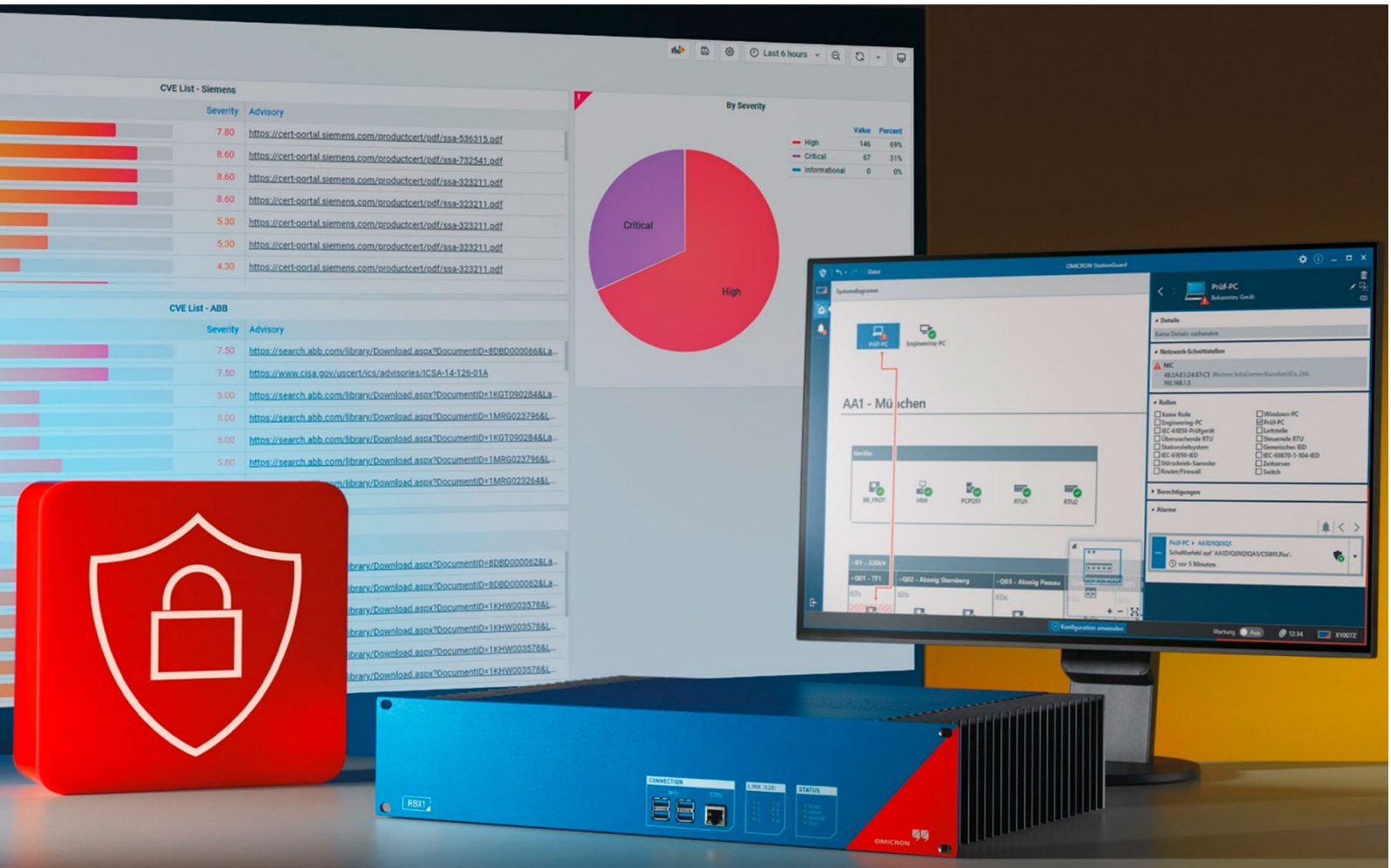
OMICRON

StationGuard Sensor

Was ist neu in Version 3.00



Version 3.00

Highlights

- > Neue Geräte mittels CSV-Import erstellen
- > Gesamte Netzwerkkommunikation visualisieren
- > DRTL (Device Role Template Library)
- > PCAP wiedergeben
- > Wartungsmodus über Binäreingänge starten und stoppen

1 Neue Geräte mittels CSV-Import erstellen

Sie können StationGuard bereits bekannte Geräte hinzufügen, indem Sie eine Asset-Inventar-CSV-Datei importieren. Die CSV-Datei kann Details wie Gerätename, Beschreibung, Typenschilddaten, MAC-Adresse und IP-Adresse enthalten. Darüber hinaus können in der Datei auch Geräterollen zugewiesen werden.

Diese Funktion erlaubt es, StationGuard vollständig und mit allen Netzwerkgeräten vorab im Büro zu konfigurieren, was die Bereitstellung vor Ort erleichtert.

Für die Implementierung gelten die folgenden Details:

- > Beim Import von Assets können Netzwerk-Schnittstellen erstellt werden.
- > Beim Import von Assets können fehlende Geräte mit Netzwerk-Schnittstellen erstellt werden.
- > Im ZeroLine-Diagramm gibt es einen separaten Bereich für importierte Assets.

2 Gesamte Netzwerkkommunikation visualisieren

Mit der Funktion *Netzwerkdiagramm-Ansicht* wird ein neuer Visualisierungsbereich eingeführt, der die Netzwerkkommunikation und deren Teilnehmer abbildet und so das Systemdiagramm ergänzt. Dieser Bereich enthält detaillierte statistische Werte und Informationen zu den aktiven Services, Protokollen und Knotenaktivitäten. Das hilft, Knoten schnell zu identifizieren, Kommunikationsmuster zu analysieren und sich einen umfassenden Überblick über den Netzwerkkontext zu verschaffen.

Für die Implementierung gelten die folgenden Details:

- > Die Netzwerkkommunikation kann grafisch visualisiert werden.
- > Knoten können im Netzwerkdiagramm anhand der in der Systemdefinition definierten Geräte miteinander kombiniert werden.
- > Im Netzwerkdiagramm können Knoten ausgewählt werden, um so die Übersicht des entsprechenden Geräts im Systemmodell aufzurufen.
- > Für Knoten im Netzwerkdiagramm, die im Systemmodell unbekannt sind, können verfügbare Informationen aufgerufen werden.
- > Das Netzwerkdiagramm kann aktualisiert werden.
- > Die vom ausgewählten Gerät verwendeten Netzwerkprotokolle/Anwendungen können nachverfolgt werden.

3 Zusätzliche Sprachen für Bedienoberfläche und Dokumentation

Die Bedienoberfläche von StationGuard ist in Deutsch, Englisch und Französisch verfügbar.

4 Wartungsmodus über Binäreingänge starten und stoppen

Der Wartungsmodus kann normalerweise über die Bedienoberfläche aktiviert werden. Mit dieser Funktion können Drittanbietersysteme den Wartungsmodus auch über Binäreingangskontakte an der RBX1 aktivieren, ohne die Bedienoberfläche verwenden zu müssen. Auf diese Weise können OT-Ingenieur:innen, SCADA-Spezialist:innen, das Personal in der Leitstelle und andere Teams den Wartungsmodus aktivieren, bevor die Wartungsaktivitäten vor Ort beginnen.

5 PCAP wiedergeben

Der in PCAP-Dateien aufgezeichnete Netzwerkverkehr kann wiedergegeben werden, um das Systemverhalten analysieren und Ereignisse erkennen zu können. Um eine genaue Analyse durch die Erkennungs-Engine zu gewährleisten, wird der Netzwerkverkehr nicht in Impulspaketen, sondern in Echtzeit wiedergegeben. Jedes Paket wird verarbeitet und mit den festgelegten Kommunikationsausgangswerten und -regeln verglichen. Etwaige Abweichungen werden als Alarme geflaggt und zur besseren Rückverfolgbarkeit mit *PCAP* gekennzeichnet.

6 Sichtbarkeit gerouteter IP-Adressen

Geroutete IP-Adressen werden unter der entsprechenden Netzwerk-Schnittstelle der Router-Geräte angezeigt. Diese Funktion ermöglicht eine schnelle netzwerkweite Identifizierung gerouteter Geräte und der zugeordneten IP-Adressen. Geroutete IP-Adressen sind nur sichtbar, wenn der StationGuard-Sensor sowohl die ein- als auch die ausgehende Seite des gerouteten Verkehrs überwacht.

7 Alarme ausgewählter Geräte im ZeroLine-Diagramm analysieren

Im ZeroLine-Diagramm ist es möglich, einfach alle Alarme auszublenden, sodass Sie sich ausschließlich auf die Alarme des ausgewählten Geräts konzentrieren können. Das vereinfacht die Analyse und hebt bestimmte Knoten hervor.

8 DRTL (Device Role Template Library)

Unsere Bibliothek enthält jetzt vordefinierte Rollen für viele Stationsautomatisierungs- und SCADA-Geräte (SIPROTEC, REL, SPRECON, A8000 …), die jeweils über voreingestellte Berechtigungen verfügen.

9 Lizenzmechanismus für VBX

Die Lizenzdatei auf der StationGuard-VBX ist zeitlich begrenzt. Das bedeutet, dass der Sensor nur bis zum Ende des festgelegten Lizenzzeitraums funktioniert. Nach Ablauf der Lizenz erfolgt keine Erkennung mehr. Es gibt aber eine dreimonatige Übergangsfrist, innerhalb derer Sie die Lizenz noch aktualisieren können, falls ihr Auslaufen übersehen wurde.

Lizenzen können online oder offline über den Lizenzserver aktiviert werden.

10 Verbesserungen bei der Erkennungs-Engine

- Es ist möglich, klassische OPC-Protokolle zu klassifizieren.
- Sie können S7CommPlus-Protokolle klassifizieren.
- Der StationGuard-Sensor erkennt, wenn in verschlüsseltem Verkehr andere als die empfohlenen Cipher Suites verwendet werden.
- Die Kernerkennungsfunktion ist unter verschiedenen Lastbedingungen sichergestellt.

11 Fehlerbehebungen und sonstige Verbesserungen

> Für importierte Rollen sind zusätzliche Symbole verfügbar.
> Dateien zur Festlegung von Rollen und Berechtigungen, die in der StationGuard-Version 3.00 oder später erstellt wurden, sind nicht mit der StationGuard-Version 2.40 und früher kompatibel. Grund für diese Inkompatibilität sind Änderungen an der Erkennungs-Engine. So wurden z. B. bestimmte Protokolle entfernt und „IEC 61850 MMS“ wurde in „MMS“ umbenannt.
> Es wurden mehrere Fehler und Probleme behoben.

12 Produktlebenszyklus- und Supporthinweis

Das Update von StationGuard 2.40 auf Version 3.00 ist kostenlos. Bitte beachten Sie, dass StationGuard-Version 3.00 die Version 2.40 als Service-Basisversion ablöst. Wir empfehlen dringend, alle Ihre Geräte auf Version 3.00 zu aktualisieren.

Wir bei OMICRON nehmen jede Art von Schwachstellen in unseren Produkten sehr ernst und freuen uns über jede Meldung, die uns hilft, die Produktsicherheit zu verbessern. Aus diesem Grund haben wir einen systematischen Ansatz für den Erhalt, die Behandlung und die Bekanntgabe solcher Schwachstellen-informationen entwickelt.

Bitte besuchen Sie https://www.omicronenergy.com/de/support/product-security für weitere Informationen.

