# StationGuard

## Cybersecurity and Functional Monitoring for Energy Systems

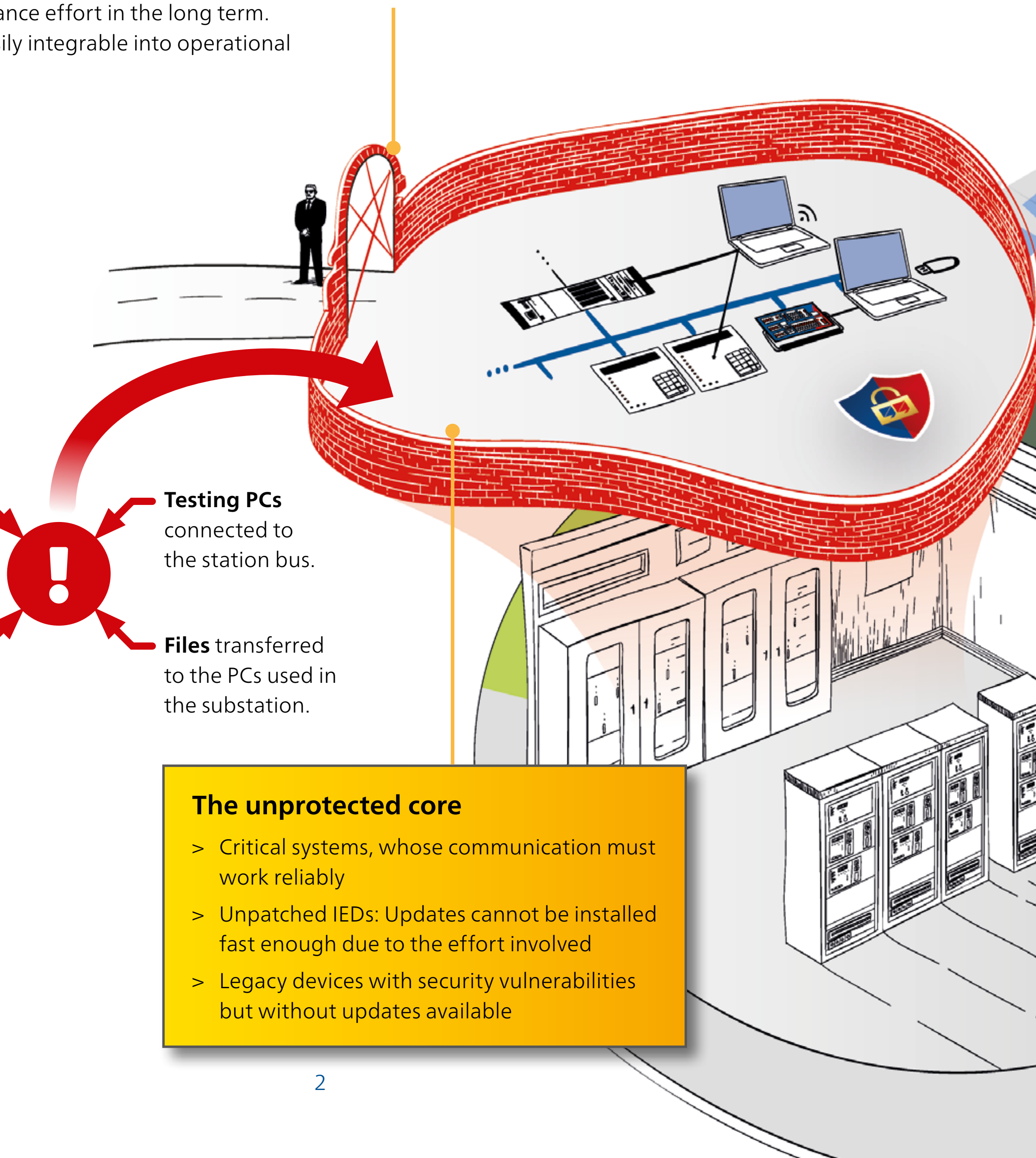
# IT security in substations

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 networks also represent critical attack vectors. As a consequence, the operation and maintenance processes of these substations must also be included in the cybersecurity 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 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 operational and maintenance workflows.

**Firewall**

Firewalls ensure that only specific endpoints can communicate with the devices in the substation, using only permitted protocols. However, there are ways of circumventing firewalls.



Attack points circumventing firewalls:

**Remote access** for maintenance and control.

**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 the firewall. Many substations employ remote access to retrieve fault records or for maintenance. These connections provide a route by which malware can find its way into the devices in the substation.

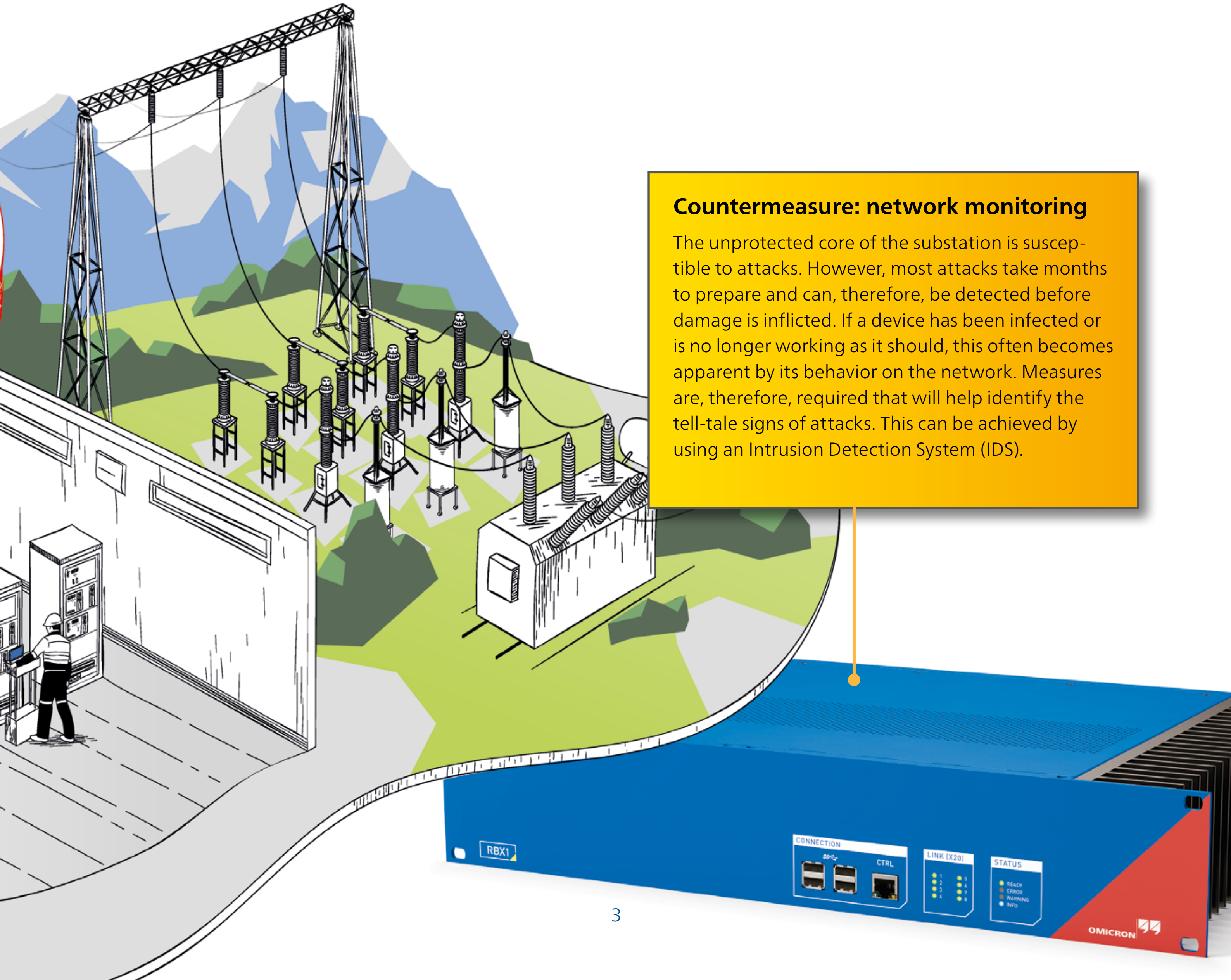
Maintenance and testing PCs provide another attack vector. These PCs are either connected to the entire network, or directly to individual protection or control devices.

