StationGuard-Lösung

Angriffserkennung, Schwachstellen-Management, Asset-Inventar und Funktionsüberwachung für das Stromnetz

Die StationGuard-Lösung

Sichtbarkeit

Sichtbarkeit und Transparenz für Kommunikation und Risiken

Angriffsüberwachung und Bedrohungserkennung

Innovativer Allowlist-Ansatz für besseres Analysieren und effizientes Reagieren

Schwachstellen-Management

Untersuchung echter Bedrohungen für Assets mit Überwachung und Einblicken

Asset-Inventar

Auflistung der Assets mit maximaler Präzision und Detailgenauigkeit

Funktionsüberwachung

Erkennung von Gerätefehlfunktionen, Kommunikationsproblemen und Konfigurationsfehlern

StationGuard-Sensoren

Unser **innovativer Allowlist-Ansatz** bietet sowohl den Fachleuten für die IT-Sicherheit als auch Schutz- und Leittechniker:innen maximale Sicherheit und Komfort. Cyberbedrohungen sowie Funktions- und Kommunikationsprobleme werden erkannt, analysiert und gleichzeitig die False-Positive Alarme auf ein Minimum reduziert. Die Sicherheit Ihrer Anlage ist zu jeder Zeit gewährleistet.

S. 4–11

Funktionsüberwachung

StationGuard erkennt **Cyberbedrohungen und unzulässige Handlungen** in Automatisierungssystemen von Energieversorgern und SCADA-Systemnetzwerken. Alle kritischen Ereignisse werden **aufgezeichnet und protokolliert**. Dazu gehören auch Geräteausfälle, Konfigurationsfehler, Interoperabilitätsprobleme und Netzwerkprobleme, die später analysiert werden können.

S. 12–13

Asset-Inventar und Schwachstellen-Management

Das **leistungsstarke zentrale Management-System GridOps** bietet eine umfassende Alarmanalyse und Bedrohungsuntersuchung. Verbessern Sie Ihr Schwachstellen-Management und verschaffen Sie sich vollständige Netzwerktransparenz, damit Sie die Kontrolle behalten.

S. 14–21

Plattform-Optionen

Sie können zwischen **drei verschiedenen Plattformen** wählen: stationär, mobil oder virtuell. Bei der Wahl der geeignetsten Plattform für Ihre Einsatzumgebung unterstützen wir Sie gern.

S. 22–23

IT-Sicherheit im Stromnetz

Kritische Steuerungssysteme in Produktionsanlagen und Energieversorgungsunternehmen sind in den letzten Jahren vermehrt zum Ziel von Cyberangriffen geworden. Aus diesem Grund etablieren viele Energieversorgungsunternehmen Maßnahmen, mit denen das Risiko von Cyberangriffen verringert werden soll. Diese Maßnahmen konzentrieren sich bisher aber hauptsächlich auf IT-Netzwerke und Leitstellen, obwohl die Schaltanlagen, Kraftwerke und Netzwerke selbst ebenfalls kritische Angriffsvektoren darstellen. Das bedeutet, dass auch die Betriebs- und Wartungsprozesse dieser Anlagen in die Bewertung der Cyber-Security-Risiken einbezogen werden müssen.

Damit sichergestellt ist, dass das Stromnetz umfassend vor Cyberangriffen geschützt ist, muss die Sicherheitsstrategie auf jeder einzelnen Ebene ansetzen. Ein Sicherheitskonzept sollte von der physischen Zugangskontrolle über die digitale Überwachung des Zugriffs bis hin zur Überwachung auf verdächtige oder nicht autorisierte Aktivitäten im Netzwerk reichen. Dies erfordert Systeme, die ein hohes Maß an Sicherheit bei langfristig geringem Wartungsaufwand bieten. Außerdem sollten sich diese Systeme einfach in die Betriebs- und Wartungsabläufe integrieren lassen.

Firewall

Firewalls sorgen dafür, dass nur bestimmte Endpunkte mit den hinter ihnen befindlichen Geräten kommunizieren können und dass für die Kommunikation nur zugelassene Protokolle zum Einsatz kommen. Firewalls sind jedoch nicht unüberwindbar.

Angriffspunkte zur Umgehung von Firewalls:

Fernzugriff für Wartungs- und Steuerzwecke

Wartungs-PCs, die an das Netzwerk oder direkt an die IEDs angeschlossen sind

Prüf-PCs, die an den Anlagenbus angeschlossen sind

Dateien, die an die Computer in der Anlage übertragen werden

Der ungeschützte Kern

- Kritische Systeme, deren Kommunikation zuverlässig funktionieren muss
- Nicht gepatchte IEDs: Updates können aufgrund des hohen Aufwands nicht schnell genug installiert werden
- Ältere Geräte mit Sicherheitsschwachstellen, für die keine Updates mehr durchgeführt werden können

Firewalls bieten keinen tiefgreifenden Schutz

Firewalls können auf vielfältige Weise umgangen werden. So kann Malware zum Beispiel über die Fernzugriffsverbindungen eingeschleust werden, die zum Abrufen von Störschrieben oder für Wartungszwecke eingerichtet wurden.

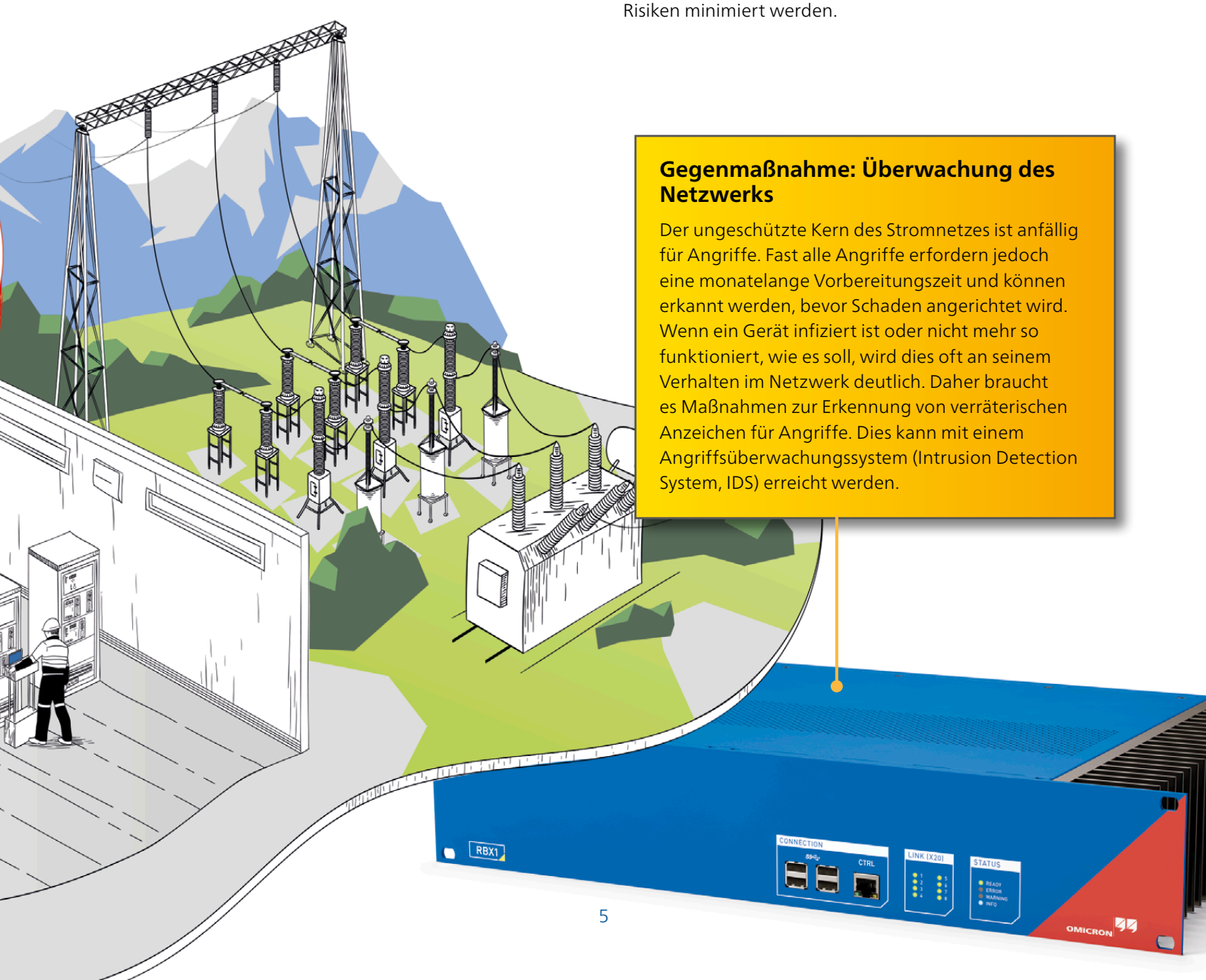
Ein weiterer Angriffsvektor sind Wartungs- und Prüfcomputer. Diese Computer sind mit dem gesamten Netzwerk oder direkt mit einzelnen Schutz- oder Steuergeräten verbunden.

Defense-in-Depth

Das in IEC 62443 beschriebene Defense-in-Depth-Prinzip empfiehlt nicht nur, Maßnahmen zur Verstärkung der „äußeren Schale“ anzuwenden, sondern führt auch mehrere Schichten und Fallback-Ebenen ein, die voneinander abgegrenzte Sicherheitszonen ermöglichen.

Eine der empfohlenen Maßnahmen besteht darin, Sicherheitsupdates für IEDs bereitzustellen. Das ist aber mit viel Aufwand und hohen Kosten verbunden, was dazu führt, dass Updates nicht immer schnell genug installiert werden können. Viele ältere Geräte können nicht mehr aktualisiert werden, weil der Hersteller keine Updates mehr zur Verfügung stellt.

Diese Systeme müssen daher überwacht werden, um sicherzustellen, dass Angriffe frühzeitig erkannt und Risiken minimiert werden.



Gegenmaßnahme: Überwachung des Netzwerks

Der ungeschützte Kern des Stromnetzes ist anfällig für Angriffe. Fast alle Angriffe erfordern jedoch eine monatelange Vorbereitungszeit und können erkannt werden, bevor Schaden angerichtet wird. Wenn ein Gerät infiziert ist oder nicht mehr so funktioniert, wie es soll, wird dies oft an seinem Verhalten im Netzwerk deutlich. Daher braucht es Maßnahmen zur Erkennung von verräterischen Anzeichen für Angriffe. Dies kann mit einem Angriffsüberwachungssystem (Intrusion Detection System, IDS) erreicht werden.

Wie funktioniert ein Angriffsüberwachungssystem (IDS)?

Es gibt zwei verbreitete Ansätze für Angriffsüberwachungssysteme:

1. Signaturbasierter Ansatz (Denylist)

Bei diesem Ansatz, der auch von Virenscannern genutzt wird, sucht das IDS nach Mustern, welche es bereits von anderen Angriffen kennt. Systeme dieser Art haben eine geringere Fehlalarmquote als Systeme auf der Basis eines lernbasierten Ansatzes. Sie haben allerdings einen wichtigen Nachteil: Bisher sind nur wenige Angriffe auf Schutz- und Steuergeräte bekannt geworden. Da aber bereits der erste Angriff schwerwiegende Folgen haben kann, ist die Verwendung des signaturbasierten Ansatzes für die Erkennung von Angriffen im Stromnetz nicht effektiv genug.