Vorherige Versionen

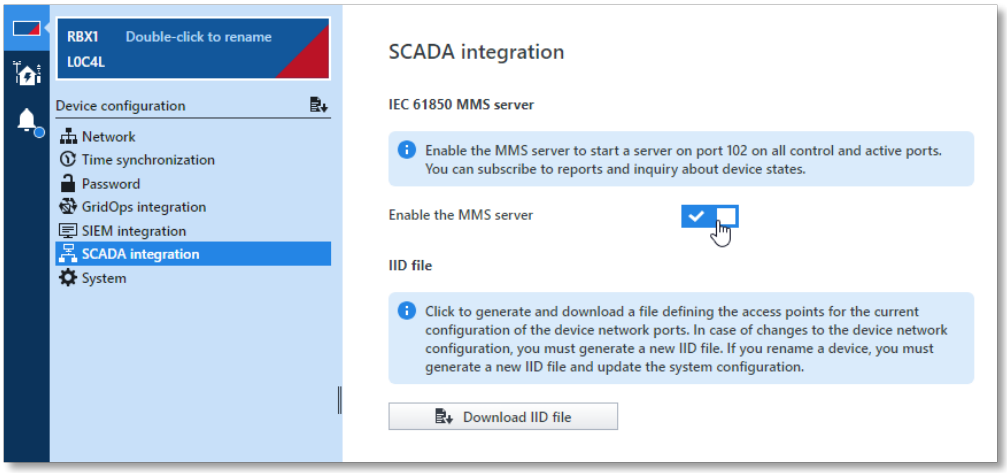
	Fokus	Veröffentlicht in
Version 2.40	Senkung des Konfigurationsaufwands	Mai 2024
Version 2.31	Aktualisierung des Installationsprogramms	Dezember 2023
Version 2.30	Rollen, Berechtigungen und Kategorisierung	Oktober 2023
Version 2.21	Kritische Sicherheitsversion	März 2023
Version 2.20	Unterstützung von GridOps	Januar 2023
Version 2.10	Verbesserungen der Bedienfreundlichkeit	Juni 2022
Version 2.00	DPI (Deep Packet Inspection)	Mai 2021
Version 1.10	Verbesserungen des Asset-Inventars	November 2020

Version 2.40

1 Vereinfachte Nutzbarkeit durch integrierten MMS-Server

StationGuard verfügt nun über einen MMS-Server, der Zugriff auf das StationGuard-Datenmodell mit aktuellen Alarmzuständen und dem Status des Wartungsmodus bietet. Sie können das Datenmodell als .iid-Datei herunterladen und an MMS-Clients für die SCADA-Integration melden. Sie werden über Sensormeldungen und Änderungen des Wartungsmodus in StationGuard benachrichtigt.

Zusätzlich sind im Datenmodell von StationGuard Informationen zu Hersteller, Modell sowie Hardware- und Softwareversionen der Typenschilder verfügbar, so dass aktive Tools zur Inventarisierung von Assets diese Daten abfragen und nutzen können.



2 Verbesserte Router-Unterstützung: Zwischen Geräten unterscheiden

StationGuard ordnet Geräte, die hinter einem Router kommunizieren, nun deren jeweiligen MAC-Adressen zu. Früher wurden mehrere IP-Adressen unter der gleichen MAC-Adresse gruppiert, was zu Verwechslungen führen konnte.

Das neueste Update ermöglicht es StationGuard nun, zwischen einzelnen Geräten zu unterscheiden, die hinter einem Router kommunizieren. Mit dieser Neuerung können Sie separate Geräteeinträge für jede IP-Adresse hinter dem Router erstellen. Sie können dann diesen einzelnen IP-Adressen spezifische Rollen und Berechtigungen zuweisen, was die Transparenz des Netzwerks und das Sicherheitsmanagement verbessert.

3 Zusammenführen und Aufteilen von Geräteschnittstellen

Oft haben Geräte mehrere Schnittstellen mit unterschiedlichen Zwecken. StationGuard kann diese Schnittstellen zusammenführen und unter einem Asset visualisieren. Mit der Funktion *Split* können Sie die Netzwerkschnittstellen und IP-Adressen aufteilen und individuelle Berechtigungen und Rollen hinzufügen. Dies ist besonders für Multifunktionsgeräte wie HMIs und RTUs nützlich.

4 Unterdrückung von Warnungen bei MMS- und IEC-104-Ereignissen

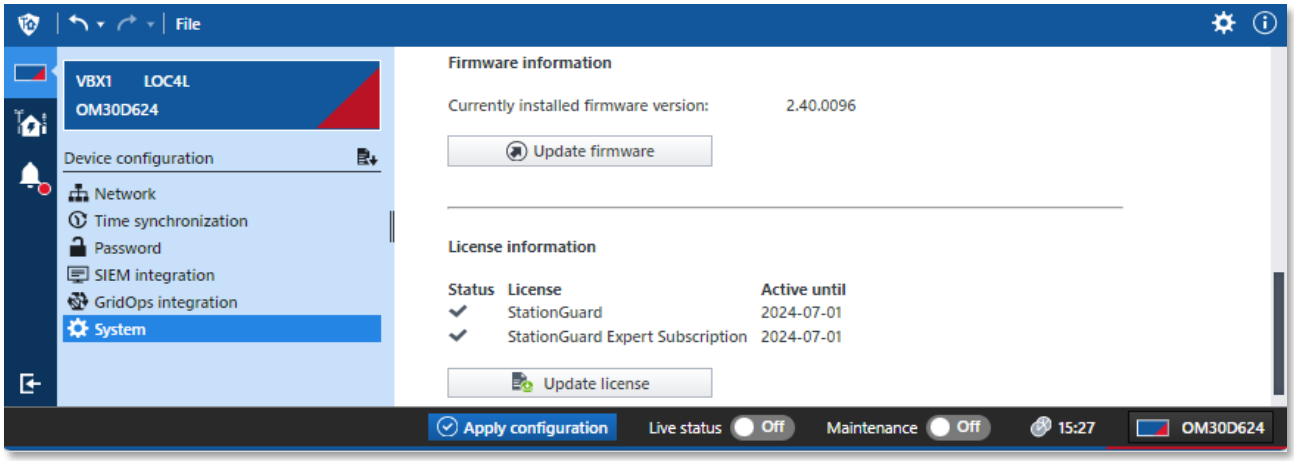
Fehlgeschlagene Steuerbefehle können manchmal zu zahlreichen Warnungen führen, die jetzt wie bei den *Info*-Ereignissen unterdrückt werden können.

5 Spezifische Zertifikate für das StationGuard-Webinterface

Für einen sicheren Zugriff auf das StationGuard-Webinterface können Sie spezifische Zertifikate verwenden.

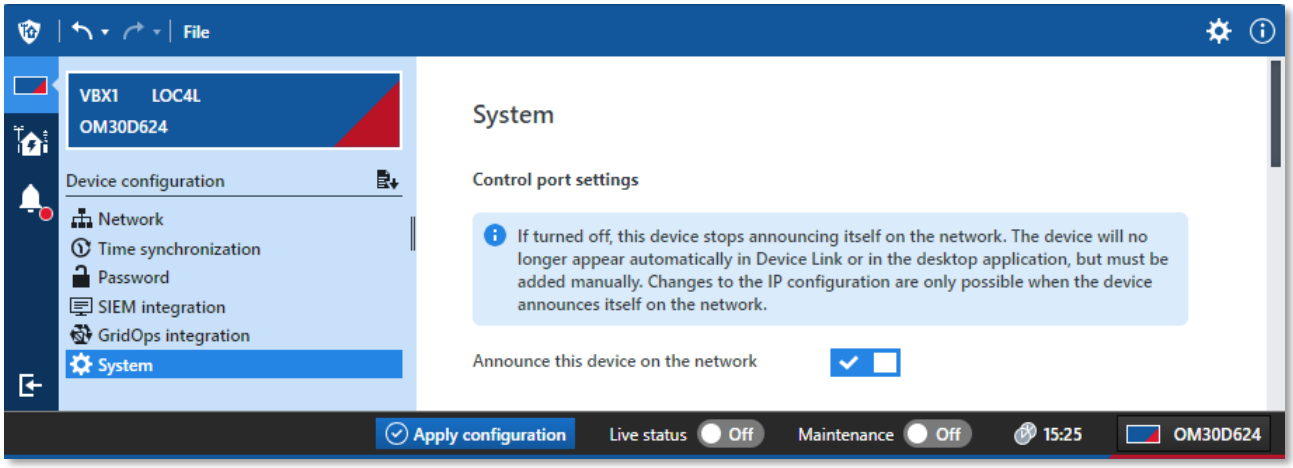
6 Aktualisierung der Firmware und der Lizenz von RBXRBX/MBX/VBX über das Webinterface

Aktualisieren Sie jetzt die Firmware und die Lizenz Ihrer RBX, MBX oder VBX direkt über den StationGuard-Webbrowser. Früher waren diese Updates nur über die StationGuard-Client-Software möglich.



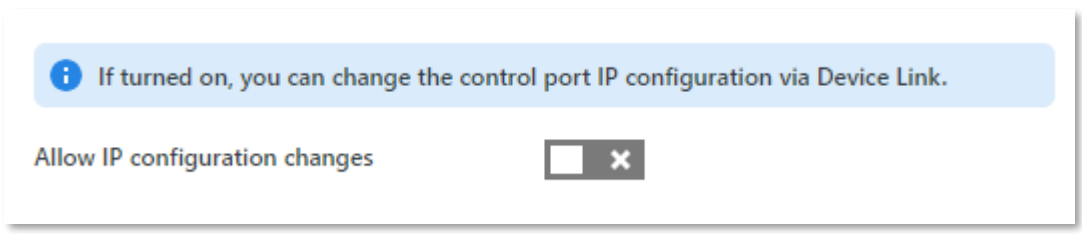
7 Gerätemeldungen deaktivieren

StationGuard signalisiert sich über den Geräteverbindungsport und die StationGuard-Client-Software. Wenn Sie diesen Datenverkehr im Netzwerk nicht wünschen, können Sie diese Meldungen deaktivieren.



8 IP-Änderungen am Kontrollport deaktivieren

Um unerwünschte IP-Adresszuweisungen zu verhindern, können Sie die Änderung der IP-Adresse durch den Sensor deaktivieren.



9 Aktiven Port mit mehreren Subnetzen verbinden

Es ist jetzt möglich, über einen aktiven StationGuard-Port Verbindungen zu verschiedenen Subnetzen herzustellen. Sie können mehrere IP-Adressen zu einem aktiven Port hinzufügen und mit verschiedenen Subnetzen und Netzwerken kommunizieren.

10 Fehlerbehebungen

> Das Problem der Priorisierung zwischen mehreren NTP-Servern für StationGuard wurde behoben.

Version 2.31

1 Update für StationGuard-Installationspaket

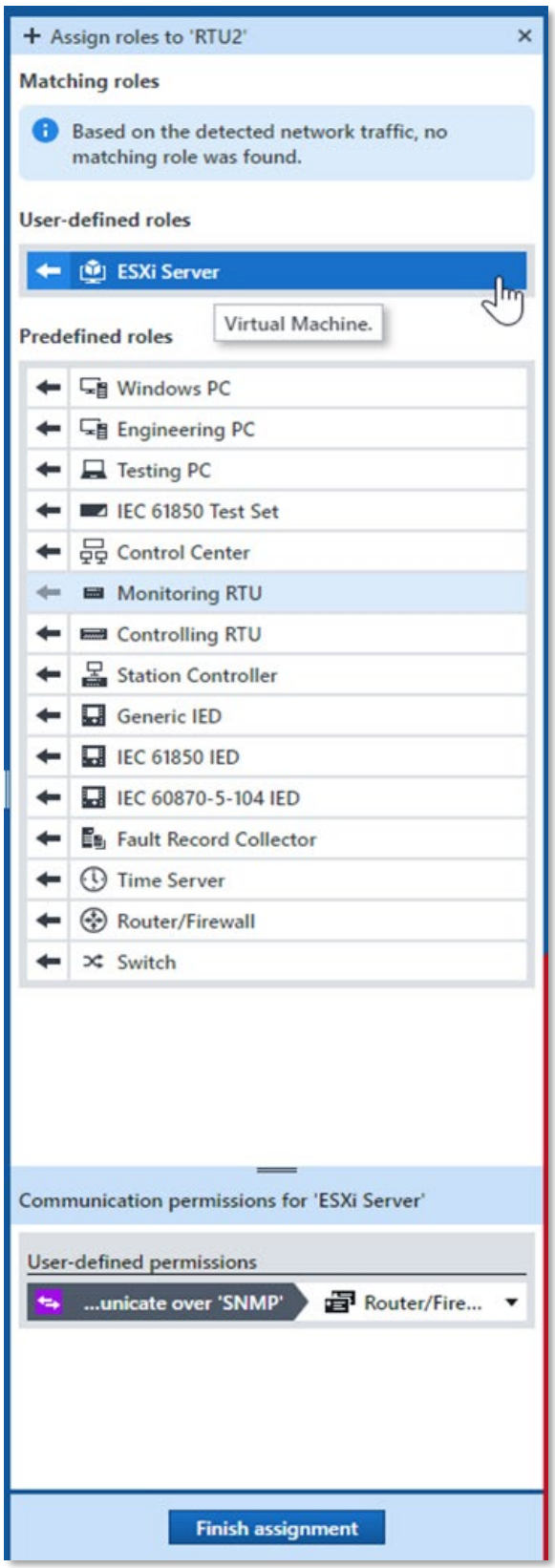
Das StationGuard-Installationspaket enthält die neueste Geräteverbindungsversion 3.00 SR1, um ältere Windows 10-Versionen wie 1809 und höher zu unterstützen.

