OMICRON

StationGuard Solution

Intrusion Detection, Vulnerability Management, Asset Inventory and Functional Monitoring for the Power Grid

The StationGuard Solution

Visibility

Make your communication and risks visible.

Intrusion and Threat Detection

Use the innovative allow-list approach for superior analysis and an efficient response.

Vulnerability Management

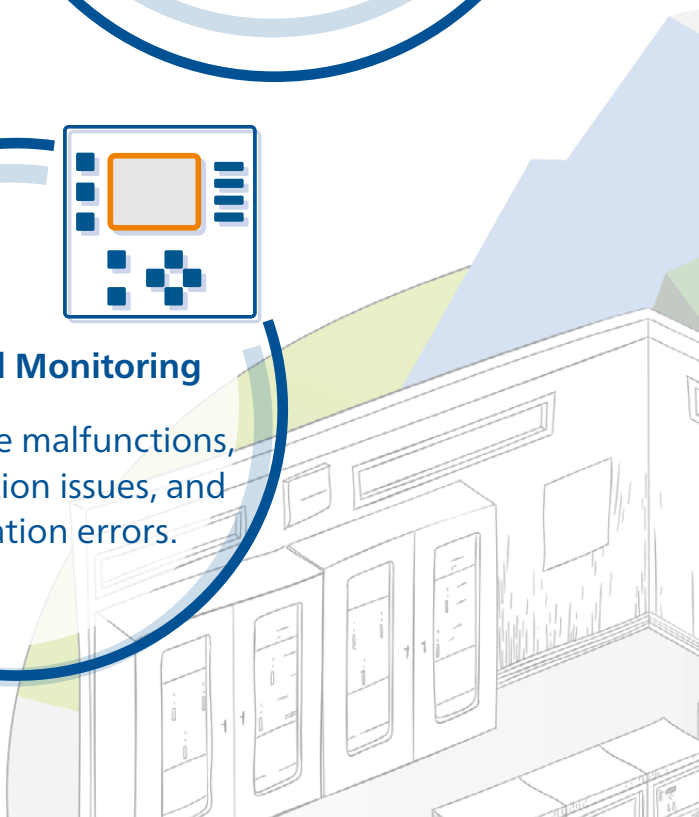
Investigate real threats to your assets with oversight and insight.

Asset Inventory

Work with the most precise and detailed asset list.

Functional Monitoring

Detect device malfunctions, communication issues, and configuration errors.



StationGuard Sensors

Our **innovative allow list (whitelist) approach** minimizes false alarms and enhances collaboration between IT and OT engineers by providing actionable alarm messages based on a deep understanding of power utility automation system events.

p. 4–11

Functional Monitoring

StationGuard not only **detects cyber threats and prohibited actions** in utility automation and SCADA system networks; it also **records and logs critical events**, such as device failures, configuration errors, interoperability issues, and network problems for later analysis.

p. 12–13

Asset Inventory and Vulnerability Management

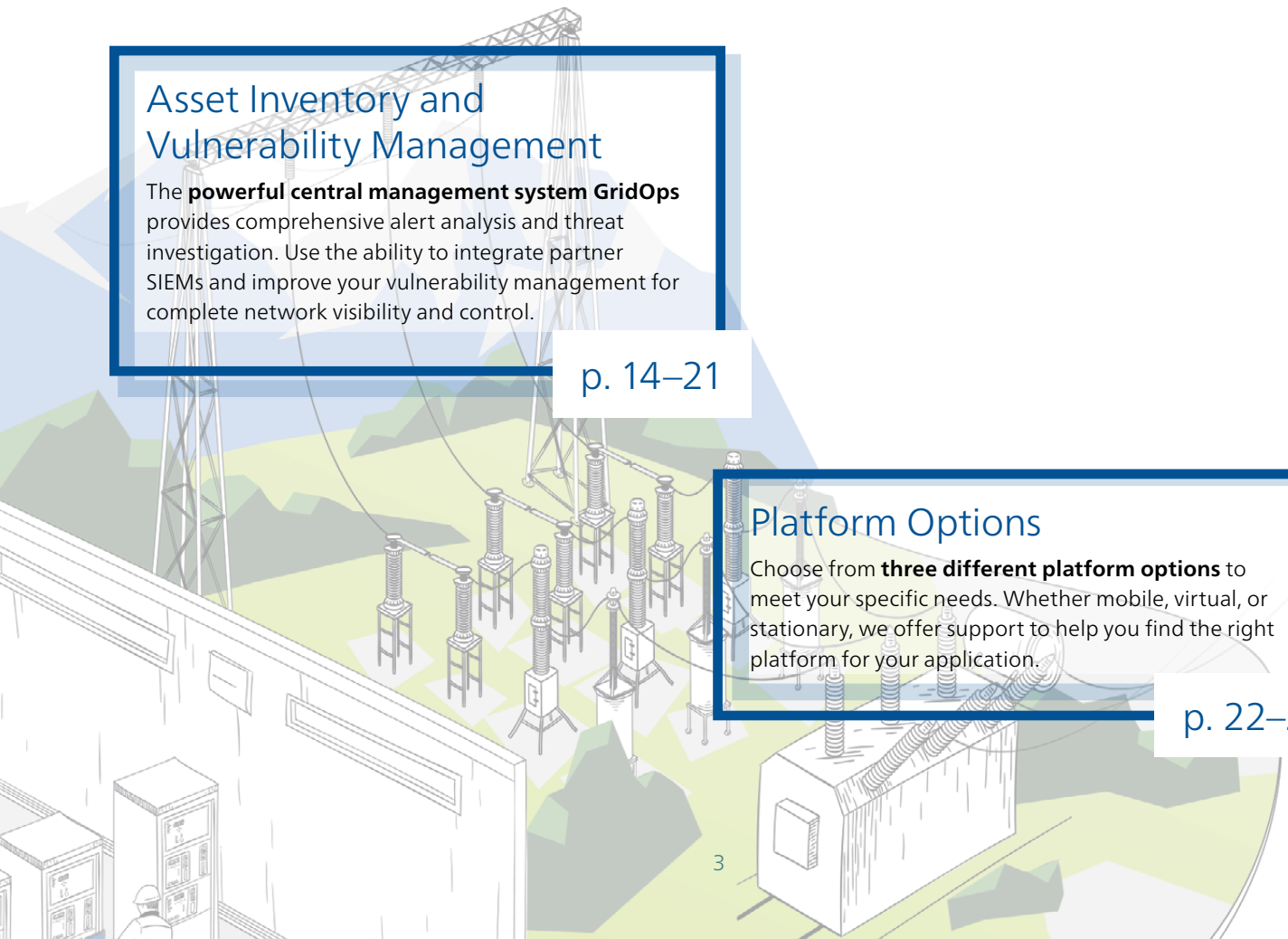
The **powerful central management system GridOps** provides comprehensive alert analysis and threat investigation. Use the ability to integrate partner SIEMs and improve your vulnerability management for complete network visibility and control.

p. 14–21

Platform Options

Choose from **three different platform options** to meet your specific needs. Whether mobile, virtual, or stationary, we offer support to help you find the right platform for your application.

p. 22–23



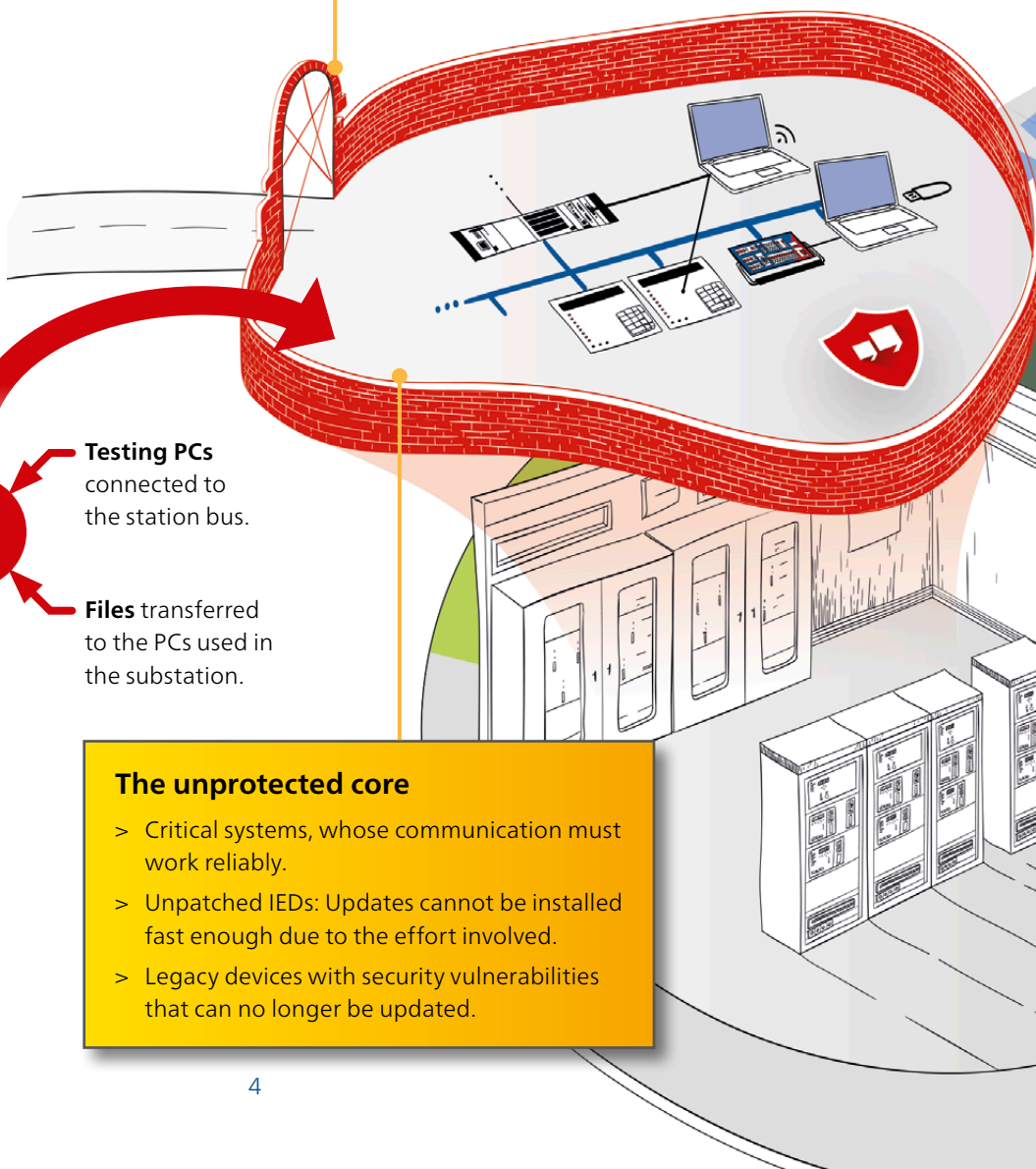
IT security in the power grid

In recent years, there has been an increase in cyber attacks against critical control systems in production facilities and energy supply companies. Therefore, many utilities are introducing processes to reduce the risk of cyber attacks. These measures have mainly focused on IT networks and control centers. However, substations, power plants, and networks represent critical attack vectors. Consequently, these plants' operation and maintenance processes must also be included in the cybersecurity risk assessment.

