HOW TO FRUSTRATE HACKERS

Network intrusion detection with functional supervision

by Yann Gosteli, Centralschweizerische Kraftwerke AG, Switzerland

An effective security concept for substations not only covers physical access control and firewalls, but it also monitors what's going on across the station network. Since cyberattacks can cause significant energy supply problems, the Swiss utility Centralschweizerische Kraftwerke AG (CKW) has implemented a series of measures designed to improve the security of its future substations.

The infrastructure that supports the supply of energy is critical, so it is becoming an increasingly attractive target for cyberattacks. If hackers are able to quietly take control of a substation or parts of its equipment, the consequences for network operations and the supply of entire cantons in Switzerland are potentially very serious and may even affect essential infrastructure. This calls for effective cyber security measures not only in the network control center, but also in the substation itself.

Swiss quality standards

Therefore, at CKW we have been paying very close attention to the subject of security in substation automation, control and protection technology. We placed a great deal of emphasis on maintaining a high level of cyber security during the planning phase of the new substation concept. It will be deployed for the first time when the new substation in Rothenburg goes live in 2020.

As we are well aware of the responsibility placed on us in this area, CKW is also a member of the VSE (Verband Schweizerischer Elektrizitätsunternehmen [Association of Swiss Electricity Utilities]) group, which published the "Handbuch Grundschutz für 'Operational Technology' in der Stromversorgung" [Handbook on Basic Protection for Operational Technology in Electricity Supply]. We are continually integrating the findings and ideas emerging from this endeavor in our own projects, including the 2020 substation concept. The aforementioned handbook was designed with the entire sector in mind. It describes a defense-in-depth approach for securing operational technology networks. It takes an in-depth look at all of the aspects of the data, information and operational security. This includes creating and implementing zoning concepts, monitoring them and detecting and responding to particular security events. As a utility, monitoring and detection should put us in a position to minimize the impact of an attack on the site.