2 Fehlerbehebungen

Zahlreiche kleine Fehler wurden korrigiert.

Version 2.30

1 Individuelle Rollen & Berechtigungen

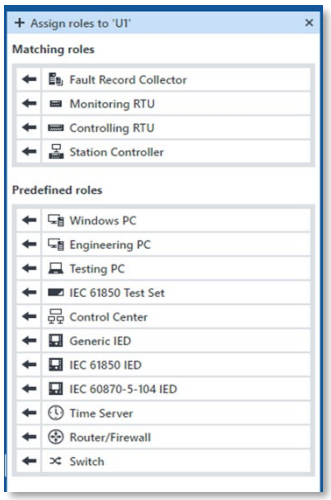


Warten Sie nicht länger auf Warnmeldungen – ergreifen Sie die Initiative und legen Sie proaktiv individuelle Rollen und Berechtigungen fest!

Jetzt können Sie maßgeschneiderte Rollen und Berechtigungen erstellen, die auf Ihre Geräte und Ihr Netzwerk abgestimmt sind. Diese erweiterte Funktion gibt Ihnen die Freiheit, die Sicherheit entsprechend Ihren spezifischen Anforderungen zu optimieren, selbst wenn noch kein Datenverkehr während der Lernphase stattgefunden hat.

Außerdem müssen Sie nicht an jedem Standort alle Rollen und Berechtigungen neu erstellen. Importieren und exportieren Sie einfach Ihre individuellen Rollen und Berechtigungen nahtlos über mehrere Sensoren und Standorte hinweg, mit unserem klar definierten JSON-Format.

2 Rollenzuweisung & automatische Gerätekategorisierung



Erleben Sie eine reibungslosere Nutzung ohne den Aufwand manueller Kategorisierung und unklarer Rollenzuweisung. Diese effiziente Lösung hilft Ihnen, schnell zwischen verschiedenen Gerätetypen in Ihrem Netzwerk zu unterscheiden und spart Ihnen wertvolle Zeit.

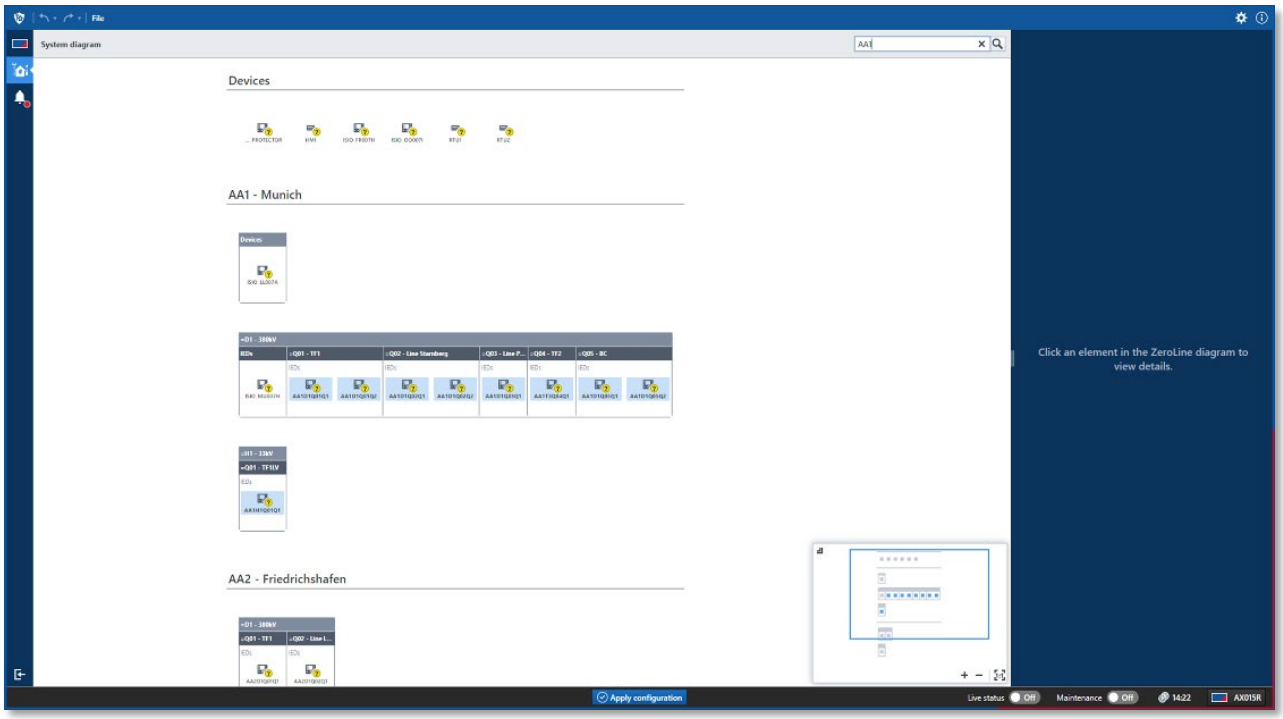
Darüber hinaus macht das intelligente Kommunikations-Matching von StationGuard die Rollenzuweisung mühelos. Das System erkennt automatisch die am besten geeigneten Rollen und schlägt sie ganz oben in der Liste vor (z.B. ACME-Protec-400-Relais, Protection Testing Laptop B), so dass Sie sie einfach zuweisen können.

Profitieren Sie von einer verbesserten Visualisierung, indem Sie grafische Gruppen für Geräte wie PCs, IEDs oder Netzwerkgeräte erstellen, und nutzen Sie diese individuelle Lösung, um Ihre Prozesse zu rationalisieren und Ihren Workflow zu verbessern.

3 Geräte in ZeroLine finden

Sind Sie es leid, mit dem Suchen, Lesen und Klicken durch unzählige IEDs Zeit zu verschwenden? Verwenden Sie die praktische Suchleiste, um Geräte anhand verschiedener Parameter wie Name, Typ, Beschreibung, Hersteller, Firmware-Version, Hardware-Version, MAC-Adresse und IP-Adresse zu finden und zu markieren. Alle Geräte, die den Suchkriterien entsprechen, werden im ZeroLine-Diagramm mit einer hellblauen Hintergrundfarbe hervorgehoben.

Die Suchfunktion kann auch dazu verwendet werden, übereinstimmende Geräte zu gruppieren, um bei der Überwachung und Analyse besser zwischen Bereichen, Zonen und Sicherheitsstufen unterscheiden zu können und so einen klaren und umfassenden Überblick zu erhalten.



4 Gerätespezifische Zertifikate für verschlüsselte Kommunikation

Sie können jetzt noch sicherer kommunizieren. Ab Version 2.30 generieren unsere MBX1- und RBX1-Plattformen nun individuelle Zertifikate für die gesamte verschlüsselte Kommunikation, was die Sicherheit weiter erhöht. Bisher wurde ein gemeinsames Zertifikat für alle Geräte verwendet, mit diesem Update wird nun für jedes Gerät ein eigenes Zertifikat generiert.

Bitte beachten Sie, dass Sie das Gerät einmalig identifizieren und bestätigen müssen, bevor Sie sich mit ihm verbinden, da die Zertifikate nicht automatisch validiert werden können.

5 VBX1: Betrieb von StationGuard, StationScout und IEDScout auf vorhandener Hardware

Nach dem erfolgreichen Abschluss einer umfangreichen Beta-Phase wurde die VBX1 in einer Vielzahl von Umgebungen ausgiebig getestet, um eine robuste Stabilität und Zuverlässigkeit zu gewährleisten.

Neben unseren bewährten Hardware-Angeboten, den Plattformen RBX1 und MBX1, sind nun auch unsere innovativen Software-Lösungen für die VBX1-Plattform optimiert. Diese sofort einsatzbereite virtuelle Maschine läuft problemlos auf VMware-Systemen und bietet kompromisslose Software-Performance direkt in Ihrer bestehenden Virtualisierungsinfrastruktur.

Um die optimale Konfiguration für Ihr Netzwerk zu gewährleisten, laden wir Sie ein, sich mit unseren Expert:innen in Verbindung zu setzen, die Ihnen bei der Auswahl der am besten geeigneten Lösung behilflich sein können.

6 Sicherheitsupdates

Weitere Informationen zu diesen Verbesserungen finden Sie in unserem Sicherheitshinweis OSA-7.

7 Fehlerbehebungen und andere Verbesserungen

- Rückmeldungen für erlaubte Kommunikation können nun für jede Berechtigung einzeln abgeschaltet werden.
- Ein Fehler wurde behoben, bei dem StationGuard die NTP-Zeit nicht als synchronisiert anzeigte, obwohl die Genauigkeit ausreichend war.
- Die Verwendung von IEC 60870-5-104 ASDU-Typen im Bereich 128-255 löst nun keinen Encoding-Alarm mehr aus. Es wird nun ein separater Alarm ausgelöst, der durch Setzen einer Berechtigung deaktiviert werden kann.

Version 2.21

1 Sicherheitsrelevantes Release

Diese Version enthält wichtige Sicherheitskorrekturen. Wir empfehlen dringend, dass Sie alle Ihre Standorte sofort aktualisieren. Weitere Einzelheiten finden Sie in den Security Advisories OSA-5 und OSA-6 unter https://www.omicronenergy.com/de/support/product-security/.

Version 2.20

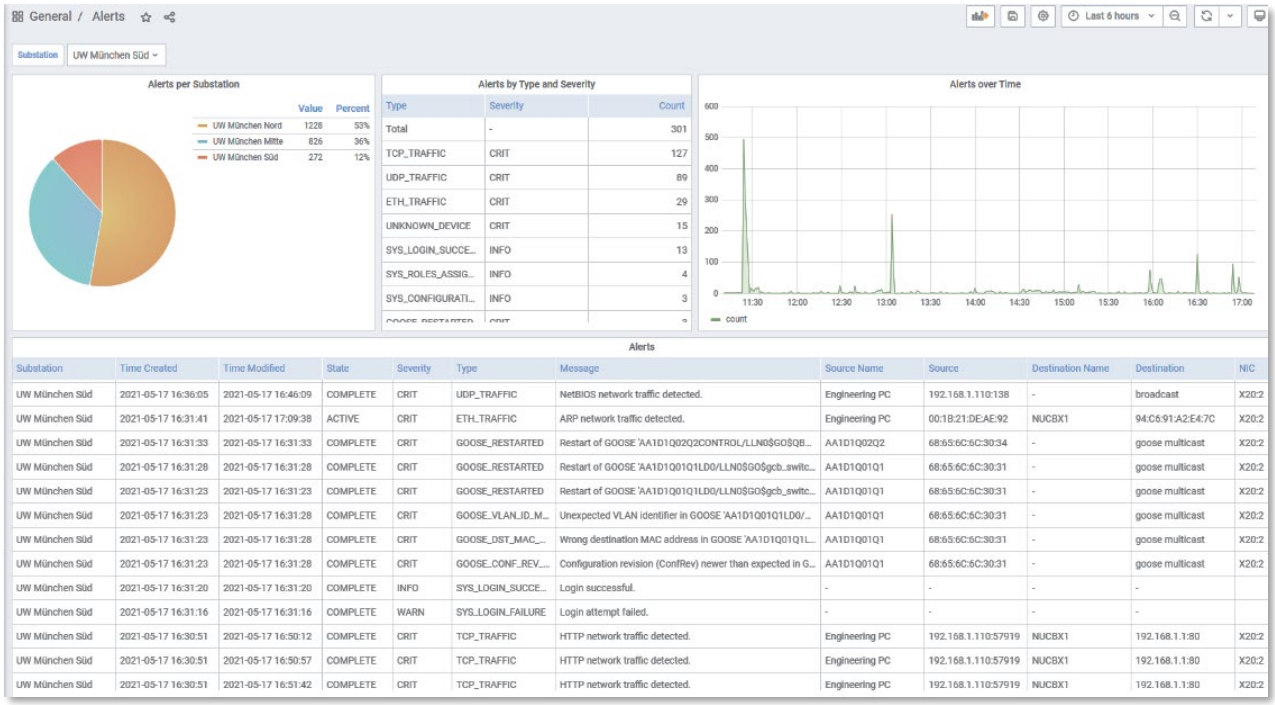
1 Einleitung

StationGuard 2.20 enthält neben diversen Verbesserungen neue Funktionalitäten auf Sensorebene und unterstützt das neue zentrale Managementsystem GridOps. Die Integration des neuen zentralen Managementsystems GridOps in StationGuard ist optional. Es besteht also weiterhin die Möglichkeit, die StationGuard-Sensoren ohne GridOps zu betreiben.
GridOps bietet mehrere Dashboards mit unterschiedlichen Ansichten zur Visualisierung des Sicherheitszustands der Operational Technology (OT)-Netzwerke im Stromnetz.