## 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 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: network monitoring

The unprotected core of the substation is susceptible to attacks. However, most attacks take months to prepare and can, therefore, be detected before damage is inflicted. If a device 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

Intrusion detection systems are typically based on one of these two approaches:

## 1. Signature-based approach (blocklist)

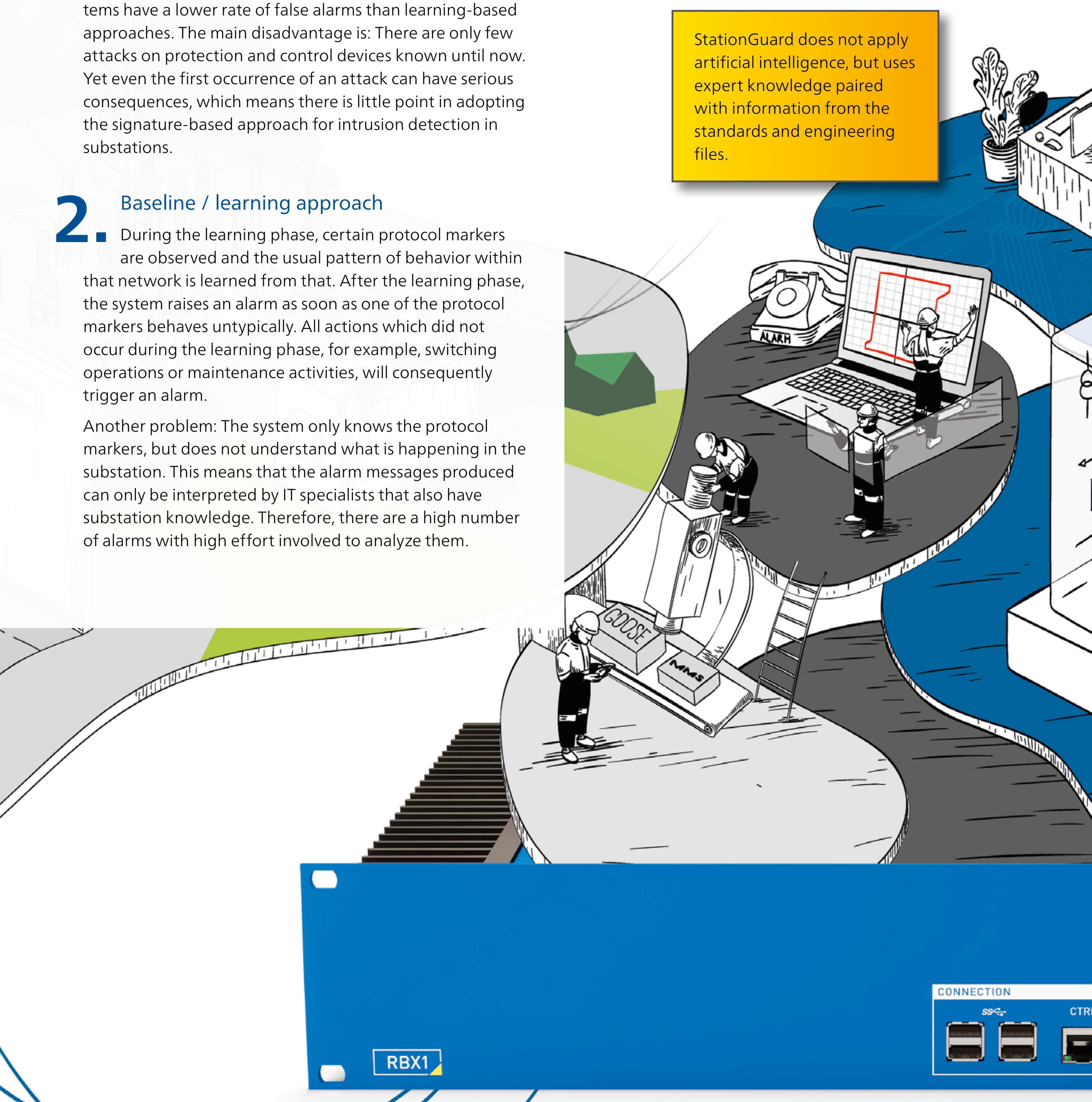
The IDS scans for patterns of known attacks, an approach that is also used by virus scanners. Such systems have a lower rate of false alarms than learning-based approaches. The main disadvantage is: There are only few attacks on protection and control devices known until now. Yet even the first occurrence of an attack can have serious consequences, which means there is little point in adopting the signature-based approach for intrusion detection in substations.

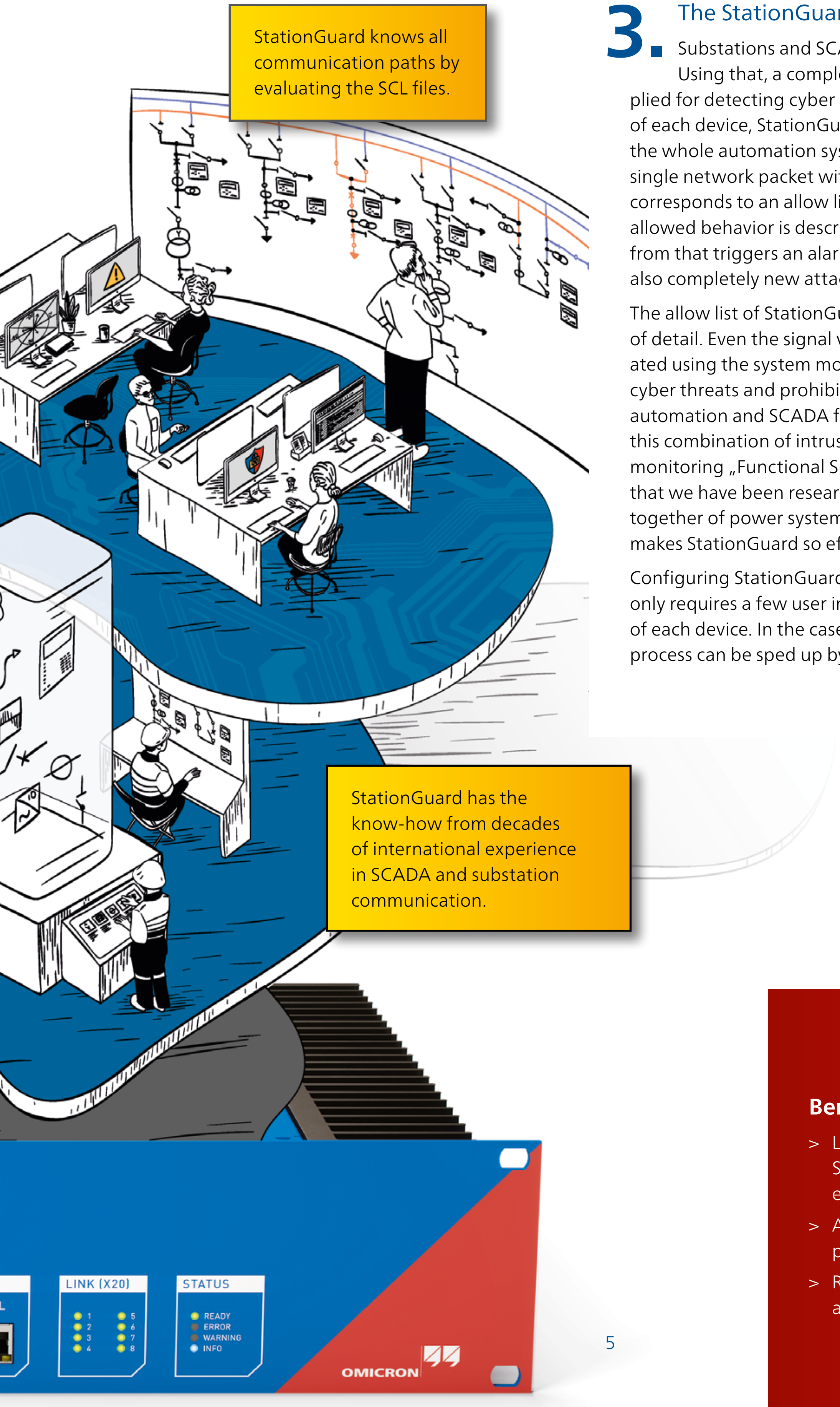
## 2. Baseline / learning approach

During the learning phase, certain protocol markers are observed and the usual pattern of behavior within that 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 what is happening in the substation. This means that the alarm messages produced can only be interpreted by IT specialists that also have substation knowledge. Therefore, there are a high number of alarms with high effort involved to analyze them.

