United Nations ECE/ENERGY/GE.6/2023/3–ECE/ENERGY/GE.5/2023/3

Economic and Social Council

Distr.: General
27 July 2023

Original: English

Economic Commission for Europe

Committee on Sustainable Energy

Group of Experts on Cleaner Electricity Systems
Nineteenth session
Geneva, 3-4 October 2023
Item 7 of the provisional agenda
Reliability and cyber resiliency of smart integrated energy systems

Group of Experts on Energy Efficiency
Tenth session
Geneva, 5-6 October 2023
Item 6 of the provisional agenda
Digitalization and energy system resilience

Key considerations and solutions to ensure cyber resiliency in the smart integrated energy systems

Note by the secretariat

Summary

Digitalization, as the application of digital technologies and business models for existing processes, is gaining more attention as a way to support and complement the energy transition. However, integration of different energy sources and interconnection of various energy system components which constitute smart integrated energy systems, involve exchange of large amounts of data that increases the exposure to cybersecurity risks.

This document was developed on the platform of the Task Force on Digitalization in Energy, by the Group of Experts on Energy Efficiency and the Group of Experts on Cleaner Electricity Systems in line with their respective Work Plans for 2022-2023 and in recognition of the growing information security threats amid increasing digitalization of the energy system. The Task Force on Digitalization in Energy further recognizes the importance of collaboration across all subsidiary bodies of the Committee on Sustainable Energy in the effort to address aspects specific to various elements of the energy value chain.

The document contains an overview of the subject, identifies, and categorizes the types of cyberattacks on the exposed energy system components and their possible consequences, and concludes with a set of managerial- and technical-level measures and policy recommendations to mitigate the cybersecurity risks.

Mention of any firm, product, service or licensed process does not imply endorsement or criticism by the United Nations. The designations employed do not imply the expression of any opinion whatsoever on the part of the United Nations Secretariat concerning the legal status of any country, territory or area, or of its authorities.

I. Introduction

1. With the increasing integration of intermittent renewable energy sources, energy surplus and shortage events occur more often. In response to such a reliability challenge, a concept of 'smart energy systems' that integrate various energy sources and energy storage and provide opportunities for an active role of the prosumer, evolve.[1]

2. Apart from integrating different energy sources, these smart systems contain various connected components, which enable gathering detailed and real-time data about energy production, transmission, distribution, and consumption, as well as analysis of this data with such tools as Artificial Intelligence (AI) providing new insights that drive better forecasts and decision-making support in planning, operations and maintenance. Because of this multi-way inter-connection, a more digital and intelligent system is available, therefore called "Smart Grid". Such systems can be either single directional (where data is collected without a feedback loop), or bidirectional (where the collected data is analyzed and used to control, operate, and/or manage specific equipment or devices). Also, smart integrated energy systems can coordinate the needs and capabilities of all generators, grid operators, end users and electricity market stakeholders. Thus, enabling the operation of the system at maximum efficiency, reliability, resilience, flexibility, and stability, while minimizing costs and environmental impacts while maximizing system.

3. With a higher level of digitalization and intelligence, different solutions can be provided, including demand side management, peaks shaving (prioritizing energy consumption during low demand periods), and energy storage of surplus energy. Also, digitalization allows predicting energy flow and provides an opportunity to change the energy supplier, consumer, and prosumer behavior via taxation, pricing signals, or policies.

4. While using a smart integrated energy system has many advantages, it also causes challenges. One of these challenges is the increased exposure to risk of cybersecurity attacks. This is an inherent consequence of going from separated physical devices to intelligent devices and integrated equipment connected over networks.

5. In general, the goal of cyberattacks is to take control of the system and/or of the data, and/or damage physical equipment, thus causing reputational damage to, or diminishing trust in an entity. This means that in the context of the smart integrated energy systems, the goal is to take control of the energy system in a way that would impede its ability to deliver energy.

6. The increase in the number of devices makes cybersecurity attacks more likely. This is because sensors, relays, machine controls, controls, etc., all have different attack surfaces. The attack surface is the sum of all entry points that hackers can use to control the system, including the network used to connect its components. In the case of a smart integrated energy system, the attack surface includes at least components related to energy production, transportation, energy transmission and distribution network, energy storage devices, energy consuming devices, and a digital communication network.

