CEATI

MANAGING CYBER SECURITY RISK AND A REVIEW OF PROTOCOLS USED IN DISTRIBUTED ENERGY RESOURCES

Overview

Cybersecurity has become increasingly important for utility and other stakeholder interactions with Distributed Energy Resources (DER).

This report addresses the key cybersecurity issues posed by the DER systems to grid resilience risks and provides recommendations for mitigating these risks. It provides insight into different types of DER architectures for communication media and protocols used by well-established utilities for interaction with the DER facilities in the system and offers good examples and reference guides to help utility personnel improve their current practices.

Infastructure Protection and Security Interest Group

Published: May 2021

How to use this research

This report facilitates important points showing the use of managing cyber risks on DERs and can help utility professionals to:

- Identify threats and vulnerabilities posed by DER systems that could impact the grid lines.
- Identify the need for including cybersecurity in cross-organizational contracts between stakeholders and discuss the potential future technologies and capabilities of DER systems
- Develop methods to minimize cyber security risks
- Develop effective cyber security communication protocol.
- Manage the risk of crucial cyber assets to be protected from failure scenarios

Key questions Addressed

- What are the key cyber security risks imposed on utilities that utilize DERs?
- What are the relevant Cybersecurity standards and guidelines for DER systems?
- What are the threats, vulnerabilities, and impacts on DERs?
- What are the primary recommended risk assessment and mitigation techniques utilities should apply?
- What is the vision of DER and Cybersecurity for the future?

Research Summary

This report addresses the cybersecurity issues posed by DER systems to grid resilience and provides recommendations to utilities to minimize the risks of such cyber events. It covers different DER types and architectures, describes typical communication media and protocols used by utilities for interactions with DER facilities, and identifies different threats and vulnerabilities posed by DER systems. It also discusses key cybersecurity measures such as role-based access control, communication protocol security, and coping methods for the inevitable security attacks.

Additionally, it identifies the need for including cybersecurity in cross-organizational contracts between stakeholders and discusses the potential future technologies and capabilities of DER systems, including possible future national or regional cybersecurity requirements.

The report covers following focus areas:

1. DER Communications Protocol Categorizations with Focus on Cybersecurity: – History of DER, recent changes, protocols, cybersecurity overview.
2. Cybersecurity Issues and Recommendations for Typical Existing Architectures of Power Systems with DER – Typical DER architectures, IEEE 1547 grid codes, communication networks, cybersecurity for DER.
3. Cybersecurity Issues and Recommendations for Possible Future Architectures of Power Systems with DER – Progress toward carbon-free states, the future power system vision, communication technologies, cybersecurity issues, and challenges.

Since cybersecurity for utility-DER interactions is still in its infancy, participation by utility power systems experts and cybersecurity experts in developing cybersecurity standards are crucial to progress toward well-vetted, targeted, and relevant cybersecurity requirements.

Cybersecurity measures require both engineering and cyber approaches to best meet these challenges. It is an ongoing battle that will not be won anytime soon. Utility experts could help develop guidelines for topics and contents that should be included in these cross-organizational contracts.

About CEATI Research

CEATI facilitates the planning and implementation of collaborative R&D projects among its electric utility members. This approach enables members to solve shared challenges and maximize their return on investment.

Get the Full CEATI Report

CEATI Infrastructure Planning and Security group members can access the report here.

If you're interested in joining the Infrastructure Planning and Security group to access the full report as well as additional research, expert guidance, networking events, and more contact us today at https://ceati.com/membership