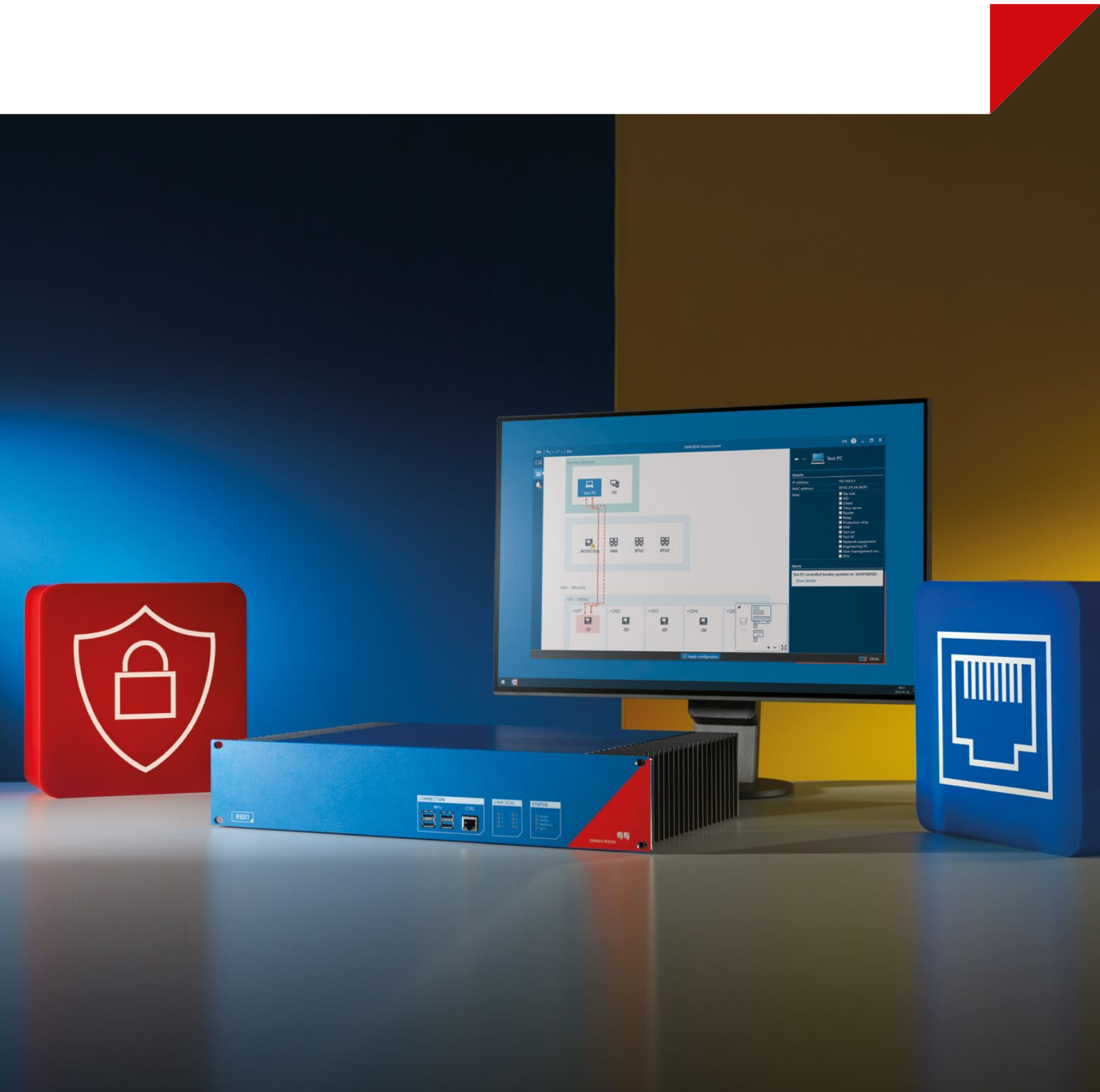
StationGuard

Functional Security Monitoring for Substations



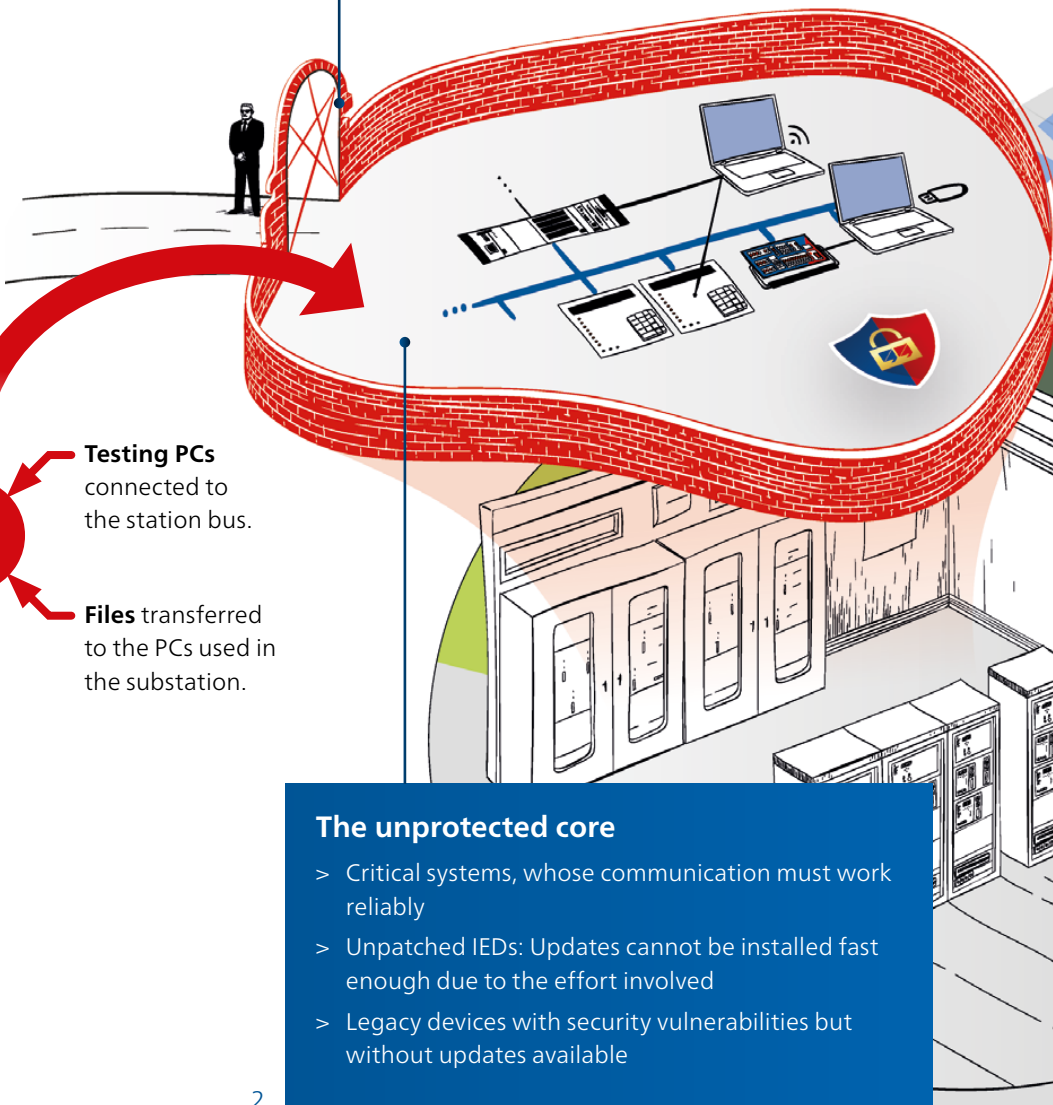
IT security in substations

There has been an increase in recent years in the number of cyber attacks against critical control systems in production facilities and energy supply companies. Many utilities are, therefore, introducing processes to reduce the risk of cyber attacks. Until now, these measures mainly concentrate on IT networks and control centers. However, substations and their station and process bus networks also represent critical attack vectors. As a consequence, the operation and maintenance processes of substations must also be included in the cyber security risk assessment.

To ensure that substations are thoroughly protected against cyber attacks, the security strategy has to address all levels. A security concept for substations extends from physical access control, through digital access monitoring, to the monitoring and detection of suspicious or forbidden activities in the network. This requires systems that offer a high level of security with low maintenance effort in the long term. Moreover, they should be easily integrable into the operational and maintenance workflows of the system.

Firewall

The use of a firewall to protect the networks in substation installations is, nowadays, as much a part of the standard equipment as fences and door locks. Firewalls ensure that only authorized endpoints can communicate with the devices in the substation, using only permitted protocols. However, there are ways of circumventing firewalls.



