DESIGN AND COMMISSIONING OF A SECURE SUBSTATION NETWORK ARCHITECTURE

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1]OMICRON electronics GmbH, Klaus, Austria (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (stefan.mattmann@ckw.ch)

Keywords: CYBER SECURITY, IEC 61850, INTRUSION DETECTION, SUBSTATION AUTOMATION

Abstract

Utilities and cyber security auditors are increasingly considering not only the control centre as critical attack vector, but also substations as potential entry points for cyber attacks. Important risk factors are the processes, how the commissioning of the protection and control systems are realized and how remote maintenance access is implemented. Therefore, the architecture of the protection and control system must be reviewed for security. To achieve this, the Swiss generation and distribution utility Centralschweizer Kraftwerke AG (CKW) started a project in 2016/2017 to develop a new reference architecture for their secondary systems. Their design addresses these attack vectors with countermeasures, while still offering a sensible balance between maintainability and security. The design includes multiple levels of security including multiple firewall layers. Additionally, an Intrusion Detection System (IDS) is applied. Selecting a suitable IDS for substations proved out to be challenging, as many IDS don't support the requirements of substation networks. This paper starts with an enumeration of the most important attack vectors on substations, followed by a description of the security architecture implemented for the first time in a new greenfield 110kV substation project by CKW. The paper concludes with the experiences in selecting a suitable IDS for substations and the lessons learned in the factory acceptance test of this project.

1. Introduction

1.1. Substation Attack Vectors

We will assume for the remainder of this article a cyber attack on a substation to be an event, where an adversary modifies, degrades, or disables a service of at least one protection, automation, or control device within the substation. To achieve this, an attacker may use one of the attack paths depicted in Figure 1 [1].

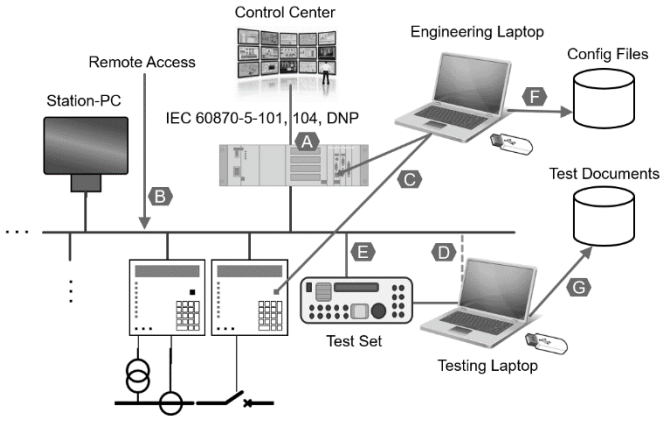

Figure 1 Attack vectors on substations [1]

An attacker could enter through the control centre connection (**A**), as it happened in the first cyber-attack on the power grid in Ukraine, where the firmware of gateway devices was modified (causing their destruction) [2], or through a remote access connection (**B**), as it happened in the second Ukraine cyber attack in 2016 [3] and in the 'TRITON' cyber attack on critical infrastructure PLCs [4].

Another entry point is through engineering PCs (**C**), either directly connected to substation equipment or to the substation network. When a protection engineer connects his PC to a relay to modify (protection) settings, malware on the PC could in turn install malware on the relay as it happened with PLCs in the famous 'Stuxnet' cyber-attack 2010 [5].

Laptops used for testing the IEC 61850 system (**D**) are often directly connected to the station bus which is also a potential way to infect Intelligent Electronic Devices (IEDs). For this reason, new IEC 61850 testing tools are available which provide a cyber-secure separation between Test PC and substation network. This leaves the testing device itself (**E**) as a potential entry path. Because of this, it is important that test set vendors invest in hardening their devices to make sure that this entry path is not attractive for an attacker to exploit.

The storage location of settings (**F**) and test documents (**G**) could also be a source of infection. Their server or storage location thus also belongs to the critical perimeter and should not be located in the office IT zone. Therefore, it makes sense to introduce a separate, isolated and protected data management solution for such data.