To ensure that the power grid is thoroughly protected against cyber attacks, the security strategy has to address each level. A security concept extends from physical access control to digital access monitoring to monitoring suspicious or forbidden activities in the network. This requires systems that offer a high level of security with low maintenance in the long term. Moreover, it should be easy to integrate them into operational and maintenance workflows.

Firewall

Firewalls ensure that only specific endpoints can communicate with the devices behind it, 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 that can no longer be updated.

Firewalls do not provide in-depth protection

There are many ways of circumventing a firewall. Many sites employ remote access for retrieving fault records or for maintenance. These connections provide a route by which malware can find its way into a substation's devices.

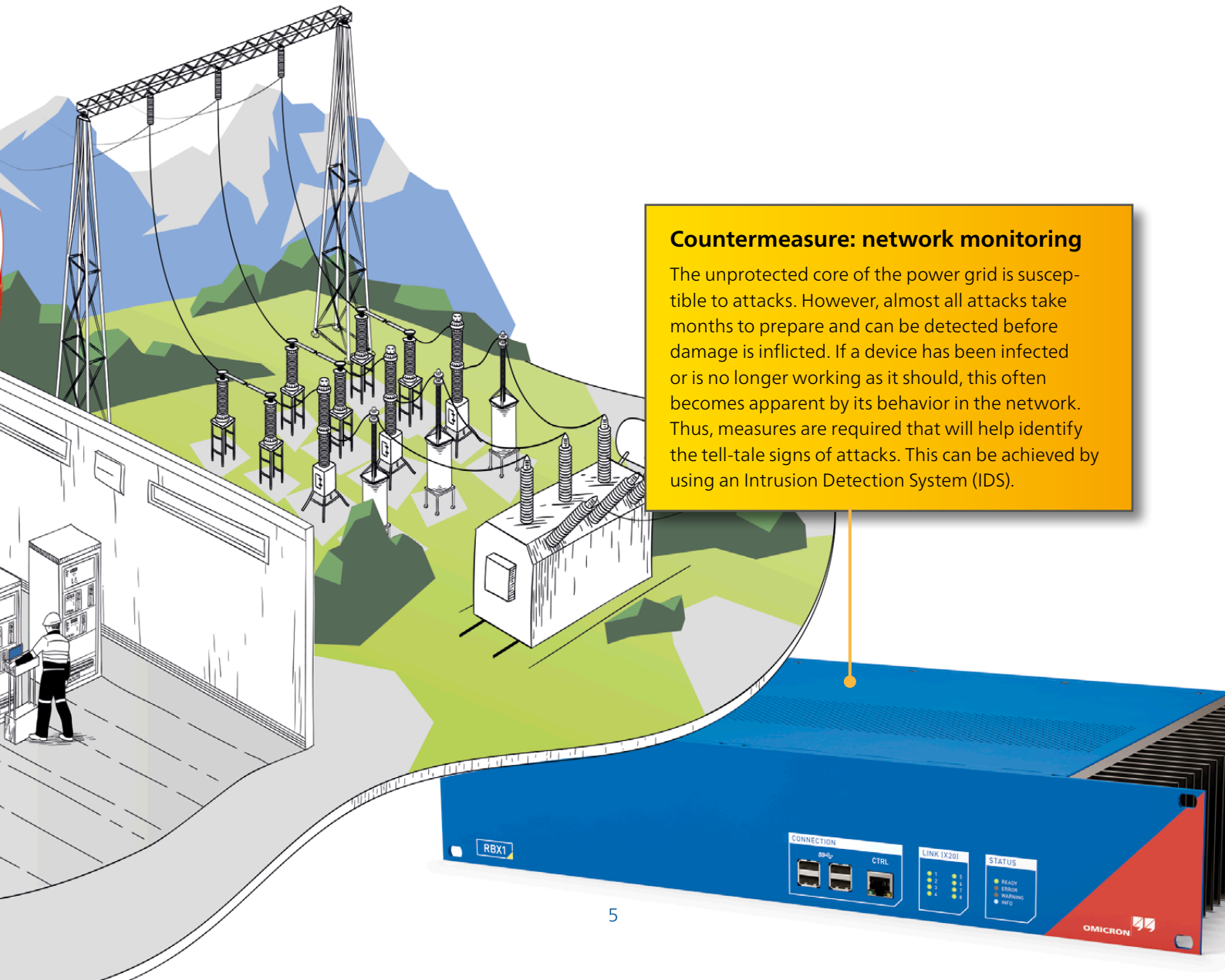
Maintenance and testing PCs provide another attack vector. These PCs are connected to the entire network or directly connected to individual protection or control devices.

Defense-in-Depth

The Defense-in-Depth principle, as set out in IEC 62443, not only recommends applying measures that „harden the shell" but also introduces several layers and fallback levels that help provide a zoned level of security.

One such measure is the provision of security updates for IEDs. However, the effort and cost involved are high, so updates cannot always be installed quickly enough. Not being able to update Legacy devices is common if the vendor is not providing updates.

Therefore, these systems must be monitored to ensure that attacks are detected early, and their consequences are minimized.



Countermeasure: network monitoring

The unprotected core of the power grid is susceptible to attacks. However, almost all attacks take months to prepare and can 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 in the network. Thus, measures are 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)

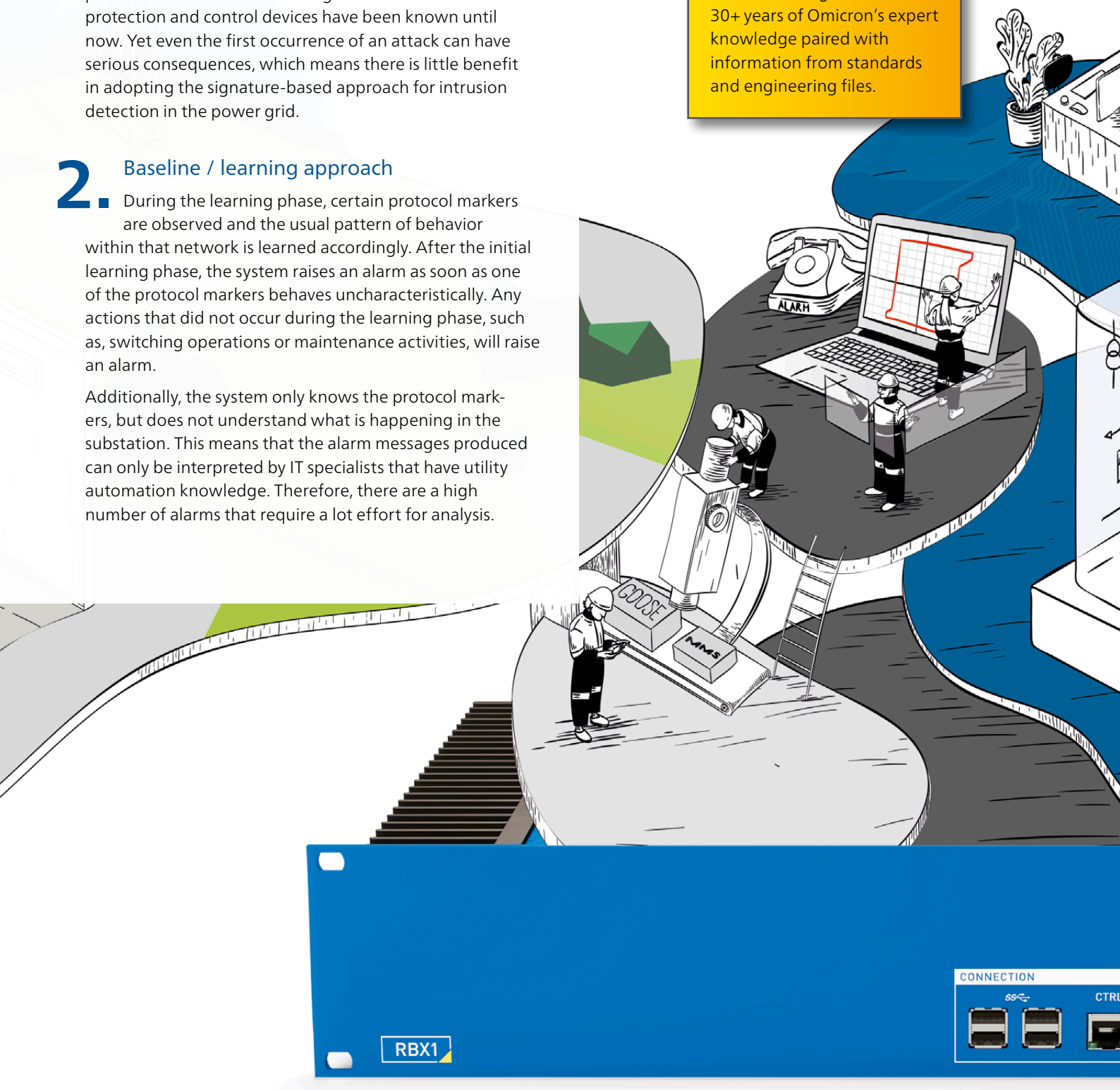
The IDS scans for patterns of known attacks. Virus scanners also use this approach. Systems like these have a lower false alarm rate than learning-based approaches. The main disadvantage is that few attacks on protection and control devices have been known until now. Yet even the first occurrence of an attack can have serious consequences, which means there is little benefit in adopting the signature-based approach for intrusion detection in the power grid.