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





StationGuard knows all communication paths by evaluating the SCL files.

StationGuard has the know-how from decades of international experience in SCADA and substation communication.

## 3. The StationGuard approach

Substations and SCADA systems are deterministic: Using that, a completely new approach can be applied for detecting cyber attacks: By knowing the function of each device, StationGuard creates a system model of the whole automation system and then compares every single network packet with this live system model. This corresponds to an allow list (whitelist) approach, where all allowed behavior is described and everything deviating from that triggers an alarm by default. Using this approach also completely new attack types are detected.

The allow list of StationGuard goes into the minutest level of detail. Even the signal values in the messages are evaluated using the system model. This allows to detect not only cyber threats and prohibited activity, but also issues in the automation and SCADA functions. That's why we named this combination of intrusion detection and functional monitoring „Functional Security Monitoring", an approach that we have been researching since 2010. It is the bringing together of power system and security knowledge that makes StationGuard so effective.

Configuring StationGuard requires no learning phase and only requires a few user inputs to describe the purpose of each device. In the case of IEC 61850 substations, this process can be sped up by importing SCL files.

### Benefits

- Low number of false alarms, as StationGuard knows the processes in energy systems
- Alarms are understandable without protocol knowledge
- Reliable detection of unauthorized actions

# The Allow List (Whitelist) approach of StationGuard

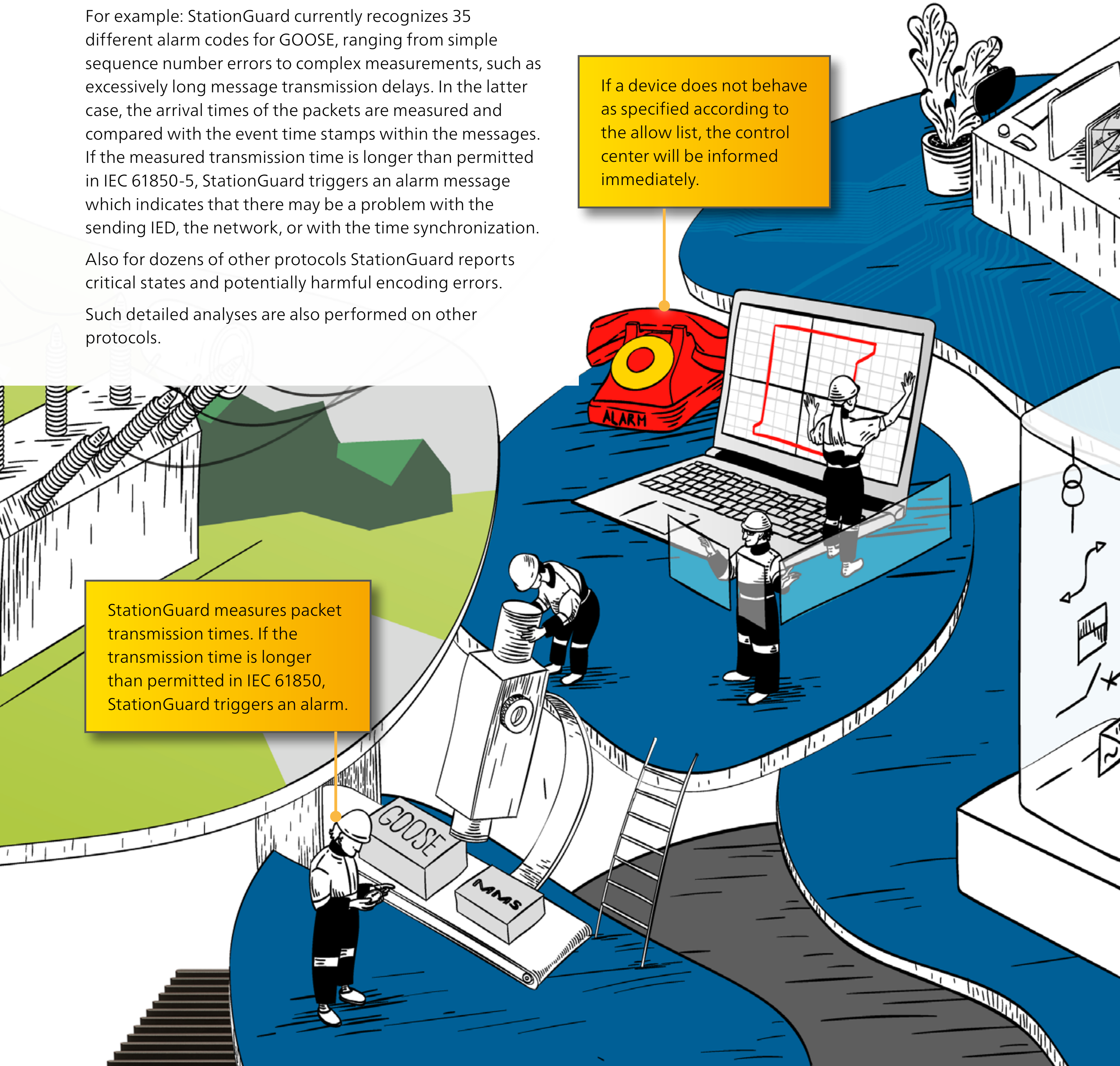
## Security down to the minutest detail

The fact that all network 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, 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.

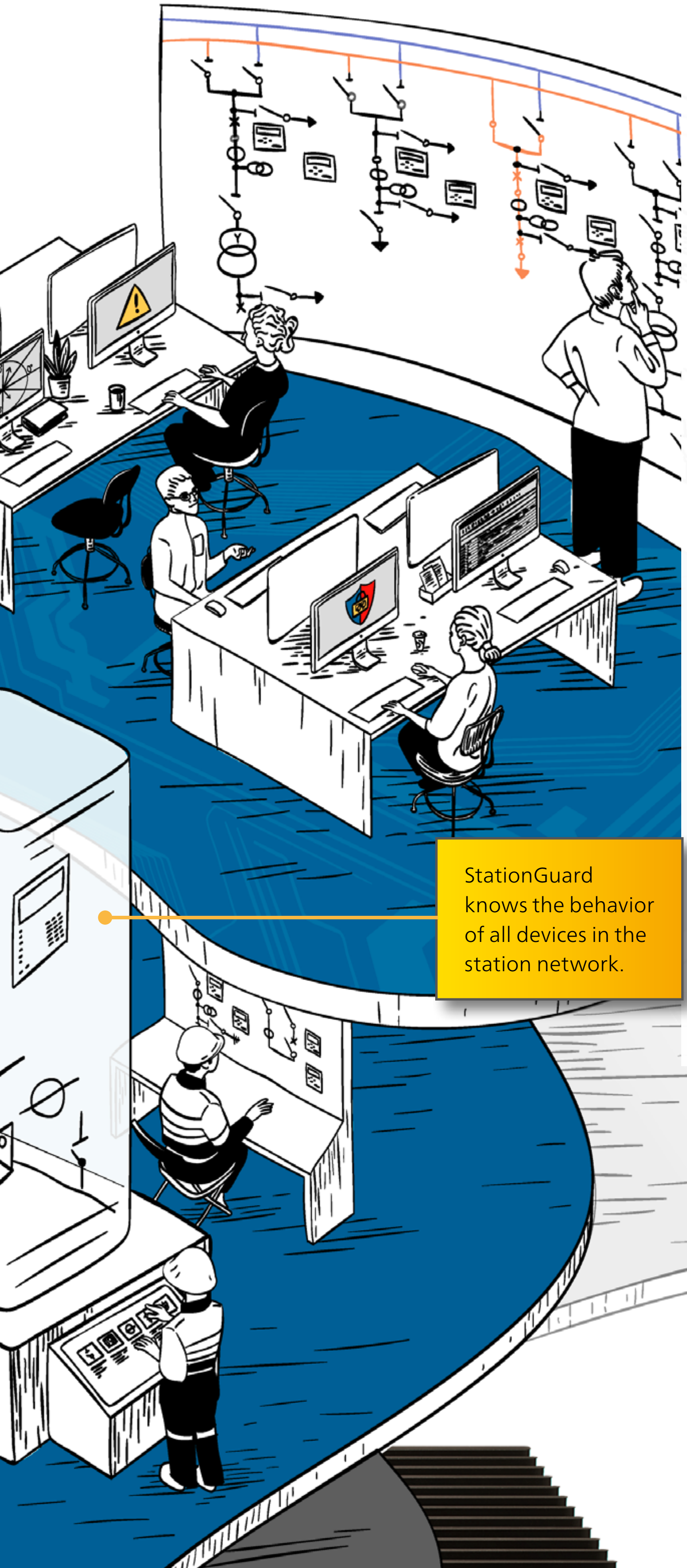
Also for dozens of other protocols StationGuard reports critical states and potentially harmful encoding errors.