2. Baseline-/Lernbasierter Ansatz

In der Lernphase werden bestimmte Protokollmarkierungen beobachtet und anhand dieser Beobachtungen lernt das System, was innerhalb dieses Netzwerks als übliches Verhaltensmuster gilt. Anschließend gibt das System bei jedem abweichenden Verhalten bei einem der Protokollparameter einen Alarm aus. Das bedeutet, dass alle Aktionen, die in der Lernphase nicht vorgekommen sind, wie Schaltvorgänge oder Wartungsaktivitäten, einen Alarm auslösen.

Ein weiterer Nachteil besteht darin, dass das System die Protokollparameter lediglich „kennt“, sie aber nicht versteht. Die ausgegebenen Alarmmeldungen können somit nur von IT-Spezialist:innen interpretiert werden, die sich mit der Automatisierung von Stromversorgungsunternehmen auskennen. Die Folge: Es werden viele Alarme ausgelöst, die sich nur mit hohem Aufwand analysieren lassen.

StationGuard arbeitet nicht mit künstlicher Intelligenz, sondern nutzt die Erfahrungen, die unsere Expert:innen in über 30 Jahren gesammelt haben, gepaart mit Informationen aus den Normen und aus Engineering-Dateien (SCL-Dateien).

3. Der StationGuard-Ansatz

Automatisierungs- und Leittechniksysteme von Stromversorgungsunternehmen sind deterministisch – ihr Verhalten, auch in Ausnahmesituationen, z. B. bei Schutzereignissen, ist klar definiert.

Das ermöglicht eine völlig neue Herangehensweise an die Erkennung von Cyberangriffen.
Weil StationGuard die Funktion eines jeden Geräts kennt, kann die Lösung ein Systemmodell des gesamten Automatisierungssystems aufbauen und anschließend jedes einzelne Netzwerkpaket mit diesem Live-Modell vergleichen. Das entspricht einem Allowlist-Ansatz, bei dem alle zulässigen Verhaltensweisen definiert sind und alles, was von dieser Norm abweicht, einen Alarm auslöst. Mit diesem Ansatz lassen sich auch ganz neue Arten von Angriffen entdecken.

Die Allowlist von StationGuard geht bis ins kleinste Detail: Sogar die in den Nachrichten enthaltenen Signalwerte werden anhand des Systemmodells ausgewertet. Das ermöglicht die einfache Erkennung von Cyberbedrohungen und unzulässigen Aktivitäten, und im Rahmen der Funktionsüberwachung auch die Erkennung von Problemen bei den Automatisierungs- und Leittechnikfunktionen.
Wir beschäftigen uns mit diesem Ansatz bereits seit 2010. Diese Kombination aus Netzwerk- und Sicherheitsexpertise ist der Grund, warum StationGuard so effektiv ist.

Das Konfigurieren von StationGuard geht auch ohne anfängliche Lernphase einfach von der Hand. Dafür werden lediglich ein paar Angaben zum Einsatzzweck der einzelnen Geräte benötigt. Bei IEC-61850-Anlagen kann dieser Prozess durch Importieren von SCL-Dateien deutlich beschleunigt werden.

Vorteile

- Geringe Fehlalarmquote, da StationGuard die Prozesse in Energiesystemen kennt
- Hohe Verständlichkeit der Alarme auch ohne Protokollkenntnisse
- Zuverlässige Erkennung unbefugter Aktionen

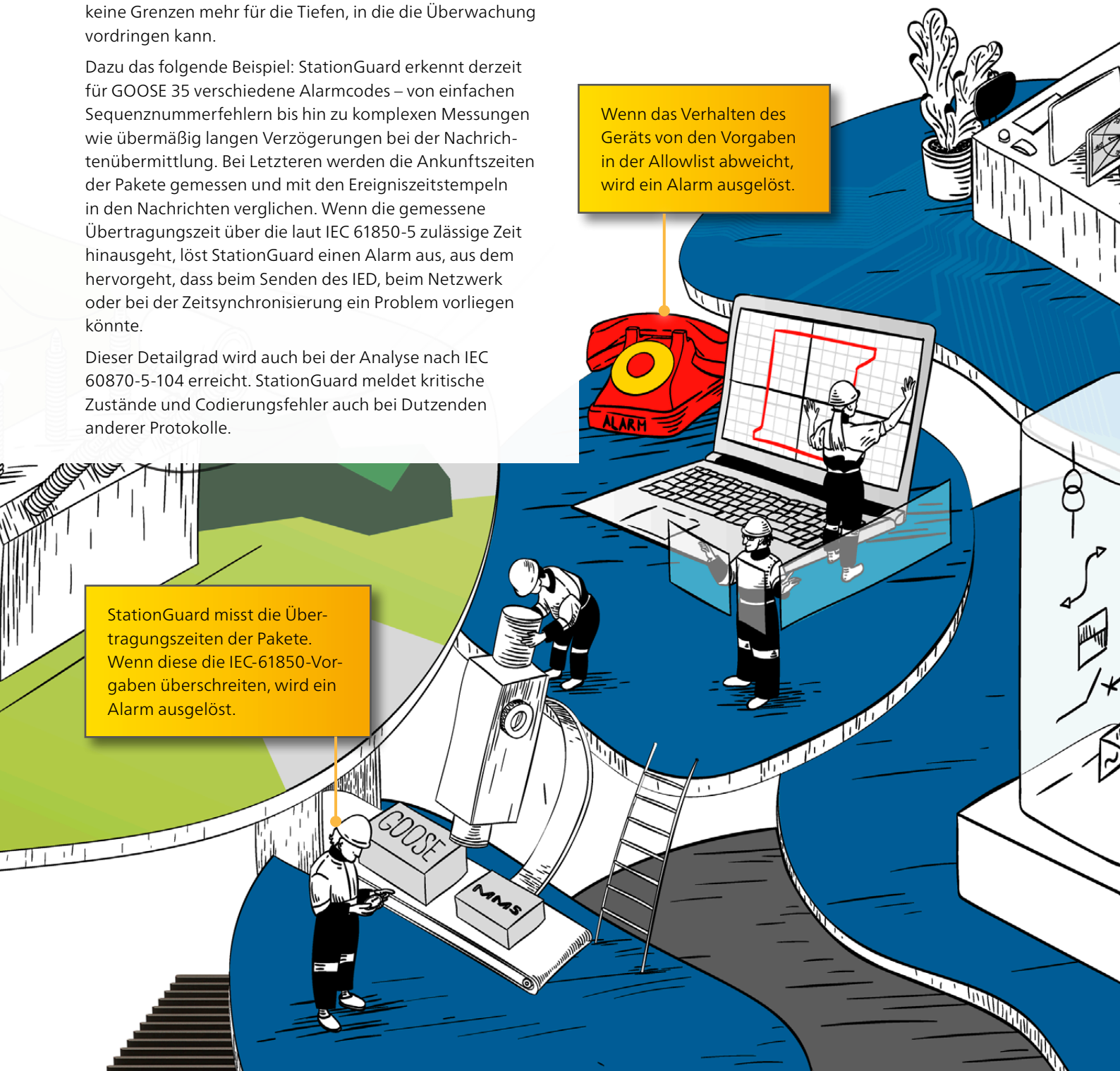
Der Allowlist-Ansatz von StationGuard

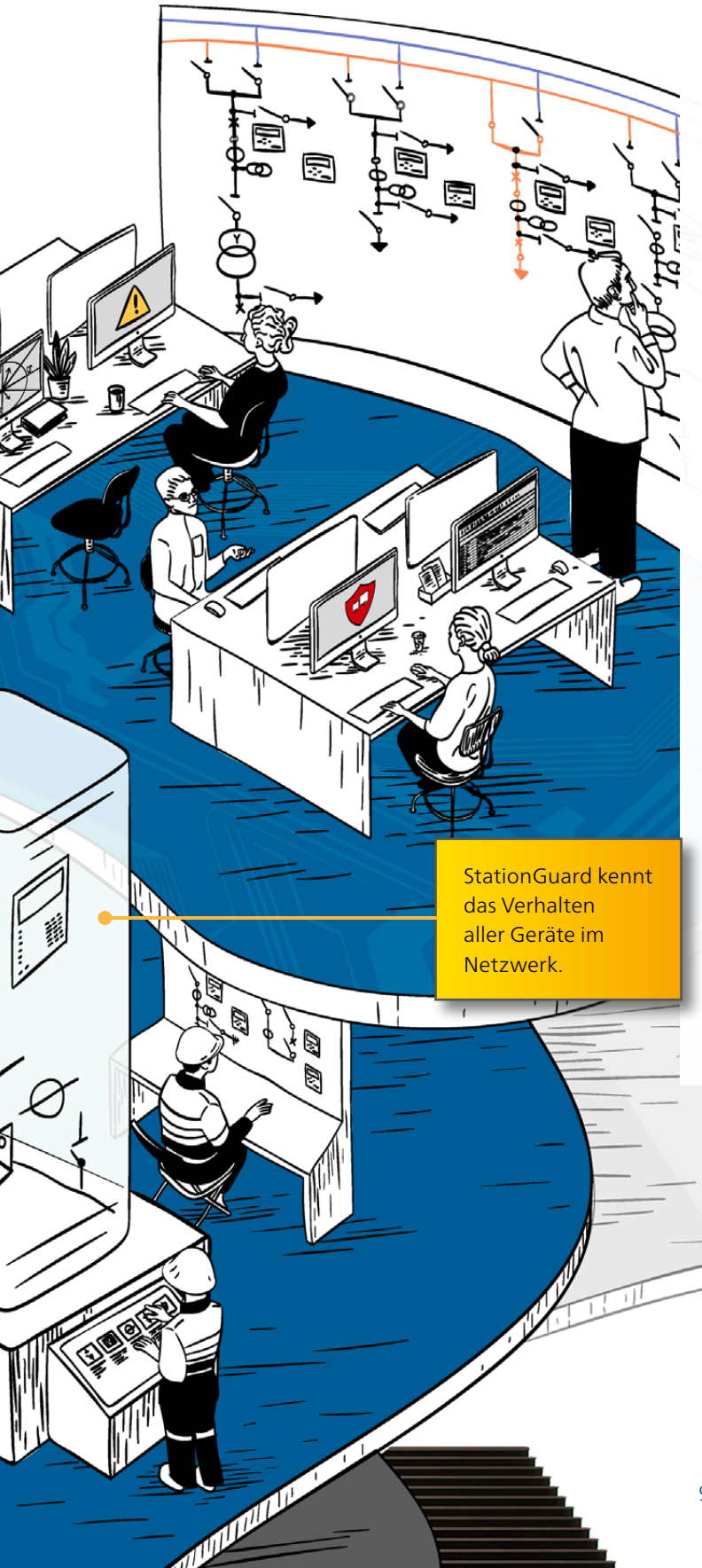
Umfassende Sicherheit auf allen Ebenen

Da StationGuard den gesamten Verkehr bis ins kleinste Detail überwacht und validiert, erkennt die Lösung nicht nur Bedrohungen für die IT-Sicherheit, wie illegale Verschlüsselungen und unbefugte Steueroperationen, sondern auch Kommunikationsfehler und Probleme mit der Zeitsynchronisierung und damit verschiedene Arten von Funktionsstörungen in der Anlage. Und wenn das IDS auch mit dem Einliniendiagramm arbeitet, gibt es praktisch keine Grenzen mehr für die Tiefen, in die die Überwachung vordringen kann.

