SIEMENS

Industrielle Kommunikation

SINEMA Server –

Making Your Network Transparent

Broschüre

Ausgabe 06/2018

siemens.de/sinema-server

SINEMA Server – für transparente Netzwerke

Industrielle Kommunikationsnetzwerke sind die Basis der Digitalisierung in modernen Unternehmen. Vollständige Informationen über den Zustand eines Netzwerkes sind für einen zuverlässigen und unternehmensweiten Austausch von Daten unerlässlich. Mit der Netzwerkmanagement-Software SINEMA Server überwachen Sie zuverlässig Ihr Netzwerk für eine transparente Diagnose.

Bis zu 15 Milliarden kommunikationsfähige Maschinen werden bis ins Jahr 2020 im industriellen Internet der Dinge (IoT) vernetzt sein. Diese riesige Anzahl von Maschinen und Anlagen muss abgebildet und diagnostiziert werden, um einen umfassenden Überblick über die im Netzwerk befindlichen Daten zu haben. Gerade im Fehlerfall vereinfacht dies die Diagnose, so dass Anlagenstillstände und Netzwerkausfälle minimiert werden.

Mit einer geeigneten Netzwerkmanagement-Software wie SINEMA Server von Siemens lassen sich Probleme frühzeitig erkennen und Maßnahmen rechtzeitig ergreifen. SINEMA Server ist beispielsweise für die diskrete Fertigung sowie die Prozessindustrie geeignet.

Im Betrieb kann schon ein einzelner Ausfall im Netzwerk eine Flut von Alarmmeldungen verursachen.
Die Verknüpfung von Topologiewissen mit Diagnosewerten einzelner Netzwerkteilnehmer (einschließlich SIMATIC- und PROFINET-Diagnose) ist daher entscheidend, um schnell den Ort und die Ursache eines Netzwerkfehlers zu identifizieren und zu beheben. Eine vollständige physikalische Karte des Netzwerks dient der Analyse möglicher Auswirkungen von Leitungs- und Gerätefehlern – das ist besonders hilfreich bei der Planung hochverfügbarer Anlagen. Auch redundante PCS 7-Architekturen lassen sich über SINEMA Server erkennen und abbilden.

SINEMA Server kann das gesamte industrielle Netzwerk abbilden – von den Netzwerkkomponenten bis hin zu Automatisierungs-Endgeräten wie Steuerungen und dezentralen Peripherien.

