New approach for detecting cyber intrusions in IEC 61850 substations

Andreas Klien, OMICRON electronics GmbH, Klaus, Austria
andreas.klien@omicronenergy.com

1 Abstract

Multiple layers are necessary to ensure the cyber security of substations. Cryptographic techniques allow to authenticate devices, but not all attacks can be prevented by these measures. Firewalls and “air gaps” can be circumvented through existing remote access tunnels, or through maintenance computers directly attached to IEDs or the station bus. Therefore, measures are needed to detect attacks to enable quick response and to minimize consequences.
For this purpose, Intrusion Detection Systems (IDSs) are used in IT networks for several years now. Because only a small number of cyber-attacks on substations are known, and even the first occurrence of an attack could have severe consequences, IDS must be able to detect attacks without knowing any signatures of the attack beforehand.
Other approaches try to detect unknown attacks by using a “learning” approach, learning the frequency of certain protocol markers. Thus, seldom but legitimate events trigger many false alarms.
This paper presents a new approach for intrusion detection in substations which uses a system model of the IEC 61850 automation system and the power system to differentiate between legitimate and malicious activity. Since all communication is verified, not only security intrusions are detected, but also communication errors and equipment failure can be detected. The configuration is retrieved automatically from the IEC 61850 SCD file and thus no learning phase is required.
After presenting the software and hardware requirements for substation IDSs, this approach – applied in OMICRON’s StationGuard – is described in detail. The paper concludes with a practical example of an implementation.

2 Attack vectors of a substation

Let us define a cyber-attack on a substation as an event where an adversary modifies, degrades, or disables a service of at least one protection, automation, or control device within the substation. Looking at Figure 1, a typical substation can be attacked through all paths marked with a number. An attacker could enter through the control center connection (1), as it happened in one of the cyber-attacks in Ukraine, where the firmware of gateway devices was modified (causing their destruction). Another entry point is through engineering PCs (2) connected to substation equipment. 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 in a comparable way as to what happened with PLCs in the Stuxnet cyber-attack. Laptops used for testing the IEC 61850 system are often directly connected to the station bus which is also a potential way to infect IEDs (3). 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 (4) 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 feasible for an attacker to exploit.
The storage of settings (2a) and test documents (3a) could also be a source. This storage server thus also belongs to the critical perimeter. Therefore, it also makes sense to introduce a separate, isolated and protected data management solution for such data.