2. Baseline / learning approach

During the learning phase, certain protocol markers are observed and the usual pattern of behavior within that network is learned accordingly. After the initial learning phase, the system raises an alarm as soon as one of the protocol markers behaves uncharacteristically. Any actions that did not occur during the learning phase, such as, switching operations or maintenance activities, will raise an alarm.

Additionally, 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 have utility automation knowledge. Therefore, there are a high number of alarms that require a lot effort for analysis.

StationGuard does not apply artificial intelligence but uses 30+ years of Omicron's expert knowledge paired with information from standards and engineering files.



3. The StationGuard approach

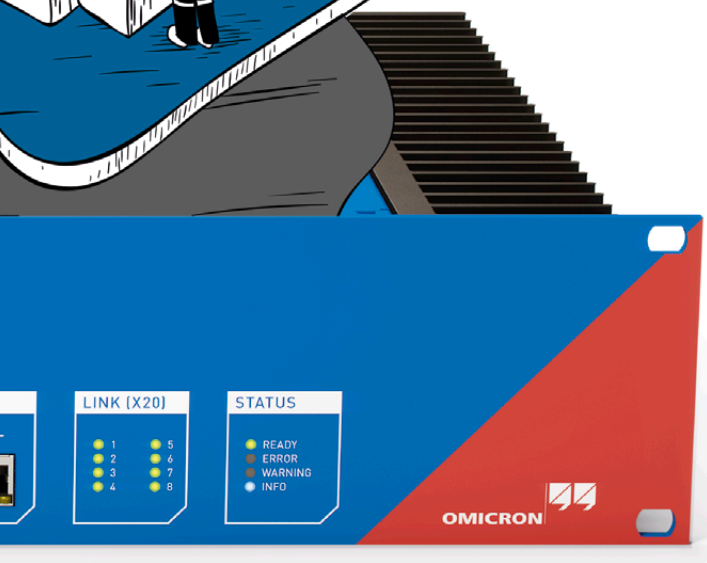
Power utility automation and SCADA systems are deterministic, which means their behavior is clearly defined, even in exceptional situations, e.g., during protection events.

By building on this feature, a completely new approach can be applied for detecting cyber-attacks.
Since it knows the function of each device, StationGuard creates a system model of the entire automation system and then compares every single network packet with this live system model. This corresponds with an allow

list (whitelist) approach, where all allowable behavior is described and everything deviating from it sets off an alarm. Completely new types of attacks can also be detected when using this approach.

StationGuard's allow list goes into detail at a granular level. Even the signal values in the messages are evaluated using the system model. This not only allows it to detect cyber threats and prohibited activity, but issues in the automation and SCADA functions can be detected as well. This is why we named the combination of intrusion detection and functional monitoring „Functional Security Monitoring". We've been researching this approach since 2010. Combining power system and security knowledge is what makes StationGuard so effective.

A learning phase is not necessary to configure StationGuard. Only a few user inputs for describing the purpose of each device are required. When it comes to IEC 61850 systems, this process can be sped up drastically 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

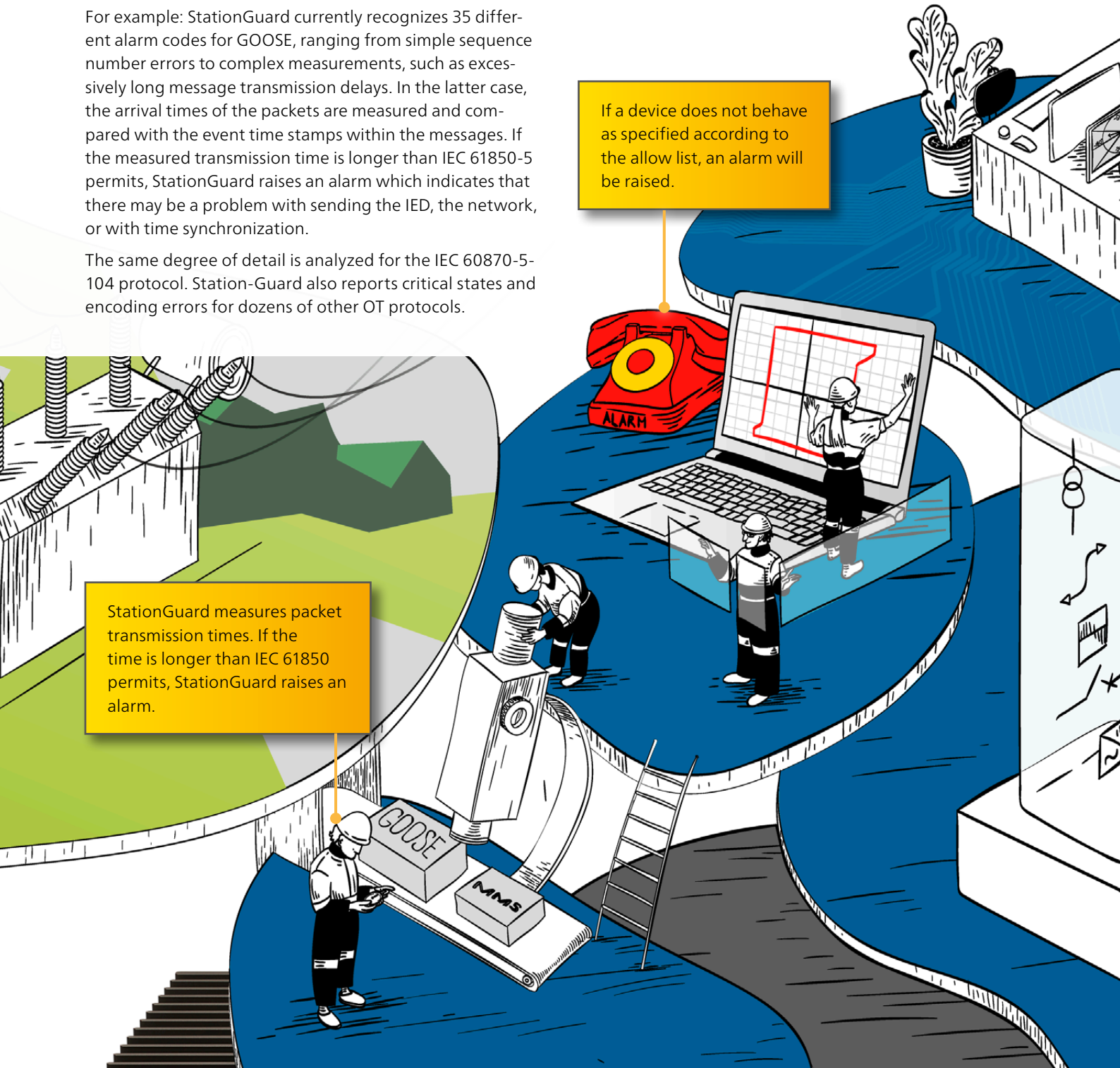
The allow list (whitelist) approach of StationGuard

Security at the granular level

The fact that all network traffic is monitored and validated in great detail means that it not only detects threats to IT security, such as illegal encoding 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 applies the single-line diagram, then there is virtually no limit to the depth of monitoring that 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 IEC 61850-5 permits, StationGuard raises an alarm which indicates that there may be a problem with sending the IED, the network, or with time synchronization.

The same degree of detail is analyzed for the IEC 60870-5-104 protocol. Station-Guard also reports critical states and encoding errors for dozens of other OT protocols.



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-tuned permissions are documented and can be reviewed in StationGuard.

Other protocols

StationGuard performs deep packet inspections on dozens of power systems and classical IT protocols. By using this, StationGuard not only detects encoding violations in these protocols, but is also aware 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
- S7
- EtherCAT
- Profinet
- ...
- 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 system model (allow list)

> Functional and communication problems are detected in addition to cyber threats

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

Faster responses with understandable alert messages

To set up, operate, and maintain conventional Intrusion Detection Systems (IDS), IT specialists and automation and control engineers are required. Both types of specialists must be on call around the clock to help analyze the cause of alarms. The costs involved with this are unacceptable for many utilities. StationGuard offers utilities a new, low maintenance alternative.