2 Neue Funktionen

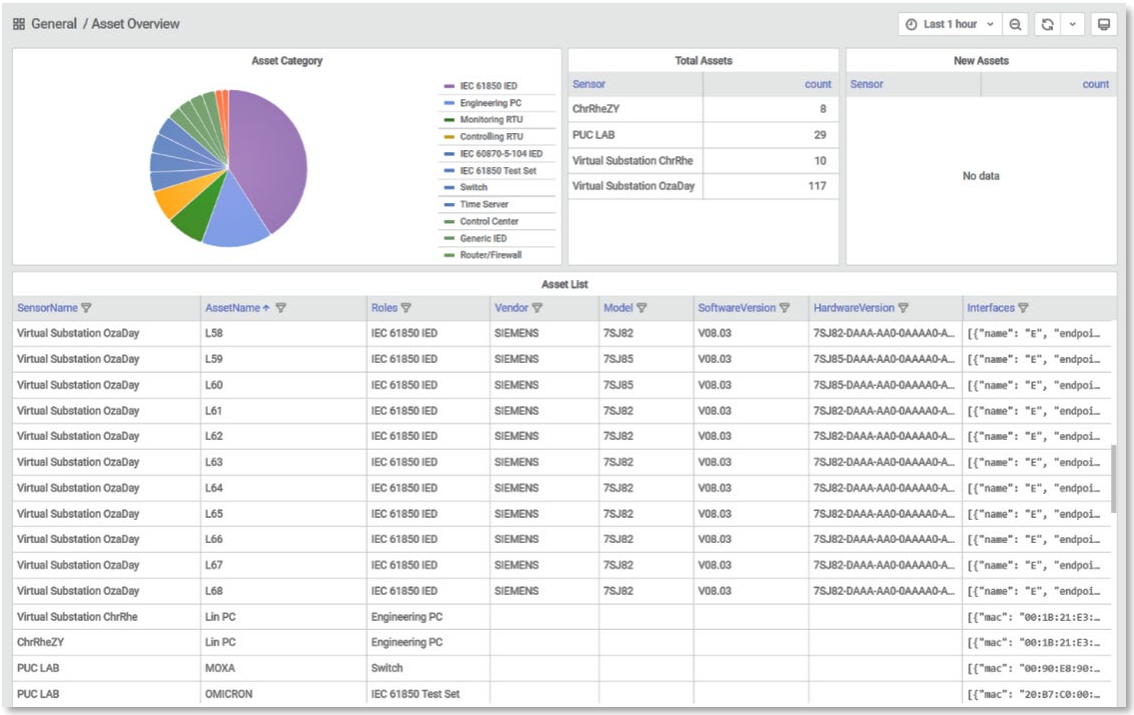
2.1 Synchronisation von Assets und Ereignissen mit GridOps

StationGuard 2.20 synchronisiert alle Ereignisse mit einer zentralen GridOps-Instanz. Wird die Verbindung zwischen GridOps und einem StationGuard-Sensor unterbrochen, führt GridOps eine Neusynchronisation durch, sobald der Sensor wieder erreichbar ist. GridOps dient somit sowohl als Sicherung für die von den StationGuard-Sensoren erzeugten Alarme als auch als Datenbank für deren Historie.
GridOps bietet unterschiedliche Dashboards für die Darstellung und Analyse von aktuellen und früheren Alarmen. Diese Dashboards liefern in Echtzeit Informationen zum Alarmstatus aller Standorte. Bei Vorliegen von kritischen Alarmen erhalten Sie eine sofortige Benachrichtigung.
Die GridOps-Plattform wurde außerdem so konzipiert, dass alle Alarmaktivitäten sämtlicher StationGuard-Sensoren in der Datenbank nachverfolgbar sind. Sie haben somit die Möglichkeit, alle über die Zeit an den Sensorpositionen aufgetretenen bisherigen Ereignisse schnell und bequem zu durchsuchen.
Zusätzlich zu den Alarmstatistiken können Sie anhand von Tortendiagrammen und Zeitreihendiagrammen genau sehen, wie die unterschiedlichen Alarmtypen über die Standorte verteilt aufgetreten sind. Die Information, für welche spezifische Art von Betriebsmitteln sie aufgetreten sind und wie sich die Alarmhäufigkeit über die Zeit entwickelt hat, erlaubt eine Analyse der jeweiligen Zusammenhänge. Anhand dieser Statistiken lassen sich für spezifische Ereignisse Trendanalysen vornehmen und über die Zeit auftretende typische Muster und verdächtige Aktivitäten erkennen. Außerdem können für sämtliche von StationGuard protokollierten betrieblichen Ereignisse (auch funktionale Ereignisse genannt) diverse weitere Analysen vorgenommen werden, also beispielsweise für erfolgreiche und nicht erfolgreiche Schaltereignisse, Aufzeichnungen von Betriebsunterbrechungen usw.



2.2 Globales Asset-Inventar

StationGuard synchronisiert alle Betriebsmittel mit der zentralen Instanz von GridOps. GridOps erstellt dann ein globales Asset-Inventar, das durchsucht und nach der Betriebsmittelart sortiert werden kann. Das Asset-Inventar enthält alle von sämtlichen StationGuard-Sensoren im Netz erkannten Geräte. GridOps zeichnet dabei auch die Historie der über die Zeit anfallenden Stände des Asset-Inventars auf. Die Anwendung aktualisiert das Asset-Inventar anhand der von den mit dem System verbundenen Sensoren erhaltenen Betriebsmittelinformationen und zeigt die Eigenschaften der Betriebsmittel in Echtzeit in Tabellenform an, sodass diese einfach eingesehen werden können. Mithilfe der Filterfunktionen kann das Inventar für das Schwachstellenmanagement nach bestimmten Betriebsmittelarten durchsucht werden.
In Verbindung mit den beispiellosen Möglichkeiten von StationGuard, genaueste Detailinformationen über jedes Betriebsmittel abzurufen, stellt die Kombination aus StationGuard und GridOps eine leistungsstarke Lösung für die Verwaltung des Asset-Inventares dar. So können beispielsweise SCL-Dateien oder Arbeitsblätter mit den Betriebsmitteldaten aus der Asset-Dokumentation importiert werden. Die Verfügbarkeit von umfassenden Daten zu einzelnen Betriebsmitteln ist für ein erfolgreiches Schwachstellen- und Risikomanagement zweifellos unerlässlich, da eine detaillierte Kenntnis der einzelnen Betriebsmittel eine exaktere Schwachstellenanalyse ermöglicht und somit die Priorisierung der Betriebsmittel umso erfolgreicher vorgenommen werden kann.
Diese Funktionalität steht neben dem automatischen Asset-Inventar auch für Sensoren zur Verfügung, die nur temporär aktiv sind, also StationGuard-Sensoren auf Basis der mobilen MBX1-Plattform.

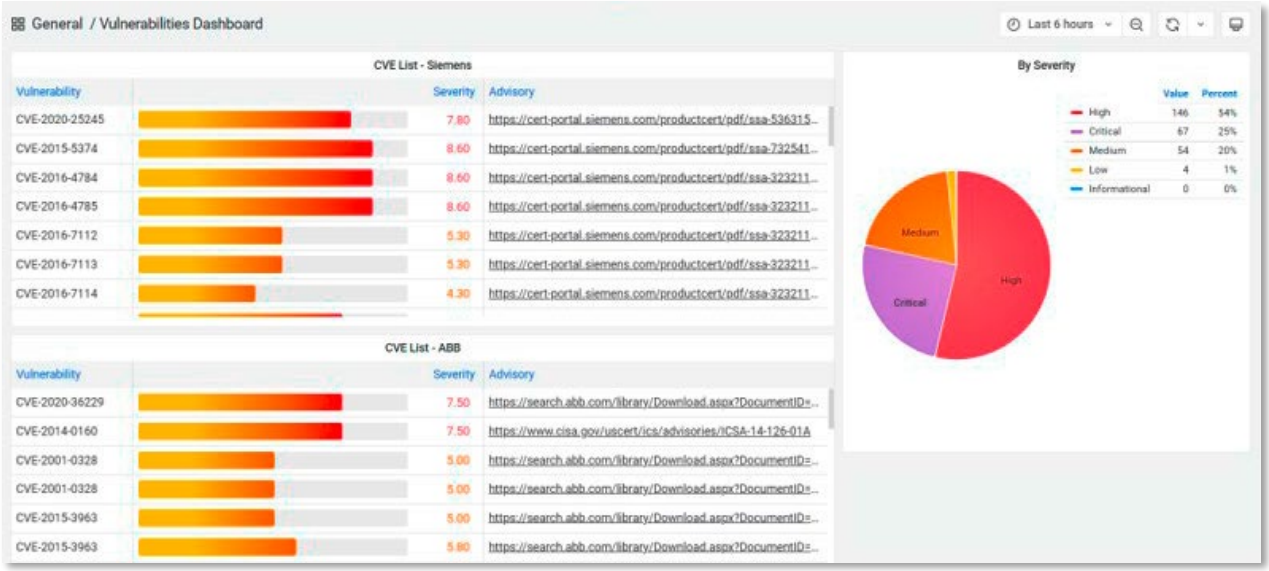


2.3 Schwachstellenmanagement

Die Einschätzung, ob für Schutz- und Leittechnikgeräte entdeckte Schwachstellen für die vor Ort installierten realen Geräte relevant sind, kann extrem schwierig sein. Für die richtigen Schlussfolgerungen muss nicht nur das Problem aus unterschiedlichen Blickwinkeln betrachtet werden, sondern es müssen außerdem noch mehrere weitere Variablen berücksichtigt werden. Um die zutreffenden Sicherheitslücken zu bestimmen, müssen der genaue Gerätetyp, die Firmware-Version und die Modulkonfiguration bekannt sein. Ein äußerst wichtiger Punkt ist, dass die Durchführung einer Risikobewertung Sie in die Lage versetzt, zu entscheiden, ob Ihre Geräte eine Schwachstelle für eine zukünftige Kompromittierung aufweisen oder nicht.
Zusätzlich muss daran gedacht werden, dass die Security Advisories manchmal nicht so genau sind, wie sie sein sollten, was die Situation komplexer macht.

Das Schwachstellenmanagement von GridOps wurde so konzipiert, dass die Auswirkungen unterschiedlicher Common Vulnerability Exposures (CVEs) analysiert werden und auf Grundlage des jeweiligen CVE oder Security Advisory identifiziert wird, welche IEDs gefährdet sind. Das Dashboard für Schwachstellen von

Betriebsmitteln gibt einen Einblick in die Situation bezüglich CVEs und deren Gefährlichkeit sowie die Optionen für das Patchen der Schwachstelle.

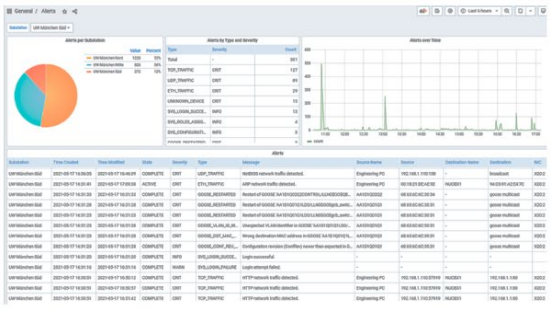


2.4 Protokollerstellung

Neben der Erstellung von Protokollen geht GridOps auch auf das Asset-Inventar und dessen Schwachstellen ein, sodass Sie bereits frühzeitig einen Einblick in die Trends und Statistiken bezüglich der Cyber Security erhalten. Durch die Analyse dieser Protokolle können Sie jederzeit die aktuelle Sicherheitslage Ihrer Organisation ermitteln. Außerdem ist die Erstellung von umfassenden Informationen und Protokollen auch für Management, Lieferanten und Regulatoren von höchstem Interesse, um Risiken rechtzeitig ermitteln und entschärfen zu können.