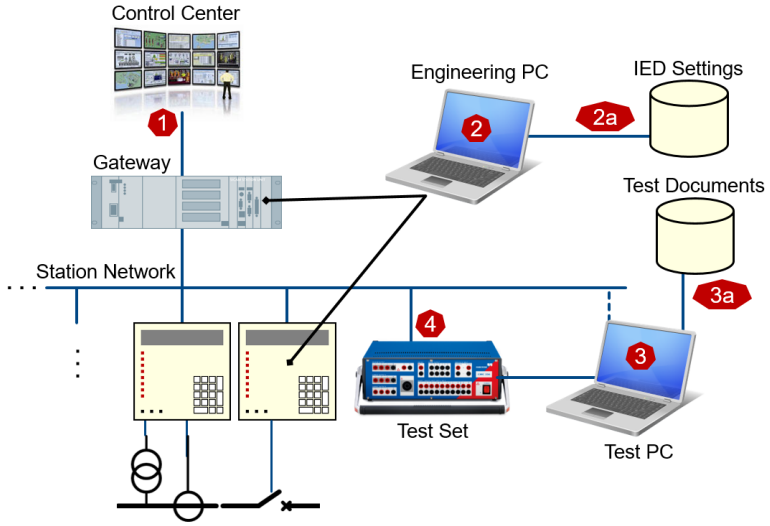

Figure 1 Attack vectors of a substation

3 Security in IEC 61850 substations

A frequent question about cyber security in IEC 61850 substations is: *"What happens if an attacker injects a trip GOOSE into the station bus – how can I prevent that?"* For this, we should not focus on the case that the attacker has physical access to the substation network. This situation is also possible through other measures: an infected engineering or testing PC connected to the station bus, or even an infected IED could start injecting GOOSE. In this context, the status and sequence numbers in the GOOSE message are quite often presented as GOOSE "security mechanisms". However, in 2019, such measures should merely be called "safety mechanisms", because any adversary can listen to the current status and sequence number and inject suitable values. Also the source MAC address of the GOOSE packet can be spoofed easily by the attacker. The IED receiving the GOOSE has no other option than to react on the first GOOSE received with correct source MAC and correct status/sequence number. The same of course applies to the sample counter in sampled values. The only real measure to prevent such injection attacks is by ensuring the authenticity and integrity of the message using authentication codes at the end of the GOOSE message, as standardized by IEC 62351-6. With this measure, the sending IED is clearly identified and it becomes impossible to manipulate the GOOSE message content. Note that it is not required to encrypt the message to get these features. To deliver and maintain these authentication keys for each IED, a key management infrastructure is needed inside the substation. Because of this, these GOOSE security mechanisms have not gained widespread use, yet – but they will. The same with MMS and Role-based access control.

Encryption

Encryption has not been mentioned, though it is often seen as the silver bullet for security. The IEC 62351 standard also provides encryption for GOOSE and MMS. However, in the substation environment there are only few applications imaginable where confidentiality of messages is important. If messages cannot be tampered with (integrity) and the originator can be verified (authentication) – which is fulfilled by using authentication in GOOSE and MMS, it is not necessary to encrypt the messages. One example where encryption could be necessary is if routable GOOSE (R-GOOSE) are transmitted over an unencrypted communication path. Encryption only provides additional CPU load on the IEDs, increases GOOSE transmission time and impedes testing scenarios, but in most cases doesn't provide additional security than authentication codes already provide. Encryption also makes a later analysis of traffic recordings difficult and it impedes monitoring approaches such as the ones described below.

Defense in depth

Most of IEC 61850 substations built up until now have not implemented IEC 62351. Even in substations where GOOSE and MMS with authentication codes are applied, infected devices in the network could still infect other devices or affect availability by disturbing the communication system. Therefore, most security

frameworks recommend the usage of “Intrusion Detection Systems” (IDS), a term known from classical IT systems, to detect threats and malicious activity on the network. Such Intrusion Detection Systems are now becoming more common in the power system domain.

4 Requirements for intrusion detection in Substations

In an IEC 61850 substation, an Intrusion Detection System would be connected as depicted in Figure 2. Mirror ports on all relevant switches forward a copy of all network traffic to the IDS. The IDS inspects all network traffic communicated over these switches. To be able to analyze the most important traffic between the gateway and the IEDs, the IDS should, as a minimum, be connected to the switch next to the gateway and all other critical entry points into the network. The bay-level switches don’t usually need to be covered as typically only multicast traffic (GOOSE, Sampled Values) originates from there. To ensure that all unicast traffic in all network branches is analyzed, it is necessary that all switches are mirrored into the IDS, which is not always possible if switch chips integrated into the IEDs are used.