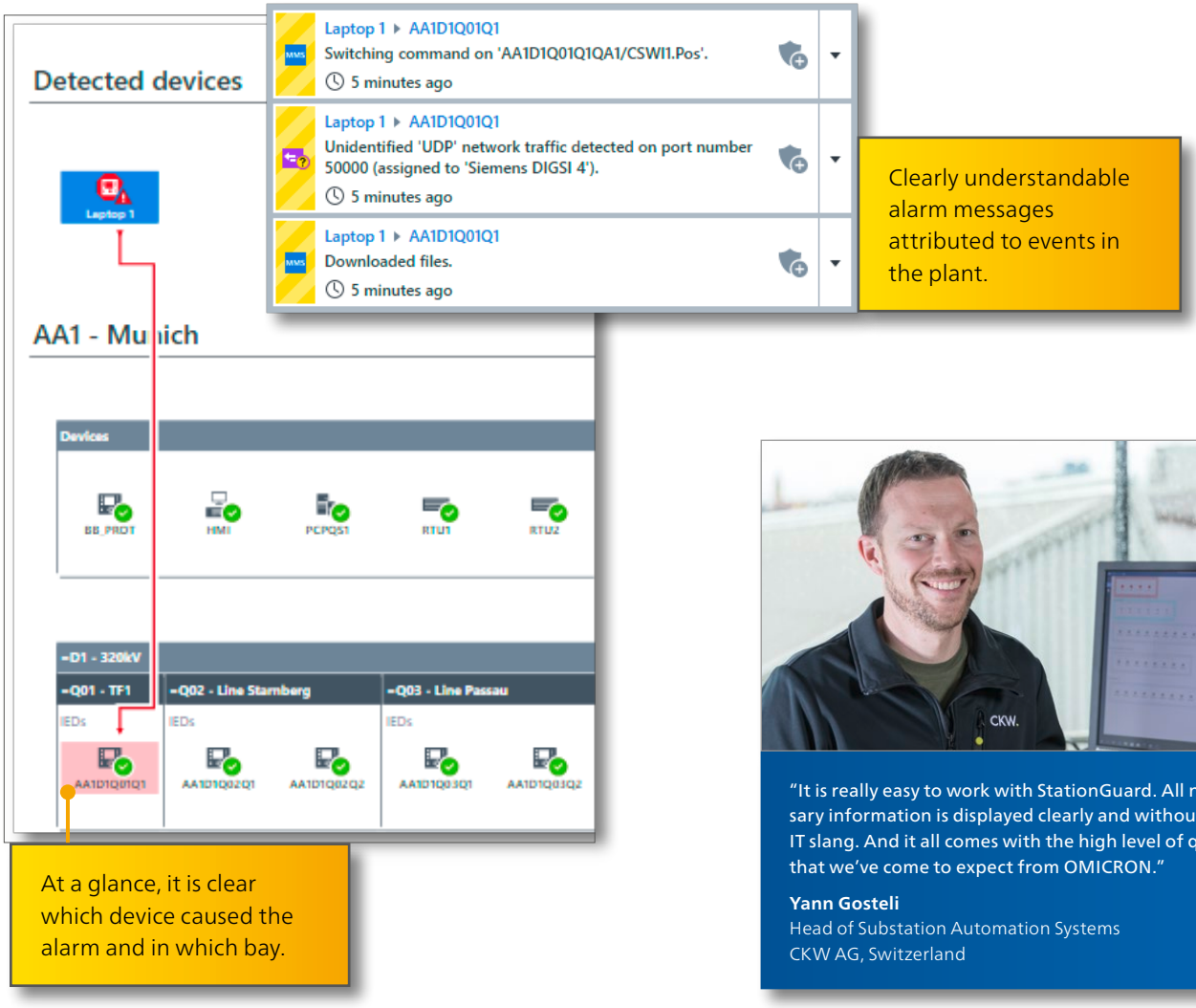
StationGuard is aware of the typical functions in substations and how the IT equipment, such as engineering PCs and test PCs, are expected to be used. As all this information is automatically available, StationGuard is set up quickly and ready to protect the network – no learning phase is required.

Reliably identifying the cause of alerts

The alerts triggered by a security system should assist the operator, not cause further confusion. Therefore, the StationGuard alerts 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.

Let us consider the following 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 happened in the substation. It contains information such as: What exactly happened? Which device is responsible?

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



"It is really easy to work with StationGuard. All necessary information is displayed clearly and without any IT slang. And it all comes with the high level of quality that we've come to expect from OMICRON."

Yann Gosteli
Head of Substation Automation Systems
CKW AG, Switzerland

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, even before they fail.

This comprehensive functional and security monitoring is unique and offers advantages that go well beyond those normally expected of an intrusion detection system (IDS).

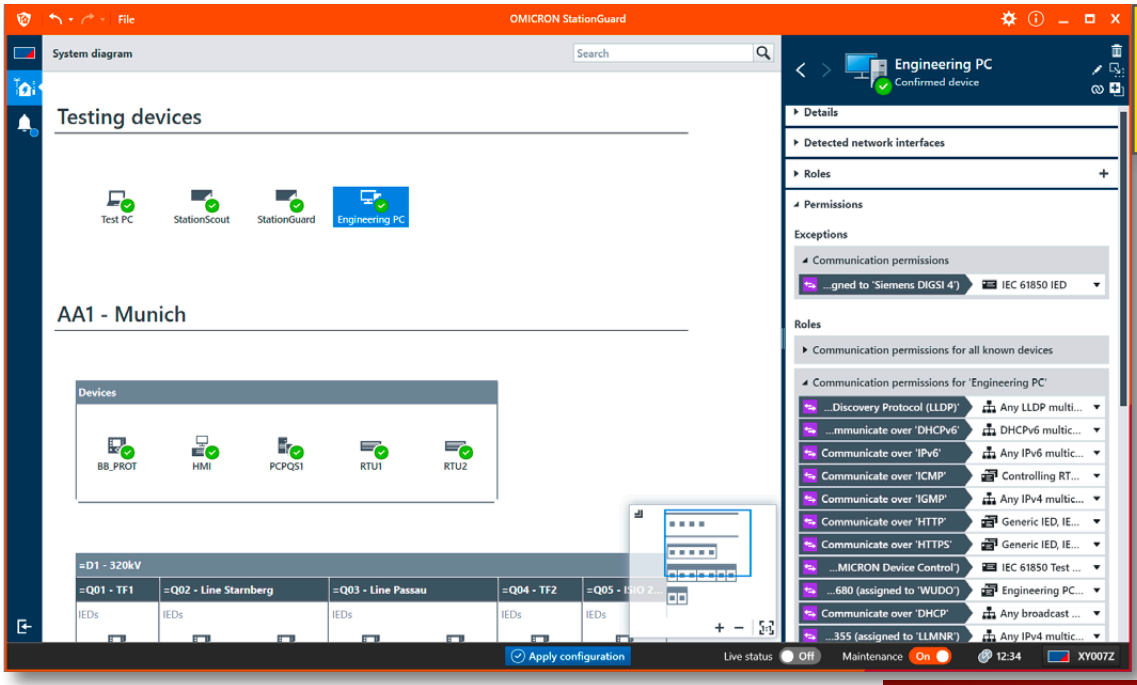
The graphical user interface allows protection and control engineers to quickly get to grips with StationGuard, as it matches the documentation diagrams and the event view in the station controllers.

Maintenance and commissioning

Testing and maintenance is important and must not result in any false alarms, yet a high level of security still 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 issue an alarm if communication with manufacturer's tools occurs 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.



Certain actions are only allowed during maintenance mode.

Advantages

- Alarms are understood by IT security officers as well as SCADA & protection engineers
- Fewer false alarms during routine testing while maintaining a high level of security
- No learning phase, immediate protection

Detecting malfunctions and configuration errors

Functional Monitoring

StationGuard not only detects cyber threats and prohibited actions in utility automation and SCADA networks; it also notifies you of critical events and malfunctions, such as failures of intelligent electronic devices (IEDs), configuration errors, and network issues, and then logs them for later analysis. In addition, all file transfers are logged with file names, for example, when disturbance records are downloaded.

In the following, there are some examples of functional issues that can be detected:

IED configuration changes

If a device's configuration changes, StationGuard issues an alarm.

StationGuard monitors the configuration revision fields from messages in the network 24/7 to detect changes in device configurations.

For example, it detects the common commissioning error that the configRevs are different on the sender and receiver sides of the communication.

Configuration errors

If a device's configuration is incorrect, StationGuard raises an alarm. It will detect mistakes immediately.

StationGuard continuously compares the IEC 61850 configuration parameters with the specifications of your prior input or SCL files.

Typical misconfigurations like incorrect VLAN configuration, erroneous GOOSE parameters, or incorrect datasets are detected.

Severity	Date and time	Message
▲	2024-06-13 17:11:37.726+02:00	TestPC ▸ HMI 'HTTP' network traffic detected.
▲	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE multicast address Restart of GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear' detected.
▲	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE multicast address Wrong destination MAC address in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
▲	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE multicast address Unexpected VLAN identifier in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
▲	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE multicast address Configuration revision (ConfRev) newer than expected in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
▲	2024-06-13 17:11:36.699+02:00	TestPC ▸ HMI 'HTTP' network traffic detected.
▲	2024-06-13 17:11:34.947+02:00	TestPC ▸ HMI 'HTTP' network traffic detected.
▲	2024-06-13 17:11:33.931+02:00	PCPQS1 ▸ AA1H1Q01Q1 Unidentified 'UDP' network traffic detected on port number 50000 (assigned to 'Siemens DIGSI 4').

Event log with various malfunctions detected

Network and time synchronization problems

StationGuard detects slowed down (GOOSE) message transmissions and failed time synchronization.

StationGuard measures the transmission time of messages by comparing sender timestamps with packet arrival timestamps. An alarm is triggered if this measurement reveals an error.

In most cases time synchronization issues cause such alarms. Using the same method, StationGuard also detects if an IED's response time is slowed down due to overload, a denial-of-service-attack, or due to the network being unreasonably slow.