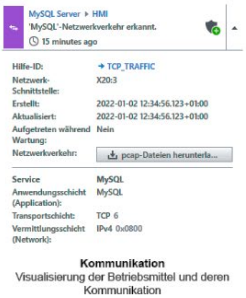
2.5 Ereignisanalyse von der Netzebene bis zur Stationsebene

Ein Schlüsselmerkmal von StationGuard ist seine einzigartige Darstellung der der Asset-Netzwerke. StationGuard stellt das gesamte Netzwerk mit allen zugehörigen Geräten grafisch dar, und zwar in einer Form, die sowohl OT-Expert:innen als auch IT-Verantwortlichen vertraut ist. Um angemessen auf aufkommende Bedrohungen reagieren zu können, bietet GridOps ein Konzept für umfassende Analysen und Untersuchungen. Es ist nun möglich, alle Alarme in der vertrauten ZeroLine-Diagrammansicht von StationGuard anzuzeigen und in die Ansicht von einer bestimmten Leitstelle, einem Kraftwerk, oder einer Anlage zu wechseln.. Das ZeroLine-Diagramm basiert meist auf der Asset-Dokumentation und wird manuell angepasst, damit die Darstellung so genau wie möglich der offiziellen Dokumentation des Betreibers entspricht.



Netzebene
Unterschiedliche Dashboards geben einen Überblick über die Status Ihrer Netzwerke

Kraftwerksebene
Intuitive Visualisierung des Netzwerks



Kommunikation
Visualisierung der Betriebsmittel und deren Kommunikation

2.6 Active-Directory-Integration und rollenbasierte Zugriffskontrolle

Unter Verwendung von LDAP kann GridOps in Active-Directory-Umgebungen integriert werden. Für die Zugriffskontrolle auf die verschiedenen Funktionsumfänge zur Anzeige und Konfiguration Ihrer StationGuard-Instanzen sind unterschiedliche Benutzer:innenrollen vorhanden. Diese legen fest, welche Funktionsumfänge für welche Benutzer:innen zur Verfügung stehen. Zusätzlich kann bei einem Ausfall eines Netzwerkes über die lokale Bedienoberfläche des StationGuard-Client auch einzeln auf die StationGuard-IDS-Sensoren zugegriffen werden. Auf diese Weise ist bei Bedarf der Zugriff auf die Sensoren als Backup-Möglichkeit weiterhin möglich.

2.7 Aktive Betriebsmittelerkennung durch Auslesen der Typenschilddaten

StationGuard 2.20 ist in der Lage, die Geräte und deren Eigenschaften durch Live-Auslesen der Typenschildinformationen aktiv zu identifizieren. Dieses Leistungsmerkmal ist optional und muss zuerst aktiviert werden.

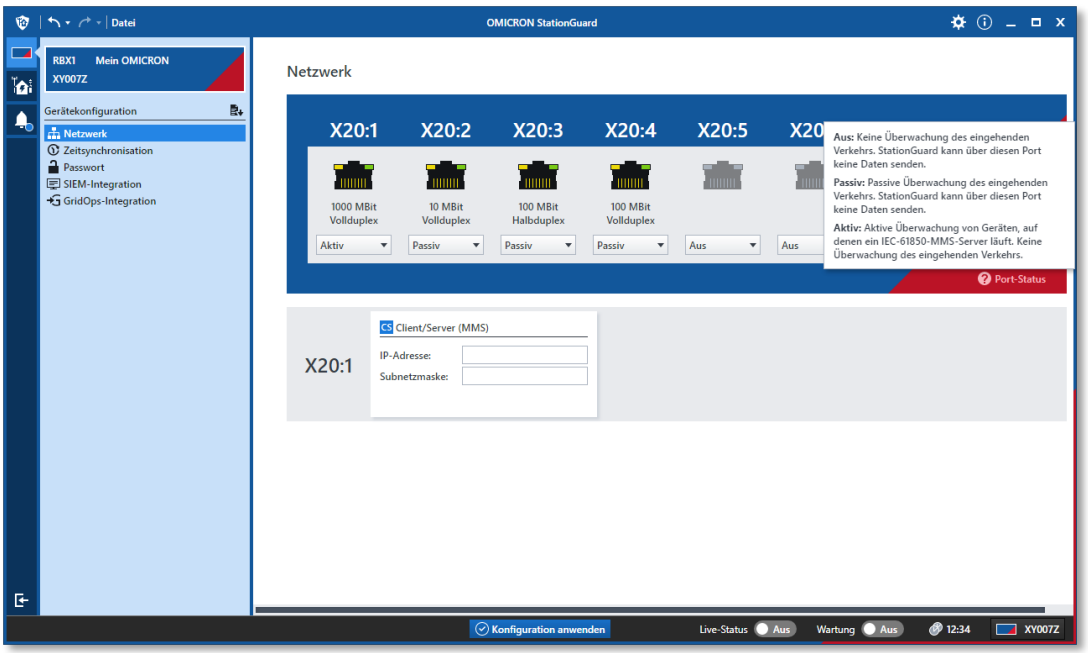
Die Grundlage einer wirksamen Reaktion auf Cyber-Bedrohungen sollte immer eine lückenlose und vollständige Kenntnis der Umgebung sein. Der Schlüssel zu einem erfolgreichen OT-Cyber-Security-Programm ist eine in Echtzeit arbeitende automatisierte Software, die in der Lage ist, alle Betriebsmittel in Echtzeit zu identifizieren und nachzuverfolgen.

Mit der aktiven Betriebsmittelerkennung erhalten Sie ein zuverlässiges Instrument, um bestimmte Konfigurationsparameter, die aktuelle Firmware-Version und sonstige Geräteinformationen abzufragen. Durch die aktive Betriebsmittelerkennung erhalten Sie ein weitaus breiteres Bild der aktuellen OT-Umgebung und weitaus mehr Informationen, als eine passive Netzwerküberwachung alleine liefern kann.

Für das Live-Auslesen der Typenschilddaten wird derzeit das IEC-61850-MMS-Protokoll verwendet. MMS ist anders als SNMP und Web Interfaces bei Stationsautomatisierungssystemen sehr weit verbreitet und das IEC-61850-MMS-Protokoll ist zweifellos die zuverlässigste Art, um Typenschilddaten in Asset zu erfassen. Zukünftige Releases werden noch weitere Protokolle für die aktive Erkennung von Betriebsmitteln im Netzwerk unterstützen.

2.7.1 Arbeitsweise der aktiven Betriebsmittelerkennung

Die aktive Betriebsmittelerkennung funktioniert nur, wenn der Status einer Netzwerk-Schnittstelle von **Passiv** auf **Aktiv** geändert und dem Port eine IP-Adresse zugewiesen wird. Somit wird dieser Port nicht mehr für die Überwachung verwendet. Das Angriffserkennungssysystem wertet nur Datenverkehr von den Ports mit dem Status **Passiv** aus.



2.7.2 Sicherheit

Dass die aktive Erkennung von IEC-61850-MMS sicher und wirkungsvoll ist, haben wir in hunderten Asset weltweit bereits demonstriert. Dies kann darauf zurückgeführt werden, dass sowohl in StationScout als auch in IEDScout über mehr als ein Jahrzehnt hinweg dieselbe Technologie verwendet wurde, und sogar akkreditierte Labore die Zertifizierung von IEDs gemäß IEC 61850 mit unserem IEC-61850-MMS-Stack durchführen.
Nach dem Herstellen der Verbindung zu einem Gerät werden die Typenschilddaten nur einmal gelesen. Eine weitere Abfrage findet nicht statt, sodass die aktive Betriebsmittelerkennung von StationGuard nahezu keinen zusätzlichen Verkehr im Netzwerk und den IEDs verursacht. Bei einem Neustart des IED wird die aktive Verbindung zwischen StationGuard und dem IED automatisch wiederhergestellt und die Typenschilddaten werden durch StationGuard erneut ausgelesen. Als Bestätigung, dass nach einem Firmware-Update die aktualisierten Betriebsmittelinformationen korrekt wiedergegeben werden, wird das Gerät auch nach einem Firmware-Update neu ausgelesen. Dies passiert automatisch, weil das Gerät aufgrund der durch das Firmware-Update erfolgten Konfigurationsänderung einen Neustart durchführt.

2.8 Verwendung der STATION-Ports für die Konfiguration von StationGuard

In früheren Versionen von StationGuard konnte als Management Interface und für NTP- bzw. Syslog-Verbindungen nur der CONTROL-Port (auf der Vorderseite der RBX1-Plattform) verwendet werden. Ab StationGuard 2.20 können für die Konfiguration von StationGuard und die Verbindung zu NTP- und Syslog-Servern zusätzlich die STATION-Ports verwendet werden. Voraussetzung hierfür ist allerdings, dass die STATION-Ports den Status **Aktiv** haben und ihnen eine IP-Adresse zugewiesen ist. Beachten Sie jedoch, dass durch ein Zurücksetzen der StationGuard-Konfiguration auch diese IP-Einstellung zurückgesetzt wird und StationGuard danach nur noch über den CONTROL-Port erreichbar ist.

2.9 Bedienung über ein Webinterface

StationGuard-Sensoren können nun auch via Browser konfiguriert werden, ohne dass die Anwendung selbst auf dem Computer installiert sein muss. Das Webinterface von StationGuard bietet dieselbe Funktionalität wie die installierte Desktop-Anwendung.

3 Fehlerbehebungen und sonstige Verbesserungen

> Die NTP-Zeitkonfiguration bietet nun umfangreichere Rückmeldungen bezüglich des Synchronisationsstatus und möglichen Synchronisationsproblemen.

Version 2.10

1 Neue Funktionen

1.1 Eigene Systemdiagramme

StationGuard bietet Ihnen neue Möglichkeiten für die Visualisierung Ihres Netzwerkes. Durch Hinzufügen und Umbenennen von Gruppen oder Verschieben von Gruppen und Geräten haben Sie nun die Möglichkeit, eigene Systemdiagramme zu erstellen. Zusätzlich zur Darstellung der Asset-Struktur können Sie nun auch die Leitstelle oder Kraftwerksverbünde entsprechend dem Purdue-Modell visualisieren. Die komplette visuelle Überarbeitung bietet außerdem eine bessere Übersicht und hilft Ihnen dabei, die gesuchten Elemente schneller und besser zu finden.

1.2 Paketerfassungen für Alarme

Für jeden durch StationGuard generierten Alarm kann der zugrunde liegende Netzwerkverkehr herunter geladen und untersucht werden. StationGuard erlaubt das Herunterladen von Paketen mit dem vor, während und nach der Detektion des Alarms aufgetretenen Netzwerkverkehr. Die Speicherung der erfassten Pakete erfolgt unabhängig von der zentralen Verbindung im StationGuard-Gerät.

1.3 Vorschläge für das Zusammenführen von Geräten

StationGuard erlaubt das Zusammenführen von mehreren Geräten und unterstützt Sie hierbei, indem Geräte mit demselben MAC-Hersteller und ähnlicher MAC-Adresse automatisch für das Zusammenführen vorgeschlagen werden. Hierdurch wird das Zusammenführen von Netzwerk-Switches und IEDs mit mehreren Ports erheblich erleichtert und beschleunigt. StationGuard bietet einen schnellen Überblick über die Berechtigungen und Alarme des für das Zusammenführen ausgewählten Gerätes.

1.4 Import des Asset-Inventars

StationGuard erlaubt das Importieren der Informationen zum Asset-Inventar aus CSV-Dateien, wenn diese dem definierten StationGuard-Format entsprechen. Diese Funktionalität unterstützt auch das Hinzufügen von zusätzlichen Details zu Betriebsmitteln aus externen Quellen, also beispielsweise von Informationen zur Hardware-Konfiguration oder zu Seriennummern oder Firmware-Versionen. Nützlich ist diese Funktion auch, um für mehrere Geräte die Namen entsprechend der Asset-Dokumentation, also beispielsweise gemäß der SCADA-Signalliste, korrekt einzustellen. StationGuard verwendet sowohl für den Import als auch für den Export dasselbe Format, sodass Geräteinformationen mit ihrem Asset-Inventar synchronisiert werden können.

Es können auch Details von Betriebsmitteln importiert werden, die durch das Begleit-Tool StationScout ermittelt wurden.