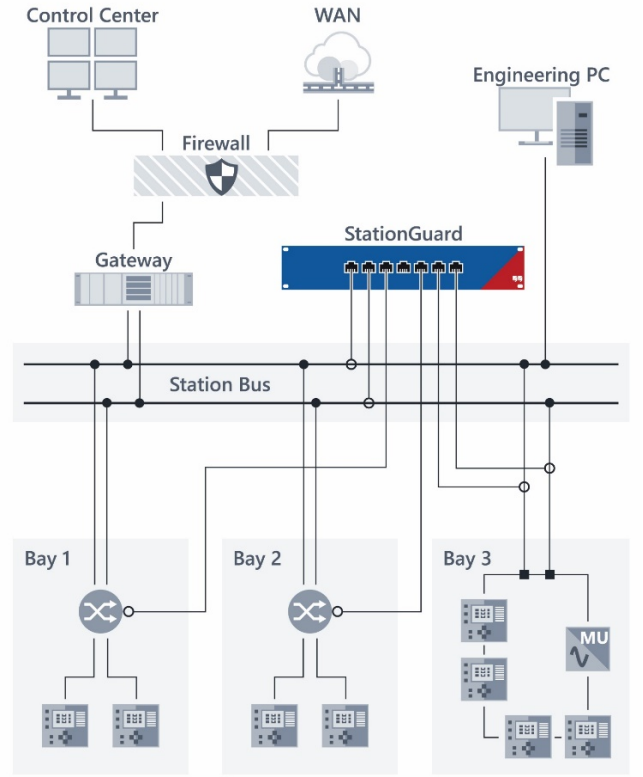

Figure 2 How IDS can be connected to the substation network

However, intrusion detection systems from classical IT are not suitable for the substation environment. While classical IT security is concerned with high-performance servers with millions of connections at the same time, substation IT security deals with devices with limited resources, custom operating systems, real-time demands, and specialized redundancy protocols. For example, a “denial-of-service” attack on an IED’s communication service often only requires 10 connections i.e., 10 Ethernet packets, to be successful. Simply because “denial-of-service” scenarios were not considered in the good old times when these devices and protocols were developed. Additionally, there are only a small number of known cyber-attacks on substations, but even the first occurrence of a new attack could have severe consequences. Thus, a substation IDS must be able to detect attacks without any previous knowledge about what the attack might look like. This is a very different approach than that of a virus scanner, which has a list of virus signatures it looks for.

5 Learning-based systems

To be able to detect unknown attacks, many vendors use a “learning-phase” approach. Such systems look at frequency and timing of certain protocol markers to attempt to learn the usual behavior of the

system. After the learning phase is complete, an alarm will be raised if one of the markers is significantly outside the expected range. This has the effect that false alarms are triggered for everything that did not occur during the learning time, such as protection events, uncommon switching or automation actions, or routine maintenance and testing. Because these systems don't understand the semantics of the protocols, the alarm messages are expressed in terms of technical protocol details. Hence, alarms can only be examined by an engineer skilled in IEC 61850 protocol details and familiar with IT network security. The engineer examining the alarm also must know about the operational situation to judge if certain IEC 61850 protocol events correspond to valid behavior. Therefore, a high number of false alarms occur for every substation all of which require highly skilled personnel to examine. This often leads to alarms being ignored or alarms discarded without investigating them, and ultimately the IDS being switched off.

6 The StationGuard Approach

For IEC 61850 substations the whole automation system, including all devices, their data models, and their communication patterns is described in a standardized format – the SCL. System Configuration Description (SCD) files normally also contain information about primary assets and for an ever-increasing number of substations even the single-line diagram is present.

This information allows a different approach to be used for detecting intrusions: The monitoring system can create a full system model of the automation and power system and it can compare each and every packet on the network against the live system model. Even the variables contained in the communicated (GOOSE, MMS, SV) messages can be evaluated against the expectations derived from the system model. This process is possible without the need for a learning phase, just by configuration from SCL. This approach is implemented in the new functional security monitoring system StationGuard.

Functional Security Monitoring

In essence, a very detailed functional monitoring is produced to detect cyber threats in the network. Because of the detail level of the verification, not only cyber security threats like malformed packets and disallowed control actions are detected, but also communication failures, time synchronization problems, and consequently also (certain) equipment failures can be detected. If the single-line diagram is known to the system, and measurement values can be observed in MMS (or even through Sampled Values) communication, the possibilities of what can be verified are endless.
For example, alone for GOOSE there are 35 alarm codes available of things that could go wrong. These range from simple stNum/sqNum glitches (as explained above) to more complex issues, such as too long transmission times. The latter is detected by accurately measuring the difference between the EntryTime timestamp in the message and the arrival time at StationGuard. If this network transmission time is significantly longer than 3 ms for a "protection" GOOSE (referring to IEC 61850-5), it indicates a problem in the network or in the time synchronization.
What is done for MMS communication? From the system model (from the SCL) it is known which Logical Nodes control which primary assets. Thus, it can be distinguished between correct/incorrect, and critical/noncritical actions. Switching a circuit breaker and switching the IEC 61850 test mode use the same sequence in the MMS protocol (select-before-operate), but the effect in the substation is quite different. So, if the Test PC from Figure 1 switches the test mode on a relay this may be a legitimate action during maintenance, but it is most probably not legitimate that the Test PC operates a breaker. There will be a more in-depth look at this example in the following paragraphs.

Developed with PAC engineers

Research on this approach started in 2011. Spin-offs of this concept, the 24/7 functional supervision of SV, GOOSE and PTP time synchronization has been available in a distributed and hybrid analysis device (OMICRON DANEO 400) since 2015. Triggered by this, we were approached by the Swiss distribution and generation operator CKW. They were familiar with the disadvantages of commercially available IDS systems and they were looking for a more suitable solution for substations and one that is friendlier for protection, automation, and control engineers. This lead to a cooperation between the PAC engineers of CKW and the development team for our solution. It was intriguing to hear how they planned intrusion detection to be part of their future substation cyber security design. Meanwhile feedback from many other utilities world-wide as well as some proof-of-concept installations found its way into our development.