Attack vectors which circumvent firewalls:

Remote access for maintenance and configuration.

Testing PCs connected to the station bus.

Maintenance PCs connected to the network or directly to IEDs.

Files transferred to the PCs used in the substation.

The unprotected core

- Critical systems, whose communication must work reliably
- Unpatched IEDs: Updates cannot be installed fast enough due to the effort involved
- Legacy devices with security vulnerabilities but without updates available

Firewalls do not provide in-depth protection

There are many ways of circumventing a firewall. Many substations employ remote access to retrieve fault records or to adapt settings in IEDs. These connections provide a route by which malware can find its way into the devices in the substation.

Maintenance and testing PCs provide another channel of infection. These PCs may be either permanently installed or be brought into the substation temporarily. These PCs are either connected to the entire network, or directly to individual protection or control devices. Files transferred to such PCs can also become attack vectors.

Defense-in-depth

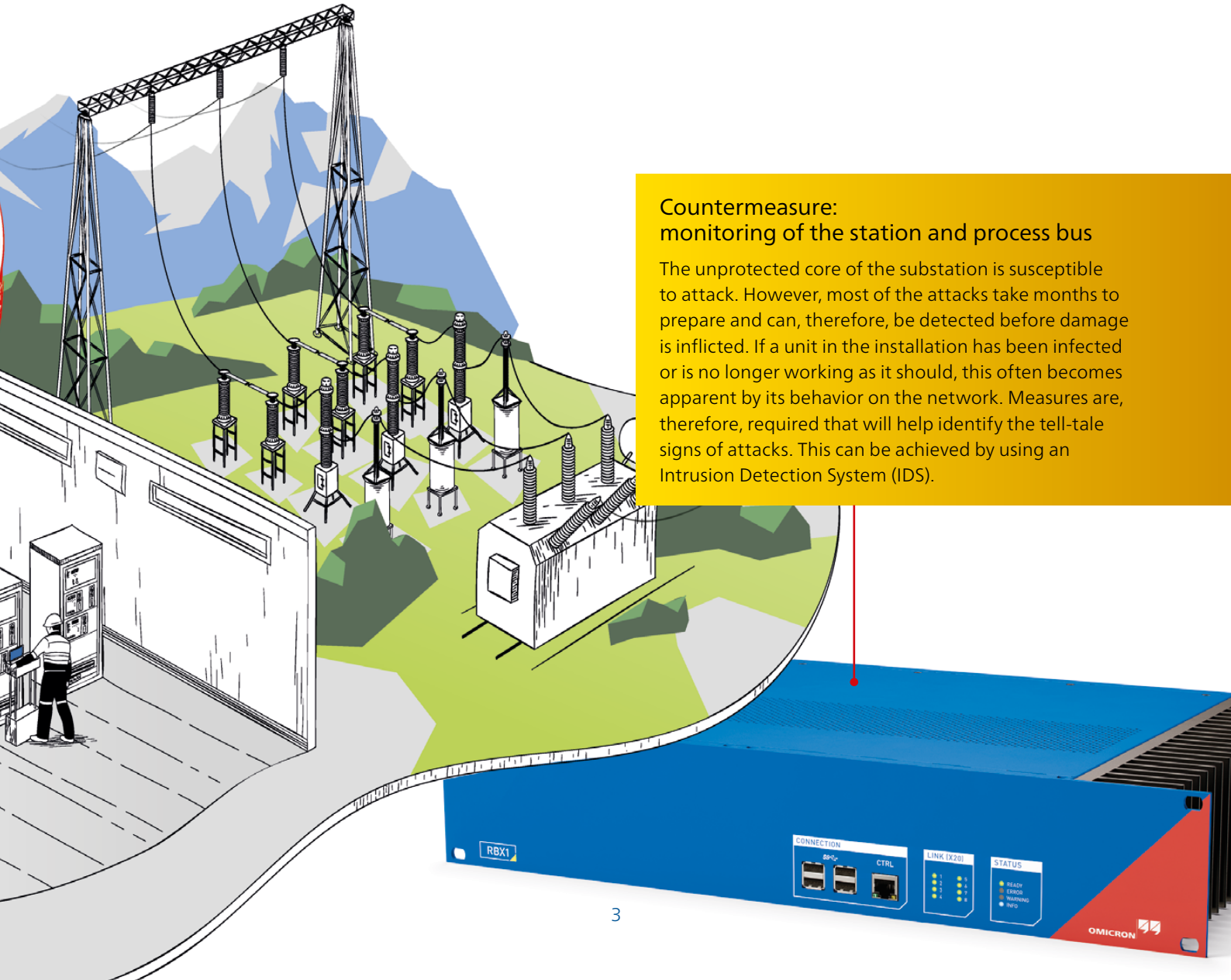
The Defense-in-Depth principle, as set out in IEC 62443, recommends to not only apply measures that „harden the shell“, but also the introduction of several layers and fallback levels that help providing a zoned level of security.