A. Cybersecurity attacks on smart integrated energy system components and their example consequences

7. As the energy system is identified as a critical infrastructure and energy is the backbone of the society, consequences of cyberattacks can be far-reaching, including economic, social, and environmental consequences. A few recent examples of ransomware cyberattacks on critical infrastructure, resulting in temporary shutdowns and data loss, show a growing trend: while, ransomware attacks nearly doubled in 2022, only last 6 months of this year witnessed a 35 per cent increase of ransomware groups that impacted industrial infrastructures and a 53 per cent increase of malware and viperware.[2]

[1] GEEE-7/2020/INF.3 (https://unece.org/sites/default/files/2020-12/GEEE-7.2020.INF_.3.pdf).

[2] Fortinet, *Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs* (February 2023).

8. This trend is not surprising considering that preventing cyberattacks and mitigating the consequences is not a simple task; moreover, cybersecurity is often neglected from design to operations whereas smart integrated energy system has a huge attack surface. The exposed components of the smart integrated energy system used for energy generation, transmission, distribution, are presented in Table 1.

Table 1
Some components of the smart integrated energy system used for energy generation, transmission, distribution, and use

Generation	*Transmission*	*Distribution, distributed energy resources, and customers*
Equipment monitoring Control Systems Protection devices (relays, etc.) Recorders Interfaces to energy management system, to supervisory control and data acquisition system, to maintenance console, etc.	Optical transformers Equipment monitoring Protection devices (relays, etc.) Phase measurement units Control systems Recorders Interfaces to energy management system, to supervisory control and data acquisition system, to maintenance console, etc. Substation automation Remote terminal units	Advanced metering infrastructures (smart meters) Automation (automatic reclosure, feeders, etc.) Protection devices Mobility devices Monitoring and control of: • Solar panels • Batteries (storage) • Electric vehicle and charging • Smart buildings • Microgrid Load management Customer interaction

9. These connected and intelligent devices, servers, computers, and systems used in the smart integrated energy system contain different parts that can all be potentially attacked in ways exemplified below:

(a) Servers: by using services that should not be available to the outside world, by exploiting outdated software that has known vulnerabilities, by exploiting insecure configuration settings such as default passwords, and by gaining unauthorized access to sensitive data;

(b) Networks: by bypassing authentication, by overloading the network so that normal functioning is impaired, by exploiting insecure configuration settings such as weak encryption, and by gaining unauthorized access to communication data of other users;

(c) Websites: by using functionalities that should not be accessible, by exploiting known vulnerabilities, by exploiting insecure configuration settings such as default passwords, by gaining unauthorized access to sensitive data such as the underlying database or unencrypted communication, by gaining unauthorized access to the underlying server, by attacking other users, and by uploading malware;

(d) Mobile applications: by using functionalities that should not be accessible, by exploiting known vulnerabilities, by exploiting insecure configuration settings such as default passwords, by gaining unauthorized access to sensitive data such as the underlying database or unencrypted communication, and by gaining unauthorized access to the underlying mobile device;

(e) Software and firmware: by bypassing authentication, by exploiting known vulnerabilities, by exploiting insecure configuration settings such incorrect right management, and by gaining unauthorized access to sensitive data such as source code;

(f) Webservices: by exploiting known vulnerabilities, by exploiting insecure configuration settings such as authentication without password, by gaining unauthorized access to sensitive data such as data from other users, and by gaining unauthorized access to the underlying server;

(g) Clouds: by obtaining unauthorized access to data from other users such as files, by gaining unauthorized access to the underlying server, by exploiting insecure configuration settings such as authentication by guessing a password, by gaining unauthorized access to sensitive data such as passwords or access keys, and by exploiting known vulnerabilities;

(h) Sensors, motors, relays, etc.: by exploiting known software vulnerabilities, by exploiting insecure configuration settings, by tampering with data sent by a sensor/motor/relay/etc, by manipulating a sensor's/motor's/relay's etc functionality, by making the sensor unavailable, and obtaining unauthorized access to data;

(i) Hardware: by manipulating the hardware, by adding malicious hardware in the network, by attacking interfaces that are made available for finding problems, and by manipulating transferred data;

(j) Users: by malicious emails such as phishing emails that invite readers to provide sensitive data or attachments with malware, by scaring people so that they are triggered to perform an action that harms them unnoticed, by disinformation activities to provoke them to sharing sensitive information.