Such detailed analyses are also performed on other protocols.



If a device does not behave as specified according to the allow list, the control center will be informed immediately.

StationGuard measures packet transmission times. If the transmission time is longer than permitted in IEC 61850, StationGuard triggers an alarm.



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

## MMS, IEC 60870-5-104 and DNP3 Communication

StationGuard is aware of which data points control which functions. For example, the same command may be used to control a circuit breaker, a tap changer and to change the test mode setting of a device. The effect in the substation is markedly different in each case. StationGuard is able to make this distinction and knows which device should control what and in which situation. These fine-grained permissions are documented and can be reviewed in StationGuard.

## Other Protocols

StationGuard performs deep packet inspection on dozens of power systems and classical IT protocols. Using this, StationGuard not only detects encoding violations in these protocols, but also if port numbers e.g., of remote connections are hijacked by unexpected applications (port spoofing).

## Supported Protocols (Deep Packet Inspection)

- IEC 61850
- IEC 60870-5-104
- DNP3
- PRP/HSR
- Modbus TCP
- Synchrophasor
- DLMS/COSEM
- AMI
- TASE.2/ICCP
- FTP
- HTTP
- RDP
- NTP
- ARP, DHCP, ICMP
- MySQL, MS SQL, PostgreSQL
- HTTPS, SSH (application detection, without decryption)
- telnet
- RIPv2
- SSDP
- ...

### Benefits

> Every single packet is compared to the allow list

> Not only cyber threats but also communication problems are detected

> StationGuard supervises the secure function of all communication in the substation and SCADA system

# Tailor-made for energy systems

To set up, operate, and maintain conventional Intrusion Detection Systems (IDS), IT specialists and automation and control 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 utilities a new, low maintenance alternative.

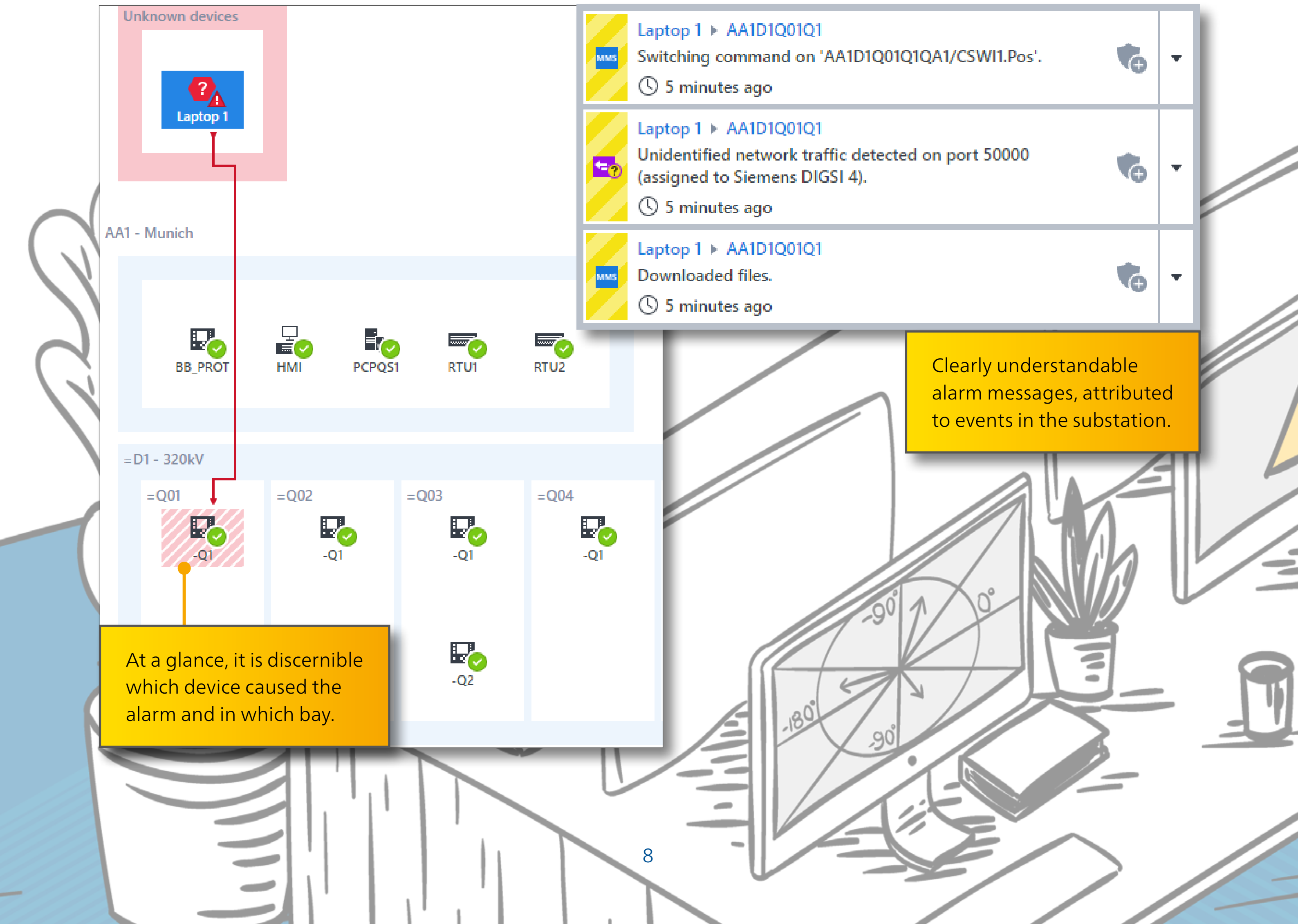
StationGuard is aware of the typical functions in substations and how the IT equipment, such as engineering PCs and test PCs, is expected to be used. As all this information is automatically available, StationGuard is quickly set up.

## Setup

After connecting StationGuard to the mirror ports of the network switches, all devices communicating in the network are detected.

For IEC 61850 substations, the engineering SCL files can be imported, to identify all IEDs automatically and to integrate them into a substation diagram. Should the communication not match the SCL file, StationGuard will report IEC 61850 configuration errors. This is particularly helpful during the factory and site acceptance testing phases.

For substations or SCADA systems using IEC 60870-5-104, DNP3 or Modbus, the IEDs and RTUs can be manually classified with a few clicks. After that, any remaining IT equipment can be assigned its respective role, such as Switch or Engineering PC. These roles can also be adapted.



Laptop 1 ▸ AA1D1Q01Q1
Switching command on 'AA1D1Q01Q1QA1/CSWI1.Pos'.
5 minutes ago

Laptop 1 ▸ AA1D1Q01Q1
Unidentified network traffic detected on port 50000 (assigned to Siemens DIGSI 4).
5 minutes ago

Laptop 1 ▸ AA1D1Q01Q1
Downloaded files.
5 minutes ago

Clearly understandable alarm messages, attributed to events in the substation.