1.5 Deep Packet Inspection (DPI) unterstützt zusätzliche Protokolle

Wir verbessern kontinuierlich unsere Detection Engine. Neben anderen Verbesserungen der Detektion haben wir Unterstützung für drei weitere OT-Protokolle hinzugefügt: Profinet, EtherCAT und CIP (Common Industrial Protocol).

1.6 Unterstützung von Zeitzonen

In StationGuard werden standardmäßig alle Zeiten in der jeweiligen lokalen Uhrzeit angezeigt, um ein einfacheres Matching mit Ereignislisten und Logdateien zu ermöglichen. Falls Ihre anderen Systeme UTC verwenden, kann die Zeitanzeige auch auf UTC umgestellt werden.

1.7 Customer Experience Improvement Program

Als Hilfe bei der ständigen Verbesserung des Nutzerlebnisses von StationGuard haben wir die Möglichkeit integriert, eine anonyme Erfassung von Nutzungsdaten vorzunehmen. Diese Erfassung von Daten kann in

dem zu Beginn angezeigten Datenschutz-Dialog ausgeschaltet werden. Dort finden Sie auch nähere Einzelheiten zum Customer Experience Improvement Program (CEIP) und Informationen zu den von uns getroffenen Maßnahmen zum Schutz Ihrer Daten.

2 Fehlerbehebungen und sonstige Verbesserungen

- In den Alarmdetails wurde ein Hyperlink zum Aufrufen einer Hilfeseite mit einer Beschreibung des Alarms eingefügt.
- Neben Alarmen der Schweregrade "Warnung" und "Kritisch" werden nun auch Alarme des Schweregrades "Info" via Syslog weitergeleitet, um in zentralen Systemen, wie beispielsweise SIEM-Systemen, auch Systembenachrichtigungen sehen zu können.
- Es werden jetzt auch Pakete analysiert, bei denen die angegebene Länge eines LLC-Netzwerkpakets (Logical Link Control) größer ist als die tatsächliche Größe der Nutzdaten. Vielen Dank an Matthias Z. von TransnetBW für die Meldung dieses Problems.
- "GOOSE nicht gefunden"-Meldungen können dem sendenden Gerät leichter zugeordnet werden.
- Die Richtung des TCP-Verkehrs wird nun zuverlässiger erkannt.
- Die Zuweisung von statischen oder dynamischen Ports ist nun unabhängig von der erkannten Richtung des TCP-Verkehrs.

Version 2.00

1 Neue Funktionen

1.1 Deep Packet Inspection für mehr als 300 OT- und IT-Protokolle

Der beispiellose Detailgrad bei der Untersuchung von IEC-61850-Protokollen wurde noch erweitert und unterstützt nun auch eine Deep Packet Inspection (DPI) für über 300 weitere IT- und OT-Protokolle. Mittels DPI kann StationGuard nicht nur Kodierungsfehler detektieren, sondern beispielsweise auch sogenanntes Port-Spoofing, also das "Entführen" der Port-Nummern von Remote-Verbindungen durch Angreifer.

Die Allowlist von StationGuard beinhaltet nun nicht mehr nur die Port-Nummern, sondern auch die zugehörigen Anwendungen, die diese Ports verwenden. Die über eine Verbindung laufende Anwendung wird der Allowlist hinzugefügt, sobald Sie in StationGuard 2.0 eine Verbindung erlauben. Ändert sich die Anwendung einer Verbindung, wird ein Alarm generiert.

Derzeit kann StationGuard über 1400 verschiedene Anwendungen detektieren.

Unterstützte OT-Protokolle

IEC-61850-Protokolle
IEC 62439-3 PRP und HSR
IEC 60870-5-104, IEC 60870-5-101 und IEC 60870-5-103 über TCP/IP
DNP3
Modbus TCP und Modbus RTU über TCP
IEC 62056 (DLMS/COSEM)
IEEE C37.118 (Synchrophasor-Protokoll)
IEEE 1703-2012 / ANSI C12.22 (AMI-Protokoll)
IEC 60870-6 (ICCP/TASE.2 - UCA 2.0)
EtherNet/IP
S7-Kommunikation

Die wichtigsten unterstützten IT-Protokolle

FTP
HTTP
SSH, HTTPS (Anwendungserkennung, ohne Entschlüsselung)
RDP
NTP
SNMP
Netbios (Windows-Dateifreigabe)
ARP, DHCP
MySQL, MSSQL, PostgreSQL
telnet
ICMP, ICMPv6
RIPv2
SSDP
MDNS
... und viele andere

1.2 Feinkörnige Berechtigungen für IEC 60870-5-104

Für IEC 60870-5-104 kann mittels Berechtigungen festgelegt werden, welche Geräte welche Aktionen durchführen dürfen, also beispielsweise Befehlsausführungen für Schaltgeräte, sonstige Befehlsausführungen, Schreibzugriffe, Lesezugriffe usw. Die vordefinierten Rollen für Geräte wurden um einen praktischen Satz von 104 Berechtigungen erweitert.

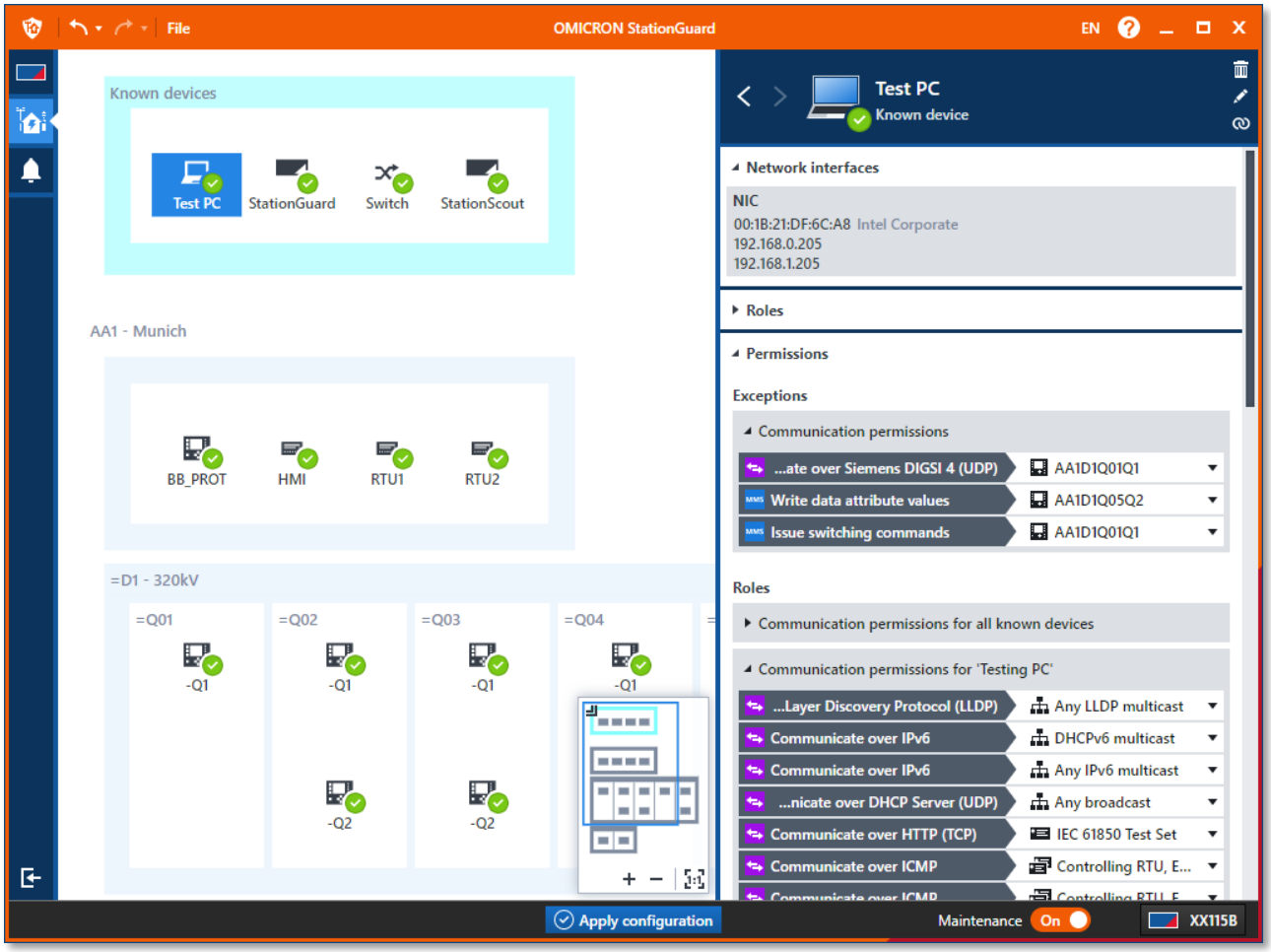
Weitere Rollen für die Leitstelle sowie für 104 IEDs und für generische IEDs erlauben eine schnelle Abdeckung des üblichen Verkehrs mittels vordefinierter Berechtigungen.

1.3 Unterstützung für Inbetriebnahme und Wartung

Engineering-Protokolle und die Web Interfaces der IEDs weisen viele bekannte Schwachstellen auf. Neue kommen ständig hinzu. Trotzdem werden diese Schnittstellen während der Inbetriebnahme und für routinemäßige Wartungen benötigt. Um Ihre Assets gegen Angriffe über diese Ports zu schützen, sollten Engineering-Aktivitäten generell verboten und nur dann erlaubt werden, wenn dies wirklich erforderlich ist. In StationGuard kann hierfür die Wartungsfunktion eingeschaltet werden. Diese sorgt für eine erhebliche Verbesserung der Sicherheit, da Engineering-Aktivitäten im normalen Betrieb untersagt und nur für Wartungstätigkeiten erlaubt sind. Durch die Wartung selbst wird nur eine geringe Anzahl von Fehlalarmen ausgelöst.

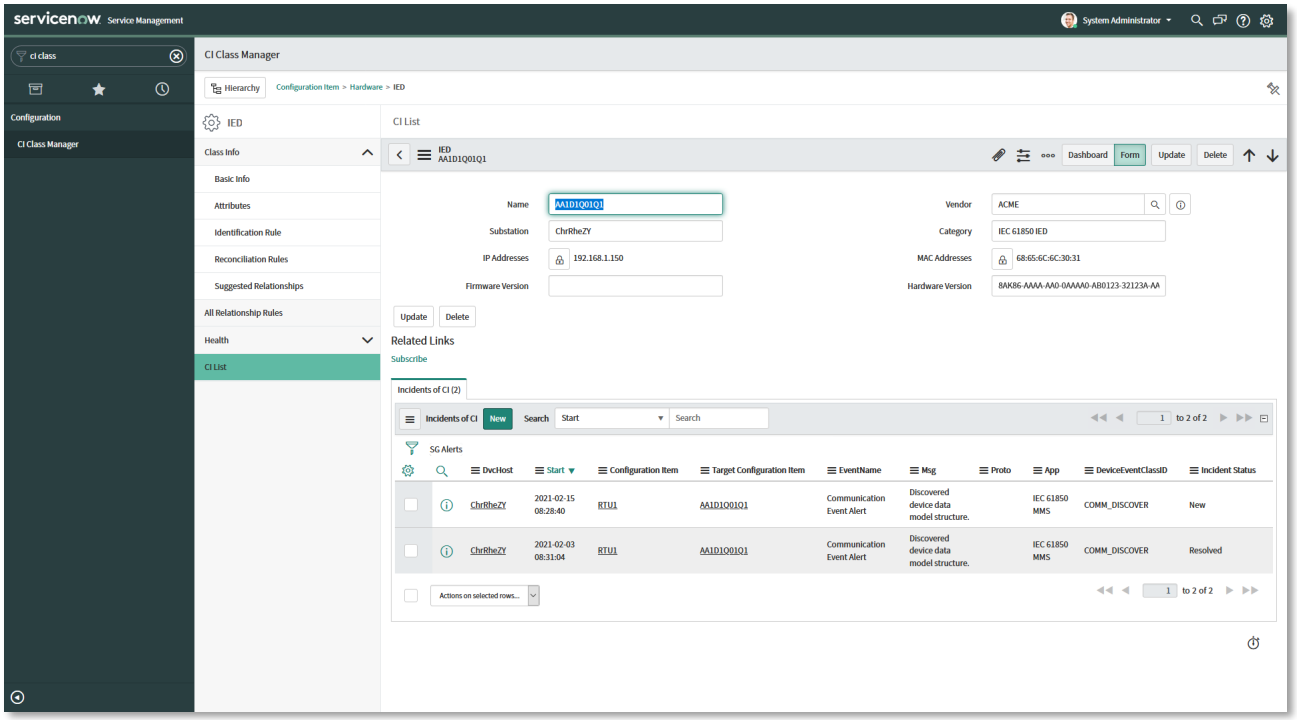
Beispielsweise darf der Engineering-PC der Anlage die meiste Zeit über nicht aktiv sein. Ist in StationGuard die Wartung aktiv, darf er nur ein bestimmtes Engineering-Protokoll verwenden oder auf das Web Interface von Schaltern zugreifen. Offenbart der Engineering-PC ein verdächtiges oder potenziell gefährliches Verhalten, führt dies immer zu einem Alarm. Im Gegensatz zu normalen oder lernbasierten Angriffsüberwachungssystemen unterstützt StationGuard die verschiedenen Phasen im Lebenszyklus von Assets durch eine hohe Selektivität der Alarme.

