Detecting cyber intrusions in substations using functional security monitoring

Eugenio Carvalheira, Andreas Klien

OMICRON electronics

eugenio.carvalheira@omicronenergy.com

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 is described in detail. The paper concludes with a practical implementation example

Keywords—**Cyber Security, Intrusion Detection Systems, Functional Monitoring, Digital Substations, IEC 61850**

I. Attack vectors of a substation

Let us define a cyber-attack on a substation as an event where an attacker modifies, degrades, or disables a service of at least one protection, automation, or control device within the substation. Looking at Fig. 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 the 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 Electronic Security Perimeter (ESP). Therefore, it also makes sense to introduce a separate, isolated and protected data management solution for such data.

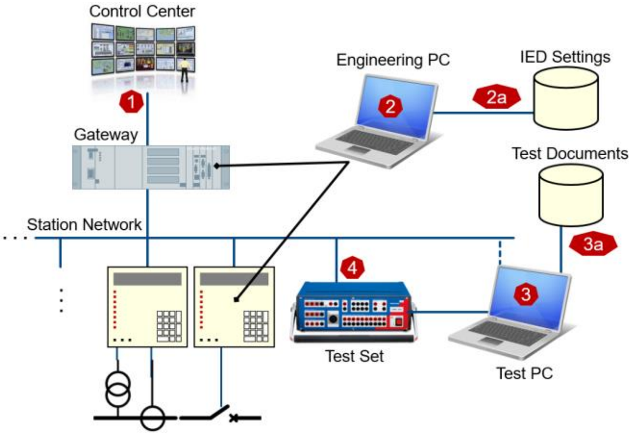


Fig. 1 Attack vectors of a Substation

II. 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 this can be prevented" 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, nowadays, such measures should merely be called "safety mechanisms", because any attacker can listen to the actual status and sequence numbers 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 numbers. 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 most likely will. The same with MMS and Role-based access control.

A. *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.

B. *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 use 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.

III. Intrusion Detection in Substations

In an IEC 61850 based substation, an Intrusion Detection System would be connected as depicted in Fig. 2. Mirror ports on all relevant switches forward a copy of all network traffic to the IDS. The IDS inspect 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.

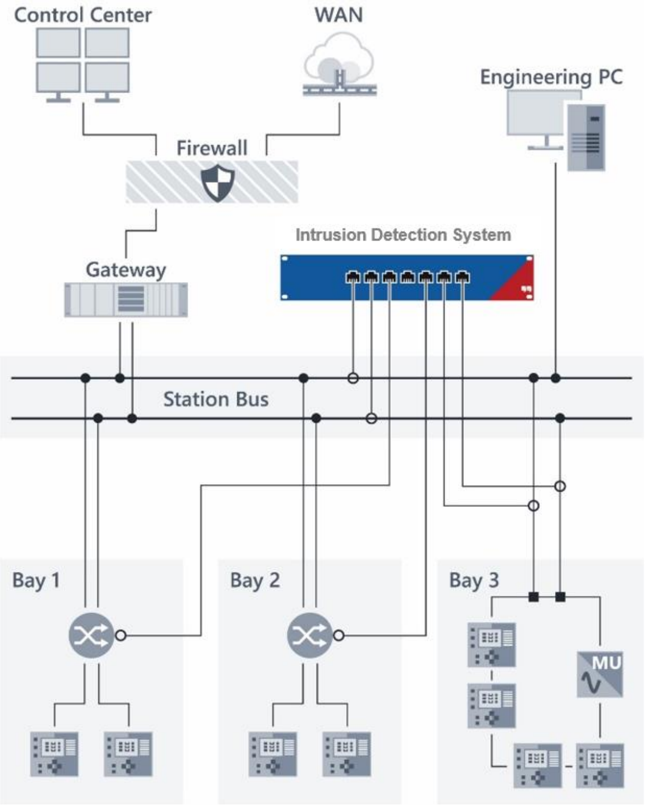


Fig. 2 How a IDS can be connected to the substation network

Intrusion detection systems from classical Information Technology (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 Operational Technology (OT) 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.

Until recently, there were only two main approaches for IDS: "signature-based" and "learning-based" approaches.

A. *Signature-based systems*

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. This is a very different approach than that of a virus scanner, which has a list of virus signatures it looks for.