Dazu das folgende Beispiel: StationGuard erkennt derzeit für GOOSE 35 verschiedene Alarmcodes – von einfachen Sequenznummerfehlern bis hin zu komplexen Messungen wie übermäßig langen Verzögerungen bei der Nachrichtenübermittlung. Bei Letzteren werden die Ankunftszeiten der Pakete gemessen und mit den Ereigniszeitstempeln in den Nachrichten verglichen. Wenn die gemessene Übertragungszeit über die laut IEC 61850-5 zulässige Zeit hinausgeht, löst StationGuard einen Alarm aus, aus dem hervorgeht, dass beim Senden des IED, beim Netzwerk oder bei der Zeitsynchronisierung ein Problem vorliegen könnte.

Dieser Detailgrad wird auch bei der Analyse nach IEC 60870-5-104 erreicht. StationGuard meldet kritische Zustände und Codierungsfehler auch bei Dutzenden anderer Protokolle.





MMS-, IEC 60870-5-104- und DNP3-Kommunikation

StationGuard weiß, welche Datenpunkte welche Funktionen steuern. Ein und derselbe Befehl kann beispielsweise zum Steuern eines Leistungsschalters, zum Steuern eines Stufenschalters oder zum Ändern der Prüfmoduseinstellungen eines Geräts verwendet werden. In der Schaltanlage hat daher jeder Fall deutlich unterschiedliche Auswirkungen. StationGuard ist in der Lage, eine entsprechende Unterscheidung vorzunehmen, und weiß, welches Gerät was und in welcher Situation steuern darf. Diese fein abgestimmten Berechtigungen werden in StationGuard dokumentiert und sind prüfbar.

Andere Protokolle

StationGuard kann bei zahlreichen Energiesystemen und klassischen IT-Protokollen sogenannte Deep Packet Inspections (DPIs) durchführen. Das erlaubt es der Lösung, nicht nur Codierungsverstöße in diesen Protokollen zu erkennen, sondern auch z. B. Port-Spoofing, also das „Kapern" der Port-Nummern von Remote-Verbindungen durch Anwendungen, für die das nicht vorgesehen ist.

Unterstützte Protokolle (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 (Anwendungserkennung, ohne Entschlüsselung)
- telnet
- RIPv2
- SSDP

Vorteile

> Jedes einzelne Paket wird mit dem Systemmodell (Allowlist) verglichen

> Zusätzlich zu Cyberbedrohungen werden auch Funktions- und Kommunikationsprobleme erkannt

> StationGuard überwacht das sichere Funktionieren der gesamten Kommunikation in der Anlage und in der Leittechnik

Schnelleres Reagieren dank verständlicher Alarmmeldungen

Für das Einrichten, Betreiben und Warten herkömmlicher Angriffsüberwachungssysteme (IDS) sind IT-Spezialist:innen und Fachleute auf dem Gebiet der Automatisierungs- und Steuerungstechnik nötig. Beide Gruppen müssen rund um die Uhr erreichbar sein, um auf ausgegebene Alarme reagieren zu können. Dies ist mit Kosten verbunden, die für viele Versorgungsunternehmen nicht tragbar sind. StationGuard bietet diesen Unternehmen eine neue, wartungsarme Alternative.

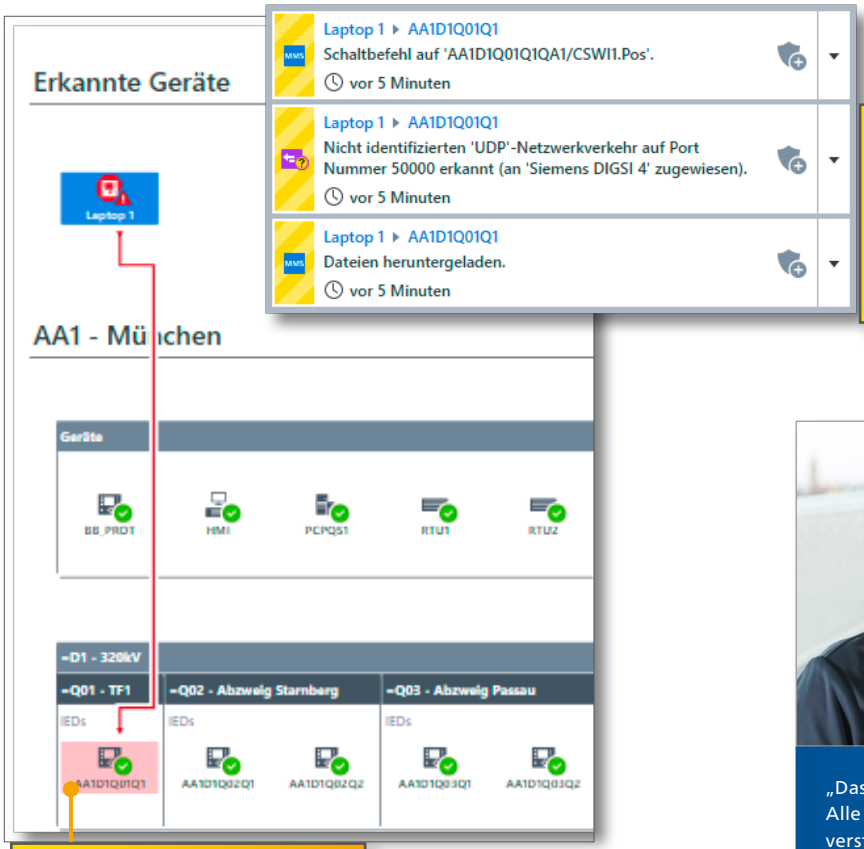
StationGuard kennt die typischen Funktionen in Schaltanlagen und weiß, wofür die vorhandene IT-Ausrüstung, wie Wartungs- und Prüf-PCs, vorgesehen ist. Da alle diese Informationen automatisch bereitstehen, lässt sich StationGuard schnell einrichten, und Ihr Netzwerk wird sofort geschützt – ganz ohne Lernphase.

Alarmursachen zuverlässig identifizieren

Wenn ein Sicherheitssystem Alarme auslöst, sollten diese eine Hilfe für die Bedienenden sein und nicht zusätzlich Verwirrung stiften. Daher werden die von StationGuard ausgelösten Alarme nicht nur in einer Ereignisliste angezeigt, sondern zusätzlich auch im Übersichtsdiagramm grafisch dargestellt. Die Ereignisse im Energiesystem hinter den Netzwerkpaketen werden identifiziert und verständlich formuliert angezeigt.

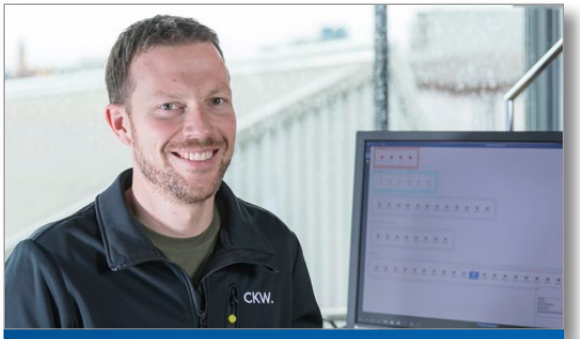
Nehmen wir das folgende Beispiel: Ein Prüf-PC versucht, über das MMS-Protokoll den Leistungsschalter zu steuern. StationGuard meldet dies, verwendet dabei aber keine Begriffe aus dem Protokoll, sondern beschreibt, was in der Schaltanlage passiert ist. Die Meldung enthält unter anderem die folgenden Informationen: Was genau ist passiert? Und welches Gerät ist verantwortlich?

Das erlaubt es IT-Sicherheitsfachleuten und Leit- und Schutztechniker:innen, bei der Ermittlung der Ursache einer Alarmmeldung effizient zusammenzuarbeiten. Das Technikpersonal in den Anlagen kann die IDS-Alarmmeldungen genauso verstehen, als würde es sich ein Betriebsprotokoll, eine Ereignisliste oder eine Warnliste in seiner HMI oder Leittechnik ansehen.



Die Alarmmeldungen sind gut verständlich und können den Ereignissen im Kraftwerk zugeordnet werden.

Es lässt sich auf einen Blick klar erkennen, welches Gerät in welchem Feld den Alarm verursacht hat.



„Das Arbeiten mit StationGuard ist wirklich einfach. Alle notwendigen Informationen werden übersichtlich, verständlich und ohne IT-Slang präsentiert. Und das alles auf dem hohen Qualitätsniveau, das wir von OMICRON gewöhnt sind."

Yann Gosteli
Leiter Bereich Sekundäranlagen
CKW AG, Schweiz

Normalbetrieb

StationGuard analysiert die gesamte Kommunikation und weiß genau, welche Informationen zu einem bestimmten Zeitpunkt übertragen oder nicht übertragen werden dürfen. Welche Geräte dürfen gerade aktiv sein? Welche Steuerbefehle sind zulässig und ergibt die Antwort auf sie Sinn? Welche gemessenen Werte werden gerade übertragen? Stimmt das Timing der Nachrichten? So können alle wahrscheinlichen Probleme mit den IEDs oder dem Netzwerk in einer frühen Phase erkannt werden, bevor es zum Ausfall von IEDs oder des Netzwerks kommt.

Diese umfassende Funktionsüberwachung ist einzigartig und bietet Vorteile, die weit über das hinausgehen, was normalerweise von einem Angriffsüberwachungssystem (IDS) erwartet wird.

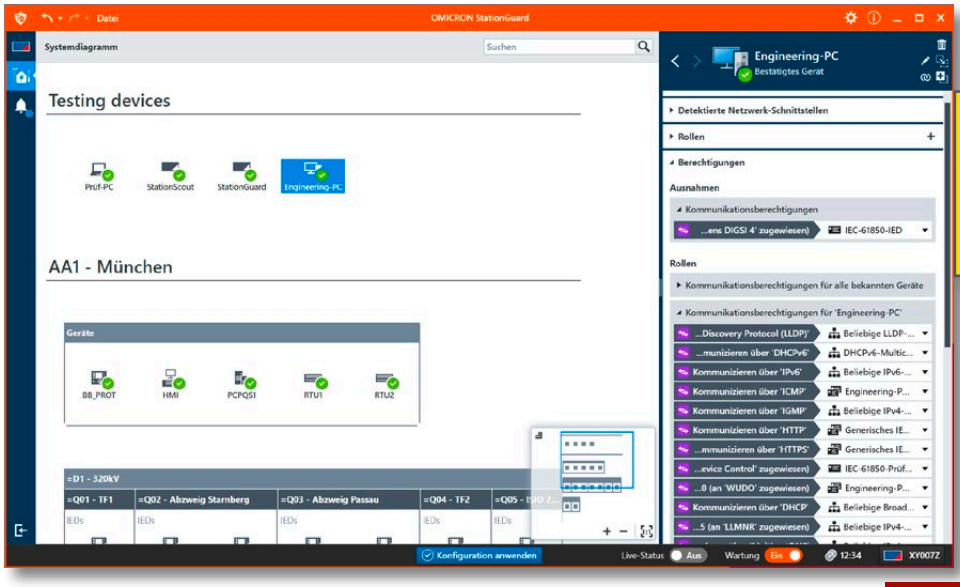
Auf der grafischen Benutzeroberfläche von StationGuard finden sich Schutz- und Steuertechniker:innen schnell zurecht, da sie mit den Dokumentationsdiagrammen und der Ereignisansicht in den Anlagensteuerungen identisch ist.

Wartung und Inbetriebnahme

Prüfungen und Wartungen sind wichtig und dürfen nicht zu Fehlalarmen führen, andererseits muss aber ein hohes Maß an Sicherheit gewährleistet werden. Zur Erfüllung dieser Anforderungen bietet StationGuard einen „Wartungsmodus“. Nur wenn dieser Modus aktiviert ist, sind Wartungs- und Prüfaktivitäten zulässig.