One such measure is the provision of security updates for the IEDs. The effort and cost involved, however, are high, which is why updates cannot always be installed in all IEDs quickly enough. Legacy devices often can no longer be updated because no updates are provided by the vendor.

It is, therefore, important that those devices that cannot be adequately protected are monitored to ensure that attacks are detected at an early stage and their consequences minimized.

Countermeasure: monitoring of the station and process bus

The unprotected core of the substation is susceptible to attack. However, most of the attacks take months to prepare and can, therefore, be detected before damage is inflicted. If a unit in the installation has been infected or is no longer working as it should, this often becomes apparent by its behavior on the network. Measures are, therefore, required that will help identify the tell-tale signs of attacks. This can be achieved by using an Intrusion Detection System (IDS).



How intrusion detection systems (IDS) work

To detect threats in the network, there are various approaches in terms of technology and usage. In most cases, these approaches are based on one of the following two technologies or a combination of both.

1. Signature-based approach (blacklist)

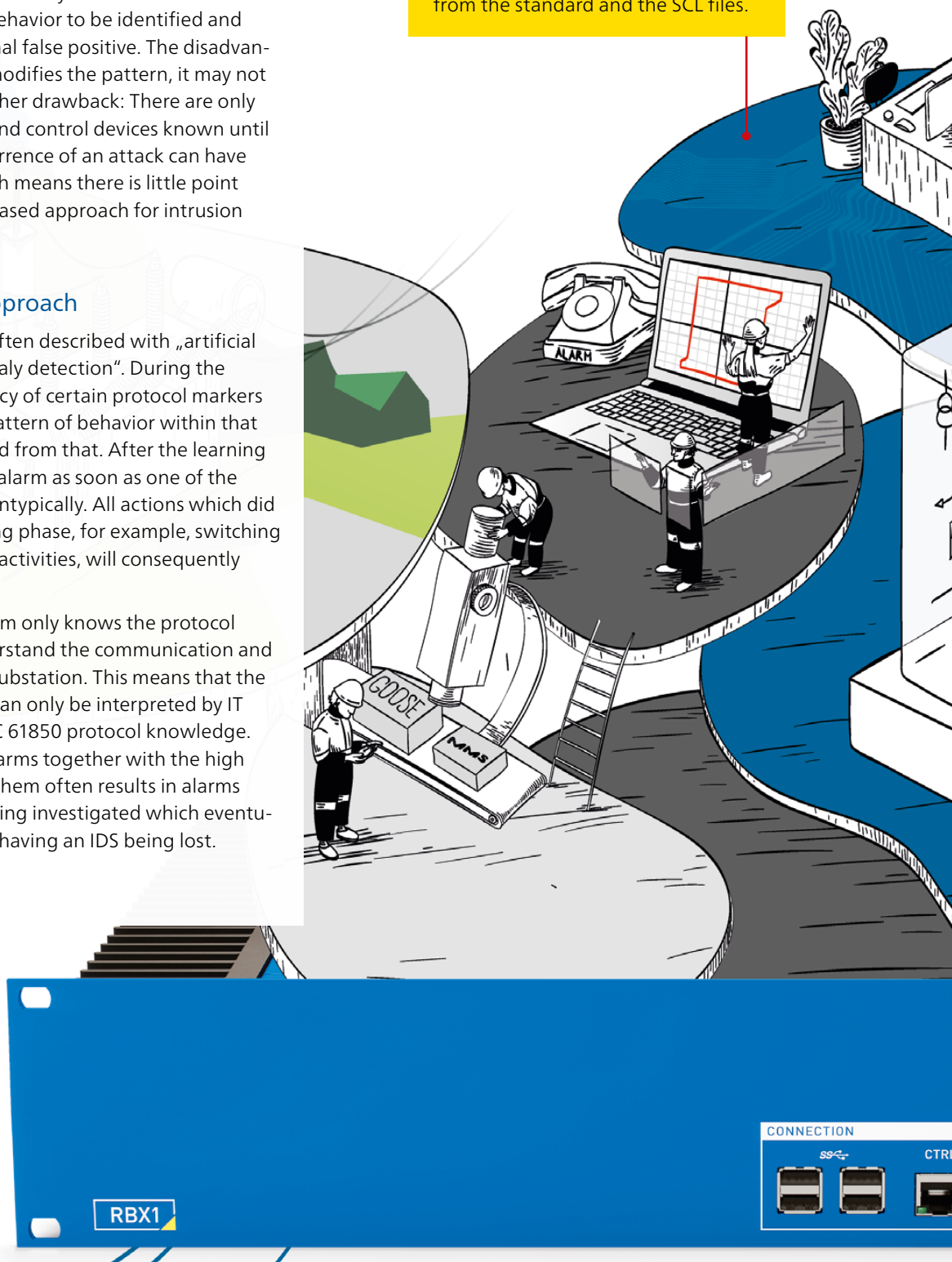
The IDS scans for patterns of known attacks, an approach that is often used by virus scanners. It allows known viruses and attack behavior to be identified and only throws up the occasional false positive. The disadvantage is that if the attacker modifies the pattern, it may not be detected anymore. Another drawback: There are only few attacks on protection and control devices known until now. Yet even the first occurrence of an attack can have serious consequences, which means there is little point in adopting the signature-based approach for intrusion detection in substations.