At a glance, it is discernible which device caused the alarm and in which bay.

## Normal operation

StationGuard analyzes all communication and knows precisely which information may or may not be transmitted at any given moment. 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.

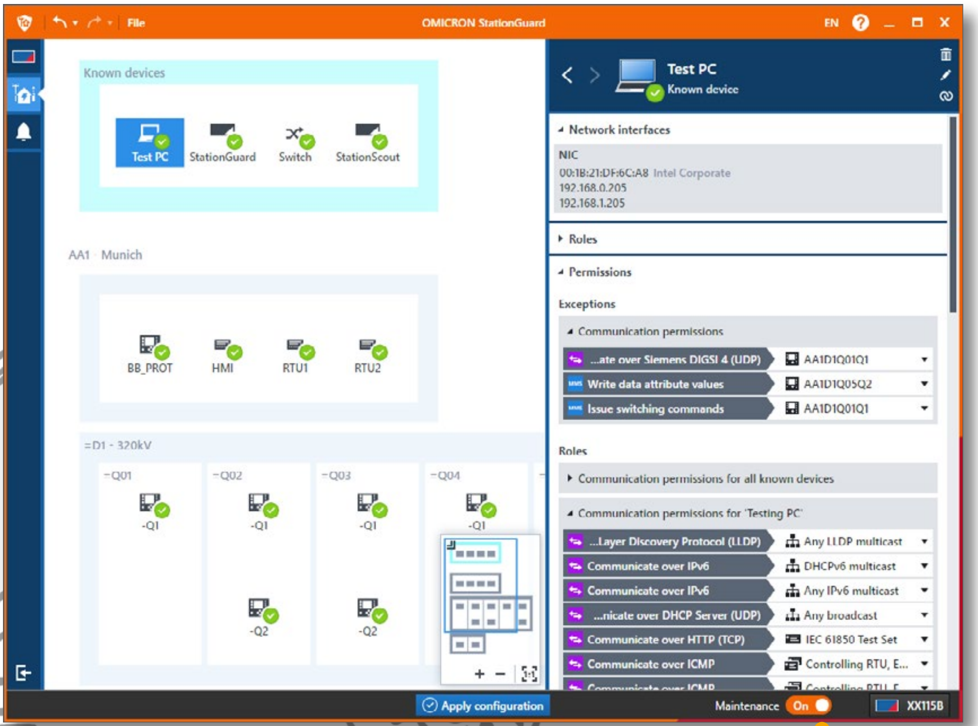
The graphical user interface allows protection and control engineers to quickly get to grips with StationGuard, as it matches the documentation diagrams and the event view in the station controllers.

## Maintenance and Commissioning

Testing and maintenance is important and must not result in any false alarms, yet still a high level of 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.

In many attack scenarios, vulnerabilities in vendor protocol or web interfaces are exploited. Therefore, StationGuard can alarm if communication with manufacturer's tools happens during normal operation and only permit it while in maintenance mode. The engineering PCs and test sets can be registered 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, an alarm will be raised.



Test PC
Known device

Network interfaces

NIC
00:1B:21:DF:6C:A8 Intel Corporate
192.168.0.205
192.168.1.205

Roles

Permissions

Exceptions

Communication permissions

| | |
|---|---|
| ...ate over Siemens DIGSI 4 (UDP) | AA1D1Q01Q1 |
| Write data attribute values | AA1D1Q05Q2 |
| Issue switching commands | AA1D1Q01Q1 |

Roles

Communication permissions for all known devices

Communication permissions for 'Testing PC'

| | |
|---|---|
| ...Layer Discovery Protocol (LLDP) | Any LLDP multicast |
| Communicate over IPv6 | DHCPv6 multicast |
| Communicate over IPv6 | Any IPv6 multicast |
| ...nicate over DHCP Server (UDP) | Any broadcast |
| Communicate over HTTP (TCP) | IEC 61850 Test Set |
| Communicate over ICMP | Controlling RTU, E... |
| Communicate over ICMP | Controlling RTU, E... |

Certain actions are only allowed during maintenance mode.

### Advantages

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

# Faster response through understandable alert messages

## Reliably identify the cause of alerts

The alerts triggered by a security system should assist the operator, not cause further confusion. This is why the alerts of StationGuard not only appear in an event list, but are shown graphically in the overview diagram. The power system events behind the network packets are identified and displayed in clear terminology.

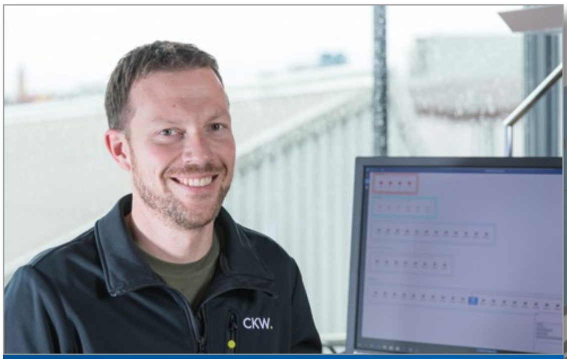
Example: A testing PC attempts to control the circuit breaker using the MMS protocol. The associated alert message is not displayed using protocol terms, but is interpreted according to what actually happened in the substation. It contains information such as: What happened? Which device is responsible?

This allows IT security officers and SCADA and protection engineers to collaborate efficiently to determine the cause of an alert. Substation engineers can thus IDS alert messages as if they were studying an operating log, an event list, or a warning list in their station controller.

## Analyzing and forwarding alerts

An easy way to integrate StationGuard into legacy substations is by using the binary outputs of the RBX1 platform. The presence of an unacknowledged alarm is signaled on the binary outputs, which can be wired to an RTU and integrated into the SCADA signal list.

Alternatively, our easily understandable alert messages can also be forwarded using the Syslog protocol. Various plug-ins are available to integrate StationGuard into Security Information and Event Management Systems and into ticketing systems of different vendors.

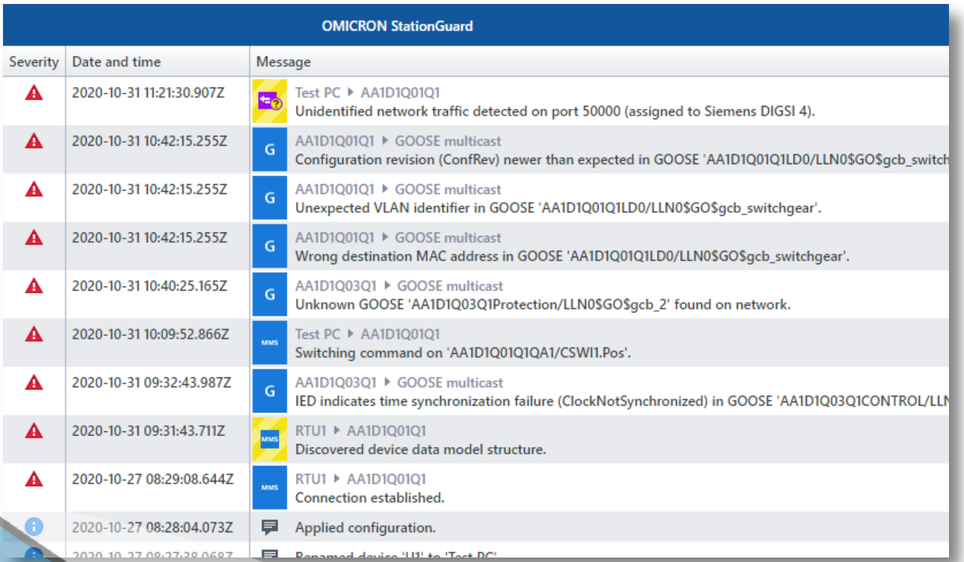


> “It is really easy to work with StationGuard. All necessary information is displayed clearly and without any IT slang. And all this in the high OMICRON quality that we are used to.”
>
> **Yann Gosteli**
> Head of Substation Automation Systems
> CKW AG, Switzerland