10. Many other types of attacks are potentially possible. These can be categorized into four types:

(a) Physical attacks (on the physical components of the system),including:

(i) Physical damage: attacking a component causing physical damage, or its inappropriate or non operation;

(ii) Social engineering: deceiving and manipulating individuals into sharing sensitive information that can be used for further attacks;

(iii) Node tampering or malicious node injection: a node in the smart integrated energy system is a part that connects a physical device to the Internet and is responsible for collecting, processing, and/or controlling data. Tampering sensitive data means not only reading but also changing it. This can be achieved by attacking an existing node, but also by adding a new node.

(b) Software attacks (on computer programmes that are executed by physical devices in the smart integrated energy system), including:

(i) Malicious scripts: adding to existing software so that the latter contains additional, harmful functions, e.g., to steal login data;

(ii) Malware: installing software, which can support all kinds of harmful activities, e.g., spyware to steal data, viruses to damage or change files and/or data, viperware to wipe data and software, and ransomware to encrypt data;

(iii) Denial-of-service: a denial-of-service (DoS) attack makes the software or device unavailable, e.g., by overloading the software or shutting it down. If such an attack is performed from many computers at the same time, it is called a distributed denial-of-service (DDoS) attack.

(c) Network attacks (gaining unauthorized access to, and perform unauthorized actions in the network), including:

(i) Traffic analysis: gaining knowledge from characteristics of a data flow that can be observed, even when the content of the data flow remains hidden;

(ii) Routing information: intercepting, changing, and/or redirecting data sent through the network to a different destination, e.g. to monitor or steal data, or disrupt the energy system service delivery;

(iii) Sinkhole: a harmful node in the grid sends bogus messages to other nodes and tricks these nodes into sending information to the harmful node;

(iv) Unauthorized access: getting access to the network without having permission.

(d) Encryption attacks (circumventing the security by adding encryption, which requires a key to turn the code back into readable information or data), including:

(i) Cryptanalysis: aiming at finding out what information or data is encrypted, without knowing the key;

(ii) Side-channel: using information that is unintentionally provided by a computer system when doing cryptographic operations to gain access to encrypted information;

(iii) Man-in-the-middle: positioning between two communicating components, so that encrypted messages can be eavesdropped and even changed.

11. Oftentimes, different types of cyberattacks can be observed at once, therefore overlapping challenges and disruptions to potential victims. Additionally, cyberattacks can also complement other types of physical attacks.

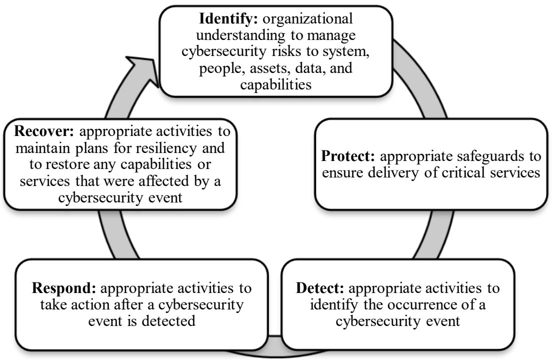
B. Measures for preventing cybersecurity attacks on smart integrated energy system components

12. As the smart integrated energy system is part of the critical infrastructure, preventing cyberattacks is essential. And when attacks nevertheless take place, the consequences should be mitigated. To do so, multiple solutions should be implemented to form an overall, unified strategy, sometimes referred to as "defense in depth".

13. Many frameworks and standards, such as National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure and International Electrotechnical Commission (IEC) 62443 Series[3], provide good starting points for development and implementation of efficient cybersecurity programmes.

14. For example, the NIST Framework details a list of activities categorized around five core development and implementation functions (Figure). It would also cover resources (human, material, and financial), oversight (governance), processes, and technology.