IEC-104 and IEC 61850 control commands

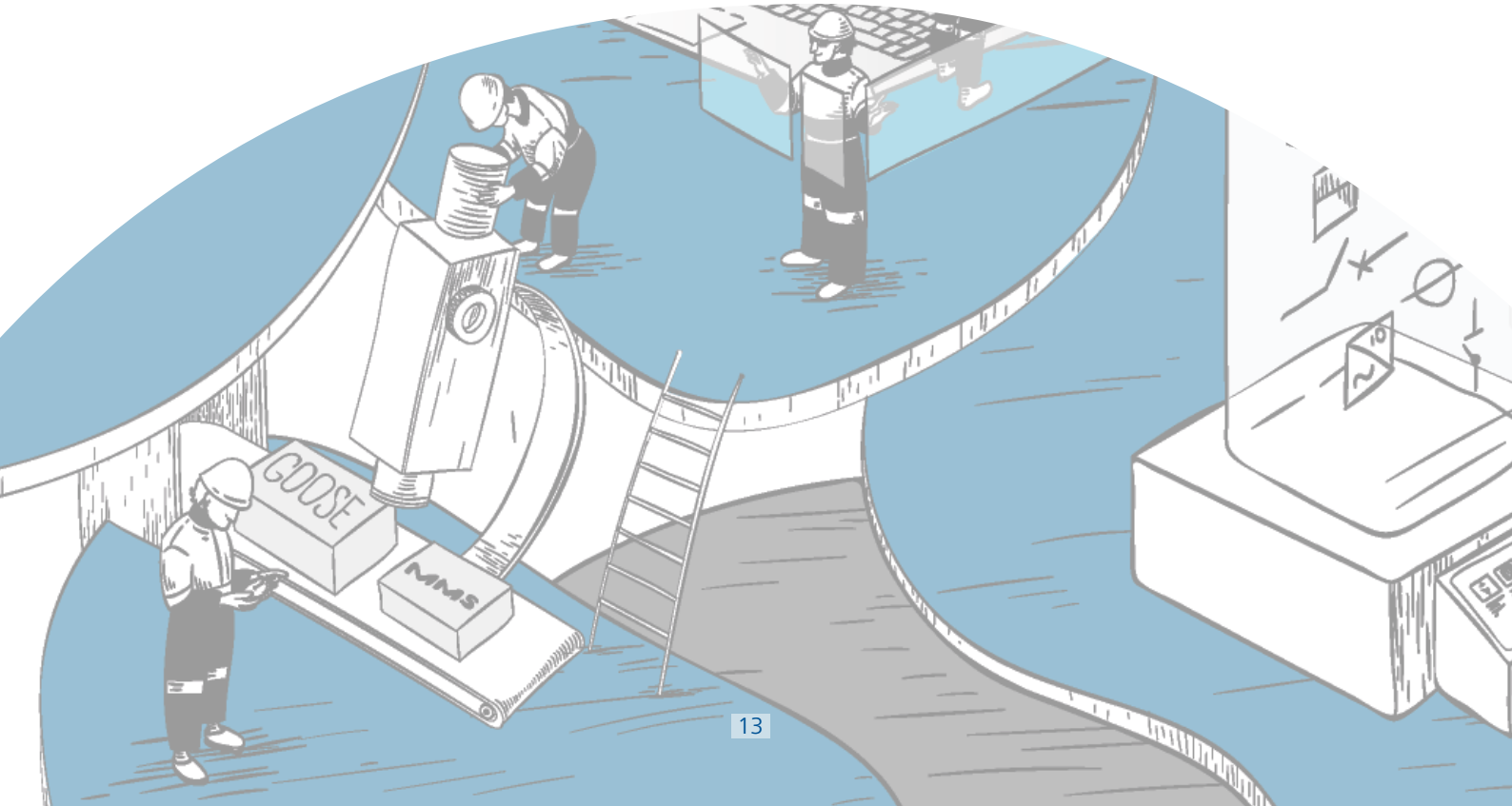
StationGuard detects and records failed control commands and interoperability issues.

StationGuard logs all IEC 60870-5-104 and MMS control commands. If a command fails, it creates warnings and records network traces for later analysis. Furthermore, it detects protocol and interoperability issues in MMS, IEC 60870-5-104, DNP3, Modbus, Synchrophasor, and many more.

Recording of file transfers

StationGuard records file downloads and uploads, such as disturbance records.

All file transfers in IEC-104 and MMS are logged along with file names and a network recording. You will see who accessed files on IEDs and when the event occurred.



Alert analysis and threat investigation

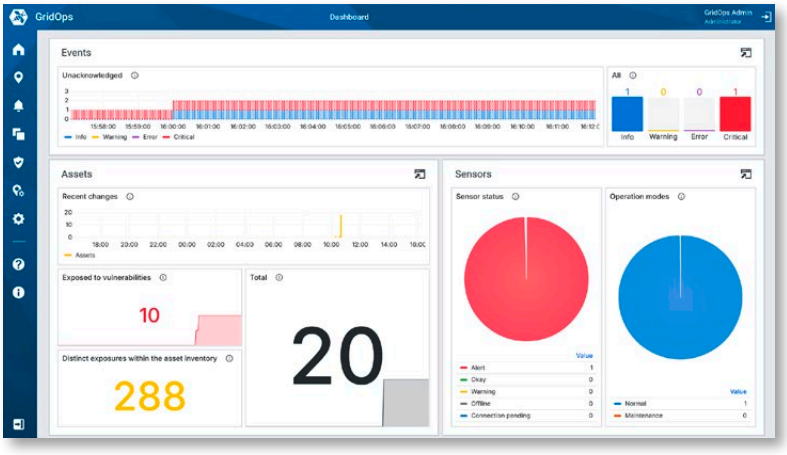
Alert investigation (GridOps)

The GridOps Alerts Dashboard was designed to provide a comprehensive picture of your power grid security posture by having access to security-related data combined with operational data that make network operations and security concerns more visible.

GridOps allows you to analyze the combined event log from all sensor locations and it visualizes all events from different perspectives, looking at various indicators. It enables you to see alert patterns and trends for specific device types or locations.

Alert logs can be reviewed and analyzed,which is essential for identifying security incidents, policy violations, operational issues, and more. Its analysis capabilities can also be used to aid with audits and forensic analyses and identifying current operational and long-term problems.

Real-time insights into all grid operation networks support multiple teams; security officers can enforce security policies that protect the networks without disrupting operation, and they benefit from communication monitoring to drive network segmentation. Protection and control engineers will gain visibility and insights that ensure the availability of utility automation networks.



Dashboard with alert statistics for multiple sites

GridOps - Central management system for StationGuard

Unified platform

- Reduces false positives and focuses on essential matters
- Full visibility 24/7 for security incidents, functional issues, and more.
- Accelerates and simplifies responses to incidents.

With GridOps you can ...

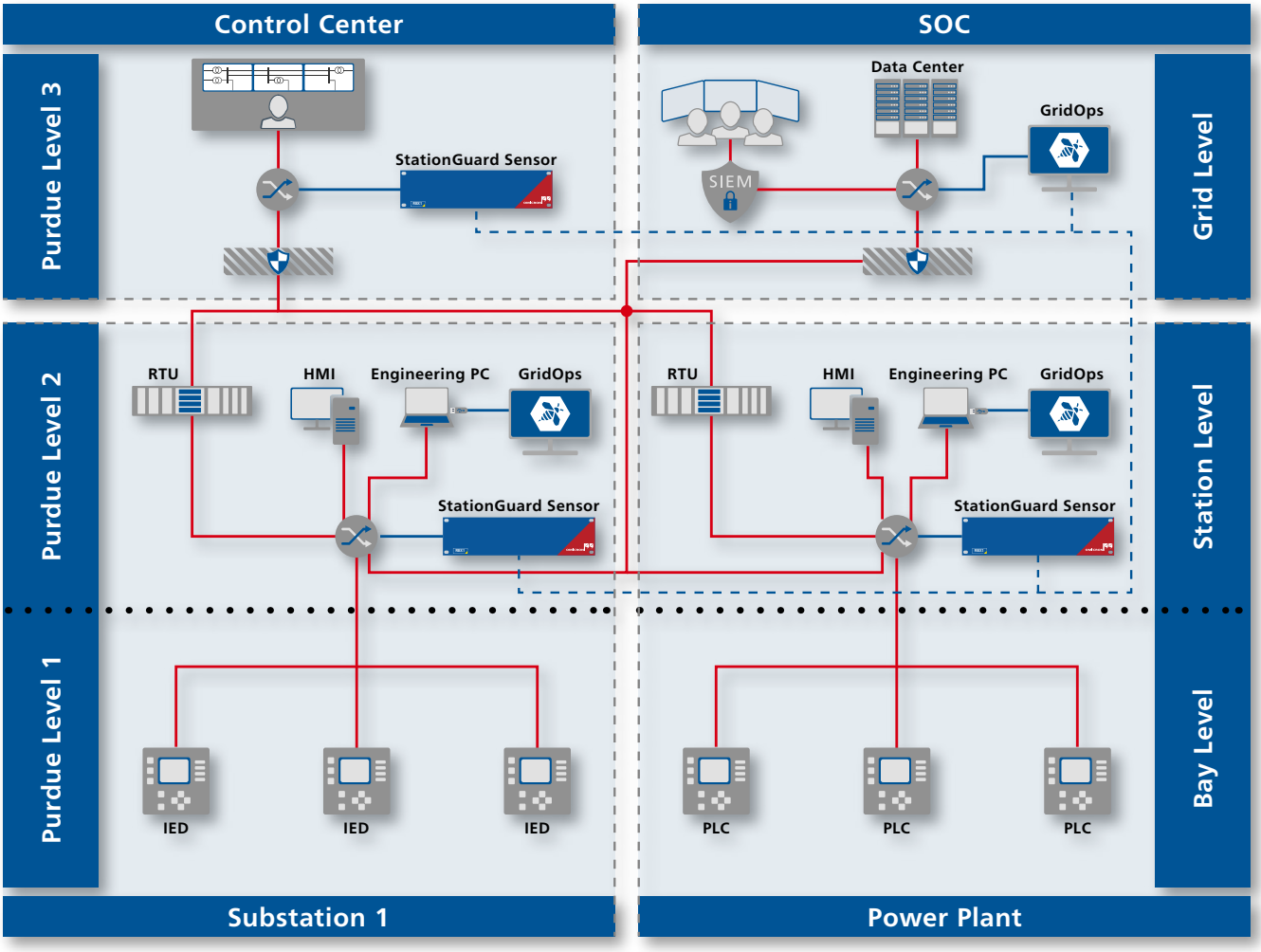
... understand how a threat appeared, what created it, if it made a connection, and more.

... seamlessly collaborate with IT security teams and OT teams for optimized handling of incidents and vulnerabilities.

... reduce operational risks by being prepared for handling security incidents.

... look for anomalies in the typical behavior of your grid to detect all types of threats.

... visualize every attempted attack and behavior deviation, no matter how subtle.



StationGuard Deployment Diagram

What does our StationGuard Solution include?