2. New Substation Architecture Proposal

2.1. State of the Art in OT Cyber Security

The Swiss power industry association VSE started a working group on security for Operational Technology (OT), which subsequently published an industry recommendation document: 'Handbook on Basic Protection of Operational Technology in Power Systems'. This handbook references to the 'Cyber Security Framework for Critical Infrastructure' by the National Institute of Standards (NIST) [7], which is continuously adapted and improved, with the latest version updated in 2018. The NIST framework is based on the assumption that there is never a 100% protection against cyber attacks. With enough knowledge and effort, all security measures can be breached. Based on that, the NIST framework recommends a process consisting of these five steps: 'Identify', 'Protect', 'Detect', 'Respond', 'Recover'. The first step is therefore the identification of attack vectors (Identify) as presented in the previous section of this paper. After that, countermeasures can be implemented in the following step (Protect). If an attacker is still able to break through these barriers, the attack must be detected (Detect) and, at best, immediately acted upon (Respond) to restore normal status as quickly as possible (Restore). With the lessons learned in Detect and Response, new attack vectors can be identified, new countermeasures can be implemented and so the process repeats itself.

The Swiss industry recommendation puts great emphasis on the interaction of people, technology and processes within the organisation. For example, continuous monitoring or intrusion detection (Detect), only makes sense if alarm messages are responded to appropriately. Thus, the alarm messages need to be understandable for everyone involved in the response process: OT engineers and IT security specialists. Otherwise the response process becomes inefficient. Additionally, if the IDS delivers too many false alarms, all alarms will be ignored, eventually.

2.2. OT Cyber Security Initiatives at CKW [6]

The topic of OT security, especially of control and protection systems has become increasingly important at CKW in recent years. This was caused by the mentioned industry recommendations in Switzerland, but above all also because of OT security assessments performed by CKW in recent years. These assessments showed weak points in both the networks and the station control technology used in substations. For example, unsafe zone transitions and some critical remote access methods on station control computers were found. Additionally, it was not possible to assess whether an attack is currently taking place in the substation network or whether there are suspicious activities on the network that could indicate an imminent attack. Based on these findings, CKW has set itself the goal to eliminate the essential weak points and to tighten the requirements for their future substation architecture and so these findings were integrated in CKW's new substation design standard.
In addition to working on this design standard, CKW was able to become involved in the Swiss working group for the mentioned OT security handbook. Based on this information exchange CKW consistently integrated the findings from the working group into its own design standards.

In 2016/2017, a project team of CKW began planning the new greenfield substation 'US Rothenburg', which will go into operation in 2020. In this project, the new secure architecture standard of CKW was applied and the latest recommendations by the Swiss OT security handbook were followed. To be able to implement these sophisticated security measures, CKW decided to implement the network architecture and switch configuration by themselves.

2.3. Network Design

In the network design of the US Rothenburg, hurdles were built into every area to make an attack as difficult as possible. Figure 2 depicts the US Rothenburg substation network.

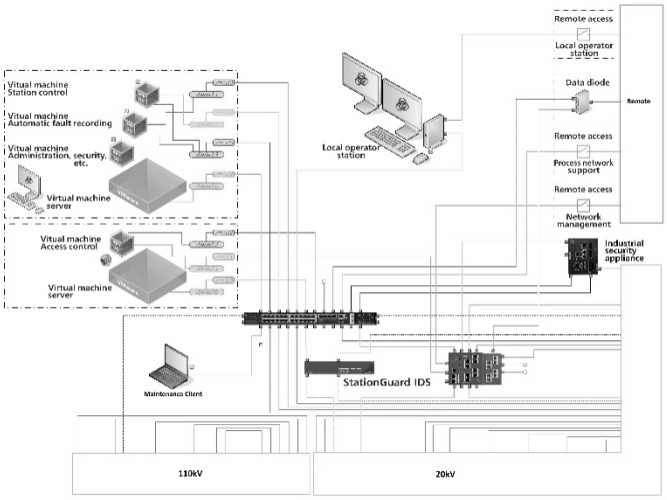

Figure 2 US Rothenburg Network Architecture [6]

In this architecture, all attack vectors described in Section 1.1 of this paper are addressed using a whole range of security measures. The remote connections of the plant were addressed with highest priority. These remote connections are not only secured using firewalls and tunnel solutions, but they are deactivated by default. Connections for remote access are only enabled when required. This means multiple people are involved to enable remote access, similar to a two-factor authentication process.

Supervisory Control and Data Acquisition (SCADA) communication with the control centre takes place using the IEC 60870-5-101 serial protocol. All access to the substation devices for maintenance purposes is exclusively done via special workstations, which are appropriately secured. These workstations are virtualized and in a central location. This maintenance remote access also must be enabled remotely.