B. *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 behaviors. 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.

C. *New Intrusion Detection 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 System Configuration Language (SCL). System Configuration Description (SCD) files can be generated by engineering configuration tools and normally also contain information about primary assets. For an ever-increasing number of substations, even information on the single-line diagram is present in this file.

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 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, but by configuring the IDS with just importing the SCL file. The information contained in the SCL file is used to create the system model and whitelist the communication messages that were designed for the system. With the comparison of the monitored network traffic against the system model, zero (or minimum) false alarms are expected to be triggered in such system.

IV. Functional Security Monitoring

With the new approach described above, a very detailed functional monitoring is implemented 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 status number (stNum) and sequence number (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 the IDS. If this network transmission time is significantly longer than 3 ms for a "protection" GOOSE (referring to the performance specified in IEC 61850-5), it indicates a problem in the network or in the time synchronization.

There are also other functional monitoring examples related to the MMS communication. From the system model (from the SCL) it is known which Logical Nodes in the IEDs control which primary switchgear. 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 Fig. 1 switches the test mode on a relay, this may be a legitim action during maintenance, but it is most probably not allowed for the Test PC to operate a breaker. There will be a more in-depth look at this example in the following sections of this paper.

A. *Alarm messages*

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 control (PAC) functions within the substation. Specific PAC engineer language is used instead of just IT-security terminology. 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. This easy to understand messages are achievable with this new approach due to all information contained in the system model, which describes the expected behavior of the system. However, this is not the case for the other IDS approaches listed above (signature-based and learning-phase), which do not know the meaning of the telegrams on the network.

To support the alarm response process even further, it should be easily possible to associate the IDS alarms with sequence of events (SOE) and event logs in the substation SCADA / HMI systems.

By using the substation section in the SCL file, an overview diagram of the substation (similar to a single line diagram) can be created automatically, and the alarms can be depicted in this diagram. Such a display as in Fig. 3 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.

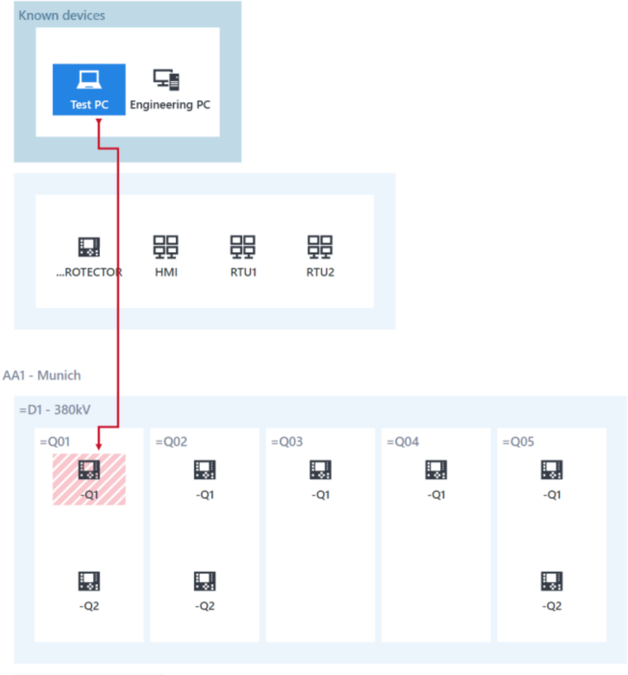
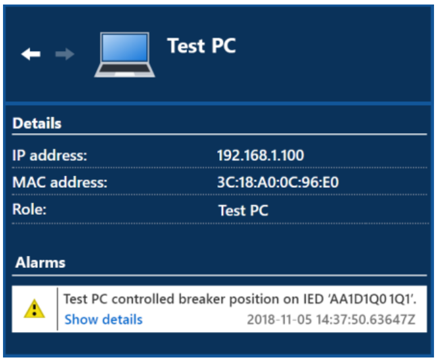


Fig. 3 Graphical alarm display

Fig. 3 shows a screenshot of a graphical alarm display. In this example, an alarm is shown as an arrow from the active participant (Test PC) performing a prohibited action, and the "victim" of the action – a bay controller in bay Q01. Fig. 4 reveals details about that alarm in an easy to understand message – a circuit breaker was operated (using a MMS control sequence), which is a not allowed action for a Test PC.