In vielen Angriffsszenarien werden Schwachstellen in Herstellerprotokollen oder Webschnittstellen ausgenutzt. StationGuard kann daher so eingerichtet werden, dass die Kommunikation mit Tools anderer Hersteller nur dann zugelassen wird, solange sich das System im Wartungsbetrieb befindet. Kommt es im Normalbetrieb zu einer Kommunikation nach außen, wird ein Alarm ausgegeben. Um sicherzustellen, dass bei der Ausführung zulässiger Aufgaben keine Fehlalarme ausgelöst werden, können die verwendeten Engineering-PCs und Prüfgeräte vorab in StationGuard registriert werden.

Die Sicherheit beim Prüfen wird dabei nicht beeinträchtigt: Wenn ein infizierter Prüfcomputer ein verdächtiges Kommunikationsverhalten zeigt, wird ein Alarm ausgegeben.



Bestimmte Aktionen sind nur im Wartungsmodus zulässig.

Vorteile

- Alarme sind sowohl für IT-Sicherheitsfachleute als auch für Leit- und Schutztechniker:innen verständlich
- Weniger Fehlalarme bei Turnusprüfungen ohne Einbußen bei der Sicherheit
- Keine Lernphase, sofortiger Schutz

Erkennen von Fehlfunktionen und Konfigurationsfehlern

Funktionsüberwachung

StationGuard erkennt nicht nur Cyberbedrohungen und unzulässige Aktivitäten im Bereich Energieanlagen-Automatisierung und Leittechnik-Netzwerke, sondern informiert Sie auch über kritische Ereignisse und Fehlfunktionen, wie z. B. Ausfälle von IEDs (Intelligent Electronic Devices), Konfigurationsfehler und Netzwerkprobleme, und protokolliert diese für die spätere Analyse. Bei Dateiübertragungen, z. B. wenn Störschriebe heruntergeladen werden, werden die Namen der übertragenen Dateien aufgezeichnet.

Im Folgenden sehen Sie ein paar Beispiele für Funktionsprobleme, die erkannt werden können:

Änderungen an der Konfiguration von IEDs

Wenn sich die Konfiguration eines Geräts ändert, gibt StationGuard einen Alarm aus.

StationGuard überwacht die Konfigurationsrevisionsfelder von Nachrichten im Netzwerk rund um die Uhr, um Änderungen in den Gerätekonfigurationen zu erkennen.

So kann beispielsweise der häufige Inbetriebnahmefehler erkannt werden, dass die Konfigurationsrevisionsfelder auf Sender- und Empfängerseite der Kommunikation unterschiedliche Werte haben.

Konfigurationsfehler

Wenn ein Gerät falsch konfiguriert ist, gibt StationGuard einen Alarm aus. Solche Fehler werden sofort erkannt.

StationGuard vergleicht ständig die IEC-61850-Konfigurationsparameter mit den Spezifikationen in Ihren Eingaben oder in SCL-Dateien,

So werden typische Konfigurationsfehler, wie eine falsche VLAN-Konfiguration, fehlerhafte GOOSE-Parameter oder falsche Datasets, aufgespürt.

Schweregrad	Datum und Uhrzeit	Meldung
	2024-06-13 17:11:37.726+02:00	TestPC ▸ HMI 'HTTP'-Netzwerkverkehr erkannt.
	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE-Multicast-Adresse Neustart von GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear' erkannt.
	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE-Multicast-Adresse Falsche Ziel-MAC-Adresse in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE-Multicast-Adresse Unerwartete VLAN ID in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
	2024-06-13 17:11:36.703+02:00	AA1D1Q01Q1 ▸ GOOSE-Multicast-Adresse Konfigurationsversion (ConfRev) neuer als erwartet bei GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
	2024-06-13 17:11:36.699+02:00	TestPC ▸ HMI 'HTTP'-Netzwerkverkehr erkannt.
	2024-06-13 17:11:34.947+02:00	TestPC ▸ HMI 'HTTP'-Netzwerkverkehr erkannt.
	2024-06-13 17:11:33.931+02:00	PCPQS1 ▸ AA1H1Q01Q1 Nicht identifizierten 'UDP'-Netzwerkverkehr auf Port Nummer 50000 erkannt (an 'Siemens DIGSI 4' zugewiesen).

Ereignisprotokoll mit verschiedenen erkannten Fehlfunktionen

Probleme mit dem Netzwerk und der Zeitsynchronisation

StationGuard erkennt eine verlangsamte Übertragung von (GOOSE-)Nachrichten und das Fehlschlagen der Zeitsynchronisation.

Die StationGuard-Lösung misst die Übertragungszeiten von Nachrichten, indem sie den Zeitpunkt des Absendens mit dem Zeitpunkt der Paketankunft vergleicht. Wenn diese Messung einen Fehler offenbart, wird ein Alarm ausgelöst.

Solche Alarme gehen meist auf Probleme mit der Zeitsynchronisation zurück. Auf die gleiche Weise erkennt StationGuard auch, wenn ein IED aufgrund von Überlast, eines Denial-of-Service-Angriffs oder eines unangemessen langsamen Netzwerks zu spät reagiert.

IEC-104- und IEC-61850-Steuerbefehle

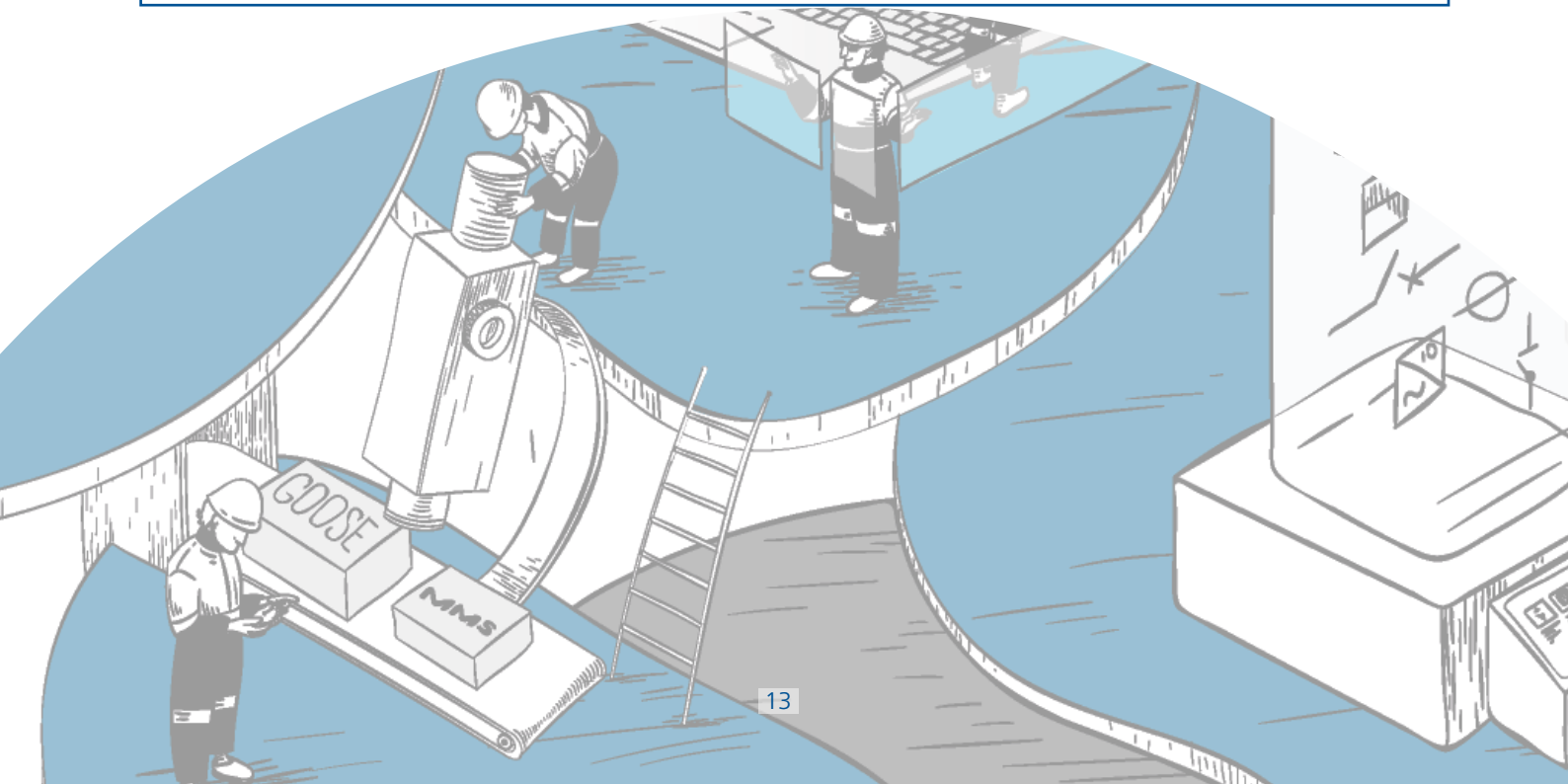
StationGuard erkennt fehlgeschlagene Steuerbefehle und Interoperabilitätsprobleme und zeichnet diese auf.

StationGuard protokolliert alle IEC-60870-5-104- und MMS-Steuerbefehle. Wenn ein Befehl fehlschlägt, werden entsprechende Warnungen erstellt und die Netzwerk-Traces werden für die spätere Analyse aufgezeichnet. Außerdem erkennt das System Protokoll- und Interoperabilitätsprobleme in MMS, IEC 60870-5-104, DNP3, Modbus, Synchrophasor und vielem mehr.

Aufzeichnung von Dateiübertragungen

StationGuard zeichnet Down- und Uploads von Störschrieben und anderen Dateien auf.

Alle Dateiübertragungen in IEC-104 und MMS werden zusammen mit den Dateinamen und einer Netzwerkaufzeichnung protokolliert. Dem Protokoll lässt sich entnehmen, wer wann auf Dateien auf IEDs zugegriffen hat.



Alarmanalyse und Bedrohungsuntersuchung

Alarm-Untersuchung (GridOps)

Das Alarm-Dashboard von GridOps bietet Zugang zu sicherheitsrelevanten Daten und zu Betriebsdaten, die den Netzbetrieb und Sicherheitsbelange transparenter machen, und ermöglicht Ihnen so einen umfassenden Überblick über die Sicherheitslage Ihres Stromnetzes.

Mit GridOps können Sie das kombinierte Ereignisprotokoll aller Sensorstandorte analysieren und alle Ereignisse aus verschiedenen Blickwinkeln und unter Berücksichtigung verschiedener Indikatoren visualisieren. So lassen sich Alarmmuster und -trends für konkrete Gerätetypen oder Standorte erkennen.

Dank der Möglichkeit, Alarmprotokolle zu prüfen und zu analysieren, können Sie ganz einfach Sicherheitsvorfälle, Richtlinienverstöße, Betriebsprobleme und mehr identifizieren. Die Analysefunktionen von GridOps können auch zur Unterstützung bei Audits und forensischen Analysen sowie zur Ermittlung akuter und langfristiger betrieblicher Probleme genutzt werden.