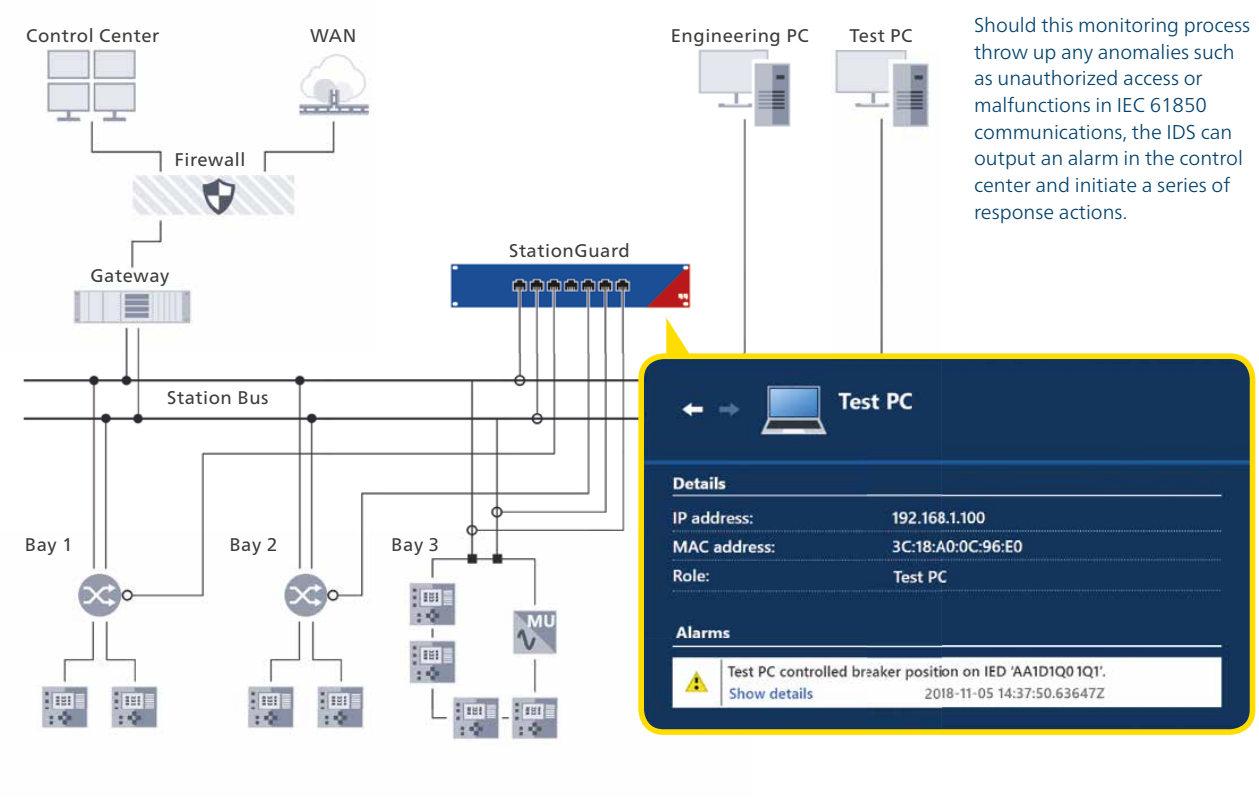
Security by design

The approach we took to designing the network for the substation in Rothenburg was to put a number of layers of defense in place in order to separate individual zones and make it more difficult to attack the process network. In order to do this we took a whole range of security aspects into consideration: IP connections from the substation to the outside world are deactivated during normal operations; remote access connections are only enabled on an on-demand basis; all access to components for support purposes are handled exclusively by special centralized workstations that have been hardened accordingly. This type of access is enabled remotely only when demanded. All other clients connected to the network are also hardened, for example by role-dependent blocking of unnecessary functionalities in the operating system.

We run the SCADA system, the disturbance record collection system and virtual security services on a server in the substation. Control over all access rights to these systems is managed in a dedicated way. This means that each local workstation can only access the systems using remote desktop connections and a local firewall. Users have to log on to these workstations via a central Active Directory (AD), which assigns them the required rights and permissions. In addition, users must log in on every IED in the substation automation system using their personal passwords, after which they are granted the relevant rights from the Access Control (AC) server via Radius. This applies both to having access to devices with engineering tools and controlling the IED display. No standard passwords are used.

«StationGuard is really easy to use. I'm presented with ***all the information I need in a clear and familiar layout –*** *there's no IT jargon at all.»*

Yann Gosteli,
Head of Substation Automation Systems, Centralschweizerische Kraftwerke AG



Should this monitoring process throw up any anomalies such as unauthorized access or malfunctions in IEC 61850 communications, the IDS can output an alarm in the control center and initiate a series of response actions.

The process and support networks are logically and physically separated. Communications using the IEC 61850 Ed. 2 protocol are implemented on a different interface from that used to access devices for engineering or maintenance purposes. The entire process network is segmented, with each segment being separated from the others by a redundant firewall.

We decided to use a data diode to handle the transfer of data from the installation to higher levels of the network. A data diode ensures that no external network traffic can access the installation.

Hacker monitoring within the installation

All of these measures provide a high degree of security, but they cannot prevent a cyberattack with 100% certainty. To cover this eventuality, we were looking around for a monitoring system that recognizes any non-conforming behavior in the network and immediately outputs an alarm. The StationGuard intrusion detection system (IDS) from OMICRON was the perfect solution for our requirements. This IDS has been specifically developed for use in substations and comprises a software solution running on a specially hardened operating system and a similarly hardened hardware platform called RBX1, which we can install directly in the substation, thanks to its rack-compatible dimensions.

During setup, StationGuard creates a system model by automatically reading out the station-specific SCL file (Substation Configuration Language) and then continuously compares it with the events in the substation. Should this monitoring process throw up any anomalies such as unauthorized access or malfunctions in IEC 61850 communications, the IDS can output an alarm in the control center and initiate a series of response actions. All events and alarms are visualized graphically in a way that is familiar to both control and protection engineers and IT specialists. In order to prevent false alarms during maintenance activities, the engineer will inform the IDS in advance about the used test equipment and switch StationGuard to maintenance mode for that session.

With its comprehensive monitoring functions and minimal set-up and support requirements, StationGuard gives us a significant increase in subsation security.