The StationGuard sensors can be installed in control centers, power plants, and substations for implementing intrusion detection, network visualization, asset discovery, and for monitoring the correct function of power utility automation systems. The StationGuard sensors allow for flexible deployment:

- RBX for a permanent installation
- VBX for a virtual platform
- MBX for temporary usage or permanent installation*

GridOps is the central management system for StationGuard. It provides functions for event analysis and alerts, asset inventory and vulnerability management, and for managing the sensors. Its main feature is a single platform for visualizing cybersecurity risks, threats and monitoring assets and events (cybersecurity as well as functional) across the grid.

GridOps can be installed at a control center or at a Security Operations Center (SOC) to centrally manage all StationGuard IDS sensors from a single location.

*via available DIN rail mounts

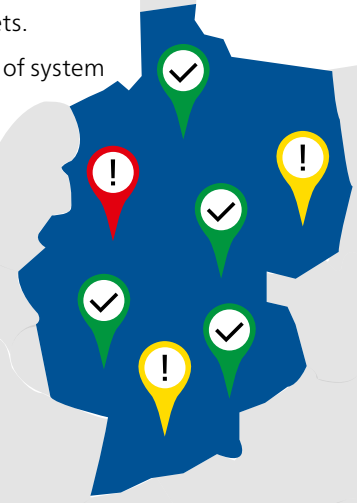
Network Visibility

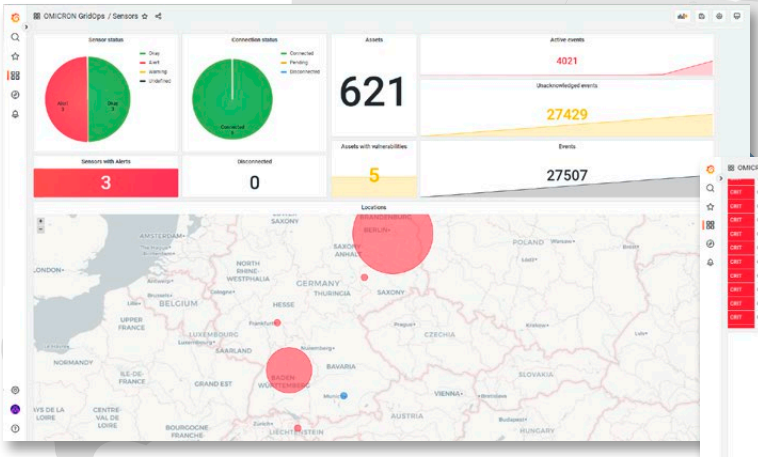
Network Visibility from Grid to Station

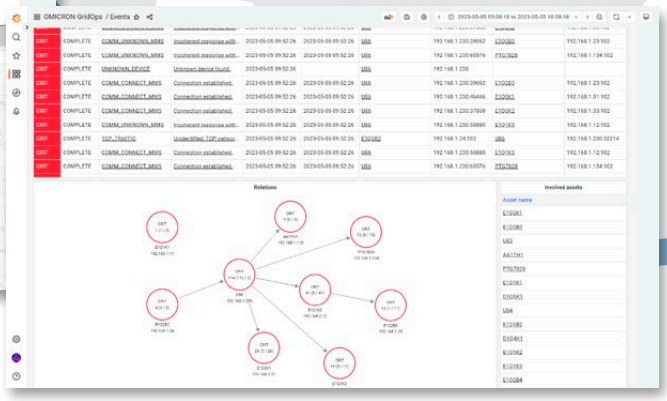
There are pressing questions that IT security officers and SCADA and OT network engineers face: What is the overall threat and risk state of our critical OT networks right now? What is the structure of these network zones and how are they interconnected? How are the devices communicating within and across these boundaries?

These questions and more demand a versatile tool that empowers users to drill down with a bird's eye view into the plant network perspective, and even further into the communication details between individual assets.

Our StationGuard solution offers this high level of system transparency.







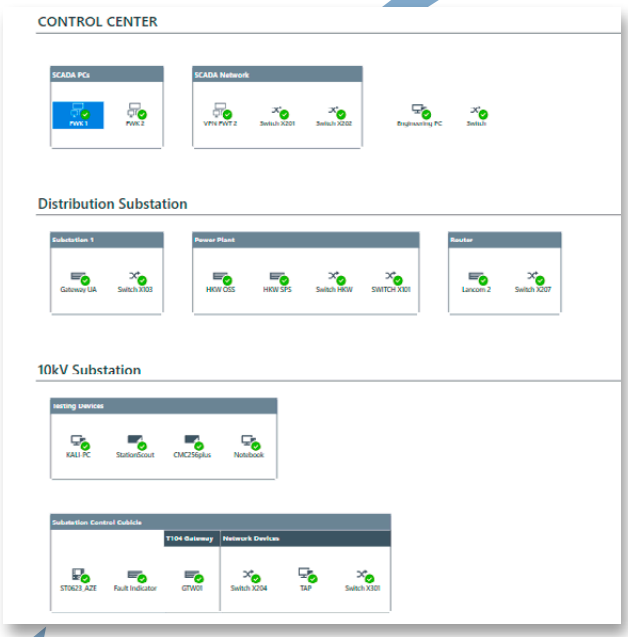
1 Grid level picture

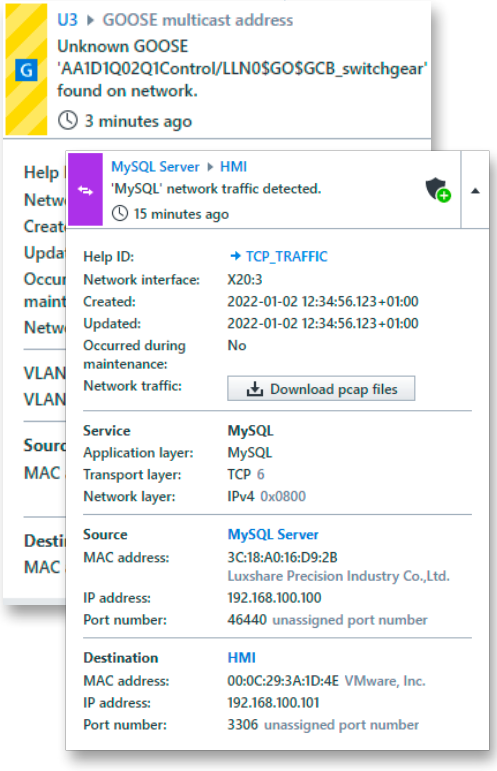
Different Dashboards allow you to oversee the status of all grid automation networks from a bird's eye view. Threats, functional issues, or vulnerabilities that need immediate action can be seen at a glance.

2 Station network diagram

Diving one level deeper allows you to observe the networks using our unique view which combines aspects of the Purdue Model diagram with single line diagrams well known to protection and SCADA engineers. This combination enables optimal collaboration between both worlds.

These diagrams can be generated automatically from SCL engineering files. They can also be improved manually and plant documentation spreadsheets can even be imported to improve equipment names.





3 Communciation relationships between devices

Eventually, the insight from the communication and protocols between devices comes to the forefront. Asset details and type plate information can be observed there. IT specialists can determine the bay and voltage level of each asset and can deliberate efficiently with OT protection engineers through the shared terminology.

Automatically collect data for enhanced vulnerability detection

An asset inventory database with precise details about each protection and control IED is crucial to successful vulnerability and risk management. The more information you have about each asset, the more accurate your vulnerability analysis and prioritization will be. Our StationGuard solution supports you throughout the entire workflow from creating and updating the asset inventory to vulnerability and risk management.

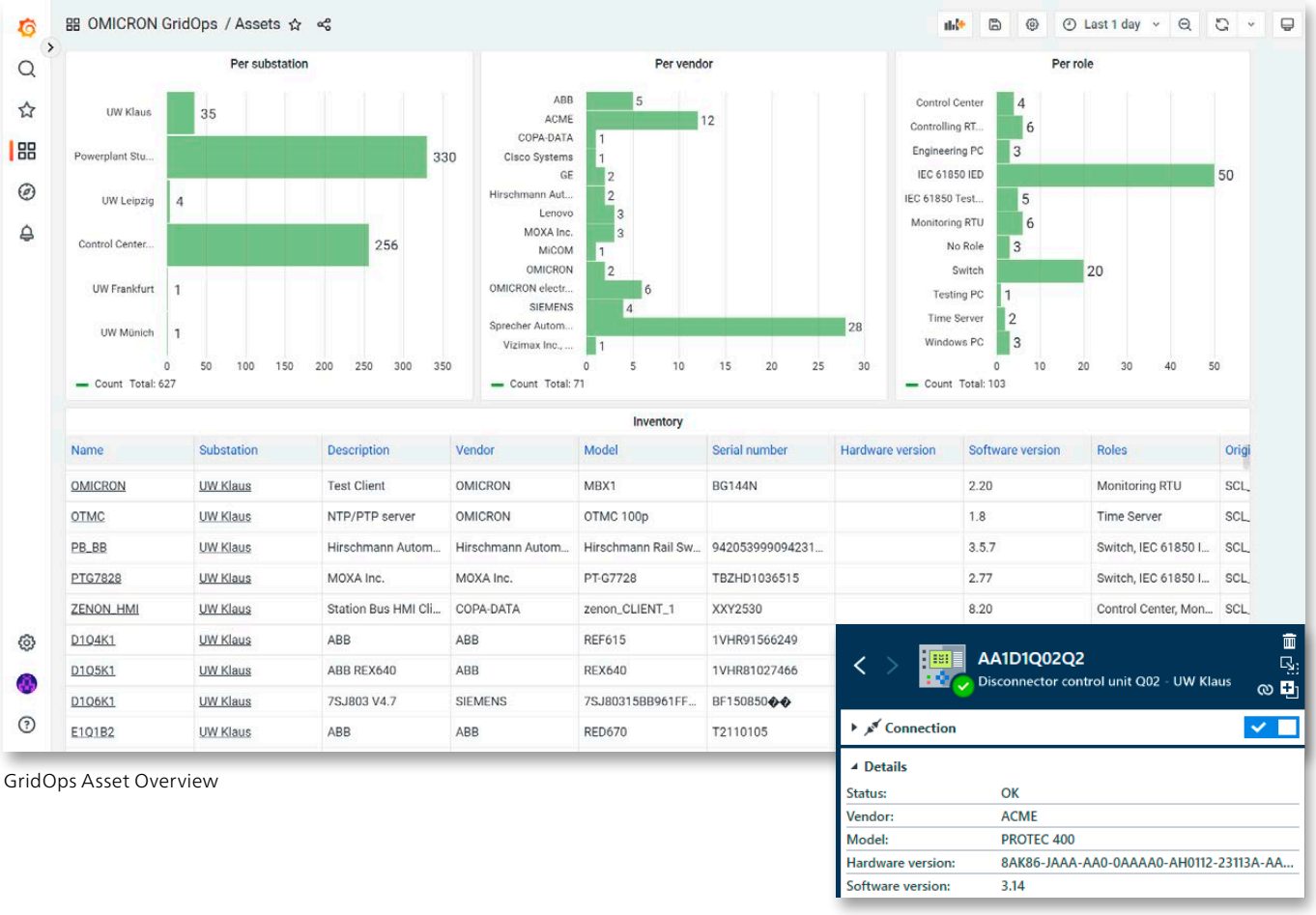
StationGuard automatically discovers all assets in the network, creates a global asset inventory database, and alerts you to new assets in your networks. It collects accurate information for each asset by combining network analysis with imported SCL engineering files and plant documentation spreadsheets. The asset inventory can be updated by importing information from external sources.