Von den Echtzeiteinblicken in alle Netzwerke für den Stromnetzbetrieb profitieren gleich mehrere Teams: Sicherheitsfachleute können Sicherheitsrichtlinien zum Schutz der Netzwerke durchsetzen, ohne den Betrieb zu unterbrechen, und dank der Kommunikationsüberwachung ihre Netzwerke weiter segmentieren.
Leit- und Schutztechnikteams erhalten Einblicke und Erkenntnisse, die ihnen dabei helfen, die Verfügbarkeit der Automatisierungsnetzwerke des Stromversorgungsunternehmens aufrechtzuerhalten.

Dashboard mit statistischen Angaben zu Alarmen für mehrere Standorte

Zentrales Verwaltungssystem für StationGuard– GridOps

Zentralisierte Plattform

- Geringe Falsch-Positiv-Rate und bessere Konzentration auf tatsächliche Probleme
- Uneingeschränkte 24/7-Transparenz bei Sicherheitsvorfällen, Funktionsproblemen und mehr
- Beschleunigung und Vereinfachung der Reaktion auf Vorfälle

GridOps ermöglicht Folgendes:

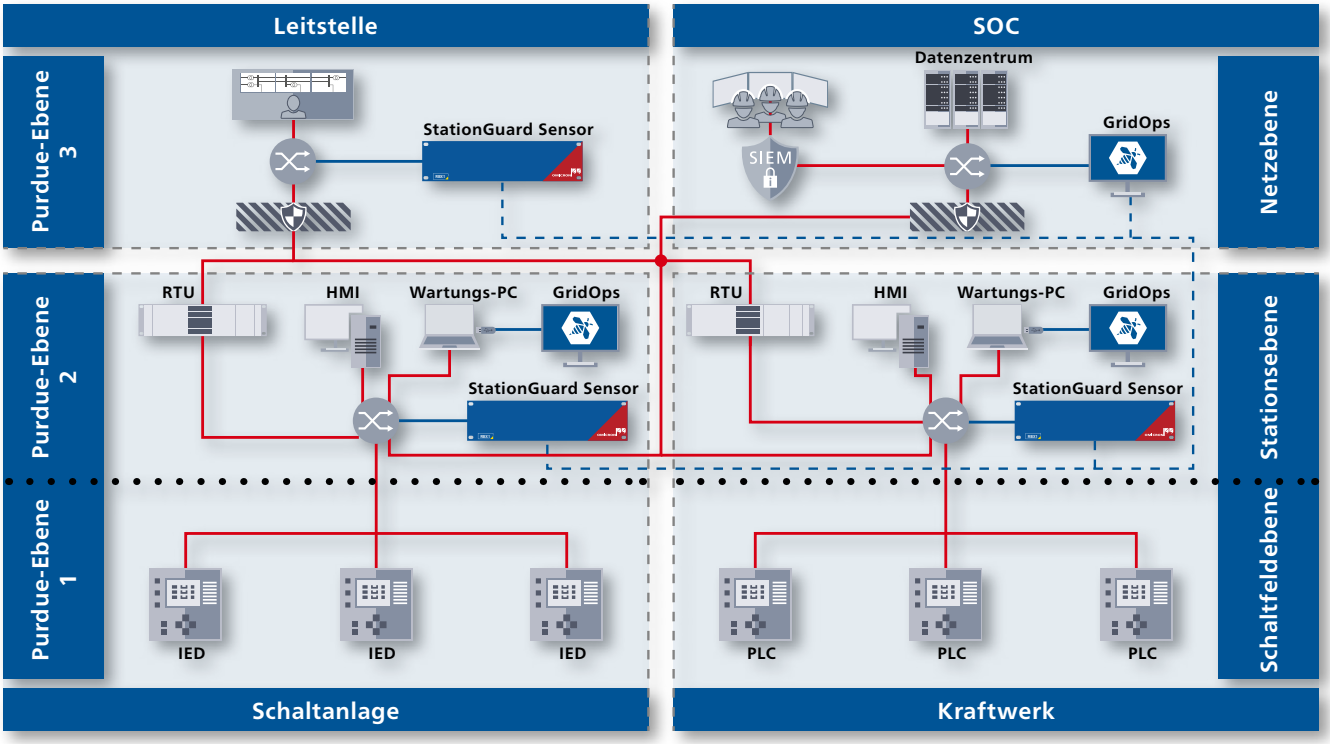
Verstehen der Hintergründe, Ursachen und Folgen einer Bedrohung, z. B., ob sie schon eine Verbindung ins System hergestellt hat

Reibungsloses Zusammenarbeiten zwischen IT-Sicherheitsteams und OT-Teams für eine bessere Reaktion auf Vorfälle und Schwachstellen

Senken des Betriebsrisikos durch Vorbereitung auf den Umgang mit Sicherheitsvorfällen

Suchen nach Anomalien im typischen Verhalten des Stromnetzes zur Erkennung aller Arten von Bedrohungen

Visualisieren aller versuchter Angriffe und Verhaltensabweichungen, so klein sie auch sein mögen



Integration von StationGuard in die Netzwerkinfrastruktur

Was beinhaltet die StationGuard-Lösung?

Mit den StationGuard-Sensoren, die in Leitstellen, Kraftwerken und Schaltanlagen installiert werden können, lassen sich Angriffe erkennen, Netzwerke visualisieren und Assets ermitteln. Außerdem können Stromversorgungsunternehmen mit ihnen das ordnungsgemäße Funktionieren ihrer Automatisierungssysteme überwachen. Die Sensoren bieten flexible Bereitstellungsoptionen:

> RBX für die dauerhafte Installation

> VBX für die Nutzung auf einer virtuellen Plattform

> MBX für die zeitweise Nutzung oder dauerhafte Installation

GridOps ist das zentrale Management-System für StationGuard. Es bietet Funktionen für die Verwaltung des Asset-Inventars, das Schwachstellen-Management, die Ereignisanalyse und Alarme sowie für die Verwaltung der Sensoren. Ihr wesentliches Merkmal ist die Bereitstellung einer zentralen Plattform für die Visualisierung von Cyber Security-Risiken und Bedrohungen sowie für die Überwachung von Assets und Ereignissen (sowohl hinsichtlich der Cyber Security als auch hinsichtlich der Funktionsweise) im gesamten Stromnetz.

GridOps kann in einer Leitstelle oder in einem SOC (Security Operations Center) installiert und für die zentralisierte Verwaltung aller StationGuard-IDS-Sensoren verwendet werden.

Vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde StationGuard (v.2.21) auf der RBX1 mit dem IT-Sicherheitszertifikat (BSZ) ausgezeichnet.

Dieses Siegel bestätigt die Einhaltung sämtlicher IT-Sicherheitskriterien für ein Angriffserkennungssystem (SzA).

*durch vorhandene Hutschienen-Halterung

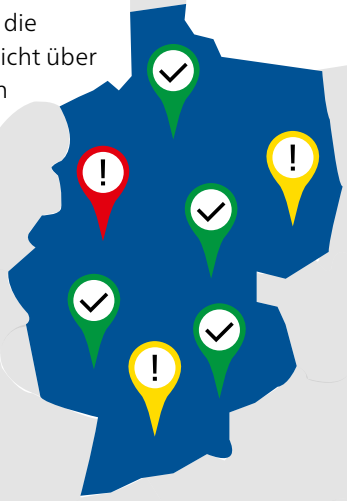
Netzwerk-Sichtbarkeit

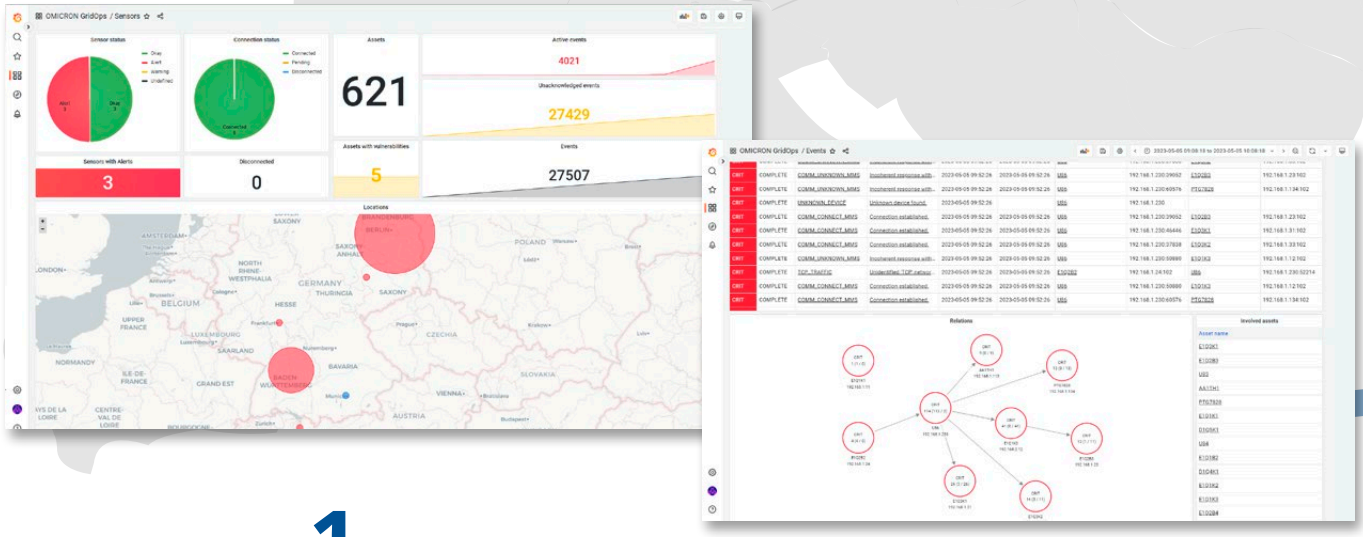
Netzwerk-Sichtbarkeit vom Stromnetz bis zur Anlage

IT-Sicherheitsfachleute sowie Leittechnik- und OT-Netzwerkingenieur:innen stehen vor drängenden Fragen: Welchen Bedrohungen und Risiken sind unsere kritischen OT-Netzwerke derzeit ausgesetzt? Wie sind die Netzwerkzonen aufgebaut und wie sind sie untereinander verbunden? Wie kommunizieren die Geräte innerhalb dieser Grenzen und über sie hinweg?

Zur Beantwortung dieser und anderer Fragen wird ein vielseitiges Tool benötigt, das den Nutzer:innen die Möglichkeit gibt, sich sowohl eine Gesamtübersicht über das Netzwerk zu verschaffen, als auch bis zu den Details der Kommunikation zwischen einzelnen Assets vorzudringen.

Unsere StationGuard-Lösung bietet diese hohe Systemtransparenz.





