

Cybersecurity survey for power plants and energy storage systems connected to the electric grid

1 Objective

The objective of this survey is to verify that the type B, C and D power plants and energy storage systems connected to the electric grid have a basic level of cybersecurity protection. The transmission grid's reliability is safeguarded by cybersecure operation.

The questions cover all systems of power plants and energy storage systems in general, including the systems for operators and administrators and their connections with the system. (E.g., manufacturers of wind power plants turbines or operators of powerplants with remote control)

Answers should briefly explain the topic in question, without any information that could compromise the system's cybersecurity. Fingrid should receive answers as a text document with no specific format, as part of the documentation process required in grid code specifications (VJV2024: chapter 10.3.6, SJV2024: chapter 10.3.7).

The survey is completed twice. During the planning phase (before the interim operational notice is granted), it shall be described how each item will be considered in the design. After the commissioning phase (before the final operational notice is granted) the implemented solution shall be described.

The questions are based on the document [The Five ICS Cybersecurity Critical Controls /1/](#) by the SANS institute.

2 Questions

2.1 Cybersecurity incident response

- Is there an incident response plan that takes in to account the differences between IT and OT systems?
- Has the plan been practiced?

2.2 Network segmentation and defensible architecture

- Does the plant have a logical or physical separation of its network?
- Does the traffic between the network segments restrict to only permit necessary traffic for the system's function?
- Are all unnecessary network ports and services removed or disabled from all network connected devices?

2.3 Network visibility and monitoring

- Is the plants network being monitored for malicious or unusual traffic?
- Is there an asset inventory of all devices that are connected to the plants network?

2.4 Secure Remote Access

- Is it possible to make a remote connection to the plants network from a remote network?
- Is Multifactor authentication required for making a remote connection?
 - o For Example, is a multi-step authentication required at any point in the login process when the user login themselves to the SCADA system of relevant operator responsible for operations (RO)?
 - o For Example, is multi-factor authentication required at some point in the login process when a user authenticates to the local control system?

2.5 Vulnerability management

- Is there an inventory of the software and firmware versions of all devices connected to the plants network?
- Is there a process to keep track of vulnerabilities affecting these devices?
- Is there a plan for mitigating the risk these vulnerabilities present?

2.6 Account management

- Have the default account passwords been changed from all devices connected to the plants network?
- Do the accounts for users and administrators have different levels of access where feasible?
- Do the user accounts in plants systems have a life cycle that is controlled?

2.7 Reliability of connections to the remotely controlled facility

- How are the control connections of the remotely controlled plant secured in the event of a single fault?
- How long is the operating time for remote connections during a power outage in the regional distribution grid?

2.8 Recovery

- Does the system owner have a plan for recovering from a hardware or configuration failure?
- Does the system owner have up-to-date backups of device configurations?

References /1/ The Five ICS Cybersecurity Critical Controls
<https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/> referenced 2.11.2023