## Event log

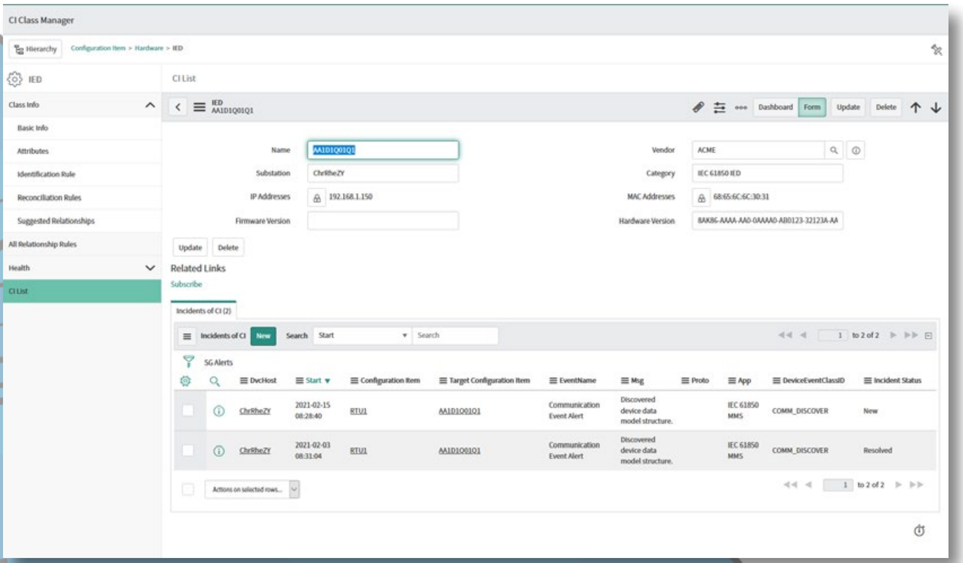
In addition to the graphical view, alarms are also recorded in an event log. If a user makes configuration changes or acknowledges alarms, this is recorded there as well as critical events, like control operations, IED test mode changes and file downloads, including the file name.

In the event log, 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.



OMICRON StationGuard

| Severity | Date and time | Message |
|---|---|---|
| ⚠ | 2020-10-31 11:21:30.907Z | Test PC ▸ AA1D1Q01Q1<br>Unidentified network traffic detected on port 50000 (assigned to Siemens DIGSI 4). |
| ⚠ | 2020-10-31 10:42:15.255Z | G AA1D1Q01Q1 ▸ GOOSE multicast<br>Configuration revision (ConfRev) newer than expected in GOOSE 'AA1D1Q01Q1LD0/LLN0$GO$gcb_switch |
| ⚠ | 2020-10-31 10:42:15.255Z | G AA1D1Q01Q1 ▸ GOOSE multicast<br>Unexpected VLAN identifier in GOOSE 'AA1D1Q01Q1LD0/LLN0$GO$gcb_switchgear'. |
| ⚠ | 2020-10-31 10:42:15.255Z | G AA1D1Q01Q1 ▸ GOOSE multicast<br>Wrong destination MAC address in GOOSE 'AA1D1Q01Q1LD0/LLN0$GO$gcb_switchgear'. |
| ⚠ | 2020-10-31 10:40:25.165Z | G AA1D1Q03Q1 ▸ GOOSE multicast<br>Unknown GOOSE 'AA1D1Q03Q1Protection/LLN0$GO$gcb_2' found on network. |
| ⚠ | 2020-10-31 10:09:52.866Z | MMS Test PC ▸ AA1D1Q01Q1<br>Switching command on 'AA1D1Q01Q1QA1/CSWI1.Pos'. |
| ⚠ | 2020-10-31 09:32:43.987Z | G AA1D1Q03Q1 ▸ GOOSE multicast<br>IED indicates time synchronization failure (ClockNotSynchronized) in GOOSE 'AA1D1Q03Q1CONTROL/LLN |
| ⚠ | 2020-10-31 09:31:43.711Z | MMS RTU1 ▸ AA1D1Q01Q1<br>Discovered device data model structure. |
| ⚠ | 2020-10-27 08:29:08.644Z | MMS RTU1 ▸ AA1D1Q01Q1<br>Connection established. |
| ⓘ | 2020-10-27 08:28:04.073Z | Applied configuration. |
| ⓘ | 2020-10-27 08:27:38.068Z | Renamed device 'U1' to 'Test PC'. |



CI Class Manager

Hierarchy Configuration Item > Hardware > IED

IED

CI List

IED AA1D1Q01Q1

Name: AA1D1Q01Q1

Substation: ChrRheZY

IP Addresses: 192.168.1.150

Firmware Version:

Vendor: ACME

Category: IEC 61850 IED

MAC Addresses: 68:65:6C:6C:30:31

Hardware Version: 8AK86-AAAA-AA0-0AAAA0-AB0123-32123A-AA

Update Delete

Related Links

Subscribe

Incidents of CI (2)

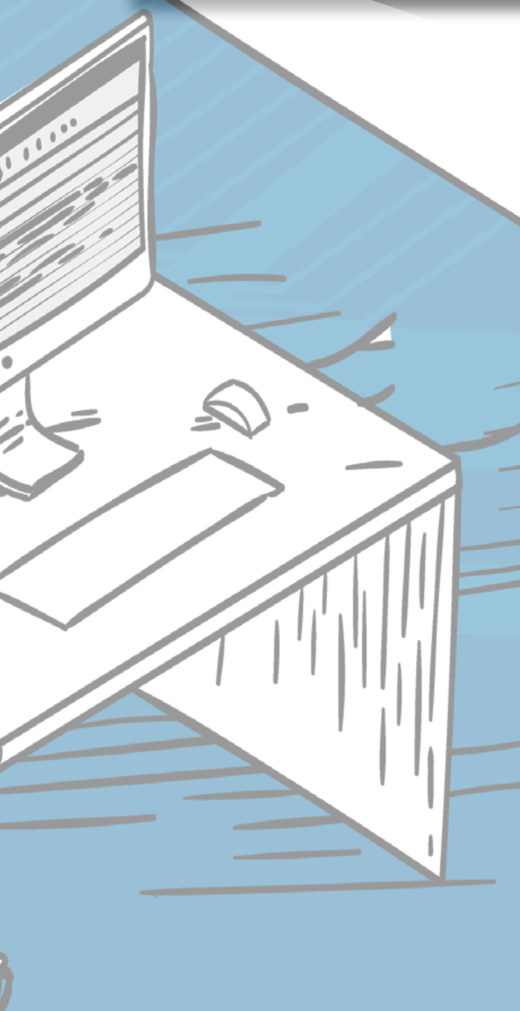
Incidents of CI New Search Start Search 1 to 2 of 2

SG Alerts

| | | DvcHost | Start ▼ | Configuration Item | Target Configuration Item | EventName | Msg | Proto | App | DeviceEventClassID | Incident Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ⓘ | ChrRheZY | 2021-02-15 08:28:40 | RTU1 | AA1D1Q01Q1 | Communication Event Alert | Discovered device data model structure. | | IEC 61850 MMS | COMM_DISCOVER | New |
| □ | ⓘ | ChrRheZY | 2021-02-03 08:31:04 | RTU1 | AA1D1Q01Q1 | Communication Event Alert | Discovered device data model structure. | | IEC 61850 MMS | COMM_DISCOVER | Resolved |

□ Actions on selected rows... 1 to 2 of 2

StationGuard ServiceNow (TM) Plug-In



# StationGuard fits into your IT-security strategy

Cybersecurity 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 alerts 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 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 security officers, all are able to work together to find the cause.

## Integrates seamlessly into OT-security processes

√ **Event log**
StationGuard records critical actions, such as switching operations, IED setting changes, or the acknowledgment of alarms.