The SCADA system, the fault recorder collection system and the security system servers are virtualised and operated on a host machine locally in the substation. Even the local HMI station only accesses these systems using remote desktop through an additional local firewall. Role-Based Access Control (RBAC) is used. This means that there is not one password per device, but one password per user. This has the advantage that an engineer can use his own password across all substations. If an employee leaves the company, his user can easily be removed, no passwords need to be changed. This user management is implemented using a central Active Directory (AD) server and a RADIUS server local in the substation. Users must log on using the AD, which assigns them the necessary permissions. If required, access to the central AD can be enabled from a central location. In addition, the users must log on to each IED with individual username and password. Hereby the IEDs use the local RADIUS server to check the authentication of the user and password and to retrieve the permissions assigned for this user. This applies both to access to the devices with engineering tools and to operation on the IED display. No standard passwords are used.

All PCs connected to the substation network are hardened. This is done, among other things, by configuring the Windows firewall in accordance to the communication matrix of the substation, and, depending on the role of that client, by blocking functions of the operating systems that are not required.

As an additional security measure, network access control is implemented via MAC authentication bypass, which means that only registered devices can connect to the network switch.

In the event of a malfunction, the switch must also recognize and accept the reserve devices from stock.

In the substation network switches and the firewall, access control lists are configured to enforce which device is allowed to communicate with which other network participant including used protocol and switch port.

The station bus network and the network for configuration and maintenance are logically (VLAN) and physically separated. This means that, on each IED, the IEC 61850 communication MMS and GOOSE runs on a different network interface than maintenance access. Additionally, the entire station bus network is segmented, whereby, among other things, the following segments are separated via a firewall:

- 110kV (GOOSE and MMS)
- 20kV (GOOSE and MMS)
- Local HMI
- Protocol gateway
- Ancillary systems
- Maintenance networks for IEDs and clients
- Management network, VM, RADIUS

The communication from the substation to higher-level network areas are additionally secured by a data diode. This data diode ensures that only

outgoing communication sessions can be initiated and provides another layer of security.
An Intrusion Detection System (IDS) monitors the entire network traffic in the system using a whitelist approach i.e., all unknown traffic, which is not on the whitelist, by default creates an alarm. The IDS reports alarm to the control centre through the RTU and to a security operation centre through specialized protocols for alarm logging.

3. Intrusion Detection

CKW's security architecture is based on the establishment of network segments, each separated by the firewall. The configuration of the firewall specifies exactly which protocols may be used for communication across the segments. However, the protocols permitted by the firewall, such as MMS/GOOSE used in IEC 61850, and vendor-specific engineering protocols can also be used to attack devices and infect them. In such scenarios, CKW wanted to be able to detect unauthorized activity at an early stage. For this purpose, it was decided that an IDS shall be used in CKW's reference architecture.
To be able to analyse the most critical traffic – i.e., the communication between the gateway and the IEDs – at least all traffic of the gateway should be mirrored into the IDS. The bay-level switches don't usually need to be covered as typically only multicast traffic like GOOSE or Sampled Values originates from there. To ensure that also all unicast traffic in all network branches is analysed, it is recommended that all switches are mirrored into the IDS.
In the CKW architecture, the IDS is connected to mirror ports on all network switches. This means that the IDS analyses the traffic on the station bus as well as the traffic coming in from remote before and after it passed the firewalls.

3.1. Requirements for Substation IDS

Selecting an IDS suitable for substations proved out to be challenging. An important requirement was that the IDS can be easily operated by the protection, control, and network engineers who are responsible for all IEDs and network equipment. To support the alarm response process, it shall be easily possible to associate the IDS alarms with events in the substation and event logs in the HMI. Therefore, the IDS should allow specific views for substations instead of just IT-security terminology.
Until recently, there were only two main approaches for IDS: Signature-based and "learning-based" approaches.
The signature-based approach works with a blacklist like a standard PC virus scanner. It scans for patterns of known viruses and malware. The problem is that there are only a small number of cyber-attacks known for substations, but even the first occurrence of a new attack could have severe consequences. A substation IDS must be able to detect attacks without any previous knowledge about what the attack might look like.
Therefore, more IDS systems use a "learning-based" approach. The IDS looks at generic protocol parameters of different protocols to learn the average values and frequency of each parameter.
After that, during normal operation, an alarm is triggered whenever the network communication deviates significantly from the learned average. As a result, false alarms are triggered for all events that did not occur during the learning phase. This includes, for example, trips and switching operations, or routine protection testing. Since the system does not know the meaning of the telegrams on the network, the alarm messages refer to generic protocol parameters, like 'MMS confirmed-write-response failed'. This results in a high number of false alarms, with each one requiring IT specialists and IEC 61850 specialists to check. Such an effort in the response process was not acceptable for CKW.