Receive detailed information about your assets

Using this aggregation of passively observed information with imported engineering files and spreadsheets, gives you the most precise asset information possible. It includes engineering descriptions, type, hardware configuration, product ordering codes, and firmware version.

You can export the inventory and import it into asset and configuration management systems, ERP systems, and spreadsheets. By importing spreadsheets (CSV-files) into StationGuard, you can close the loop and synchronize it with any other source. You can optionally enable StationGuard's Active Asset Identification to automatically read device configuration and firmware version information on the network.

As a result, our StationGuard solution compiles an asset inventory with in-depth information from multiple sources to provide the best possible foundation for vulnerability management.



GridOps Asset Overview

Vulnerability Management

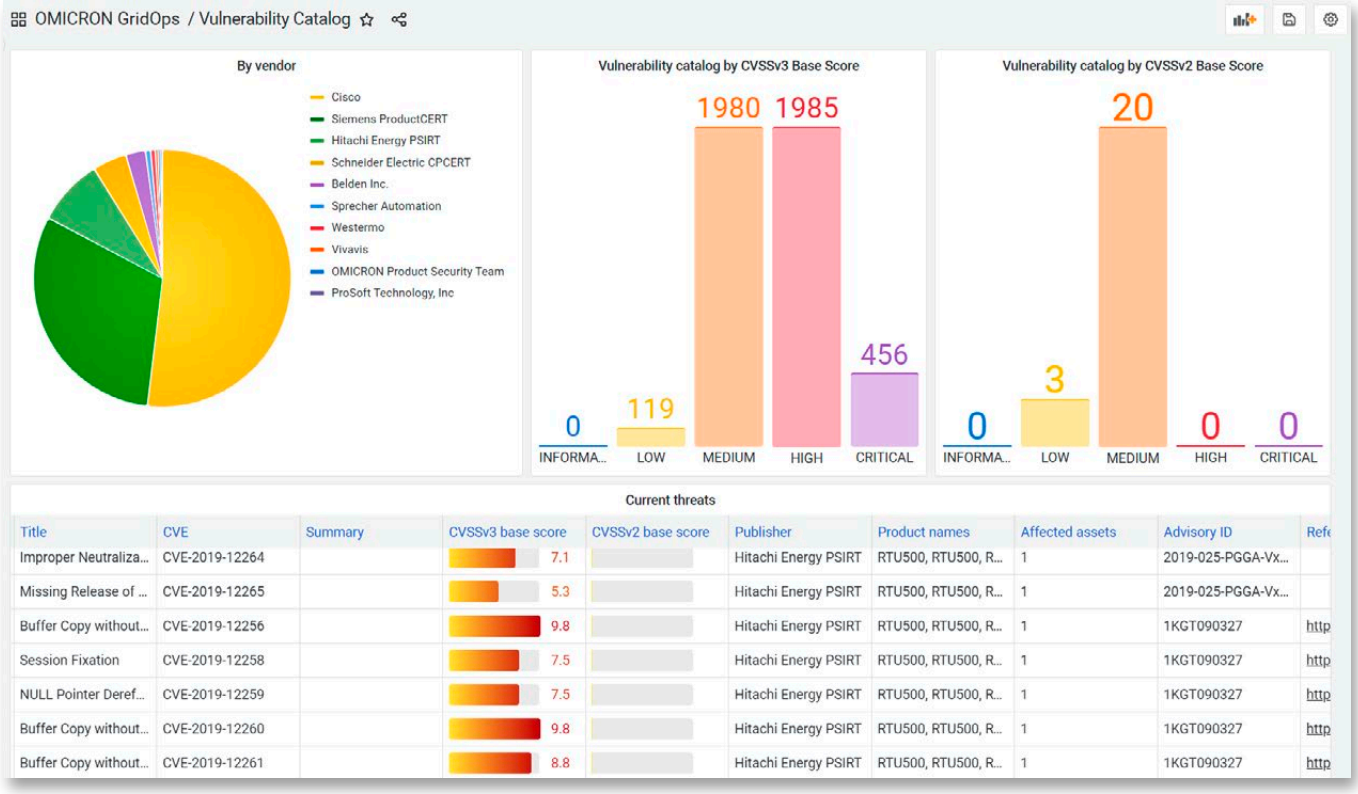
Security regulations for critical systems, such as the EU NIS directive and NERC-CIP, stipulate vulnerability management as a vital aspect of any cybersecurity program for the power grid. Only with an optimal vulnerability management in place, you can determine and implement an appropriate mitigation strategy by mapping officially known vulnerabilities to your system infrastructure.

You can only protect, what you see

Our vulnerabilities dashboard gives you a better understanding of the network's critical points and your overall security vulnerability exposure. It also informs users about recently discovered vulnerabilities by continuously auditing these assets for any potential threats. The more information users have about each asset, the more accurate the detection, analysis, and prioritization will be.

A decisive advantage: Users may only look at the vulnerabilities which are relevant to them. It only takes a few clicks – using OMICRON's custom-built vulnerability database for power grid automation and network devices. The system quickly identifies which assets are vulnerable to a particular CVE (Common Vulnerability Exposure).

Additionally, the compilation of comprehensive and meaningful reports for management, auditors, and regulators for assisting in risk prioritization and mitigation is simpler than ever before. Stakeholders will welcome increased visibility and the system's highlighted security posture and risk.



GridOps Vulnerabilities Dashboard

Beneficial integrations and partnerships

The StationGuard Solution provides plugins for ticketing systems, like ServiceNow, for automatically creating work tickets that respond to IDS alerts. By importing the asset inventory from StationGuard, tickets are automatically assigned to the engineer responsible for the asset or site involved in the alert.

Access control for protecting data and networks

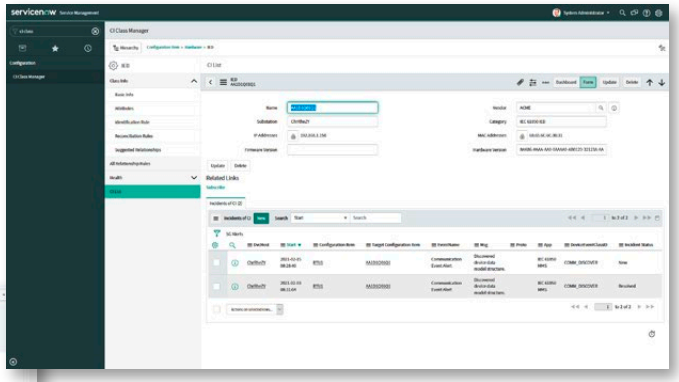
Integration into LDAP/ ActiveDirectory can be configured via the central management system. It has different user roles for controlling access to the various functions for viewing and configuring your StationGuard instances. For example, only authorized users can change the configuration or activate the Maintenance Mode. If all networks are down, StationGuard sensors can also be accessed individually using the StationGuard local client user interface.

Insider threats can be reduced and even eliminated using RBAC (Role-Base Access Control). It improves the security of the system and networks. It also enhances efficiency by minimizing the need for password changes and human error in privilege assignment.

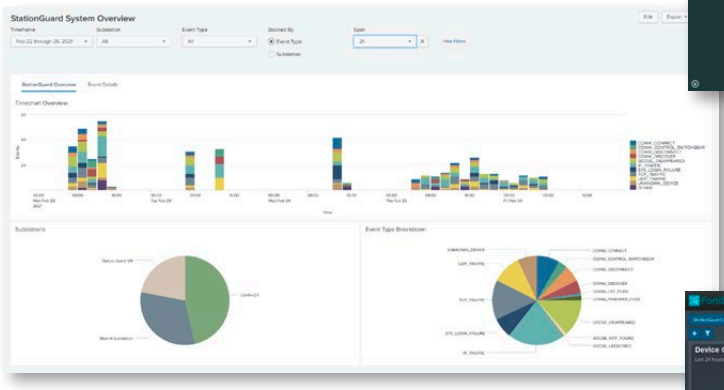
Simple integration into your network

An effortless way to integrate StationGuard sensors into legacy systems is by using the binary outputs from the RBX1 platform. The presence of an unacknowledged alarm is signaled in the binary outputs, which can be wired to an RTU (Remote Terminal Units) and integrated into the SCADA signal list.

