support the critical security needs of energy owners and operators by pursuing the following goals and objectives over the next five years:

Goal 1: Strengthen Energy Sector Cybersecurity Preparedness

1.1 **Enhance information sharing and situational awareness capabilities**: Define cyber situational awareness information needs and data; provide timely threat briefings and facilitate private-sector clearances; strengthen cyber preparedness among state/local stakeholders in energy assurance planning; and develop effective national and international partnerships.

1.2 **Develop and improve tools for bi-directional, real-time, machine-to-machine information sharing**: Grow energy sector participation in the Cybersecurity Risk Information Sharing Program (CRISP); expand CRISP capabilities to monitor, analyze, and share OT threat indicators; and develop a virtual crowdsourced malware forensic analysis platform.

1.3 **Strengthen sector risk management capabilities**: Update the Cybersecurity Capability Maturity Model (C2M2) and Risk Management Process (RMP); and work with electric cooperatives and public power utilities to foster a culture of security.

1.4 **Reduce critical cybersecurity supply chain vulnerabilities and risks**: Establish an energy delivery system testing and analysis capability.

Goal 2: Coordinate Cyber Incident Response and Recovery

2.1 **Establish a coordinated national cyber incident response capability for the energy sector**: Develop cyber incident response processes and procedures; and leverage technical capabilities to augment cyber mutual assistance.

2.2 **Conduct cyber incident response training and improve incident reporting**: Train emergency responders and update incident reporting processes.

2.3 **Exercise cybersecurity incident response processes and protocols**: Establish annual cyber incident response exercise program; and increase cyber exercises with non-federal government stakeholders.

Goal 3: Accelerate Game-Changing RD&D of Resilient EDS

3.1 **Research, develop, and demonstrate innovative tools and technologies to prevent, detect, and mitigate** a cyber incident in today's energy delivery systems and transition to the energy sector.

3.2 **Research, develop, and demonstrate game-changing cybersecurity tools and technologies** that: anticipate future energy sector attack scenarios and design cybersecurity into emerging energy delivery system devices from the start; and make future systems and components cybersecurity-aware and able to automatically prevent, detect, mitigate, and survive a cyber incident.

3.3 **Build strategic core capabilities** in the National Laboratories and **build university collaborations** dedicated to advancing cybersecurity for energy delivery systems.

Putting Goals and Objectives into Action

The DOE Plan is designed to achieve tangible, actionable improvements in energy sector cybersecurity where they are needed most. DOE has a robust portfolio of dozens of targeted activities and RD&D projects now underway to achieve the broad goals and objectives outlined in the Plan. Specific activities are described under each objective, and Appendix C presents past and current RD&D projects. Three selected examples below demonstrate how the Plan's goals and objectives translate into actionable projects that get results.

Goal 1: Strengthen Energy Sector Cybersecurity Preparedness

Objective 1.2: Develop and improve tools for bi-directional, real-time, machine-to-machine information sharing

CRISP (Cybersecurity Risk Information Sharing Program)

CRISP provides energy sector owners and operators with a **capability to voluntarily share cyber threat data in near-real-time, analyze this data using U.S. intelligence, and receive machine-to-machine threat alerts and mitigation measures**. Using technologies originally developed to defend DOE's networks, CRISP helps companies identify malicious traffic within their IT systems by analyzing the data streams and enhancing the analysis with classified DOE intelligence and cyber tools.

CRISP delivers cyber alerts and mitigations directly to affected companies and broadly to the energy sector. This voluntary program is now managed by the Electricity Information Sharing and Analysis Center (E-ISAC) with the goal to create a sustainable program owned and operated by the private sector enabling near real-time data sharing and analysis. **CRISP's 26 participating utilities account for 75% of U.S. electricity customers**.

This Plan includes activities to expand energy sector participation in CRISP and advance CRISP analysis capabilities through OE's Cyber Analytics Tools and Techniques (CATT) project. The Plan also seeks to expand CRISP capabilities to analyze and share threat indicators in *operational technology* systems by piloting real-time OT data sharing and analysis with four utilities in OE's Cybersecurity for the OT Environment (CYOTE) project.

Goal 2: Coordinate Cyber Incident Response and Recovery

Objective 2.1: Establish a coordinated national cyber incident response capability for the energy sector

Technical Capabilities to Augment Cyber Mutual Assistance

OE is working with the DOE National Laboratories to **develop an integrated mix of specialized cyber resources and capabilities that can be deployed during a cyber incident** to help energy companies identify and respond to a cyber attack. Each lab is expanding technical capabilities in specific topic areas to build an integrated Energy Cyber Resource Partnership. This partnership's robust incident response capability will support DOE's mandate to provide cyber-specific technical expertise and assistance to support energy sector response during a cyber incident and restore or maintain critical functions.

Goal 3: Accelerate Game-Changing RD&D of Resilient EDS

Objective 3.2: Research, develop, and demonstrate game-changing cybersecurity tools and technologies

Automated Defense Techniques for Next-Generation Systems

ABB is leading a research partnership to **enable high-voltage DC systems to detect and automatically reject commands that could destabilize the grid** if implemented. Using the physics of the grid, the capability will anticipate how the grid would react to a received command—rejecting commands that would jeopardize grid stability while executing legitimate commands in time. The project builds on a prior OE RD&D project, which successfully demonstrated the capability in transmission-level AC systems. This technology allows the grid to continue functioning during a cyber attack and prevent or limit energy disruption.