2. Learning-based approach

Such approaches are often described with „artificial intelligence“ or „anomaly detection“. During the learning phase, the frequency of certain protocol markers is observed and the usual pattern of behavior within that particular network is learned from that. After the learning phase, the system raises an alarm as soon as one of the protocol markers behaves untypically. All actions which did not occur during the learning phase, for example, switching operations or maintenance activities, will consequently trigger an alarm.

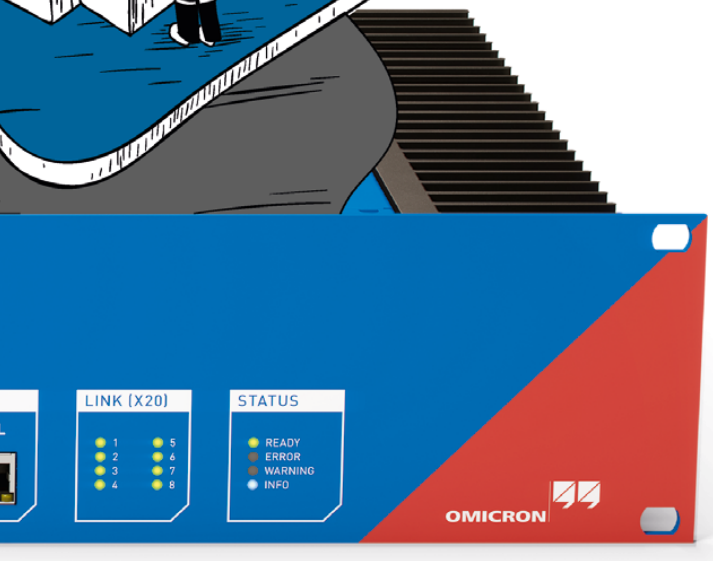
Another problem: The system only knows the protocol markers, but does not understand the communication and what is taking place in the substation. This means that the alarm messages produced can only be interpreted by IT specialists that also have IEC 61850 protocol knowledge. The high number of false alarms together with the high efforts involved to analyze them often results in alarms being discarded without being investigated which eventually results in the benefit of having an IDS being lost.

StationGuard does not apply artificial intelligence, but uses expert knowledge paired with information from the standard and the SCL files.



StationGuard knows all communication paths by evaluating the SCL files.

StationGuard has the know-how from many decades of international experience in substations.



3. The StationGuard approach

In the case of IEC 61850 substations, the entire automation system, with all its IEDs, data models, and communication parameters, is described in a standardized format known as the SCL (Substation Configuration Language). This also includes the primary assets and frequently even the single-line diagram of the substation. This information can be utilized to develop a completely new approach for detecting cyber attacks.

StationGuard creates a complete system model of the automation system and the substation and then compares every single network packet with this live system model. Even the signal values contained in messages are evaluated using the system model. This process requires no learning phase and is only using the substations SCL description and a few user inputs.

The name given to this combination of attack detection and functional monitoring is „Functional Security Monitoring“, a patented approach that we have been working on since 2010. Some aspects of this approach were implemented years ago in OMICRON products designed for IEC 61850 network analysis and monitoring, and it is the bringing together of these experiences that now makes StationGuard so intelligent.

Benefits

- Low number of false alarms, as StationGuard knows the processes in substations
- Reports are also understandable without protocol knowledge
- Reliable detection of unauthorized actions

The Whitelist Approach of StationGuard

Security down to the minutest detail

The fact that all traffic is monitored and validated in such detail means that it detects not just threats to IT security, such as illegal encodings and unauthorized control operations. StationGuard also identifies communication errors, time synchronization problems, and hence different kinds of malfunctions in the substation. If the IDS also knows the single-line diagram, then there is virtually no limit to the depths to which monitoring can be carried out.

For example: StationGuard currently recognizes 35 different alarm codes for GOOSE alone, ranging from simple sequence number errors to complex measurements, such as excessively long message transmission delays. In the latter case, the arrival times of the packets are measured and compared with the event time stamps within the messages. If the measured transmission time is longer than permitted in IEC 61850-5, StationGuard triggers an alarm message which indicates that there may be a problem with the sending IED, the network, or with the time synchronization.

Further GOOSE alarms report dangerous encoding errors or indicate critical states of the transmitted IEC 61850 quality bits.

If a device does not behave as specified according to SCL and IEC 61850, the control center will be informed immediately.

StationGuard is able to measure transmission times of packets. If the measured transmission time is longer than permitted in IEC 61850, StationGuard outputs an alarm.

StationGuard knows the behavior of all devices in the station network.

What about MMS communication? The IEC 61850 standard provides information about which data points control which items of equipment. For example, the same sequence (Select-Before-Operate) is used in the MMS protocol to control a circuit breaker or to change the IEC 61850 test mode setting. The effect in the installation is markedly different in each case. StationGuard is able to make this distinction and knows which device should be allowed to control what and in which situation.

What's the situation with other protocols? StationGuard analyzes several protocols right down to the minutest detail; this list of protocols will grow more and more in the future. In the case of proprietary protocols, for example the engineering protocols of protection relays, the transmitted information itself cannot be analyzed. However, StationGuard still monitors the connection establishment to determine whether a particular device is permitted to carry out a particular action at a particular time. Only the engineering PC, for example, can then be permitted to configure protection parameters only during maintenance. More information on this can be found in the following pages.