In 2018, one of the first proof-of-concept installations was installed in a 110kV CKW substation and has been running since then. Figure 3 shows the installation using the mobile hardware platform MBX1 at the bottom of the picture. In this setup, all traffic of the “core” switch was mirrored to StationGuard. This ensures that all the communication from the gateway to and from all IEDs is visible. Because remote maintenance connections also enter through that switch, all this traffic can also be inspected by StationGuard. Since GOOSE communication is multicast, and because the network setup allows it, all GOOSE from the IEDs in the substation bays are also visible to StationGuard.

Figure 3 Installation in 110kV substation of CKW using the mobile platform variant of StationGuard

Alert Display

Besides the avoidance of false alarms, it is also of vital importance that the alarm messages delivered are understandable for the engineers who are responsible for the operation of the protection, automation and network functions within the substation. This allows faster reaction times because often these alarms are triggered by engineers working in the substation (or from remote activities). Additionally, this allows security engineers and PAC engineers to collaborate when tracing events within a substation.
Figure 4 shows a screenshot of the graphical alarm display: The alarm is shown as an arrow from the active participant (Test PC) performing the prohibited action, and the “victim” of the action – a bay controller in bay Q01. Figure 5 reveals details about that alarm – a circuit breaker was operated (using an MMS control sequence), which is not allowed for a Test PC.

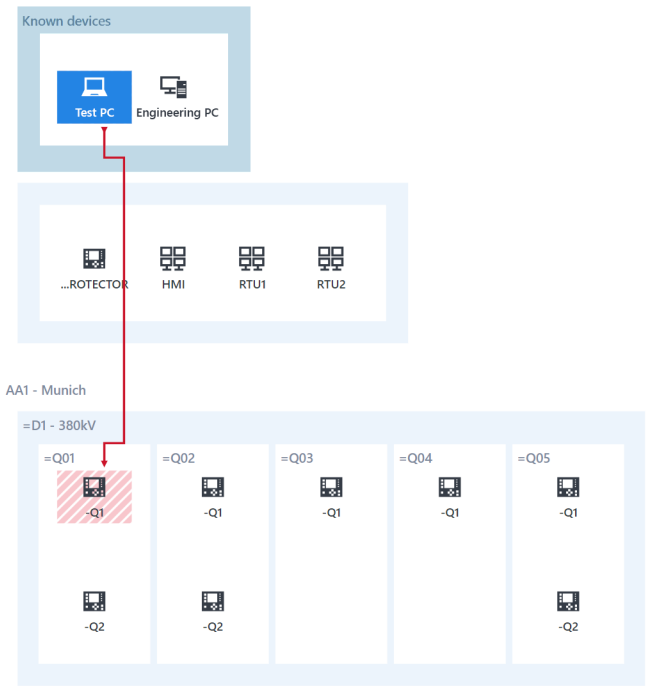

Figure 4 Graphical alarm display instead of event list

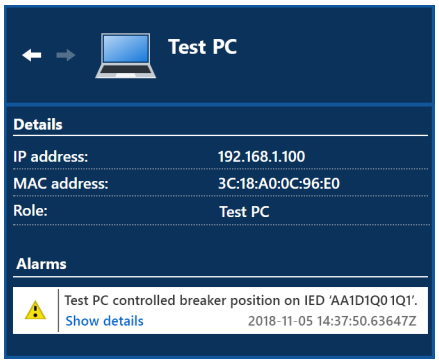

Figure 5 Details for Fig. 4: Test PC attempting unauthorized control of circuit breaker

Maintenance Mode

To avoid false alarms, routine testing and maintenance conditions must be included in the substation system model. This means that the testing and engineering equipment, including protection test sets, can be introduced into the system. In Figure 6 we see that maintenance was activated for Bay Q01. Now the Test PC from the example above can do more than before. There will be no alarm if the Test PC controls the IEC 61850 test or simulation mode of IED -Q1 in this bay. However, the same alarm as before will be triggered if the Test PC operates a breaker in that bay, since critical actions like this are not authorized for a Test PC. Of course, if company policies allows such actions, these rules can be modified.