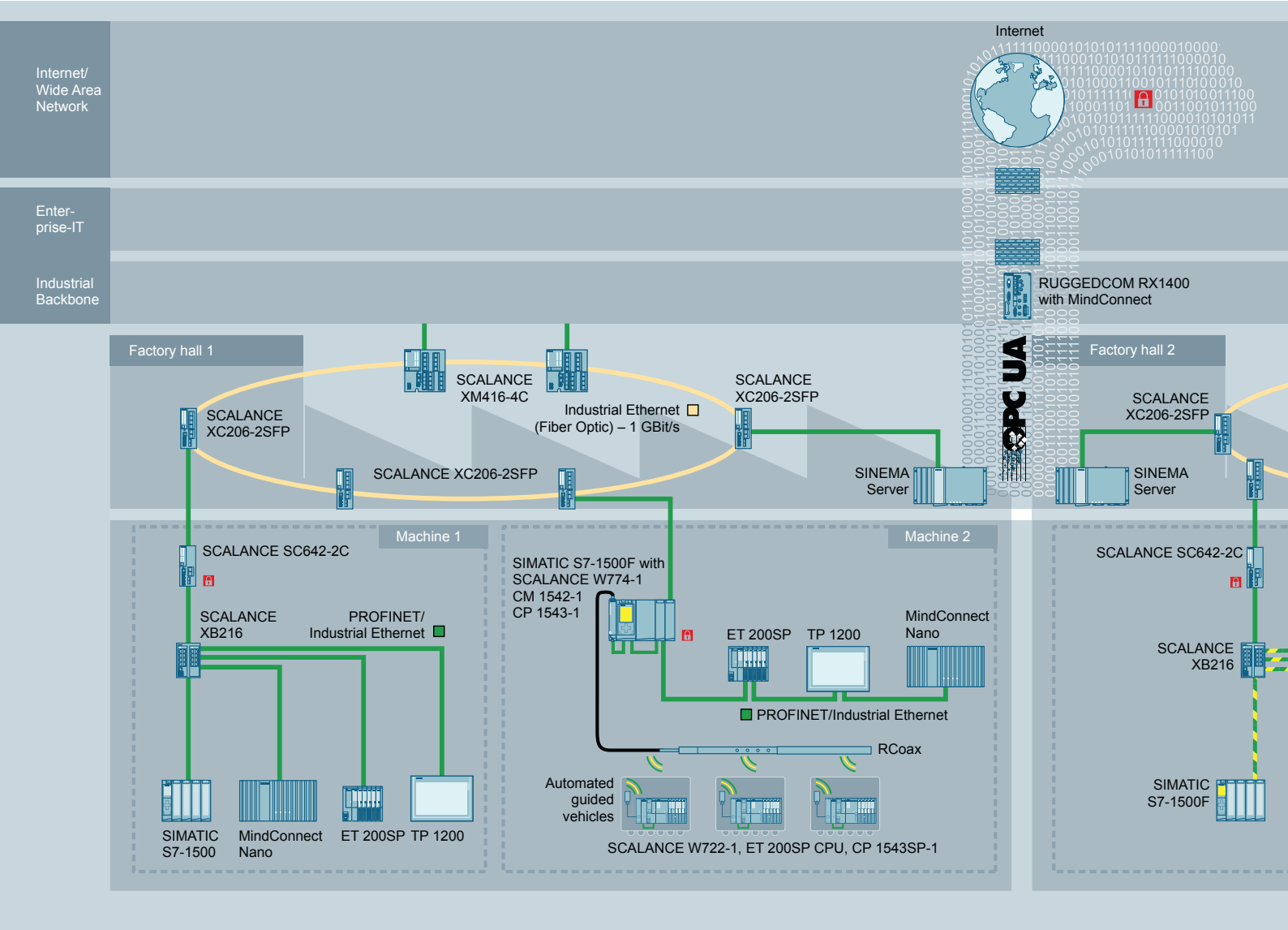
Vorteile im Überblick:

- Übersichtliche Darstellung der Netzwerktopologie dank automatischer Komponenten- und Topologieerkennung
- Umfangreiche Diagnosemöglichkeiten über SNMP, PROFINET und SIMATIC
- Ereignisbasiertes Meldesystem zur transparenten Darstellung der Netzwerkdiagnose
- Standardisierte Netzwerkdokumentation (Reports)
- Geräteprofilkonzept zur Überwachung von Siemens- und Fremdgeräten
- Datentransfer über verschiedene, standardisierte Protokolle (z. B. OPC UA) in cloudbasierte Systeme
- Validierung von Netzwerkparametern
- Zentrales Firmware- und Konfigurationsmanagement geräteübergreifend per CLI
- Überwachung mehrerer Anlagen mit identischen IP-Adressen mittels Network Address Translation (NAT)