Benefits

- Every single packet is compared to the whitelist
- Not only cyber threats but also communication problems are detected
- StationGuard supervises the secure function of all communication in the substation

Tailor-made for substations

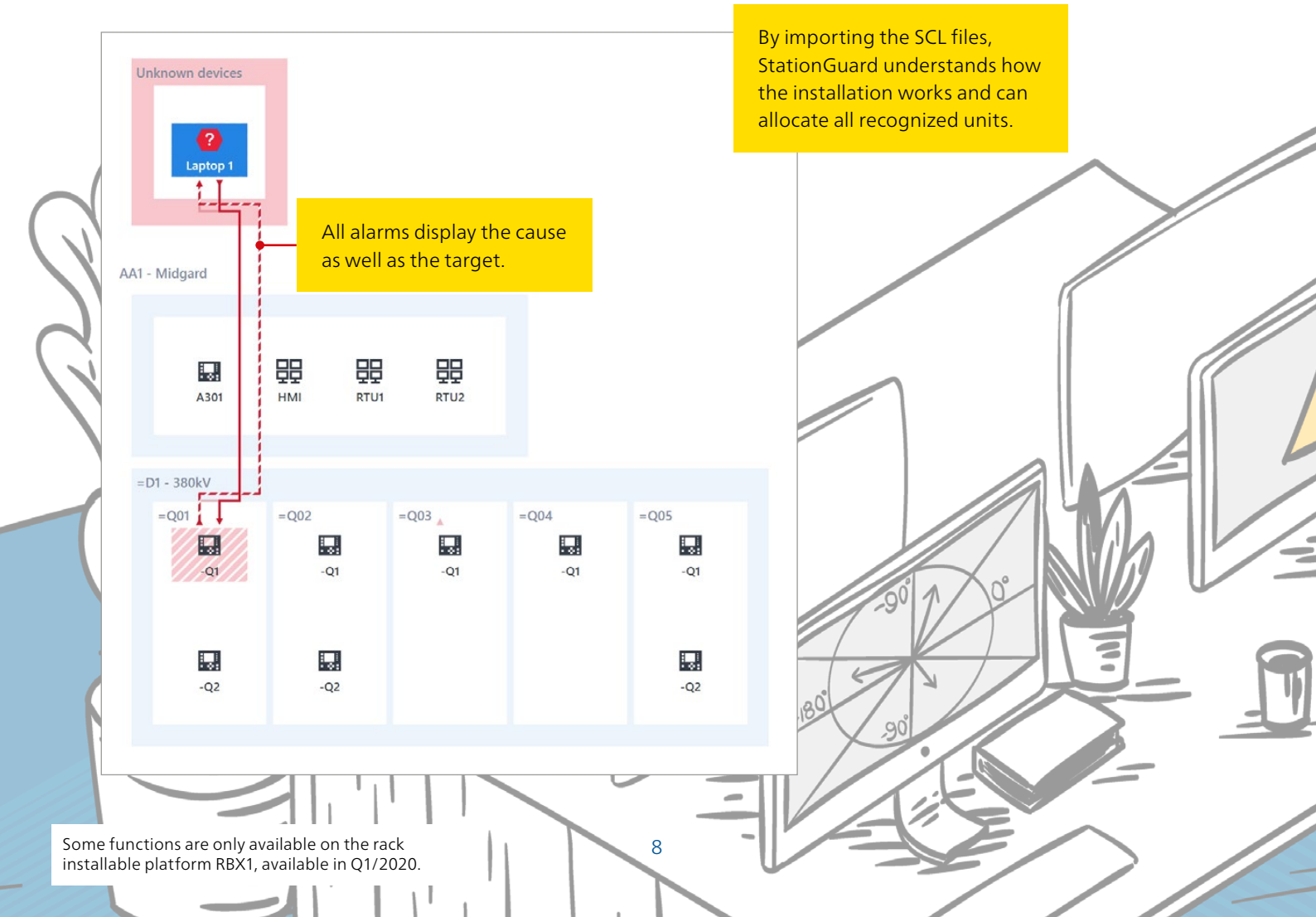
The protection system and the substation automation system (SAS) are part of the critical infrastructure of the power grid. To set up, operate, and maintain conventional Intrusion Detection Systems (IDS), IT specialists and substation engineers are needed. Both types of specialists must be on call around the clock to be able to respond when an alarm occurs. The costs involved with this are unacceptable for many utilities. StationGuard offers substation operators a new, low maintenance alternative.

IEC 61850 substations are documented in detail through their SCL files. StationGuard can import these files to determine the expected behavior of all the substation automation devices. In addition, StationGuard is aware of the typical functions in substations and how the IT equipment deployed in substation installations, such as engineering PCs and test PCs, is expected to be used. As all this information is available automatically, the setup of StationGuard is completed in just a few minutes.

Setup

After connecting StationGuard to the mirror ports of the network switches, all devices active in the network are discovered and displayed automatically. After importing the SCL files, all IEDs are identified and integrated into a diagram of the substation. After that, any IT equipment not included in the SCL can be assigned its respective role, such as an engineering PC or testing PC. If required, or if the SCL files were incomplete, manual editing is possible. StationGuard can analyze up to eight network segments simultaneously.

Should the communication not match the SCL file, StationGuard will report IEC 61850 configuration verification errors. This is particularly helpful during the factory and site acceptance testing phases.



Some functions are only available on the rack installable platform RBX1, available in Q1/2020.

Normal operation

StationGuard analyzes all communication and knows precisely which information may or may not be transmitted at any given moment in time. It is also aware of the workflows and conditions during normal operations: Which devices are allowed to be active now? Which control commands are permitted and does the response to them make sense? Which measured values are being transmitted? Is the timing of the messages correct? This enables any likely problems with the IEDs or the network to be detected at an early stage or before they fail.

This comprehensive functional and security monitoring is unique and offers advantages that go well beyond those normally expected of a security system.