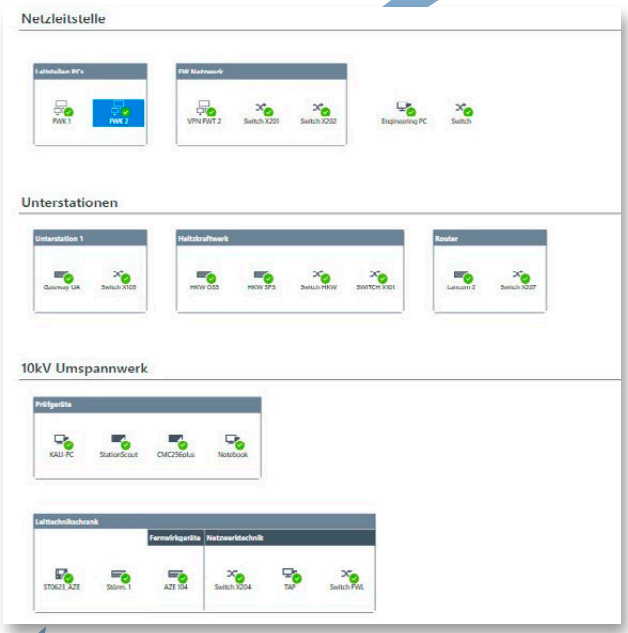
1 Überblick über das gesamte Stromnetz

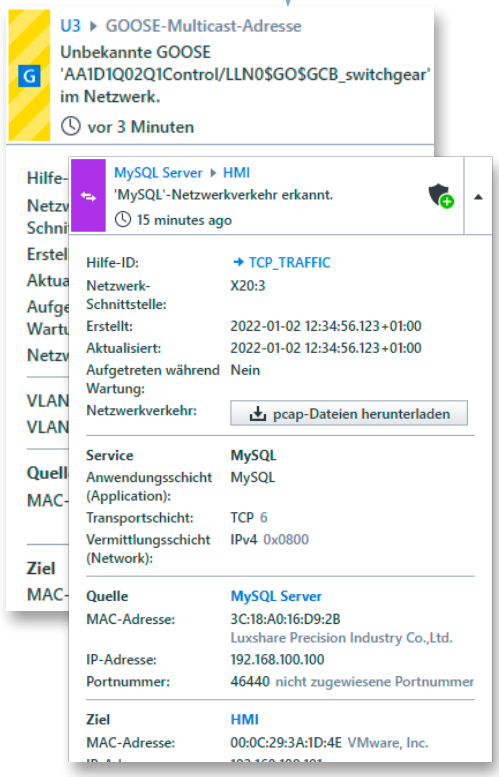
Verschiedene Dashboards bieten einen Gesamtüberblick über den Status aller Automatisierungsnetzwerke des Stromnetzes. Bedrohungen, Funktionsprobleme oder Schwachstellen, die sofortiges Handeln erfordern, sind auf einen Blick erkennbar.

2 Netzwerk-Diagramm der einzelnen Anlagen

Eine Ebene tiefer lassen sich die Netzwerke überwachen. Dabei hilft unsere einzigartige Ansicht, die Aspekte des Purdue-Referenzmodell-Diagramms mit denen des Schutz- und Leittechniker:innen vertrauten Einliniendiagramms zu verbinden. Diese Kombination ermöglicht eine optimale Zusammenarbeit beider Welten.

Die Diagramme können automatisch aus SCL-Engineering-Dateien generiert und bei Bedarf manuell verbessert werden. Außerdem besteht die Möglichkeit, Tabellendateien aus der Dokumentation mit den korrekten Asset-Namen zu importieren.





3 Kommunikationsbeziehungen zwischen Geräten

Auf der untersten Ebene geht es um die Kommunikation zwischen den Geräten und die verwendeten Protokolle. Hier können Details zu den Assets und Typenschildinformationen überwacht werden. IT-Teams können für jedes Asset das Feld und den Spannungswert ermitteln und sich dank der auf beiden Seiten einheitlichen Terminologie effizient mit den OT-Schutztechnikteams beraten.

Automatisches Erfassen von Daten für eine bessere Schwachstellenerkennung

Eine wichtige Voraussetzung für ein erfolgreiches Schwachstellen- und Risikomanagement ist das Vorhandensein eines Asset-Inventars mit präzisen Angaben zu jedem Schutz- und Steuer-IED. Je mehr Informationen zu jedem einzelnen Asset vorliegen, desto genauer lassen sich Schwachstellen analysieren und priorisieren. Unsere StationGuard-Lösung unterstützt Sie während des gesamten Prozesses – vom Erstellen und Aktualisieren des Asset-Inventars bis zum Schwachstellen- und Risikomanagement.

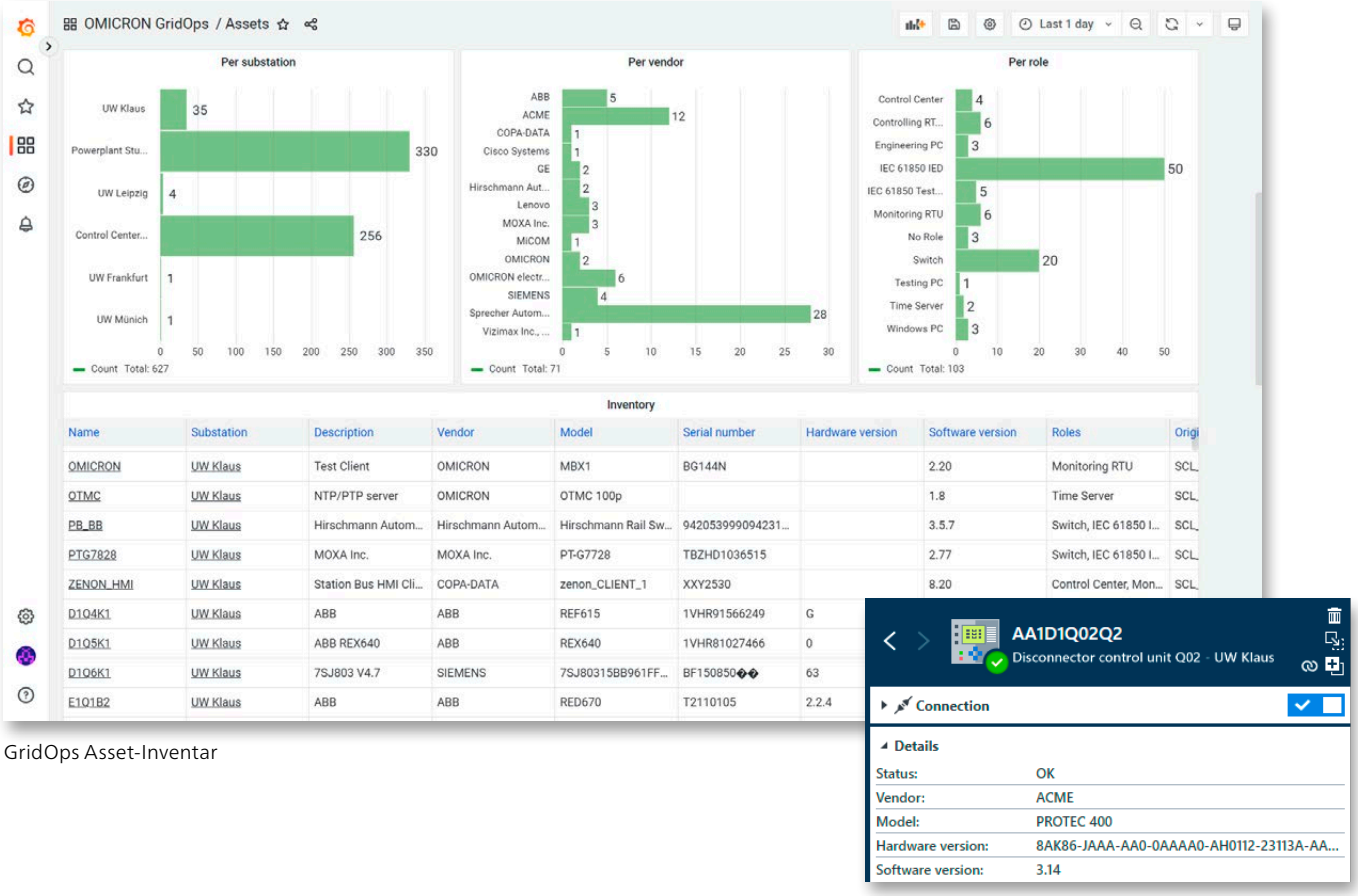
StationGuard findet automatisch alle Assets im Netzwerk, erstellt ein globales Asset-Inventar und informiert Sie über neue Geräte in Ihren Netzwerken. Die Lösung sammelt genaue Informationen zu den einzelnen Assets, indem es die Netzwerkanalyse mit importierten Engineering-Dateien (SCL) und Tabellen aus der Anlagendokumentation kombiniert. Das Asset-Inventar kann durch den Import von Informationen aus externen Quellen aktualisiert werden.

Detaillierte Informationen zu Ihren Assets

Durch die Kombination aus passiv beobachteten Informationen und importierten Engineering-Dateien und Tabellen erhalten Sie hochgradig präzise Angaben zu Ihren Assets. Diese umfassen Engineering-Beschreibungen, Angaben zum Typ und zur Hardware-Konfiguration, Produkt-Bestellnummern und Firmware-Versionsnummern.

Sie können das Verzeichnis exportieren und in Asset-Inventarisierungs-/CMDB-Systeme, ERP-Systeme oder Kalkulationstabellen importieren. Die Möglichkeit, Tabellen im CSV-Format in StationGuard zu importieren, ermöglicht die Nachverfolgung von Vorgängen und die Synchronisation mit beliebigen anderen Quellen. Sie können optional die Active Asset Identification von StationGuard aktivieren, um automatisch Informationen zur Gerätekonfiguration und Firmware-Version über das Netzwerk auszulesen.

Unsere StationGuard-Lösung stellt dann ein Asset-Inventar mit detaillierten Informationen aus verschiedenen Quellen zusammen, das eine optimale Basis für Ihr Schwachstellen-Management darstellt.



GridOps Asset-Inventar

Schwachstellen-Management

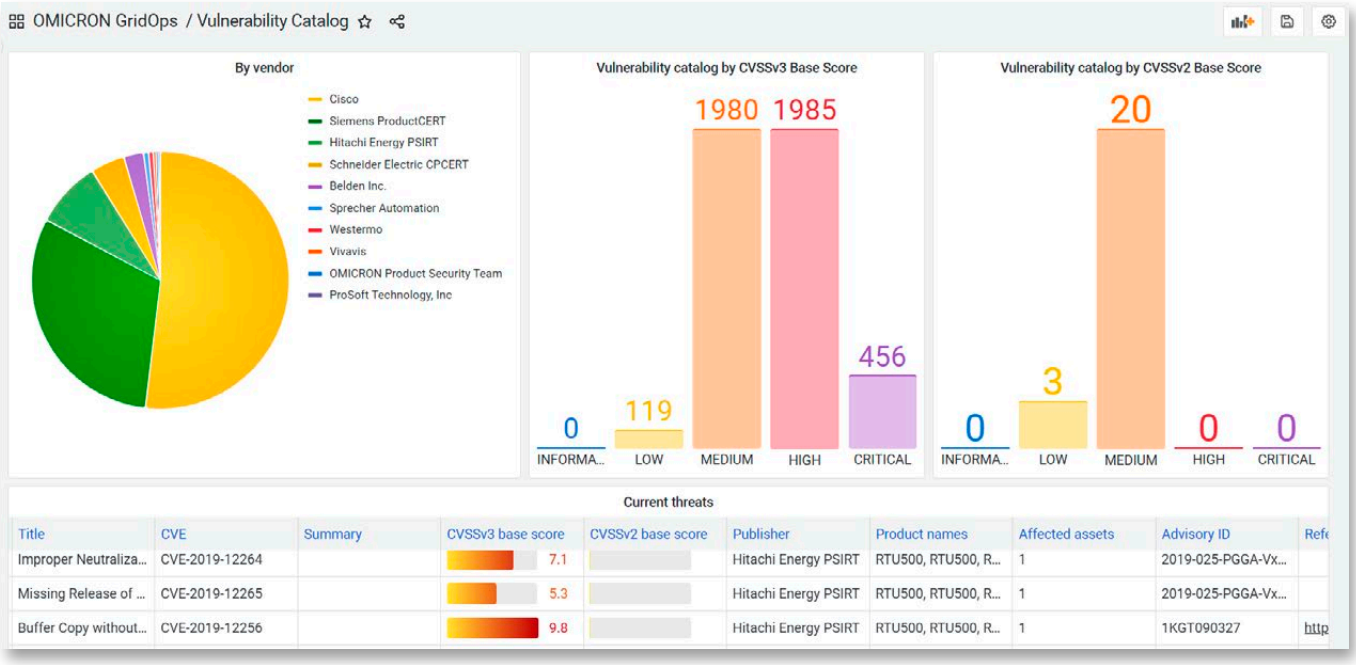
Sicherheitsvorschriften für kritische Systeme wie z. B. die NIS-Richtlinie der EU und der US-amerikanische Standard NERC-CIP verlangen als wesentlichen Aspekt eines jeden Cyber-Security-Programms ein Schwachstellen-Management. Der Abgleich offiziell bekannter Schwachstellen mit Ihrer Systeminfrastruktur ermöglicht es Ihnen, eine geeignete Risikostrategie festzulegen und umzusetzen.

