SECURITY ASSESSMENT FINDINGS

IN SUBSTATIONS AND POWER PLANTS

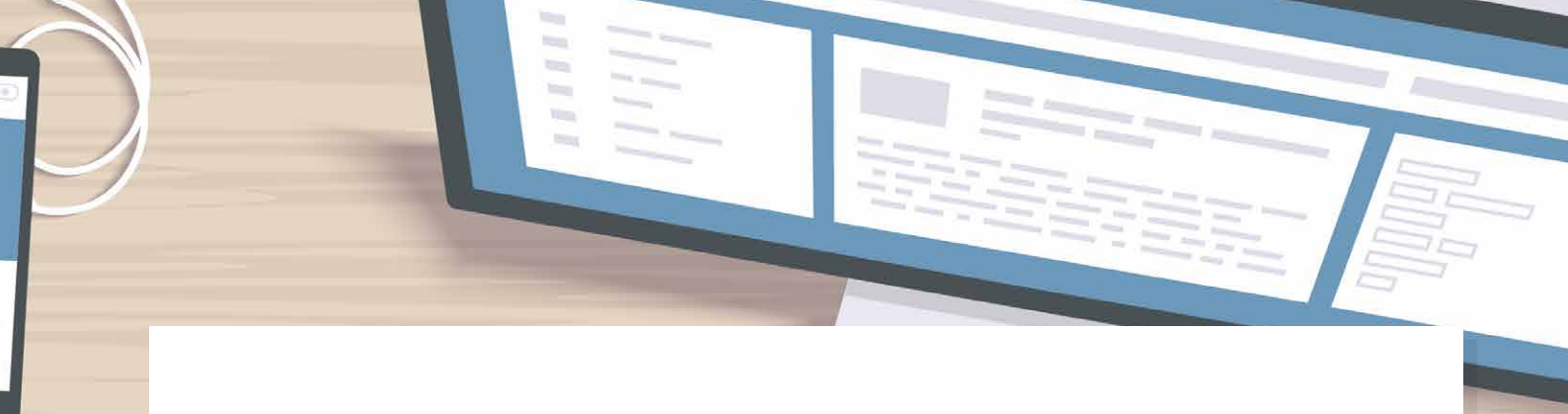
Frequently occurring risks encountered while traveling around the world

About the author

Ozan Dayanc is an OT security engineer, product specialist, and technical support member at OMICRON. He shares his insights about the protection of power utility automation networks, which he garnered assessing OT networks around the globe.

At the end of 2020, I was contacted by a colleague who tasked me with creating a security assessment report for one of our customers using StationGuard our Intrusion Detection System (IDS). I received engineering files from said customer and was familiarized with the utility's network architecture. These documents always constitute the conventional basis for a security assessment before my colleagues and I continue our assessment on-site.

The data from my first security assessment proved highly unexpected to substation engineers and



IT specialists. Among the risks which our assessment brought to light were multiple unnoticed external connections, unexpected devices in the network, outdated firmware, unsuccessful RTU operations, configuration errors, and issues with the network and its redundancy protocol (RSTP).

Since then, we have conducted (and improved on) many security assessments worldwide. In addition to substations, we've also conducted these assessments for power plants and control centers, including utilities with IEC 61850, IEC 60870-5-104, DNP3, Modbus TCP/IP, and many other IT protocols.

The findings from our security assessments were always interesting and, sometimes, alarming. In the following text, I've highlighted some frequently occurring risks that I have encountered in recent years:

Are you interested in our security assessments? Scan the code or message us at

✉ info.puc@omicronenergy.com

OUTDATED FIRMWARE

with known vulnerabilities

In every security assessment, I come across outdated firmware versions. As part of our assessment, we provide a passively discovered asset inventory to the utility engineers and IT experts. We augment the asset information by importing engineering files with more details, like the software version, hardware configuration, and serial numbers.

This asset inventory is a sound basis for performing vulnerability and risk analysis.

EXTERNAL CONNECTIONS

Power plants and control centers with remote connections from the corporate IT network always have the highest risk of a cyberattack. While assessing a Latin American substation network, we captured the activity of multiple clients with external IP addresses. This utility allowed their engineers to connect and configure IEDs from home using a remote connection (VPN tunnel). One finding that concerned the IT security officers was an IP and a MAC address which weren't recognized or documented by anyone in their team. Eventually, we could track the IP address and find where this connection originated from and blocked its access to the system.

Pay closer attention to potential security risks by making all connections in your network visible.

UNUSED SERVICES

Open/unused services offer a disproportionate increase of opportunities for hackers to attack your automation or SCADA system. Thankfully, we can easily detect these unused services through network monitoring. Here are some common unused services we found during our assessments:

- IPv6: Mostly activated on PCs, sometimes on IEDS. IPv6 was never actually used but provided several attack vectors in the network.
- Windows file sharing: The file sharing service was always activated on PCs and Windows-based RTUs and Gateways, but not used.
- PTPv2: It was enabled by default on some industrial switches, even if it has never been used.

Simply turning off these open/unused services will decrease the number of cyber risks to your assets.

DETECTING CONFIGURATION CHANGES

In a North America substation, we detected misconfigured GOOSE messages. This problem occurred because two individual engineering parties configured the devices. In turn, this lack of communication between engineers caused communication problems between these OT devices. We discovered that certain remote command activities in the substation didn't function properly due to invalid interlocking conditions. This means they wouldn't have been able to operate their switchgears remotely in urgent scenarios.

This case showed me that minor GOOSE communication issues could cause more significant plant problems. Therefore, we still offer these basic security assessments for free, allowing us to contact other power plants, substations, and control centers to further our knowledge.

SCADA COMMUNICATION CONFIGURATION ERRORS

Misconfiguring RTU and SCADA devices can slow down communication and might result in failed transmissions for critical on-site events. For example, in a European substation, MMS Reports were configured to be sent to the wrong client IP address. After resolving these configuration errors, there was a verifiable improvement in the IED's communication speed.

Checking impeded communication speed will lower the operational risk of obstructed response processes.

MOST FREQUENT SECURITY RISKS

in plant networks

Undocumented external connections accessing IEDs & switches directly
Outdated firmware with known vulnerabilities
Unused services
Unauthorized access

Usually, these security problems are fostered by functional problems, such as:

Configuration issues in IEDs, RTUs, and network switches
Time synchronization failures
Network redundancy issues