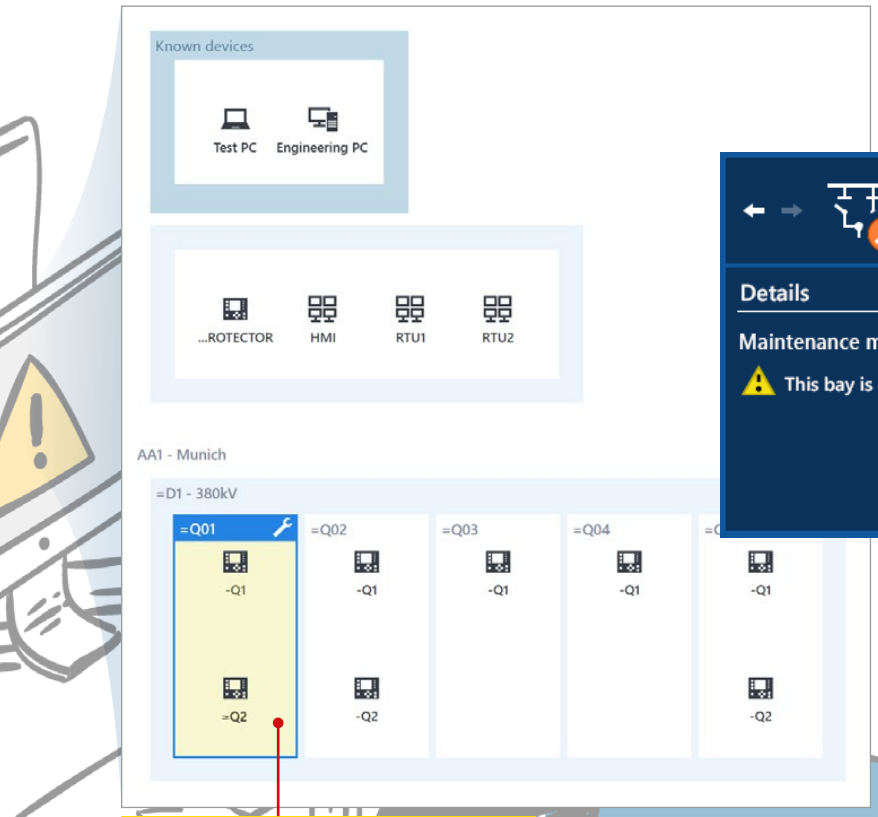
The graphical user interface allows protection and control engineers to quickly get to grips with StationGuard, as it matches the documentation diagrams and the event view in the station controllers.

Behavior during routine testing

Testing and maintenance is important and must not result in any false alarms, yet still a high level of IT security has to be ensured. To satisfy these requirements, StationGuard offers a „maintenance mode". Maintenance and testing activity will only be permitted when this mode is activated for a particular bay or for the substation as a whole.

Some attack scenarios use the engineering interface of IEDs. Therefore, StationGuard can alarm if communication with manufacturer's tools happens during normal operation and only permit it while in maintenance mode. A list of testing PCs and test sets can be imported in StationGuard before they are used so that authorized tasks can be performed without triggering false alarms.

This has no adverse impact on the security while testing: If an infected testing PC communicates suspiciously, not to mention tries to initiate a switching operation, an alarm will be raised.



Maintenance and testing operations permitted in bay 1

In routine testing, individual bays can get permission for temporary maintenance actions.

Advantages

- Particularly easy to set up
- No false alarms during routine testing but still a high security level
- No learning phase, immediate protection

Easily understandable alarm messages

Reliably identify the cause of alarms

The reports triggered by a security system should assist the operator, not cause further confusion. This is why the alarms of StationGuard not only appear in an event list, as it is the case with firewalls, but are shown graphically in the overview diagram. The language and terms used in the alarm messages are understandable – special IT terminology is avoided.

Example: A testing PC tries to control the circuit breaker. The associated alarm message is not displayed using protocol terms, but is interpreted according to what actually happened in the substation. It will contain information such as: What happened? Which device is responsible?

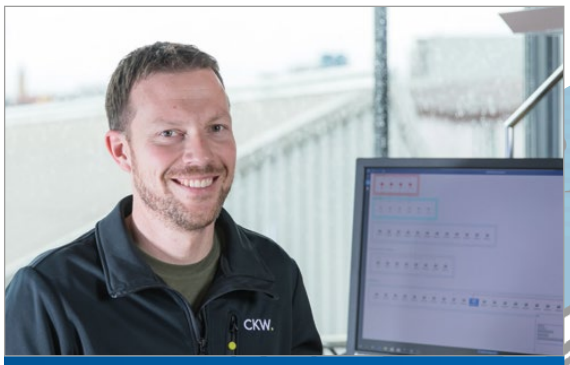
Protection and control engineers will, in most cases, now be able to identify most of the alarms without any help of IT security specialists. Substation engineers can thus use the IDS as if they were studying an operating log, an event list, and/or a warning list in their station controller.

Analyzing and forwarding alarms

When an alarm occurs, it is output via the binary outputs on the RBX1 hardware platform which enables easy forwarding to the control center via the gateway. In this case, alarm signaling takes place without any network communication and the alarms can be integrated into the SCADA signal list just like any other hard-wired signal.

Alternatively, alarms can also be forwarded to a dedicated Security Incident Event Management (SIEM) system, whose function is to collect the security warnings from all devices in the substation.

Furthermore, the StationGuard control software supports security specialists by providing detailed views about protocols IT security relevant parameters. This combination of views enables substation engineers and IT experts to jointly analyze the generated alarms.