Das Einschalten der Wartung kann in der StationGuard Client-Software erfolgen. Zukünftig wird es auch möglich sein, die Wartung durch einen Hardware-Kontakt an einem Binäreingang zu aktivieren. Die vordefinierten Rollen für Engineering-PCs und Prüf-PCs enthalten bereits einen sicheren Satz von Berechtigungen, welcher alles abdeckt, was nur für Wartungen erlaubt sein sollte. Zur Anzeige, dass die Wartung eingeschaltet ist, wird das Anwendungsfenster von StationGuard während Wartungen mit einem orangen Rahmen angezeigt. Als Unterstützung bei der Auswertung werden alle während einer Wartung auflaufenden Alarme entsprechend markiert.



1.4 ServiceNow-Integration

Die Integration von StationGuard-Alarmen in die Service-Management-Plattform ServiceNow ermöglicht ein effizientes Störfallmanagement. Das Asset-Inventar kann aus StationGuard in die ServiceNow CMDB importiert werden. Dort können für die verschiedenen Assets oder Anlagen verantwortliche Ingenieur:innen festgelegt werden. Dies ermöglicht eine automatische Zuweisung von ServiceNow-Tickets zu den jeweils zuständigen Ingenieur:innen.



StationGuard integriert sich außerdem in Ihre SIEM-Systeme. Hierfür unterstützt StationGuard viele verschiedene Systeme, unter anderem FortiSIEM©, ArcSight©, IBM QRadar und Splunk.

Für Splunk ist auch eine entsprechende App für StationGuard verfügbar.

2 Sonstige Verbesserungen

2.1 Neue Alarme und Details zu Problemen bezüglich der Protokollkodierung

StationGuard liefert nun zusätzliche Details zu Parsing-Problemen. So kann ermittelt werden, welche Teile eines Paketes fehlerhaft sind oder manipuliert wurden.

Außerdem gibt es nun neue Alarme für den Fall, dass eine veraltete SSL/TLS-Version verwendet wird, oder dass StationGuard für ein bestehendes Gerät mit einer bereits bekannten MAC-Adresse eine neue IP-Adresse detektiert.

2.2 Globale Berechtigungen für GOOSE VLAN-Alarme

Wenn StationGuard aufgrund von Konfigurationsproblemen oder anderen Einschränkungen VLAN-Tags in GOOSE-Meldungen nicht erkennt oder wenn die VLAN-Information durch einen Switch verändert wird, weisen alle GOOSE im Netzwerk dasselbe VLAN-Problem auf. Falls notwendig, können Sie solche für alle GOOSE-Meldungen im Netzwerk auftretenden VLAN-Probleme nun mit Hilfe von globalen Berechtigungen abdecken.

2.3 Stabilität und Performance

StationGuard legt nun bei jedem erfolgreichen Anwenden einer Konfiguration eine Sicherung der Konfiguration an. Geht etwas schief, kehrt StationGuard automatisch zu der zuletzt funktionierenden Konfiguration zurück.

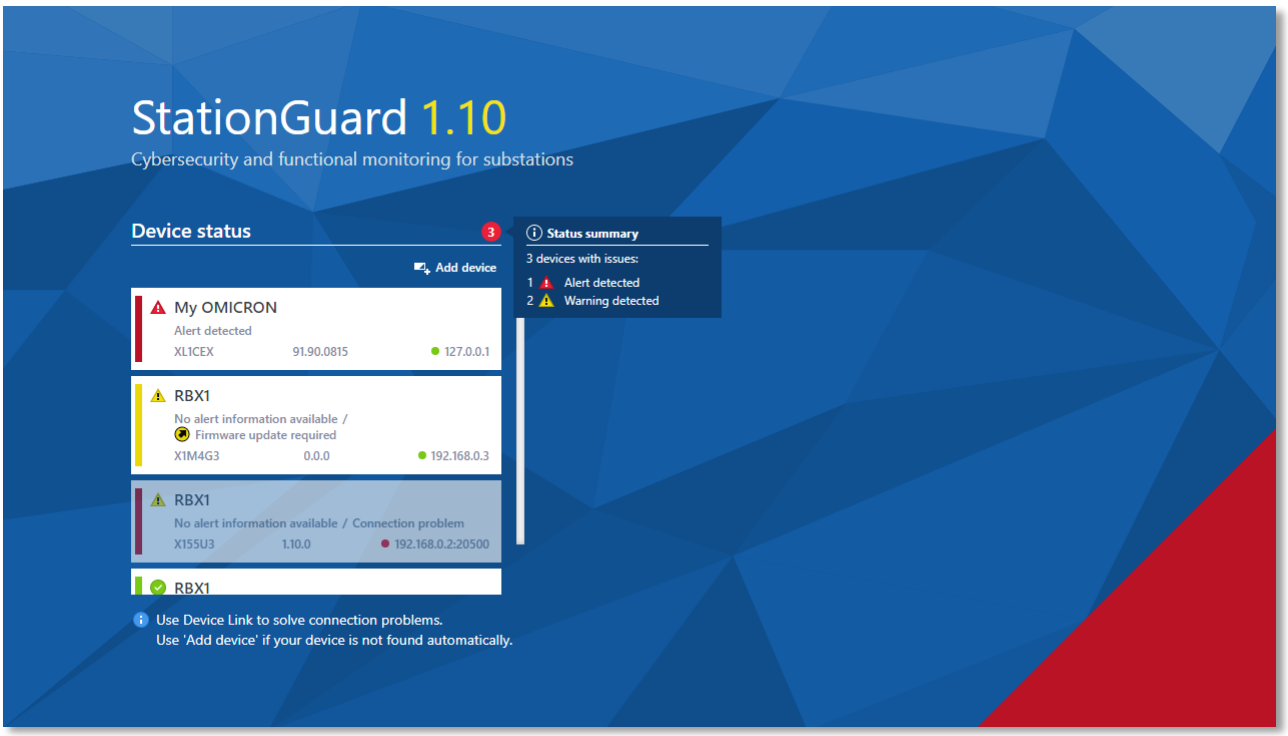
Zusätzlich zu den oben genannten Funktionen und Verbesserungen arbeitet unser engagiertes Team ständig an der Verbesserung des Nutzerlebnisses, der Performance und der Stabilität von StationGuard.

Version 1.10

1 Neue Funktionen und Verbesserungen

1.1 Zentrales Dashboard mit Anzeige der Alarmstatus aus allen Anlagen

StationGuard verfügt nun über ein zentrales Dashboard mit Anzeige des Alarmstatus aller StationGuard-Geräte in allen Anlagen. Der Status jedes Gerätes wird je nach Alarm- und Verbindungsstatus in Grün/Gelb/Rot angezeigt. Ein Summensymbol zeigt auf einen Blick, für wie viele Geräte ein Alarm oder eine Warnung vorliegt.



1.2 Export des Asset-Inventars im CSV-Format

Sie haben nun die Möglichkeit, Informationen zu allen von StationGuard detektierten Geräten in eine CSV-Datei zu exportieren und so alle im Netzwerk aktiven Geräte zu dokumentieren. Dies kann insbesondere im Rahmen von Sicherheitsaudits oder bei der Inbetriebnahme von Anlagen nützlich sein.

Die für die einzelnen Geräte exportierten Informationen sind dabei eine Kombination aus passiv im Netzwerk erfassten Informationen (MAC-Adresse, IP-Adressen) und den Informationen aus der SCD-Datei, wie beispielsweise IED-Name, Beschreibung, Hardware-Version (bei manchen Herstellern mit Bestellnummer), Hersteller, Modell, Seriennummer und Firmware-Version.

Diese Exportfunktion ist auch in StationScout 1.30 enthalten. StationScout ist eine Software zur Visualisierung und Prüfung von Stationsautomatisierungssystemen und liest durch aktives Abfragen der IEC-61850-Geräte sämtliche Informationen zu den Typenschilddaten und der Firmware-Version der Geräte aus.

Eine Kombination aus StationScout und StationGuard bildet so eine leistungsstarke Lösung zur Dokumentation des Asset-Inventars.

	A	B	C	D	E	F	G	H	I	J	K
1	Name	Description	Hardware version	Model	Serial	Softwa	Vendor	IP addresses	Origin	MAC addresses	Roles
2	AA1D1Q01Q1	Transformer infeed bay Q01	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.150	system_scd_v3.2	68:65:6C:6C:30:31	IEC 61850 IED
3	AA1D1Q02Q1	Bay control unit Q02 - Starnberg	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.152	system_scd_v3.3	68:65:6C:6C:30:33	IEC 61850 IED
4	AA1D1Q02Q2	Disconnector control unit Q02 - S	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.153	system_scd_v3.3	68:65:6C:6C:30:34	IEC 61850 IED
5	AA1D1Q03Q1	Bay control unit Q03 - Passau	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.154	system_scd_v3.3	68:65:6C:6C:30:35	IEC 61850 IED
6	AA1D1Q03Q2	Disconnector control unit Q03 - P	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.151	system_scd_v3.3	68:65:6C:6C:30:36	IEC 61850 IED
7	AA1D1Q04Q1	Transformer bay Q04	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.155	system_scd_v3.3	68:65:6C:6C:30:37	IEC 61850 IED
8	AA1D1Q05Q2	320kV measuring bay - Merging U		MU 300			ACME	192.168.1.157	system_scd_v3.3	68:65:6C:6C:30:39	IEC 61850 IED
9	AA1H1Q01Q1	Transformer 33kV bay Q01	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.160	system_scd_v3.3	68:65:6C:6C:30:32	IEC 61850 IED
10	AA1H1Q02Q1	Transformer 33kV bay Q02	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.161	system_scd_v3.3	68:65:6C:6C:31:30	IEC 61850 IED
11	BB_PROT	Busbar Protection	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.173	system_scd_v3.3	68:65:6C:6C:30:30	IEC 61850 IED
12	HMI	IHMI		HMI 300			ACME	192.168.1.200	system_scd_v3.3	68:65:6C:6C:31:31	Monitoring RTU
13	PCPQS1	Disturbance data collector		COLLEC 400			ACME	192.168.1.190	system_scd_v3.3		Monitoring RTU
14	RTU1	RTU for transformer bays		RTU 600			ACME	192.168.1.201	system_scd_v3.3	68:65:6C:6C:31:32	Monitoring RTU
15	RTU2	RTU for feeder bays		RTU 600			ACME	192.168.1.202	system_scd_v3.3	68:65:6C:6C:31:33	Monitoring RTU

1.3 Alarmausgabe an Binärkontakten

Die Hardware-Plattform RBX1 für StationGuard verfügt über 8 Binärausgänge. Die Kontakte dieser Ausgänge werden betätigt, sobald unquittierte StationGuard-Alarme oder -Warnungen vorliegen. Dies ermöglicht die Integration von StationGuard-Alarmen in die Leittechnik-Signalliste, indem die Kontakte für die Signalisierung von Alarmen und Warnungen auf eine RTU geführt werden.