Schützen lässt sich nur, was man sieht.

Anhand unseres Schwachstellen-Dashboards können Sie sich ein besseres Bild von der Sicherheitsgefährdung des Netzwerks insgesamt und von kritischen Punkten im Besonderen machen. Es gibt auch Auskunft über neu entdeckte Schwachstellen, indem es die Assets fortlaufend auf potenzielle Bedrohungen prüft. Je mehr Informationen zu den Assets vorliegen, desto genauer können Bedrohungen erkannt, analysiert und priorisiert werden.

Ein entscheidender Vorteil: Nutzer:innen können sich nur die Schwachstellen anzeigen lassen, die für sie relevant sind. Mit der von OMICRON entwickelten Schwachstellen-Datenbank für Stromnetzautomatisierungs- und Netzwerkgeräte reichen dafür ein paar wenige Klicks. Dabei wird schnell ermittelt, welche Systeme anfällig für eine bestimmte CVE (Common Vulnerability Exposure) sind.

Das Zusammenstellen umfassender und aussagekräftiger Reports für Vorgesetzte, Auditor:innen und Aufsichtsbehörden zur Unterstützung bei der Risikopriorisierung und -minderung war noch nie so einfach. Alle Beteiligten profitieren von mehr Transparenz und übersichtlicheren Informationen zur Sicherheitslage des Systems und den bestehenden Risiken.



GridOps Schwachstellen-Dashboard

Vorteilhafte Integrationen und Partnerschaften

StationGuard bietet Plug-ins für Ticketing-Systeme wie ServiceNow, mit denen automatisch Arbeitstickets zur Bearbeitung von IDS-Alarmen erstellt werden können. Durch Importieren des Asset-Inventars aus StationGuard werden die Tickets automatisch den Techniker:innen zugewiesen, die für das betreffende Assets oder den Standort zuständig sind.

Zugriffskontrolle zum Schutz von Daten und Netzwerken

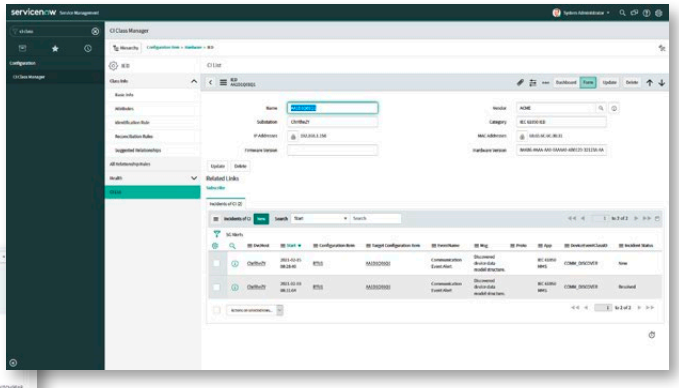
Die Integration in LDAP/Active Directory kann über das zentrale Verwaltungssystem konfiguriert werden. Für die Kontrolle des Zugriffs auf die verschiedenen Funktionen zur Anzeige und Konfiguration Ihrer StationGuard-Instanzen können unterschiedliche Nutzer:innenrollen definiert werden. So lässt sich zum Beispiel festlegen, dass Änderungen der Konfiguration oder das Aktivieren des Wartungsmodus nur entsprechend befugten Nutzer:innen vorbehalten sind. Bei einem Ausfall aller Netzwerke kann über die lokale Bedienoberfläche des StationGuard-Clients auch einzeln auf die StationGuard-Sensoren zugegriffen werden.

Bedrohungen von innen können mit rollenbasierter Zugriffskontrolle (Role-Base Access Control, RBAC) reduziert und sogar eliminiert werden. Das sorgt für eine höhere Sicherheit des Systems und der Netzwerke und gleichzeitig auch für mehr Effizienz, denn Passwörter müssen weniger häufig geändert werden.

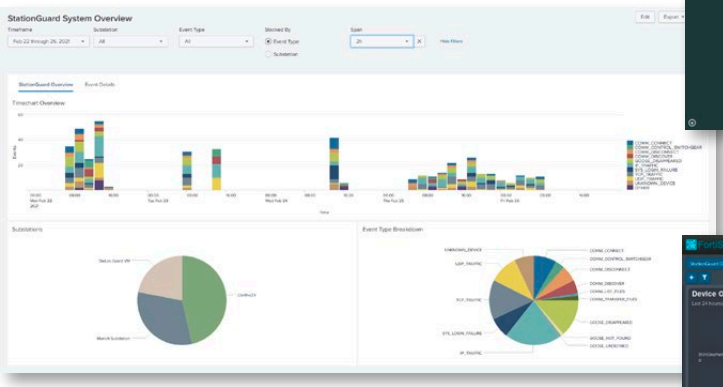
Einfache Integration ins Netzwerk

Für das einfache Integrieren von StationGuard in ältere Systeme können die Binärausgänge der Plattform RBX1 verwendet werden. Das Vorhandensein eines unbestätigten Alarms wird an den Binärausgängen signalisiert, die mit einer RTU (Remote Terminal Unit, Fernbedienungsterminal) verdrahtet und in die Leittechnik-Signalliste integriert werden können.

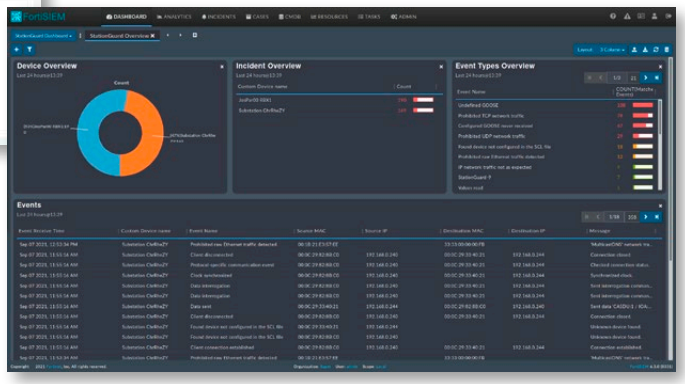
Alternativ dazu können unsere leicht verständlichen Alarmmeldungen auch über das Syslog-Protokoll weitergeleitet werden. Für die Integration von StationGuard-Sensoren in SIEM(Security Information and Event Management)- und Ticketing-Systeme verschiedener Hersteller:innen stehen mehrere Plug-ins zur Verfügung.



ServiceNow-Integration



„StationGuard for Splunk"-App



FortiSIEM-Integration

Unsere Partner für sichere Stromnetze

Technologie-Partner

Fortinet

Das Open Fabric Ecosystem von Fortinet bietet Ihnen integrierte Lösungen für umfassende End-to-End-Sicherheit.

Integration der StationGuard-Lösung in FortiSIEM:

Sorgt für mehr Sicherheit, Compliance und Geschäftsagilität.

Splunk

Splunk erfasst, indexiert und korreliert Echtzeitdaten in einem durchsuchbaren Datenspeicher, der als Basis für die Erstellung von Diagrammen, Reports, Warnungen, Schnittstellen und Visualisierungen dient.

„StationGuard for Splunk"-App auf Splunkbase:

Reports auf Abruf mit statistischen Analysen

Content- und Vertriebspartner

NTS

Gemeinsam mit High-End-Herstellern übernimmt NTS digitale Verantwortung und schafft IT-Lösungen mit zuverlässigen Services für die Bereiche Netzwerk, Security, Zusammenarbeit, Cloud und Data Center.

Kombination von StationGuard mit dem Threat Detection Service von NTS:

Sie erhalten umfangreiche Analyse-Reports für die Risikoerkennung und die Verbesserung der Sicherheit des Systems.

ALSEC

Die Cyber-Security-Expert:innen von ALSEC unterstützen Sie mit kompetenten und individuellen Dienstleistungen, von Schulungen über die Entwicklung von Prozessen und das Evaluieren von Produkten bis hin zu deren Implementierung.

Kombiniertes Wissen von OMICRON und ALSEC:

Risiko-Reporting und Business Security Intelligence für die Planung und die Vorbereitung auf die Zukunft.

Mehr über unsere Partner und Communities wie EE-ISAC erfahren Sie auf unserer Homepage:
https://www.omicronenergy.com/de/cybersecurity-partners/

Drei verschiedene Plattform-Optionen

Die StationGuard-Sensoren sind auf drei verschiedenen Plattformen verfügbar. Je nach Anforderungsprofil kann StationGuard auf den Hardware-Plattformen RBX und MBX oder auf einer Virtual Machine (VBX) eingesetzt werden. Da die gesamte „Intelligenz“ von StationGuard im Sensor enthalten ist, laufen die Sensoren autonom, d. h., es muss keine dauerhafte Verbindung zu einem zentralen Server bestehen.

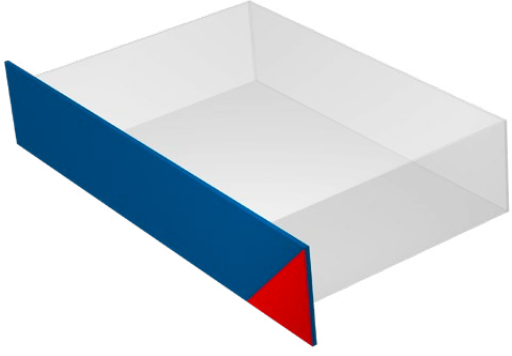
StationGuard auf der Plattform RBX

Die Ausführung von StationGuard auf der Hardware RBX ist eine maßgeschneiderte IDS-Lösung für den Schutz von Automatisierungs- und Leittechniksystemen von Stromversorgungsunternehmen vor Cyberbedrohungen und Zero-Day-Angriffen. Die für die 19-Zoll-Rack-Installation vorgesehene Plattform RBX ist für die Anforderungen rauer Stromnetzumgebungen ausgelegt. Sie verfügt über genügend Leistung und Speicher, um alle Ereignisse und den damit verbundenen Datenverkehr aufzuzeichnen, auch wenn das Ereignis schon lange zurückliegt.

RBX bietet einzigartige Sicherheitsfunktionen, wie z. B. Festplattenverschlüsselung, einen ISO/IEC-11889-konformen Kryptoprozessor-Chip und ein angepasstes, sicheres UEFI. Außerdem bietet die Plattform Binärausgänge, die es einfach machen, IDS-Alarme in die Leittechnik-Signalliste zu integrieren.

StationGuard auf der Plattform VBX

Die StationGuard-Sensoren sind auch als Virtual Appliance verfügbar, die auf vorhandenen Rechnerplattformen installiert werden können.