3.2. IDS Approach Used

For IEC 61850 substations the whole automation system, including all IEDs, their data models, and their communication patterns is described in a standardized format – the SCL. This information allows a different approach to be used for detecting intrusions: The monitoring system can create a system model of the substation automation system and it can compare each packet on the network against this model. Even the variables contained in the communicated (GOOSE, MMS, SV) messages can be evaluated against the expectations derived from the system model. This system model thus comprises a whitelist, because all packets not matching the system model will trigger an alarm.

CKW selected an IDS which is based on this approach (OMICRON StationGuard).
The advantage of this approach is that not only cyber security threats like malformed packets and prohibited MMS control actions are detected, but also communication failures, time synchronization problems, and consequently also certain equipment failures are detected and alarmed.
By using the substation section in the SCL file, an overview diagram of the substation can be created automatically, and the alarms can be depicted in this diagram. Such a display can help identifying if an action which triggered an alarm was performed intentionally: For example, the event could have been caused by an engineer in a testing situation, or it could correspond to malicious activity by an infected testing laptop.

At the time of writing of this article, the Factory Acceptance Test (FAT) of the US Rothenburg was done and commissioning has been in progress. Already for the FAT, almost the full network configuration had to be finished to be able to test if the design works. We also learned that the IDS needs support for the routing performed by the multiple levels of firewalls. There are multiple duplications of the traffic before and after the firewalls which could confuse the IDS display. However, the selected IDS supported this scenario correctly. Additionally, it is considerable effort to create the communication matrix for the firewall configuration as this must be done manually. Since the IDS already has such a whitelist from SCL, also this process could be automated in the future.

4. Conclusion and Outlook

If an attacker can influence one or more substations, this can have severe consequences for the grid. Substations provide several attack vectors where the firewall can be circumvented. CKW's secure substation network architecture provides numerous countermeasures to the attack vectors identified in this paper. The security measures provide a high level of security while still allowing efficient maintenance and engineering procedures using remote access. This architecture relies on intrusion detection in the core of the network. For IEC 61850 substations, an IDS approach is available which uses the SCL to automatically build a whitelist of all allowed network traffic. This also allows to display detected events in the language of protection, automation and control engineers so that they can collaborate with security engineers to determine the cause of events efficiently.

It is in the nature of cyber security that each design can be improved. Among the improvements is for example certificate-based network access control according to 802.1X [8] instead of the currently used MAC-based approach. However, for this, more IEDs have to support the 802.1X standard which is currently not the case. Follow-up papers should collect the findings from the commissioning of this project and document the results of future security assessments and penetration tests performed in this substation.

5. References

[1] Klien, A.: 'New approach for detecting cyber intrusions in IEC 61850 substations', PAC World Conference Europe, Glasgow, 2019

[2] 'Analysis of the Cyber Attack on the Ukrainian Power Grid', SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accessed November 2019

[3] 'WIN32/INDUSTROYER - A new threat for industrial control systems', https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, accessed November 2019

[4] 'Threat Research - Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure', https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accessed November 2019

[5] D. Kushner: 'The Real Story of Stuxnet
How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program', IEEE Spectrum, February 2013

[6] Gosteli, Y., Klien A.: 'Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg', bulletin.ch, 2019, 6, pp 50-52

[7] NIST: 'Framework for improving critical infrastructure cybersecurity, version 1.1, National Institute of Standards and Technology, April 2018

[8] IEEE: '802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control', International Standard, February 2010

OMICRON is an international company serving the electrical power industry with innovative testing and diagnostic solutions. The application of OMICRON products allows users to assess the condition of the primary and secondary equipment on their systems with complete confidence. Services offered in the area of consulting, commissioning, testing, diagnosis and training make the product range complete.

Customers in more than 160 countries rely on the company's ability to supply leading-edge technology of excellent quality. Service centers on all continents provide a broad base of knowledge and extraordinary customer support. All of this together with our strong network of sales partners is what has made our company a market leader in the electrical power industry.

For more information, additional literature, and detailed contact information of our worldwide offices please visit our website.

www.omicronenergy.com