

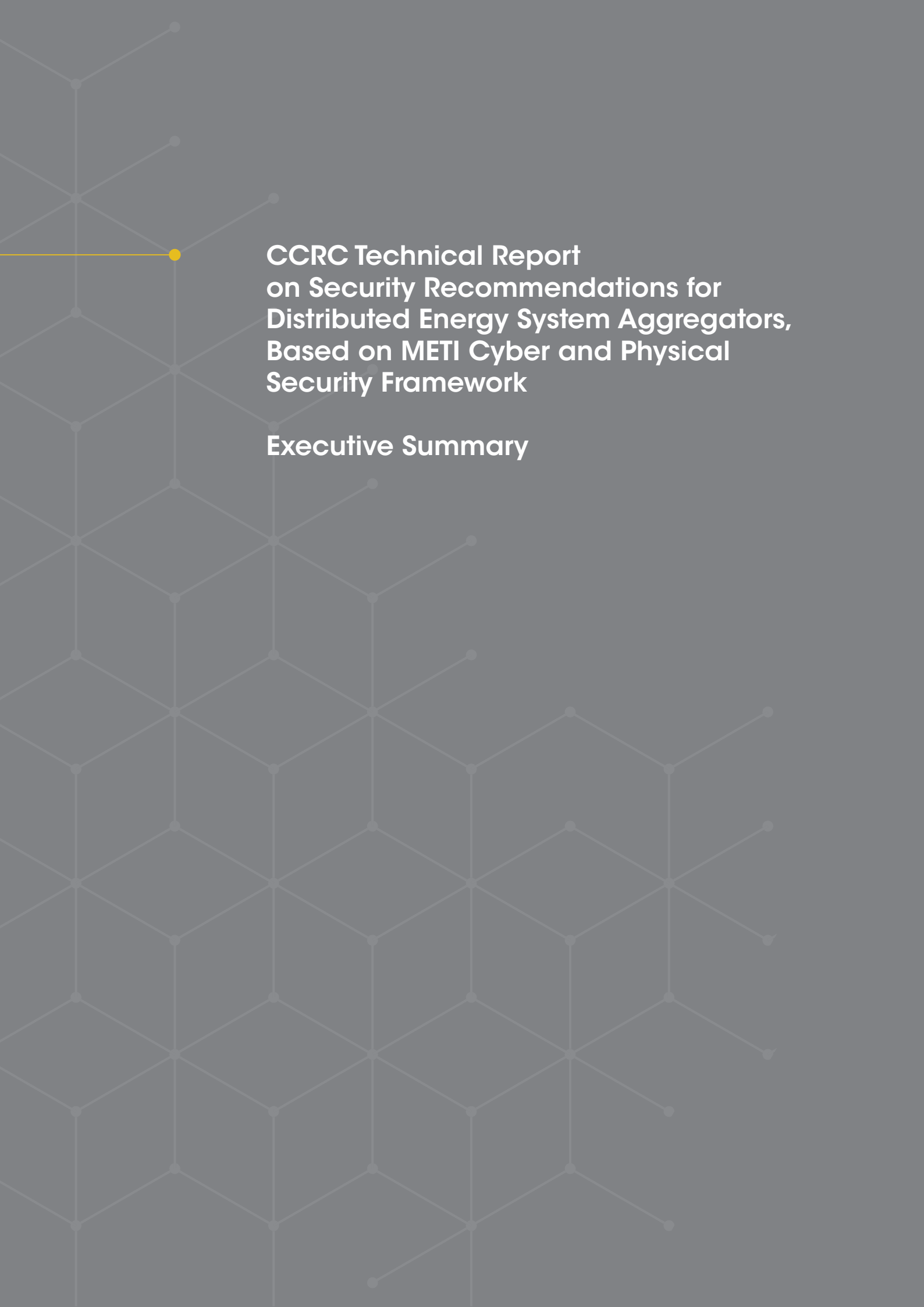
CCRC Technical Report

on Security Recommendations for Aggregators
with Distributed Energy Resource System,
based on METI Cyber and Physical
Security Framework

Executive Summary

September 2021

Keio University Cyber Civilization Research Center
Keio University Research Institute at SFC



CCRC Technical Report on Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework

Executive Summary

CCRC Technical Report

The market for alternative power generation is continuing to grow for both renewables and combined heat, power, and battery storage, thus creating an opportunity for demand response and ancillary services via Distributed Energy Resources (DERs). DERs have been in use throughout the world, are parallel to the electric grid, and typically operate in the 3 KW to 75 MW range. In concept, these systems provide both supply and demand shaping capabilities that lower the cost of handling peak loads and create a more fault-tolerant and robust electrical power grid with simplified central generation and storage requirements. In addition, building physical infrastructure around distributed availability of renewable energy sources also provides the potential for meaningful environmental benefits.