Figure
NIST framework



Identify: organizational understanding to manage cybersecurity risks to system, people, assets, data, and capabilities

Protect: appropriate safeguards to ensure delivery of critical services

Detect: appropriate activities to identify the occurrence of a cybersecurity event

Respond: appropriate activities to take action after a cybersecurity event is detected

Recover: appropriate activities to maintain plans for resiliency and to restore any capabilities or services that were affected by a cybersecurity event

Source: adapted from NIST, "NIST Releases Version 1.1 of its Popular Cybersecurity Framework" 16 April 2018.

15. Also, prevention, mitigation, and recovery should be done on a management level and on a technical level (Table 2).

[3] ISA/IEC 62443 series of standard, Automation and Control Systems Cybersecurity Standards.

Table 2

Some prevention, mitigation, and recovery activities for cybersecurity programmes

Level	*Prevention*	*Mitigation*	*Recovery*
Management (top-down): policies and regulations inform the workforce *	(i) Risk management: involves identifying digital assets, whereas a digital asset is anything digital that is valuable, such as files with photos, videos, audio files, and text. (ii) Asset management: reviewing existing security measures and implementing additional measures. (iii) Update or patch management: as outdated software increases the attack surface of software, update management regulations should inform administrators about installation and deployment of updates. (iv) Cybersecurity systems: firewalls can be used to control incoming network traffic based on predefined security rules, thus ensuring only authorized access to the network or network segment. Network Access Control NAC ensures that only users who are authenticated and devices that are authorized and compliant with security policies can enter the network. (v) Network segregation: i.e., separating networks, especially a critical network from the Internet and other less critical networks such as administrative networks, thus making it is less likely that unauthorized access to a critical network is obtained. (vi) Access management (including authentication and key management): usernames and passwords, as well as other authentication means such as keys, shall be stored and managed (involves generating, distributing, storing, and updating). To make sure that different parts of the smart integrated energy system work together, the authentication methods have to match. Which method is most suitable depends on different factors such as scalability and security. (vii) Code attestation and code analysis: code attestation means checking the integrity of the software and ensuring that it has not been tampered with. Code analysis means checking the quality of code and making sure the code does not contain security issues that can potentially be used by attackers. A zero-trust approach is another possible solution to secure a system. (viii) Device and software security: the security of components of a smart integrated energy system needs to be tested, for example by performing a penetration test. (ix) Cryptography: to make sure that data can be exchanged securely and remains hidden from unauthorized access. To transform data into unrecognizable codes, different algorithms and methods can be used depending on the security criteria and context. Also, the strength of the algorithm is important in this context.	(i) Intrusion detection system: to continuously observe a system and look for anomalies. Anomalies can take many different forms, for example an unusual number of login attempts for an account, an unusual amount of network traffic from a computer, an additional device in the network, etc. If an anomaly is detected, it is isolated. Or when an unusually high amount of traffic is sent by a computer, this computer is blocked. Often, network administrator is informed about the anomaly, so that further appropriate measures can be taken. As false alarms are possible, machine learning and artificial intelligence can be used to improve detection. (ii) Data loss prevention techniques: these are used when a virus tries to use or send confidential information. The goal of these techniques is to prevent information loss and prevent obtaining data that is affected by a virus. This can be done by isolating an infected device or	Can be specified in regulations based on these standards, include recovery planning which includes processes and procedures to be executed to ensure restoration of systems or assets affected by a cybersecurity incident. These shall be used as part of business continuity management to revert to normal operations as soon as possible.

* Note: The types of prevention and mitigation strategies should be specified. These prevention and mitigation strategies should preferably be documented in regulations. For example, such regulation can be implemented in the context of the IEC 62443 Series and the ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity standard (https://www.iso.org/standard/44375.html). The first addresses cybersecurity for operational technology in automation and control systems, and the latter focuses on protecting sensitive data, systems, and online operations and activities from being hacked, sabotaged, or modified. When taking security at a higher level, to the information level, the ISO/IEC 27001:2022 Information security management systems standard (https://www.iso.org/standard/27001), which helps organizations manage their information security by addressing people, processes, and technology, could be implemented.