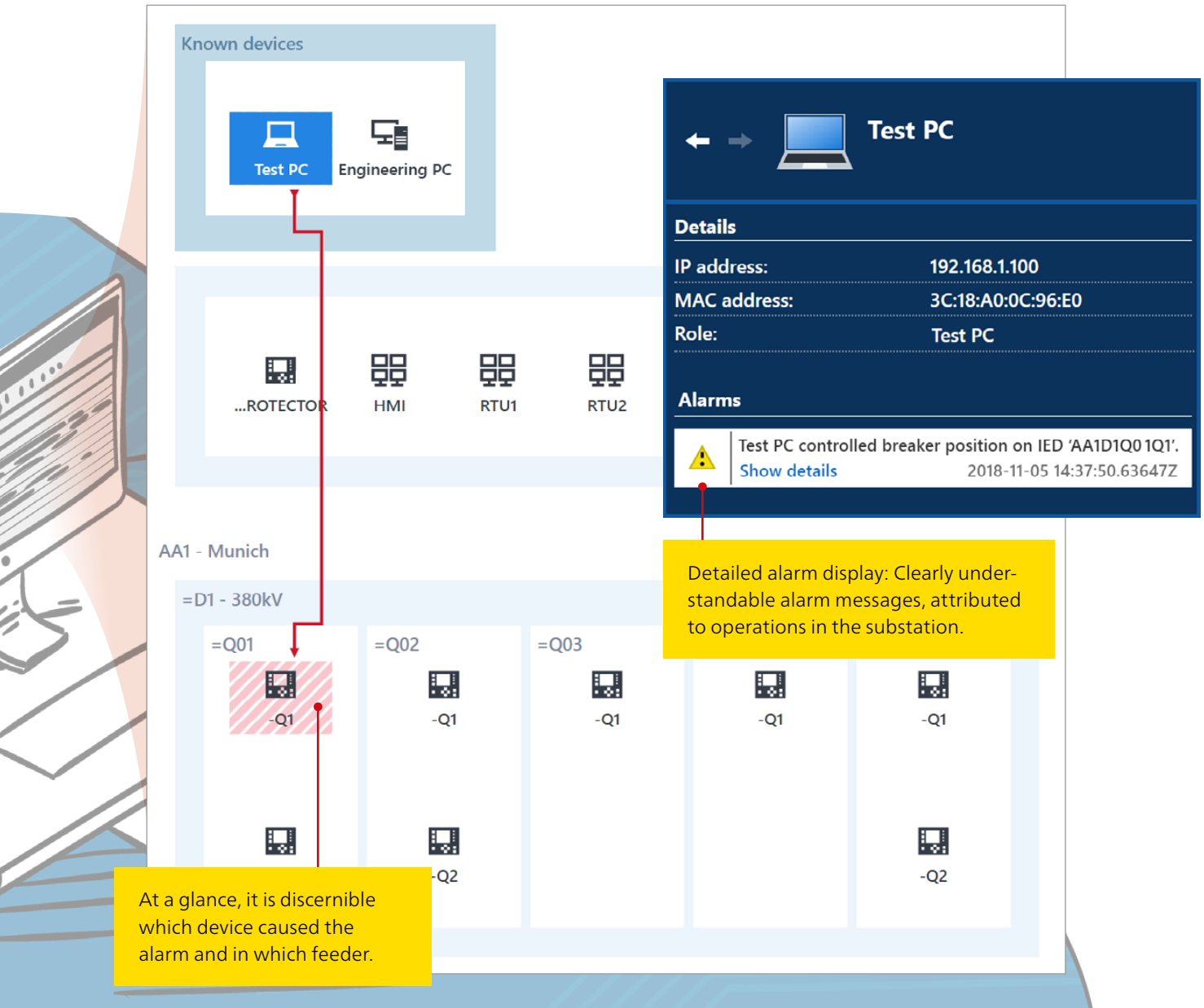
> It is really easy to work with StationGuard. All necessary information is displayed clearly and without any IT slang. And all this in the high OMICRON quality that we are used to.
>
> **Yann Gosteli**
> Head of Substation Automation Systems
> CKW AG, Switzerland

„It was important for us in development that the logbook cannot be modified. Events can be archived, but not deleted."

Logbook

In addition to the graphical view, alarms are also recorded in an event log, the logbook. If an authorized user makes configuration changes or acknowledges alarms, this is recorded there.

In the logbook, for example, all past events relating to a particular device can be accessed. With that, trends can also be detected even for events only occurring sporadically.



StationGuard fits into your IT-Security Strategy

Cyber security only works properly when people, processes, and technology work together. One of the key questions is, therefore: What are the processes when security alarms occur? Our objective with StationGuard is to support these response processes.

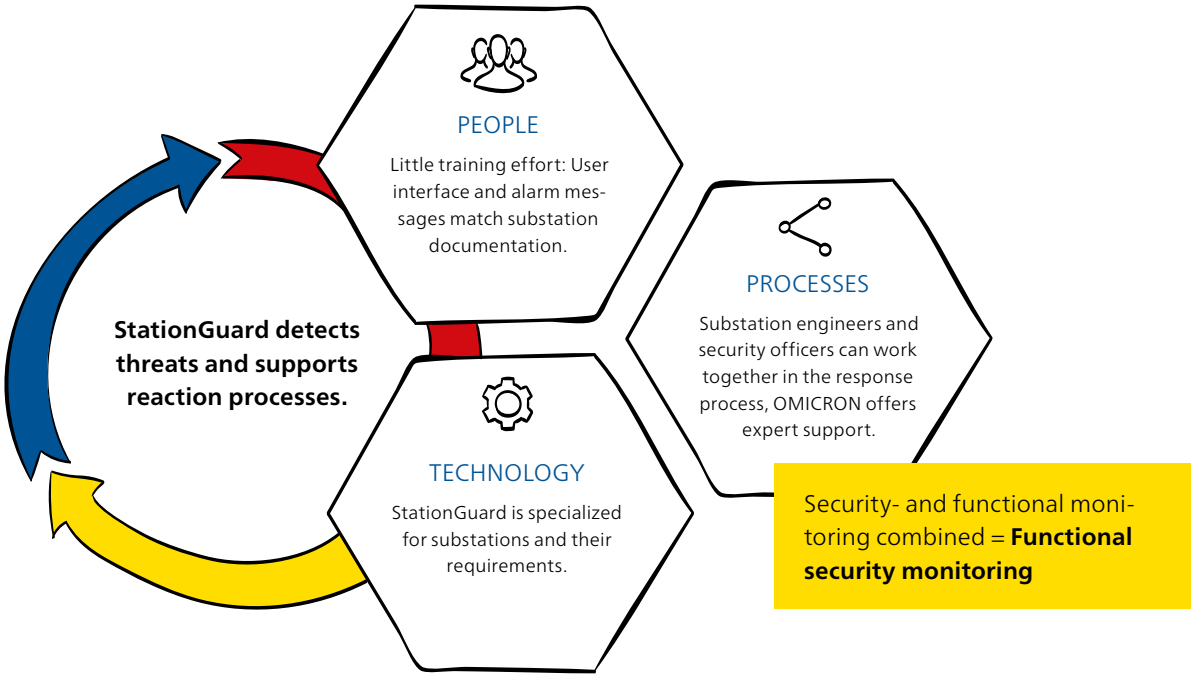
False alarms often occur when engineers are carrying out work on the substation, restart devices, or protection events happen. StationGuard is familiar with the typical events and the user interface is adapted to the diagrams and terminology used in substations. This enables protection and control engineers to quickly determine whether an alarm is the result of a known operation, or whether it warrants further investigation by security officers.