Test PC

Details

IP address: 192.168.1.100

MAC address: 3C:18:A0:0C:96:E0

Role: Test PC

Alarms

Test PC controlled breaker position on IED 'AA1D1Q01Q1'.

Show details 2018-11-05 14:37:50.63647Z

Fig. 4 Alarm details: Test PC attempting unauthorized control of circuit breaker

B. Maintenance Mode

To avoid false alarms, routine testing and maintenance conditions can be included in the substation system model. This means that the testing and engineering equipment, including protection test sets, can be added into the system. In Fig. 5, an example is shown where maintenance was activated for Bay Q01. When in maintenance mode, the Test PC from the example of Fig. 3 can now do more actions with the IEDs of this bay. For example, 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 in any case. Of course, if company policies allow such actions, these rules can be modified in the system by changing the roles of the individual asset types.

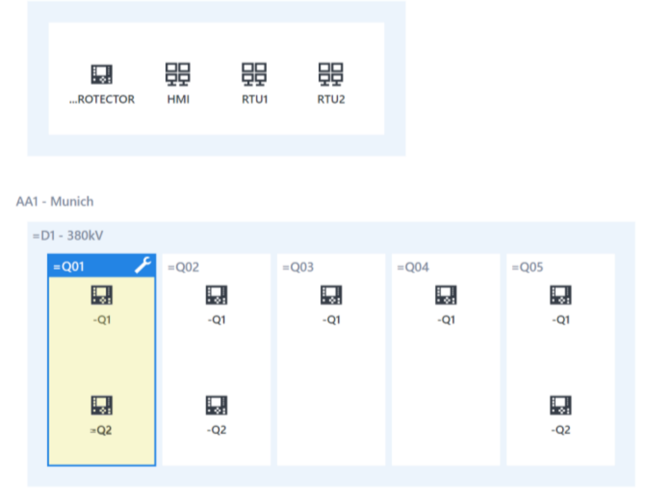


Fig. 5 Maintenance mode activated for bay Q01

C. IDS as a Passive System

It is important to note that such IDS is usually purely passive. If an action is "not allowed", it will trigger an alarm. This alarm can be communicated to a Gateway/RTU and control center or to a separate system collecting security alerts – known as Security Incident Event Management (SIEM) system. The IDS does not actively react or interfere with the substation. Depending on the chosen hardware platform, user-definable binary outputs can be 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.

D. Cyber Security Requirements of the IDS

As we know it from movies, burglars always attack the burglar alarm system first. So, what about the security of this alarm system? An important aspect is in the selection of the hardware platform, if it will be a standalone and secure hardware or if the application will run in a virtual machine. Both approaches require different measures to be implemented. If for example a standalone hardware is used, it is important to have a platform hardening. One of the measures is to have a secure crypto-processor 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 manufacturer certificates on this chip during production, a secure, measured boot chain can be 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 the manufacturer. The storage of the devices can be encrypted with a key unique for that hardware and can be protected inside the crypto-chip. Because nobody (including the manufacturer) knows this key, all data on the device will be lost when the hardware is replaced on repair. Many other mechanisms can be implemented to 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.

V.CONCLUSION

Substations provide potential attack vectors for cyber-attacks. If an attacker can 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 a new approach for intrusion detection is available which provides a small number of false alarms and still low configuration overhead due to the benefits provided by the SCL configuration files. 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 in a more efficient way.

VI. BIOGRAPHIES

Eugenio Carvalheira received his B.Sc. in Electrical Engineering in Brazil and his M.Sc. in Computational Engineering in Germany. He has over 17 years of experience in the design and commissioning of power systems protection, automation and control systems. He joined OMICRON in 2008 as an Application Engineer and is currently Engineering Manager for North America based in Houston, TX. He is also an active member of IEEE-PES-PSRC.

Andreas Klien received the M.Sc. degree in Computer Engineering at the Vienna University of Technology. He joined OMICRON in 2005, working with IEC 61850 since then. Since 2018, Andreas has been responsible for the Power Utility Communication business of OMICRON. His fields of experience are substation communication, SCADA, and power systems cyber security. As a member of the WG10 in TC57 of the IEC he is participating in the development of the IEC 61850 standard series.