Level	*Prevention*	*Mitigation*	*Recovery*
	(x) Awareness: e.g., live hacks in which it is shown how hackers attack different components, might be an important part of cybersecurity culture or hygiene. They can not only be used to teach technical staff but also non-technical staff what they can do to improve cybersecurity. (xi) Cybersecurity programme and culture: providing organizations the confidence that all aspects of cybersecurity are covered taking account of any the economic, societal, and environmental risks. (xii) Use zero-trust strategy based on the idea of "never trust, always verify," which means that users and devices should not be trusted by default, even if they are connected to a permissioned network.	blocking access from unauthorized devices.	
Technical (bottom-up): identified issues are reported to the management, providing feedback so that improving policies and regulations	(a) Code analysis (when possible as it may not be possible for all operational devices): code analysis means analyzing the source code of an application for vulnerabilities. This analysis can be static or dynamic. Static code analysis means that the security analyst has full access to the source code and looks for vulnerabilities in the lines of code. In dynamic code analysis, the analyst does not have access to the source code and instead executes the computer program. During execution, the program can be scanned for vulnerabilities. (b) Vulnerability scanning: vulnerability scanning involves automatically assessing security issues on systems and the software that is executed on these systems. These scans are helpful to identify possible entry points that attackers can use to enter a system and potentially use as a stepping stone for further attacks. (c) Penetration test: a penetration test is an authorized cyber attack on a network, system, device, or software with the goal of testing the security level of the tested object. The goal of these tests is to find a wide range of security issues. (d) Red teaming: red teaming is like a penetration test, an authorized cyber attack. The main differences are that the scope of the test is usually wider, such as a company, as the goal is to find an exemplary way of the far-reaching consequences of a cyber attack as opposed to identifying a wide range of security issues.	Security operation centre: A team of security professionals that monitors an organization's entire information systems infrastructure, to detect cybersecurity events in real time and address them as quickly and effectively as possible. It selects, operates, and maintains the organization's cybersecurity technologies, improves threat detection, security posture, response, and prevention capabilities by coordinating all cybersecurity technologies and operations. To perform its functions, it analyses data from various sources including intelligence shared by authorities and industry, including a Security Information and Event Management (SIEM) system, which analyses behavioural anomalies with artificial intelligence to automatically detect and respond to cyberattacks.	(a) Digital forensics: involves gathering evidence, by identifying, collecting, and analysing data and devices that potentially provide information about cyberattack. It also provides valuable insights on the ways to avoid future cyberattacks. (b) Elimination: Eliminating the source of the incident and rebuilding the attacked system(s) is essential to be able to return them to normal operations (utilizing backups, recovery plans, and business continuity plans).

III. Policy recommendations

16. In view of the foregoing discussion on cybersecurity of smart integrated energy systems, the following conclusions, actions, and policy recommendations are proposed for consideration:

(a) Regulatory: enforcing implementation of applicable standards and guidelines which address matters of improving cybersecurity for operational technology in automation, control systems, and cybersecurity for critical infrastructure;

(b) Financial: offering tax incentives for companies that have implemented relevant cybersecurity standards, and allocating funding for cybersecurity initiatives such as cybersecurity-related research and development and education;

(c) Structural:

(i) Setting up national cybersecurity strategies that: describe how to prevent and manage cyberattacks on smart integrated energy system and; identify roles and responsibilities of different stakeholders, including government agencies, businesses, and individuals;

(ii) Collaborating with other countries to benchmark their standards and share information on potential threat actors to be able to manage cybersecurity risks more effectively;

(iii) Implementing business continuity management plans describing how to manage cybersecurity events, including e.g., those leading to power outages;

(iv) Ensuring proper allocation of responsibilities of cybersecurity in the energy sector (governance) across stakeholders on national and supranational levels.

(d) Reporting: requiring data protection and cybersecurity reporting to official bodies to stimulate bottom-up strategies;

(e) Awareness-raising: identifying industry leaders to lead by example, and providing education and training to support companies and governmental bodies to implement cybersecurity measures on both management and technical levels.