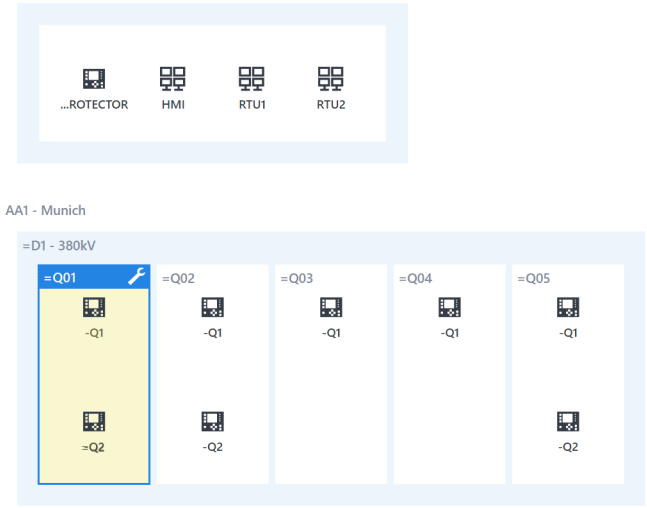

Figure 6 Maintenance mode activated for bay Q01

Configuration

As mentioned before, no learning phase is required. The detection starts right from the time that the device is powered up and it cannot be turned off – for security reasons. Until the SCD file of the substation is loaded, all IEDs will be detected and presented as unknown devices. Once the SCD file is loaded, the IEDs will be indicated as known devices and the substation structure is assembled into a “zero-line” diagram, as it was introduced with StationScout. The configuration can also be prepared in the office and then installed on site one after the other with fast commissioning. If not all IEDs were engineered into one file (things happen), then additional IEDs can also be imported one by one. Once the import is done, the user can add roles such as “Test PC”, “Engineering PC”, etc. to any remaining unknown devices.

What happens in case of an alarm?

It is important to note that the StationGuard is purely passive, if an action is “not allowed” it will trigger an alarm. This alarm can be communicated to the Gateway/RTU and control center or to a separate system collecting security alerts – known as Security Incident Event Management (SIEM) system. StationGuard does not actively react or interfere with the substation. But it allows for a fast reaction, for example, the isolation of the device in question from the network before any damage can occur. Depending on the chosen hardware variant, user-definable binary outputs are available to be wired directly to the RTU. In this case the alarm signalization happens without network communication and the alarms can be integrated into the normal SCADA signal list like any other hard-wired signal of the station.

7 Cyber security of StationGuard itself

As we know it from b-grade movies, burglars always attack the burglar alarm system first. So what about the security of this alarm system? An important aspect is that a standalone, secure hardware is used and not a virtual machine. Both hardware variants of StationGuard, the mobile (MBX1) and the 19”-variant for permanent installation (RBX1), have the same platform hardening. They both have a secure cryptoprocessor chip according to ISO/IEC 11889. This ensures that cryptographic keys are not stored on the flash storage but in a separate chip which is protected against tampering. By installing the OMICRON certificates on this chip during production, a secure, measured boot chain is created. This means that each step in the firmware bootup process verifies the signatures of the next module or driver to load. This makes sure that only software can be executed that is signed by OMICRON. The storage of the devices is encrypted with a key unique for that hardware and is protected inside the cryptochip. Because nobody (including OMICRON) knows this key, all data on the device will be lost when the hardware is replaced on repair. Many other mechanisms make sure that the processes on the device cannot be attacked or misused, so that the “defense in depth” approach is also applied deep into the software running on the device. Covering all these mechanisms would be a complete topic for another article.

8 Conclusion

Substations provide potential attack vectors for cyber-attacks. If an attacker is able to influence one or more substations, this can have severe consequences for the grid. Therefore, effective cyber-security measures must be implemented not only in the control centers, but also in substations. For IEC 61850 substations an approach for intrusion detection is available which provides a small number of false alarms and still low configuration overhead due to the power of the SCL. This system not only detects security threats, but also functional problems of IEC 61850 communication and of the IEDs are detected – which is also helpful in the FAT and SAT phase. Intrusion detection systems that display detected events in the language of protection, automation and control engineers have the advantage that PAC and security engineers can work together to find the cause of events.

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