By combining substation-specific visualizations for protection engineers and detailed information for IT specialists, all those involved in analyzing alarms are able to work together to find the cause.

Integrates seamlessly into the substation IT environment

- **Logbook**
  StationGuard records critical actions, such as configuration changes or the acknowledgment of alarms. These entries cannot be modified.
- **Network traces** [1]
  A Wireshark-compatible (PCAP) network trace is created for every event for subsequent analysis.
- **User authentication** [1]
  StationGuard can be integrated into the user authentication system RADIUS. Only authorized users can change the configuration or activate maintenance mode.
- **SIEM system integration** [1]
  StationGuard also makes alarms available in the Syslog protocol so they can be integrated into a Security Incident Event Management (SIEM) system.
- **Time synchronization**
  StationGuard can be time-synchronized with the installation using the NTP or PTP [1] protocol.

[1] Available with RBX1 platform in Q1/2020



Rigorously hardened platform

- **Secure crypto chip**
  Keys and certificates are exclusively stored on an anti-tampering, anti-counterfeiting chip according to ISO/IEC 11889.
- **Secure boot chain**
  The crypto chip is used to help enforce a secure boot chain, which means that at every stage of the startup process, the signatures of the next module to be loaded are verified. This ensures that only OMICRON software can be executed on the device.
- **Signed and encrypted updates**
  The StationGuard device will only accept firmware updates that have been signed by OMICRON. PC software updates are also signed.
- **Secure production process**
  The keys are securely stored on OMICRON's premises on hardware security modules; private keys cannot be extracted.
- **Full disk encryption**
  The crypto chip is used to encrypt all data with a key unique for each device.
- **Customized BIOS**
  We use our own, specific BIOS to ensure that only certificates from OMICRON are installed for the boot process and that secure default values are loaded in the event of a BIOS reset.
- **Special, hardened operating system**
  A dedicated, hardened Linux system is used in which only services are deployed which StationGuard needs for its operation. Each process only gets the privileges and capabilities absolutely required for the task it is to perform.
- **Encrypted communication between unit and PC**
  Communication between StationGuard and the PC is encrypted using TLS (Transport Layer Security) and protected against tampering.
- **Our specialists continue to develop...**
  Security researchers are constantly developing new measures to harden platforms even more, and OMICRON experts are constantly implementing these in StationGuard. Most updates to StationGuard will be accompanied by new hardening measures.

Exceptional support

StationGuard expert support

If an alarm indicates unauthorized behavior of PCs or field devices, or behavior that is not standards-compliant, the StationGuard experts can offer you support in analyzing the alarm. Our specialists can analyze network captures and they can determine, based on the communication behavior and the known vulnerabilities for the involved devices, if the event could represent a threat or if it was caused by a technical problem.

Feel free to approach our technical support who will, after the secure transmission of the related event data, contact an expert in one of the OMICRON offices. Our specialists know the communication behavior as well as the vulnerabilities known for protection, automation, and control devices of almost all vendors worldwide.

Of course, we treat all data submitted to us as strictly confidential.

„As a member of standardization working groups and author of numerous articles about substation communication, I am often contacted by utilities when it comes to sophisticated problems with GOOSE, Sampled Values and MMS communication."

Dr. Fred Steinhauser
Expert for digital substations

"As an expert for security vulnerabilities in field devices, I know exactly how to recognize attacks in the network. With this knowledge I support you gladly!"

Stefan Lässer
Expert for security vulnerabilities in IEC 61850 IEDs

24/7 technical support

Should you require rapid assistance, you will receive excellent support from our highly trained and dedicated technicians, 24 hours a day, seven days a week.

We pride ourselves on exceptional customer service and premium quality.

"I joined the OMICRON technical support in 2010 and I have been focusing on IEC 61850 since."

Lukas Gassner
OMICRON support

24/7 support

Technical Specifications of the RBX1 Platform

The RBX1 platform was specifically designed to be installed in substations.

Environmental conditions

Temperature (in operation)	-20 °C ... 55 °C / -4 °F ... 131 °F
Temperature (on stock and transportation)	-25 °C ... 70 °C / -13 °F ... 158 °F
Rel. air humidity	5 to 95 % (non-condensing)
Protection category	IP30

Standards

Product standards	IEC 61850-3:2013 IEEE 1613-2009 Severity Level: Class 1
EMC standards	IEC 61326-1, IEC 60255-26, IEC 61000-6-5
Safety	EN 60255-27, EN 61010-1, EN 61010-2-030

See further details in the technical data sheet.

USB
4x USB 3.0

Network
1x 1 Gbit/s RJ45 with
IEEE 1588 Power Profile support

Binary inputs
4 inputs in 2 potential groups,
CAT III 250 V

Configurable threshold

Binary outputs
8 outputs in 2 potential groups,
≈ 250 V / 8 A

Performance
Cooled passively,
Quad-Core processor

16 GB ECC RAM
(error correcting)

Specific crypto chip

**Watchdog/
life contact**

Network
4x 1 Gbit/s SFP + RJ45 as combo ports

4x 1 Gbit/s SFP

All with IEEE 1588 Power Profile support

Supply
100 ... 240 V DC /+10%
and 85 ... 240 V AC /+10%

44 ... 70 V DC /+10%

(redundant supply
optional)

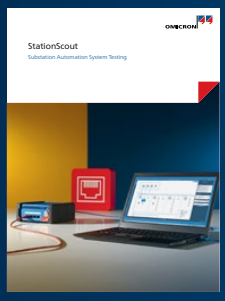
Screen port
1x HDMI

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.

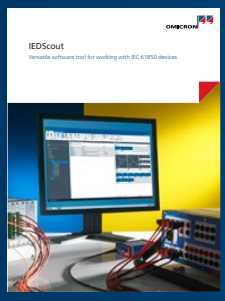
Customers in more than 160 countries rely on the company's ability to supply leading-edge technology of excellent quality. Service centers on all continents provide a broad base of knowledge and extraordinary customer support. All of this together with our strong network of sales partners is what has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

The following publications provide further information on the solutions described in this brochure:

IEC 61850
Brochure



StationScout
Brochure



IEDScout
Brochure

DANEO 400
Brochure

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

www.omicronenergy.com