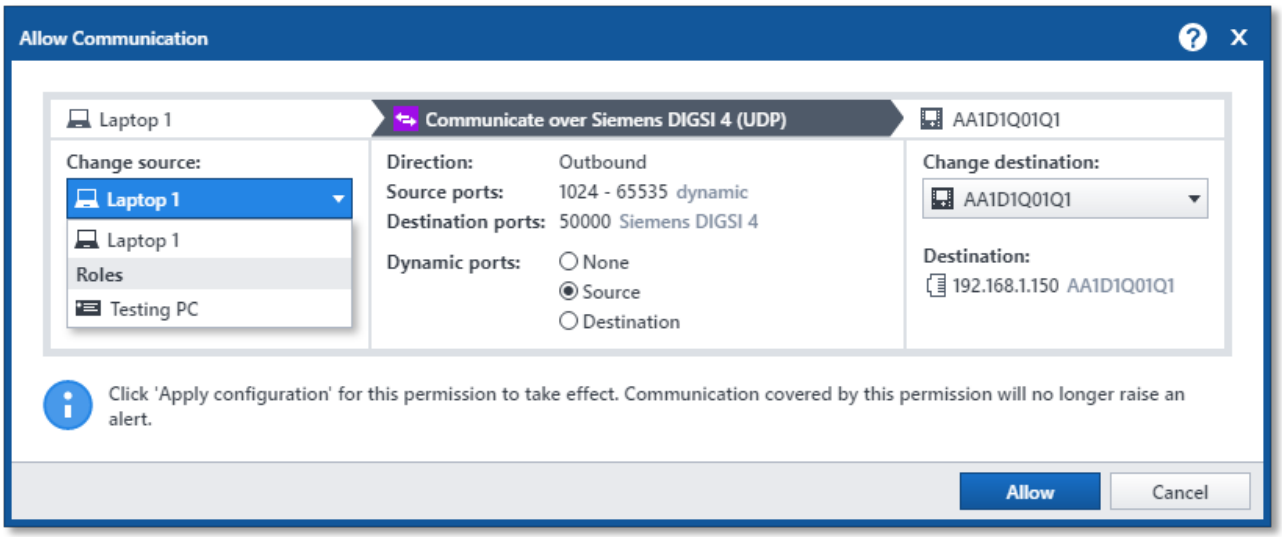
Der Schaltzustand der Binärausgänge wird auch durch LEDs auf der Frontpatte der RBX1-Plattform angezeigt.

Die Alarminformationen können auch durch die einzelnen Geräte des StationGuard-Systems via syslog-TCP oder -UDP gesendet werden. StationGuard ist kompatibel mit den SIEM-Systemen aller relevanten Hersteller.

2 Sonstige Verbesserungen

2.1 Erweitern der vordefinierten Rollen durch Hinzufügen von neuen Berechtigungen für eine Rolle

Es besteht nun die Möglichkeit, vordefinierte Rollen wie "Engineering PC" und "IEC 61850 IED" durch Hinzufügen von neuen Berechtigungen zu modifizieren. StationGuard zeigt einen Dialog an, in dem Sie auswählen können, ob Sie eine bestimmte Kommunikation nur zwischen zwei Geräten erlauben möchten oder für alle Geräte mit diesen Rollen.

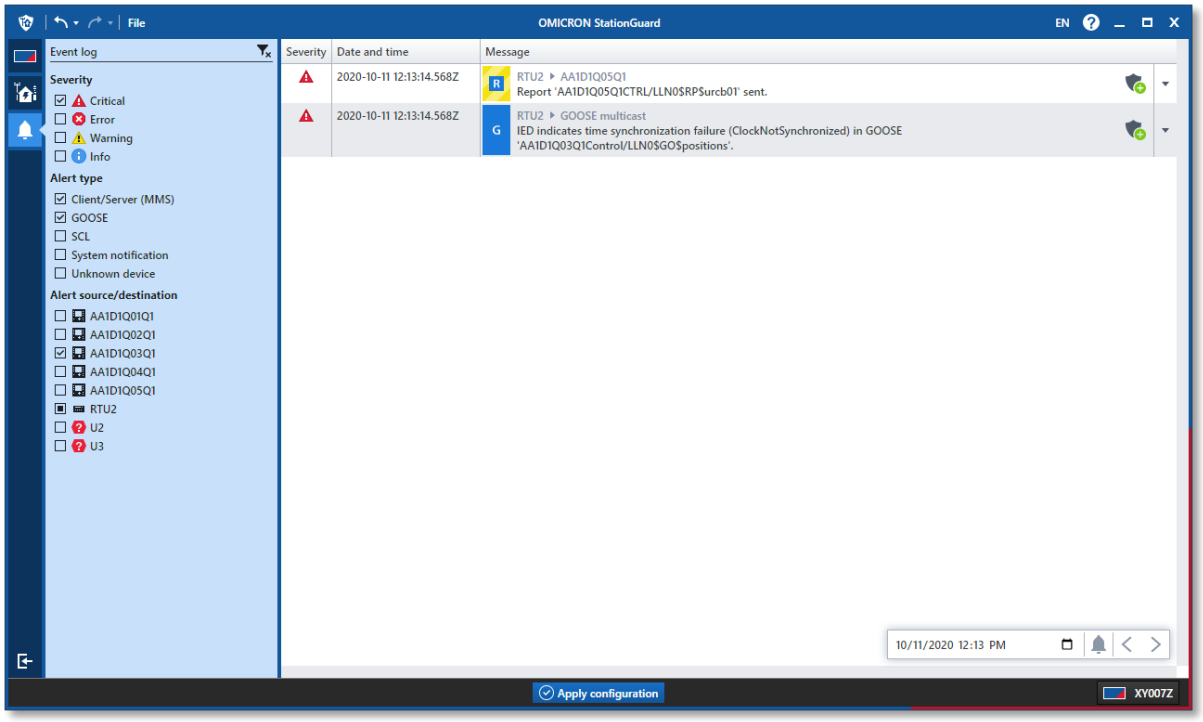


2.2 Anzeige des Gerätestatus im ZeroLine-Diagramm

Bei den Gerätesymbolen im ZeroLine-Diagramm wird zusätzlich ein Symbol zur Anzeige von Alarmen, Problemen oder des aktuellen Status angezeigt.

2.3 Anzeige der vollständigen Ereignishistorie für ein Gerät

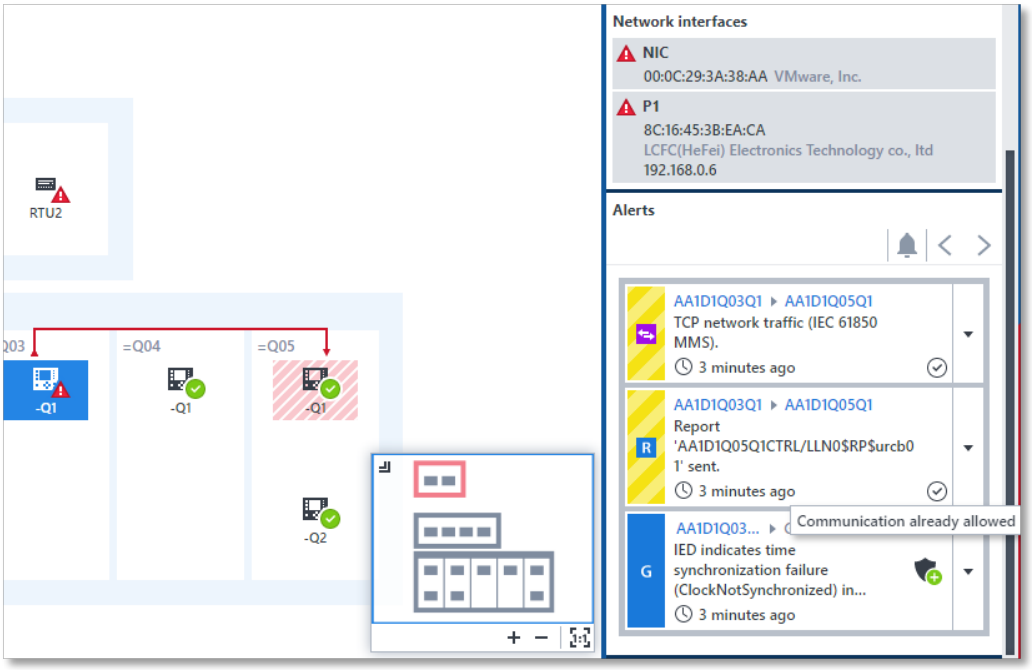
Das Ereignisprotokoll kann nun auch nach Geräten gefiltert werden, sodass nur noch die mit einem bestimmten Gerät verbundenen Alarme und Probleme angezeigt werden (also diejenigen Alarme, für die das Gerät entweder die Alarmquelle oder das Ziel für die den Alarm verursachende Kommunikation war).



2.4 Erkennung, ob Alarme bereits durch Berechtigungen abgedeckt sind

Beim Hinzufügen einer Berechtigung oder einer neuen Rolle für ein Gerät werden nun die Auswirkungen auf die anderen vorhandenen Alarme angezeigt. Würde ein Alarm mit den aktuellen Einstellungen für die Berechtigung/Rolle zukünftig nicht mehr auftreten, erscheint neben dem Alarm ein Häkchen.

Dies funktioniert auch für Alarme im Ereignisprotokoll.



2.5 Export des Ereignisprotokolls zusammen mit einer Sicherung der Detektionskonfiguration

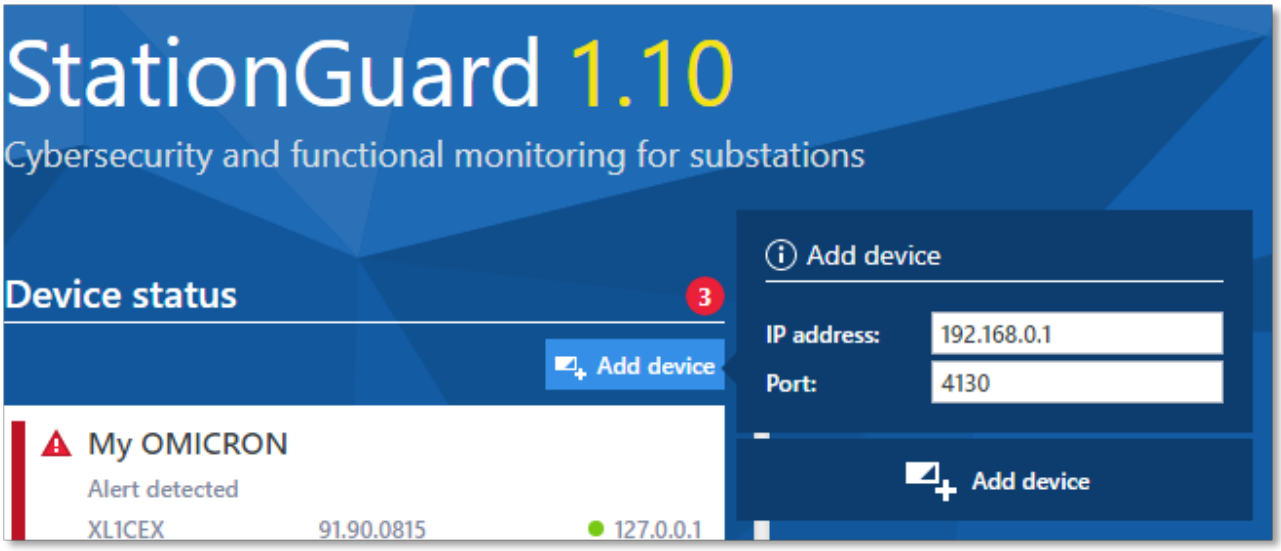
Es ist nun möglich, im Zug einer Sicherung der Detektionskonfiguration auch das Ereignisprotokoll zu exportieren. Beim Import einer Detektionskonfiguration aus einer Sicherung können Sie auswählen, ob nur die Konfiguration importiert werden soll, oder auch das Ereignisprotokoll.

Durch Importieren in ein anderes RBX1- oder MBX1-StationGuard-Gerät ermöglicht dies auch eine nachträgliche Analyse des Ereignisprotokolls im Büro.

2.6 Weniger Netzwerk-Ports erforderlich; Verwendung von StationGuard hinter NAT-Geräten zur Netzwerkadressübersetzung möglich

Für die Verbindung mit der StationGuard Client-Software muss nun in der Firewall der Anlage nur noch ein Port (TCP 20499) geöffnet sein. Weitere Einstellungen sind nicht erforderlich. Nähere Informationen zu Netzwerk-Ports und Sicherheit finden Sie in der Hilfe zu StationGuard.

Sie können so auch mit Geräten arbeiten, die sich hinter einem Router oder in einem Netzwerk mit einem NAT-Gerät zur Netzwerkadressübersetzung befinden.



OMICRON

Weitere Informationen und Literatur
sowie detaillierte Kontaktinformationen
finden Sie auf unseren Webseiten:

www.omicronenergy.com und
www.omicroncybersecurity.com