Virtual Power Plants (VPPs) represent distributed energy resources that collectively participate in the electricity market or related aggregation markets. Control and management of such systems will necessarily involve secure cloud-based coordination of various mission-critical devices such as power supply facilities, fixed and mobile batteries, sensors, smart meters, and other energy management systems. Effectively scaling DERs will present significant logistical and security challenges. Both residential and commercial devices will be required to communicate securely and with extremely low latency to effectively satisfy their missions. In DER systems, regulators, designers, installers, and operators must work together to ensure that all DER network elements are properly authenticated and securely communicate to ensure both smooth DER performance and safeguard the networks they operate on. The successful widescale rollout of DERs will present a significant challenge to the mindset of energy companies, which historically are accustomed to operating closed (and often proprietary) networks that by design require less security than networks operating jointly and/or involving the public cloud.

Nearly all organizations are struggling today with the unprecedented growth of the Internet of Things (IoT) devices that are potentially vulnerable. As a result, DER networks must be

designed to safely isolate their network elements while minimizing the overall impact on the network, consumers, and business partners when breaches do occur. In other words, DERs should be designed to assume breaches will in fact occur and that their impact will be both minimal and within the design tolerances for the overall DER mission. This is particularly important because breaches of DER security could disrupt the broader energy grid, having consequences such as the failure of life-sustaining medical devices and exposure of information related to consumers, like their location and when their homes are vacant.

The challenges of implementing secured VPPs will only scale up in complexity over time. Implementation is currently in the early phases, with an experimental VPP pilot carried out in a Lawson stores in 2019. In the future, it may be possible to leverage the high-capacity lithium-ion batteries found in Electric Vehicles (EVs) to further extend DERs both for demand-shaping and supply-storage—a capability that will only become more important in cities as electric vehicles become more widespread.

Standardization of security protocols in hardware and software engineering is critical to the implementation of VPPs. The Cyber and Physical Security Framework presented by the Japanese Ministry of Economy, Trade, and Industry aims to align the implementation of DER devices with international standards for the configuration of products and services within the global supply chain. The requirement for trust in organizing, implementing and securing DER systems informs the creation of a multi-tiered approach to gaining trustworthiness.

First, organizational certification based on ISO/IEC 27001 validates the trustworthiness of management between organizations for shared security policies. The second layer, including construction and maintenance, aims to establish the trustworthiness of transcription between physical events and data. Finally, the third layer focuses on the secure transfer of data within cyberspace. Layers of trust are necessary, as even with standardization of device protocols, a network of distributed devices is subject to physical tampering and specific attacks.

In a classic example of IoT security challenges, the United States retailer Target had its point-of-sales systems breached in 2013 via its remotely controlled Heating, Ventilation, and Air Conditioning (HVAC) controllers due to insufficient network compartmentalization and inadequate monitoring. DERs and aggregators must create firewalled subnets or Virtual Local Area Networks (VLANs) to isolate and safeguard both DER elements and the host networks they operate on (or transit through). In addition, DER access patterns and data usage should be monitored for anomalies (indicating attempts to breach secure parts of the network), connectivity patterns (indicating denial-of-service attacks), or anomalous outlier data (indicating tampering with sensors or metering). To implement these recommendations in a manner that safeguards both public trust and grid operation, DER operators must ensure the network segments their equipment operates on (whether commercial or consumer) adhere to basic security guidelines such as being isolated via VLANs and being sufficiently monitored for alerts in network breaches. Given the increasing presence of potentially highly vulnerable IoT devices, DER operators should take extra care to ensure that their network elements are safely segmented from them.

Although many of the security, authentication, and network best practice recommendations in this paper follow international standards, they are not novel or revolutionary. Instead, the challenge is in implementing them at scale while driving adoption by industry in a manner that matches consumer behavior. With these challenges met, DERs and the VPPs will enable a future that offers a cleaner, greener, and (if implemented properly) more robust and resilient power infrastructure.

About Keio University Cyber Civilization Research Center
Keio University has long been a bold leader in integrating a rich Asian tradition with modern technology. Keio's mission is to pioneer the development of emerging technologies while safeguarding their establishment, benefits, and adoption by society. The university is located in a highly developed democracy in Northeast Asia that is technologically robust, open, diverse, and accessible.

The Keio University Cyber Civilization Research Center (CCRC) is comprised of a cross-disciplinary team of researchers that explores the risks and benefits posed by technological advancements, analyzes their expected societal impact, and devises tools and methods to support effective future planning. CCRC researchers also actively participate in developing and managing technologies that foster trust among diverse user communities and reflect social awareness. To ensure the delivery of equal, inclusive, and meaningful contributions in support of this pivotal and pioneering field of research, the Center engages local and global actors in collaborative discussions and exchanges.

Starting in 2019, the Keio Research Institute at SFC (KRIS), and CCRC, in partnership with the Lawson convenience store chain, designed and operated a prototype DER with Virtual Power Plant capabilities at Lawson's Keio University campus store.