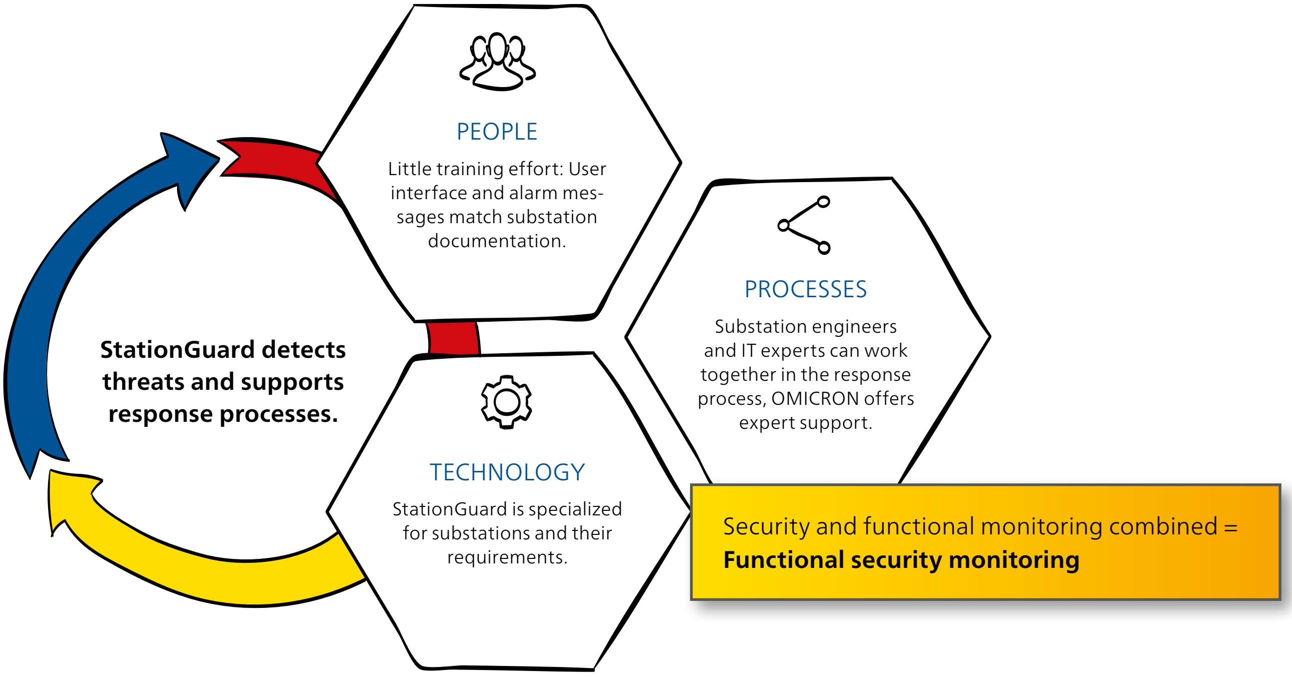
√ **Asset discovery and export**
All devices in the network are detected and the asset inventory can be exported. Asset details are collected from network traffic and imported engineering files (SCL) to include detailed information about HW and firmware.

√ **SIEM and ticket system integration**
StationGuard can be integrated into many SIEM and ticketing systems using Syslog and our plug-ins for many vendors.

√ **Network traces**[1]
A Wireshark-compatible (PCAP) network trace is created for every event for subsequent analysis.

√ **User authentication**
StationGuard can be integrated into LDAP / Active-Directory[1]. Only authorized users can change the configuration or activate Maintenance Mode.

[1] Functionality available in future updates.



**StationGuard detects threats and supports response processes.**

PEOPLE
Little training effort: User interface and alarm messages match substation documentation.

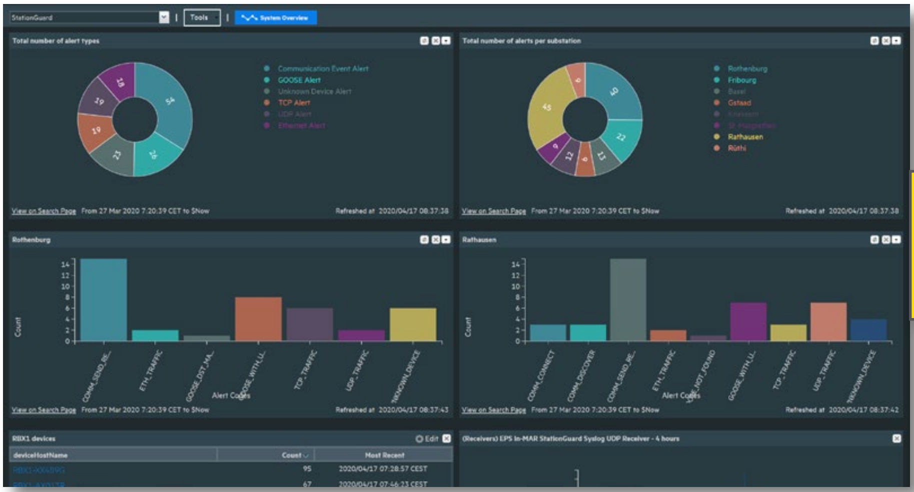
PROCESSES
Substation engineers and IT experts can work together in the response process, OMICRON offers expert support.

TECHNOLOGY
StationGuard is specialized for substations and their requirements.

Security and functional monitoring combined =
**Functional security monitoring**

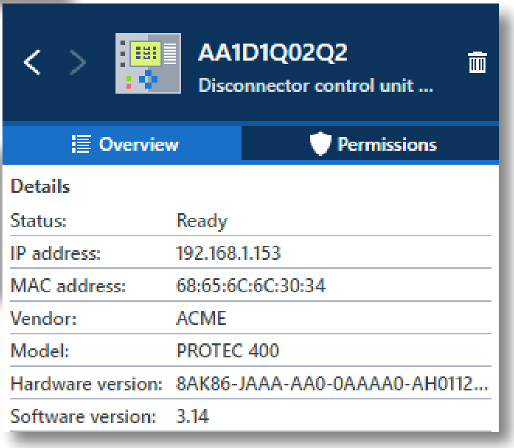
## Rigorously hardened platform

- √ **Secure cryptoprocessor**
  Keys and certificates are exclusively stored on an anti-tampering, anti-counterfeiting chip according to ISO/IEC 11889.
- √ **Secure boot chain**
  The cryptoprocessor is used to verify the signatures of each software module loaded. This ensures that only OMICRON software can be executed.
- √ **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 hardware security modules; private keys cannot be extracted.
- √ **Full disk encryption**
  The crypto processor is used to encrypt all data with a key unique for each device.
- √ **Special, hardened operating system**
  A dedicated, hardened Linux system is used. Each process only gets the privileges 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).
- √ **Our specialists continue to develop...**
  OMICRON's experts are constantly implementing new measures to harden our platform even more.


StationGuard
Tools
System Overview
Total number of alert types
54
26
23
19
19
18
Communication Event Alert
GOOSE Alert
Unknown Device Alert
TCP Alert
UDP Alert
Ethernet Alert
View on Search Page From 27 Mar 2020 7:20:39 CET to $Now
Refreshed at 2020/04/17 08:37:38
Total number of alerts per substation
40
22
13
6
12
9
45
6
Rothenburg
Fribourg
Basel
Gstaad
St. Margrethen
Rathausen
Rüthi
View on Search Page From 27 Mar 2020 7:20:39 CET to $Now
Refreshed at 2020/04/17 08:37:38
Rothenburg
Count
Alert Codes
Refreshed at 2020/04/17 08:37:43
Rathausen
Count
Alert Codes
Refreshed at 2020/04/17 08:37:42
RBX1 devices
deviceHostName
Count
Most Recent
95
2020/04/17 07:28:57 CEST
67
2020/04/17 07:46:23 CEST
(Receivers) EPS In-MAR StationGuard Syslog UDP Receiver - 4 hours

StationGuard's root cause analysis in the alerts enables intelligent statistics in SIEMs of all vendors.

Asset information aggregated from network traffic and SCL information.



**AA1D1Q02Q2**
Disconnector control unit ...

Overview | Permissions

**Details**

| | |
|---|---|
| Status: | Ready |
| IP address: | 192.168.1.153 |
| MAC address: | 68:65:6C:6C:30:34 |
| Vendor: | ACME |
| Model: | PROTEC 400 |
| Hardware version: | 8AK86-JAAA-AA0-0AAAA0-AH0112... |
| Software version: | 3.14 |

# Three different platform options

The StationGuard sensors are available on three different platforms. Depending on your needs, you can choose to use StationGuard on the RBX1 or MBX1 hardware platform or on a virtual machine. Since all of StationGuard's intelligence is contained in the sensor, the sensors run autonomously - no permanent connection to a central server is required.