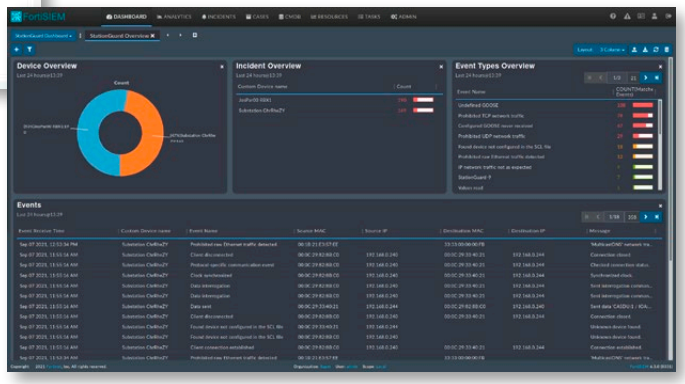
Alternatively, our easy-to-understand alert messages can also be forwarded using the syslog protocol. Various plugins are available for integrating StationGuard sensors into security information and event management (SIEM) systems and ticketing systems of different vendors.



ServiceNow integration



StationGuard for Splunk App



FortiSIEM integration

Our Partners for secure power grids

Technology partners

Fortinet

Fortinet's Open Fabric Ecosystem provides you with integrated solutions for comprehensive end-to-end security.

Integrating StationGuard Solution into FortiSIEM:

Improves security, compliance, and business agility.

Splunk

Splunk captures, indexes, and correlates real-time data in a searchable repository from which it generates graphs, reports, alerts, interfaces, and visualizations.

Explore the StationGuard for Splunk App on Splunkbase:

On-demand reports with statistical analysis.

Content and sales partners

NTS

Together with high-end manufacturers, NTS assumes digital responsibility and creates IT solutions with reliable services for the areas of network, security, collaboration, cloud, and data center.

Combine the StationGuard Solution with NTS Threat Detection Service:

Deliver rich analytical reports that support risk identification and improve security posture.

ALSEC

Their cybersecurity experts support you with proficient and individual services: Starting with training, the development of processes and evaluation of products to their implementation.

Combined knowledge of OMICRON and ALSEC:

Risk Reporting & Business Security Intelligence for planning & preparing for the future.

Explore more of our partners and communities, such as EE-ISAC, on our homepage:

https://www.omicronenergy.com/en/cybersecurity-partners/

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 RBX or MBX hardware platform or on a virtual machine (VBX). Since all of StationGuard's intelligence is contained in the sensors, the sensors run autonomously - a permanent connection to a central server is not required.

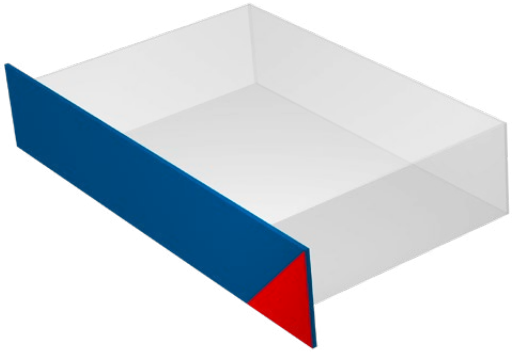
StationGuard on RBX platform

Running StationGuard on the RBX hardware is a tailor-made IDS solution for protecting utility automation and SCADA systems against cyber threats and zero-day attacks. The 19"-rack-mountable RBX 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 RBX comes with unmatched security features like full disk encryption, an ISO/IEC 11889 compliant cryptoprocessor chip and a customized secure (UEFI BIOS). It also includes Binary outputs that easily integrate IDS alerts into the SCADA signal list.

StationGuard on VBX platform

The StationGuard sensors are also available as a virtual appliance that can be installed on existing computing platforms.



Like the hardware platforms, the virtual variant can also run completely independently, recording and logging events even without a permanent connection to the central server. Please note that on virtual machines, there may be technical limitations when it comes to functional monitoring of process bus applications, compared with StationGuard on the RBX and MBX platforms.

StationGuard on MBX platform

With the mobile version of StationGuard you can perform a quick security assessment of a plant network, or quickly generate an asset inventory list from all devices in the network.

During the commissioning or maintenance phases, many engineers and external service providers connect their equipment to the vulnerable plant network. StationGuard on the MBX is perfectly suited for temporarily monitoring the network during this period to alert you to prohibited behavior and to record critical actions during commissioning and maintenance.

Optionally, the portable MBX hardware unit can also be installed peramently via the included DIN rail mounts.

Technical specifications of the RBX1 platform

Environmental conditions

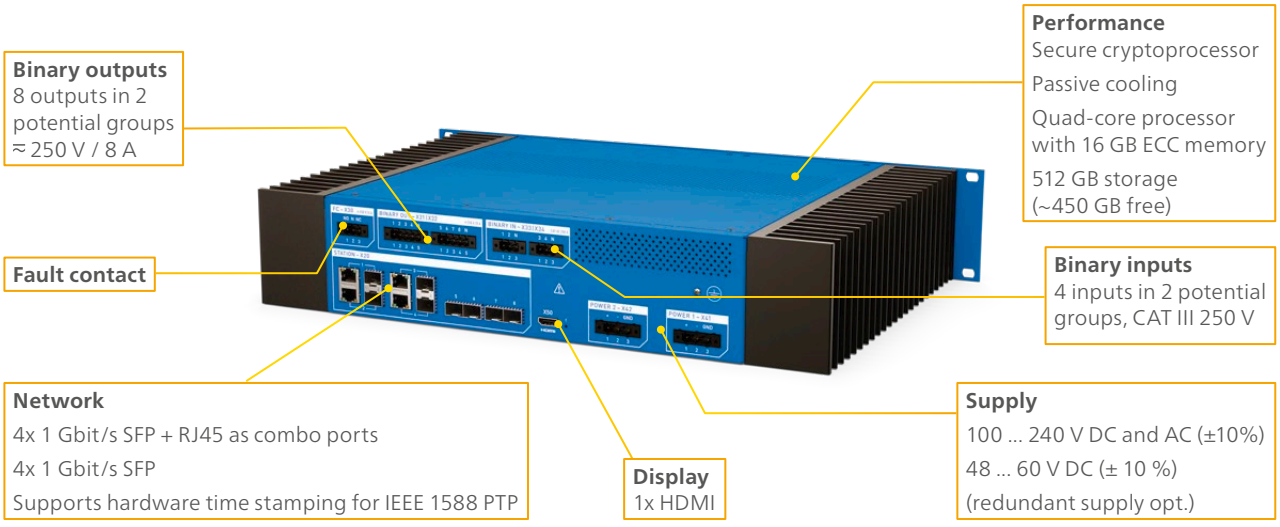
Operating temperature	-20 °C ... +55 °C / -4 °F ... +131 °F
Storage temperature	-25 °C ... +70 °C / -13 °F ... +158 °F
Relative humidity	5 % ... 95 % (non-condensing)
Ingress protection according to IEC 60529	IP30

Standards

Product standards	IEC 61850-3 IEEE 1613 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.

RBX1 platform back view



RBX1 platform front view

We create customer value through ...

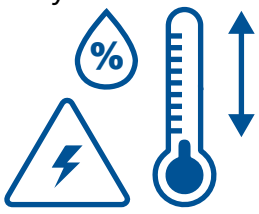
Quality

We always want you to be able to rely on our testing solutions. This is why our products have been developed with experience, passion and care and are continually setting ground-breaking standards in our industry sector.

You can rely on the highest safety and security standards

Superior reliability with up to

72



hours burn-in tests before delivery

More than

30.000

automated software tests executed 24/7

ISO 9001
TÜV & EMAS
ISO 14001
OHSAS 18001

Compliance with international standards

Innovation

Thinking and acting innovatively is something that's deeply rooted in our genes. Our comprehensive product care concept also guarantees that your investment will pay off in the long run – e.g. with free software updates.

Save up to

80%

of time
in set-up and operation

More than

200

developers keep
our solutions up-to-date

I need...

... a product portfolio
tailored to my needs

More than

15%

of our annual sales is
reinvested in research and
development

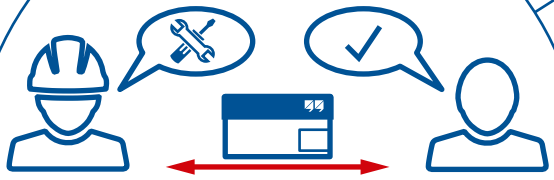
We create customer value through ...

Support

When rapid assistance is required, we're always right at your side. Our highly-qualified technicians are always reachable to ensure minimized downtimes.

Professional technical support at any time

offices worldwide for local contact and support



Cost-effective and straight-forward repair

Cybersecurity experts provide solutions quickly and easily

Knowledge

We maintain a continuous dialogue with users and experts. Customers can benefit from our expertise with free access to application notes and professional articles. Additionally, the OMICRON Academy offers a wide spectrum of training courses and webinars.

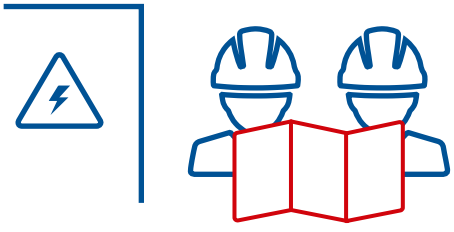
More than

300

Academy and numerous hands-on trainings per year

Frequently OMICRON hosted user meetings, seminars and conferences

to thousands of technical papers and application notes



Extensive expertise in commissioning and consulting

OMICRON is an international company that works passionately on ideas for making electric power systems safe, secure, 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. Customers worldwide rely on the accuracy, speed, and quality of our reliable, user-friendly solutions for electrical testing of medium- and high-voltage equipment, protection systems, digital substations, and cybersecurity.

Founded in 1984, OMICRON draws on their decades of profound expertise in the field of electric power engineering. A dedicated team of more than 1,300 employees provides solutions with 24/7 support at 23 locations worldwide and serves customers in more than 170 countries.

Emotions are energy. Our energy moves.

Move with us! Scan the QR code to explore our events, training courses, and products. Stay connected by following us on social media.

omicroncybersecurity.com
omicronenergy.com