Wie die Hardware-Plattformen kann auch die virtuelle Variante völlig unabhängig laufen und Ereignisse auch dann aufzeichnen und protokollieren, wenn keine permanente Verbindung zum zentralen Server besteht.

Zu beachten ist, dass es bei Ausführung auf einer Virtual Machine – im Vergleich zur Ausführung auf RBX und MBX – einige technische Einschränkungen im Bereich der Funktionsüberwachung von Prozessbusanwendungen geben kann.

StationGuard auf der Plattform MBX

Mit der Mobilversion von StationGuard können Sie eine schnelle Sicherheitsbewertung eines Anlagennetzwerks vornehmen oder schnell eine Asset-Inventarliste aller Geräte im Netzwerk erstellen.

Während der Inbetriebnahme oder in Wartungsphasen verbinden viele Techniker:innen und auch externe Dienstanbieter:innen ihre Geräte mit dem für Bedrohungen anfälligen Anlagennetzwerk. StationGuard auf der Plattform MBX ist perfekt geeignet, um das Netzwerk während dieser Zeit vorübergehend zu überwachen, um bei unzulässigem Verhalten zu warnen und kritische Aktionen während der Inbetriebnahme und Wartung aufzuzeichnen.

Optional bietet die tragbare MBX-Hardware-Einheit, durch Einsatz der verfügbaren Hutschienen-Halterung, die Möglichkeit zur Fixinstallation.

Technische Spezifikationen der Plattform RBX1

Umgebungsbedingungen

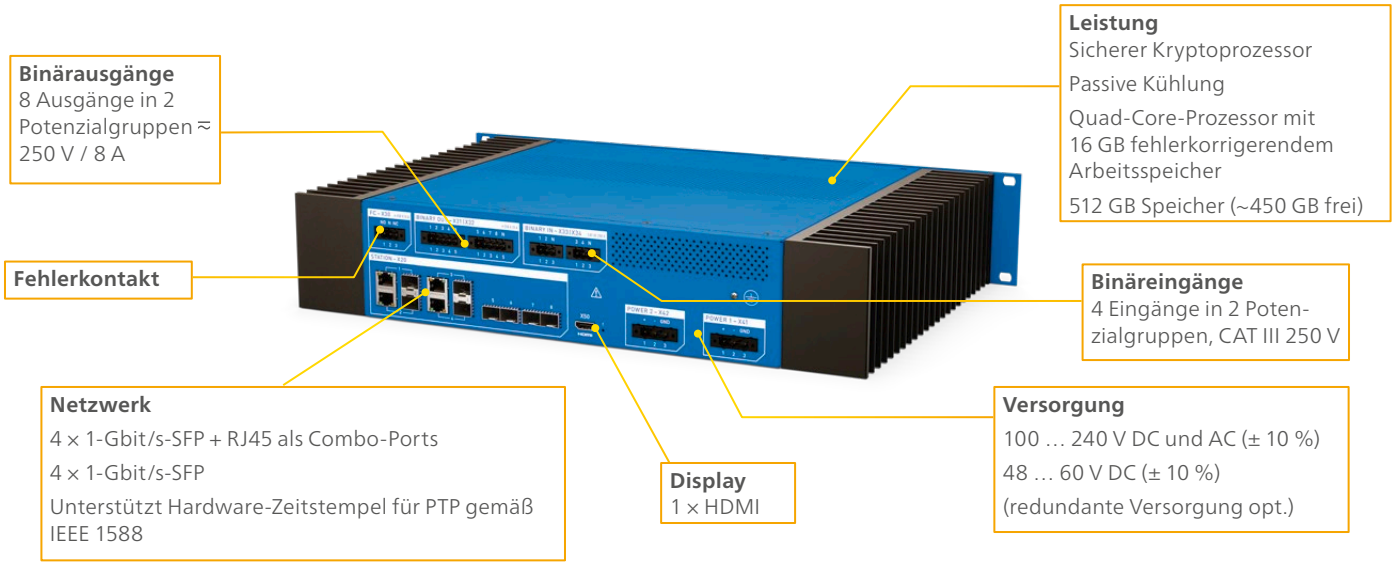
Betriebstemperatur	–20 °C … +55 °C
Lagertemperatur	–25 °C … +70 °C
Relative Feuchte	5 % … 95 % (nicht kondensierend)
Schutz gegen Wasser gemäß IEC 60529	IP30

Normen

Produkt-Normen	IEC 61850-3 IEEE 1613 Severity Level: Class 1
EMV-Normen	IEC 61326-1 IEC 60255-26 IEC 61000-6-5
Sicherheit	EN 60255-27 EN 61010-1 EN 61010-2-030

Weitere Details sind im technischen Datenblatt zu finden.

Rückseite der Plattform RBX1



Vorderseite der Plattform RBX1

Wir schaffen Nutzen für unsere Kund:innen durch …

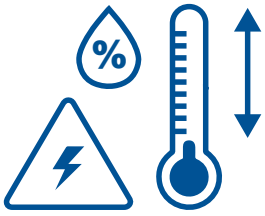
Qualität

Wir möchten, dass Sie sich stets auf unsere Prüflösungen verlassen können. Aus diesem Grund entwickeln wir unsere Produkte mit Erfahrung, Leidenschaft und Sorgfalt und setzen kontinuierlich neue Standards in unserer Branche.

Vertrauen Sie höchsten Arbeitsschutz- und Sicherheitstandards

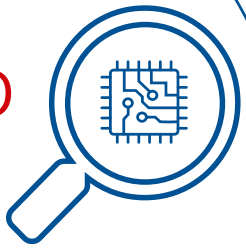
Maximale Zuverlässigkeit durch bis zu

72



Stunden Burn-in-Tests vor Auslieferung

100%



Routineprüfungen aller Prüfgeräte-komponenten

ISO 9001
TÜV & EMAS
ISO 14001
OHSAS 18001

Einhaltung internationaler Normen

Innovation

Innovatives Denken und Handeln sind tief in unserer DNA verwurzelt. Unser umfassendes Produktpflege-Konzept garantiert, dass sich Ihre Investition auch langfristig auszahlt – z. B. durch kostenlose Software-Updates.

Ich brauche...

… ein auf die Bedürfnisse unserer Kund:innen abgestimmtes Produktportfolio

Mehr als

200

Entwickler:innen halten unsere Lösungen up-to-date

Mehr als

15%

unseres Jahresumsatzes investieren wir in Forschung und Entwicklung

Bis zu

70%

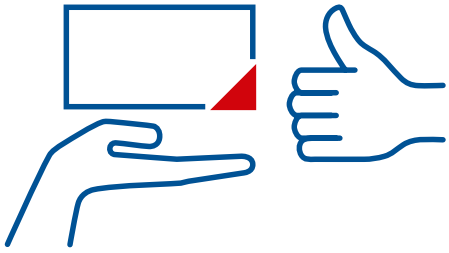
Zeitersparnis durch Prüfvorlagen und Automatisierung

Wir schaffen Nutzen für unsere Kund:innen durch …

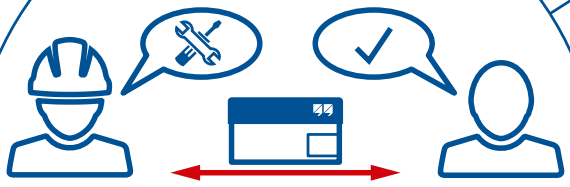
Support

Wenn schnelle Hilfe gefragt ist, stehen wir Ihnen stets zur Seite. Unsere hochqualifizierten Techniker:innen sind rund um die Uhr für Sie erreichbar. Darüber hinaus helfen wir Ihnen, Ausfallzeiten zu minimieren, indem wir Ihnen Testgeräte von einem unserer Servicezentren ausleihen.

Professioneller technischer Support rund um die Uhr



Leihgeräte helfen, Ausfallzeiten zu reduzieren



Kostengünstige und unkomplizierte Reparatur und Kalibrierung

Niederlassungen weltweit für Kontakt und Unterstützung vor Ort

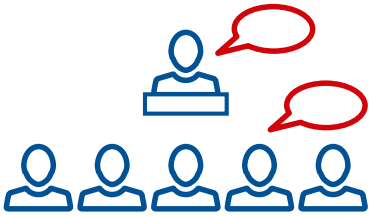
Wissen

Wir stehen in einem ständigen Dialog mit Anwender:innen und Expert:innen. Durch einen kostenlosen Zugang zu Application Notes und Fachartikeln können Kund:innen von unserem Fachwissen profitieren. Zusätzlich bietet die OMICRON Academy ein breites Spektrum an Schulungen und Webinaren an.

Mehr als

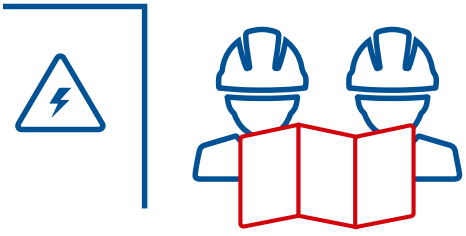
300

Academy-Trainings und zahlreiche Praxis-Schulungen pro Jahr



Von OMICRON ausgerichtete Tagungen, Seminare und Konferenzen

auf tausende Fachbeiträge und Application Notes



Umfassende Kompetenz in der Beratung, Prüfung und Diagnostik

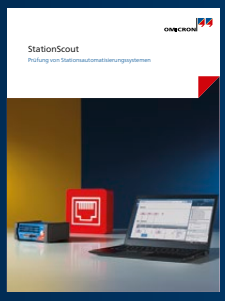
OMICRON arbeitet mit Leidenschaft an wegweisenden Ideen, um Energiesysteme sicherer und zuverlässiger zu machen. Mit unseren neuartigen Lösungen stellen wir uns den aktuellen und zukünftigen Herausforderungen unserer Branche. Wir unterstützen unsere Kund:innen mit vollem Einsatz: Wir gehen auf ihre Bedürfnisse ein, bieten ihnen hervorragenden Vor-Ort-Support und teilen unsere Expertise und unsere Erfahrungen mit ihnen.

In der OMICRON-Gruppe entwickeln wir innovative Technologien für alle Bereiche elektrischer Energiesysteme. Im Fokus stehen elektrische Prüfungen an Mittel- und Hochspannungsbetriebsmitteln, Schutzprüfungen, Prüfungen digitaler Schaltanlagen und Cyber Security. Kund:innen in aller Welt vertrauen auf unsere einfach zu bedienenden Lösungen und schätzen deren Genauigkeit, Schnelligkeit und Qualität.

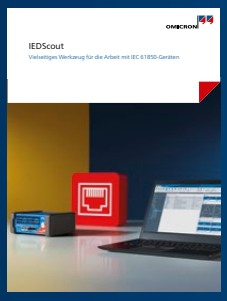
Wir sind seit 1984 in der elektrischen Energietechnik tätig und verfügen über fundierte, langjährige Erfahrung in der Branche. Rund 1.100 Mitarbeiter:innen an 24 Standorten unterstützen unsere Kund:innen in mehr als 170 Ländern und unser technischer Support kümmert sich 24 Stunden am Tag, 7 Tage die Woche um sie.

Detaillierte Informationen zu den in dieser Broschüre beschriebenen Lösungen sind in den folgenden Veröffentlichungen enthalten:

IEC-61850-Broschüre



StationScout-Broschüre



IEDScout-Broschüre

Weitere Informationen und Literatur sowie detaillierte Kontaktinformationen finden Sie auf unsereren Websiten.

www.omicronenergy.com
www.omicroncybersecurity.com

© OMICRON, 06 2024
Änderungen vorbehalten.