## StationGuard on RBX1 platform

StationGuard running on the RBX1 hardware is a tailor-made IDS solution to protect substation automation and SCADA systems against cyber threats and zero-day attacks. The 19"-rack-mountable RBX1 platform is made for harsh power grid environments. It has enough performance and memory to record all events and associated traffic, even though the event may have occurred a long time ago.

The RBX1 comes with unmatched security features like full disk encryption, an ISO/IEC 11889 compliant cryptoprocessor chip and a customized secure Unified Extensible Firmware Interface (UEFI). Binary outputs to easily integrate IDS alerts into the SCADA signal list are included as well.

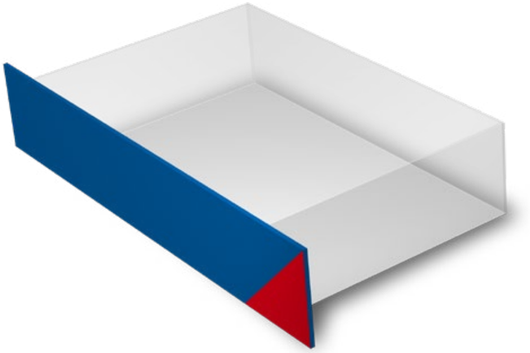
## StationGuard on MBX1 platform

StationGuard on the portable MBX1 hardware unit provides the same high level of security as the rack-mountable solution. With the mobile version of StationGuard you can perform a quick security assessment of a substation or SCADA network, or quickly generate an asset inventory list of all devices in the network.

During commissioning or maintenance phases, many engineers and also external service providers connect their equipment to the vulnerable substation network. StationGuard on the MBX1 is perfectly suited for temporarily monitoring the network during this time to alarm on prohibited behavior and to record critical actions during commissioning and maintenance.

## StationGuard on virtual machine platform

The StationGuard sensors are also available as virtual appliance to be installed on existing computing platforms in substations.



Same as the hardware platforms, the virtual variant can also run completely independently, recording and logging events even if there is no permanent connection to the central server. Please note that on virtual machines, there may be technical limitations in the area of functional monitoring of process bus applications, compared to StationGuard on the RBX1 and MBX1 platforms.

# Technical specifications of the RBX1 platform

### Environmental conditions

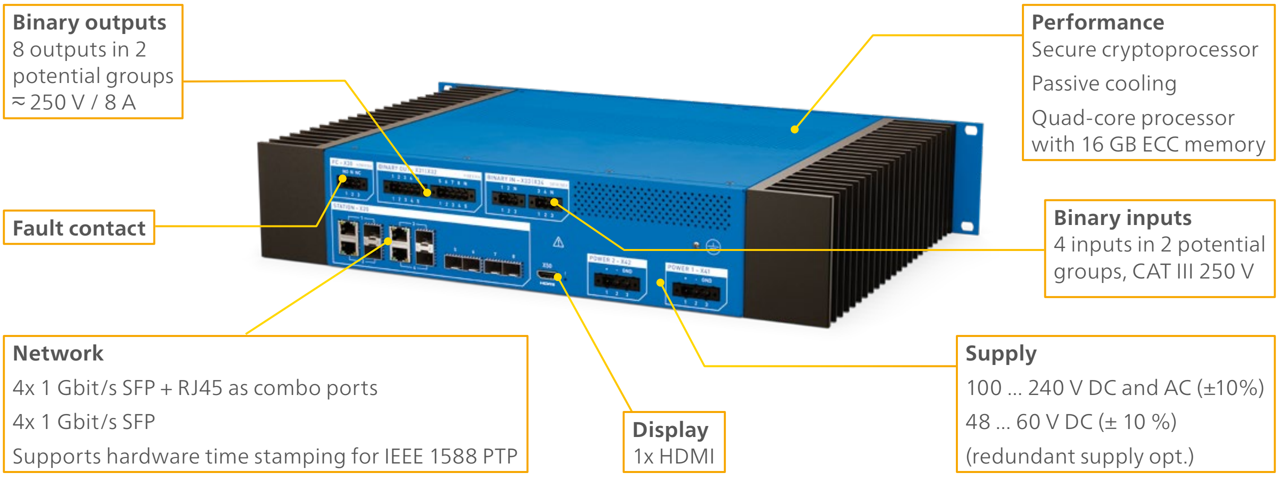
| | |
|---|---|
| Operating temperature | -20 °C ... +55 °C /<br>-4 °F ... +131 °F |
| Storage temperature | -25 °C ... +70 °C /<br>-13 °F ... +158 °F |
| Relative humidity | 5 % ... 95 %<br>(non-condensing) |
| Ingress protection according to IEC 60529 | IP30 |

### Standards

| | |
|---|---|
| Product standards | IEC 61850-3<br>IEEE 1613<br>Severity Level: Class 1 |
| EMC standards | IEC 61326-1<br>IEC 60255-26<br>IEC 61000-6-5 |
| Safety | EN 60255-27<br>EN 61010-1<br>EN 61010-2-030 |

See further details in the technical data sheet.

## RBX1 platform back view



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

**Fault contact**

**Network**
4x 1 Gbit/s SFP + RJ45 as combo ports
4x 1 Gbit/s SFP
Supports hardware time stamping for IEEE 1588 PTP

**Display**
1x HDMI

**Performance**
Secure cryptoprocessor
Passive cooling
Quad-core processor with 16 GB ECC memory

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

**Supply**
100 ... 240 V DC and AC (±10%)
48 ... 60 V DC (± 10 %)
(redundant supply opt.)

## RBX1 platform front view

**USB**
4x USB 3.0

**Network**
1x 1 Gbit/s RJ45
Supports hardware time stamping for IEEE 1588 PTP

# 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 alert. 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 of protection, automation, and control devices of almost all vendors worldwide.

*"As an expert for security vulnerabilities in IEDs, 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

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

**Dr. Fred Steinhauser,**
Expert for digital substations

## 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

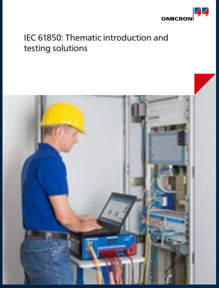
24 7 support

OMICRON is an international company that works passionately on ideas for making electric power systems safe and reliable. Our pioneering solutions are designed to meet our industry's current and future challenges. We always go the extra mile to empower our customers: we react to their needs, provide extraordinary local support, and share our expertise.

Within the OMICRON group, we research and develop innovative technologies for all fields in electric power systems. When it comes to electrical testing for medium- and high-voltage equipment, protection testing, digital substation testing solutions, and cybersecurity solutions, customers all over the world trust in the accuracy, speed, and quality of our user-friendly solutions.

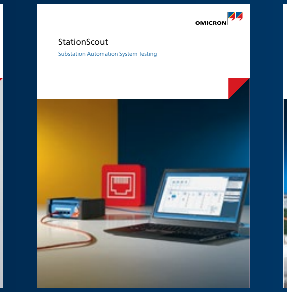
Founded in 1984, OMICRON draws on their decades of profound expertise in the field of electric power engineering. A dedicated team of more than 900 employees provides solutions with 24/7 support at 25 locations worldwide and serves customers in more than 160 countries.

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


OMICRON

IEC 61850: Thematic introduction and testing solutions

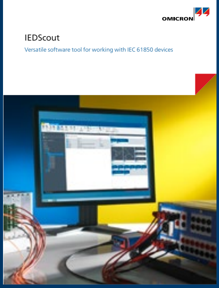
IEC 61850
Brochure


OMICRON

StationScout

Substation Automation System Testing

StationScout
Brochure


OMICRON

IEDScout

Versatile software tool for working with IEC 61850 devices

IEDScout
Brochure

OMICRON

DANEO 400

Hybrid signal analyzer for
power utility automation systems

DANEO 400
Brochure

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

www.omicronenergy.com