SINEMA Server

Diagnosedaten vom Feld bis in die Cloud

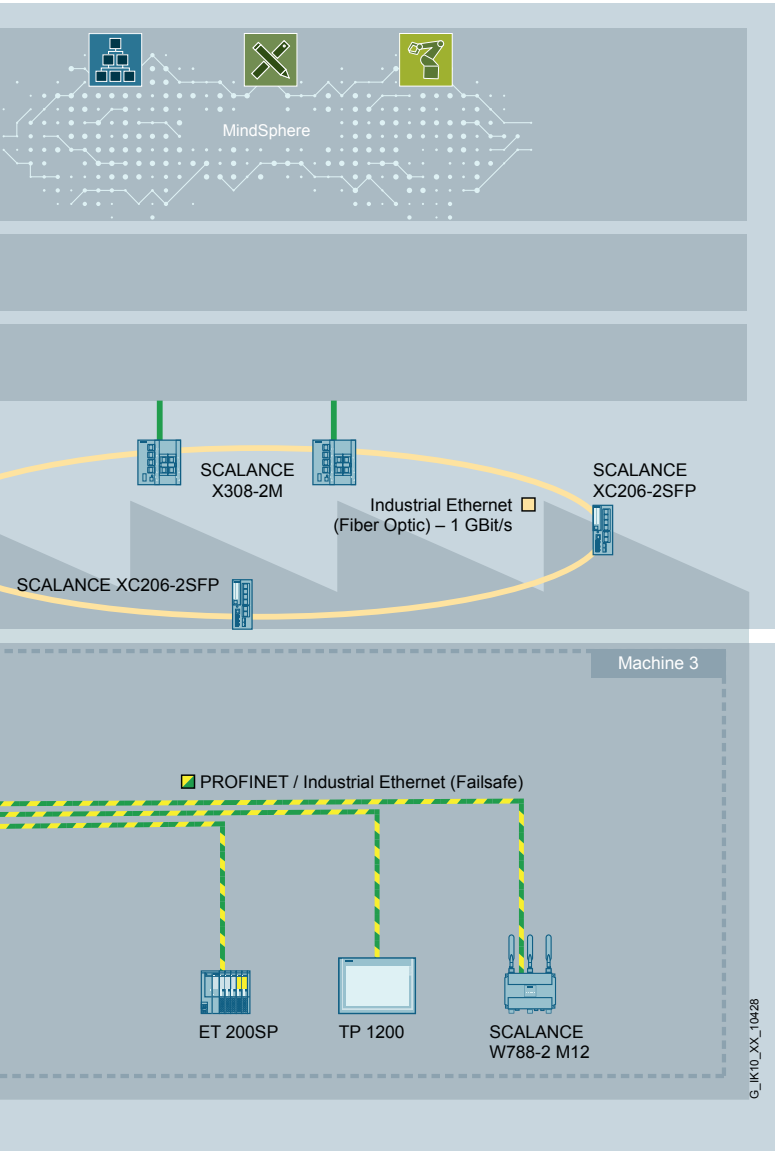
Fertigungsstandorte liegen häufig weit auseinander. Deshalb ist es wichtig neben der Diagnose möglichst vieler Netzwerkkomponenten in einer Software auch eine standortübergreifende Zustandsübersicht zu erhalten. Der Vorteil von cloudbasierten Systemen ist es, Daten zentral abzurufen unabhängig vom Ort, an dem sich die Anwender befinden. Der Status ihrer weltweit verteilten Anlagen und Maschinen lässt sich damit jederzeit abrufen – beispielsweise über das offene und cloudbasierte IoT-Betriebssystem MindSphere. Die SINEMA Server-Daten (z. B. Geräte- und Portstatus sowie Statistikdaten) lassen sich über das OPC UA-Protokoll und dem RUGGEDCOM RX1400 mit MindConnect an die MindSphere übertragen. Damit sind Wertänderungen, wie ein nicht erreichbares Gerät selbst in weit verteilten Anlagen sichtbar, was vorausschauende Wartung ermöglicht und lange Stillstandszeiten im Fehlerfall vermeidet.



Merkmale im Überblick

SINEMA Server bietet viele Möglichkeiten im Bereich des Netzwerkmanagements und der -diagnose. Beispielsweise bietet die Reporting-Funktion eine Darstellung von Statistiken über beliebige Zeiträume. Zur Verfügung stehende Profile ermöglichen die Anzeige von Fremdkomponenten in SINEMA Server und vieles mehr.

Die wichtigsten SINEMA Server-Funktionalitäten im Überblick:



Diagnostic

Übersichtliche Diagnose – Auswertung und Darstellung von Diagnosezuständen:

Reporting

Darstellung von Statistiken über beliebige Zeiträume:

Topology

Topologische Darstellung des Netzwerkes:

Validation

Validierung von Netzwerkparametern:

Monitoring

Auslesen von Statusinformationen:

Propagation

Weitergabe von Daten an andere Systeme:

Inventory

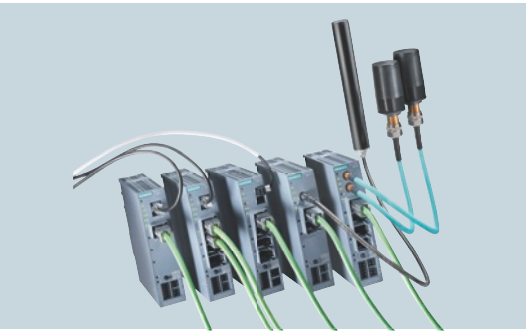
Inventarisierung und Dokumentation aller Netzwerkteilnehmer:

Management

Konfiguration von Geräten per CLI / Firmware-Management:

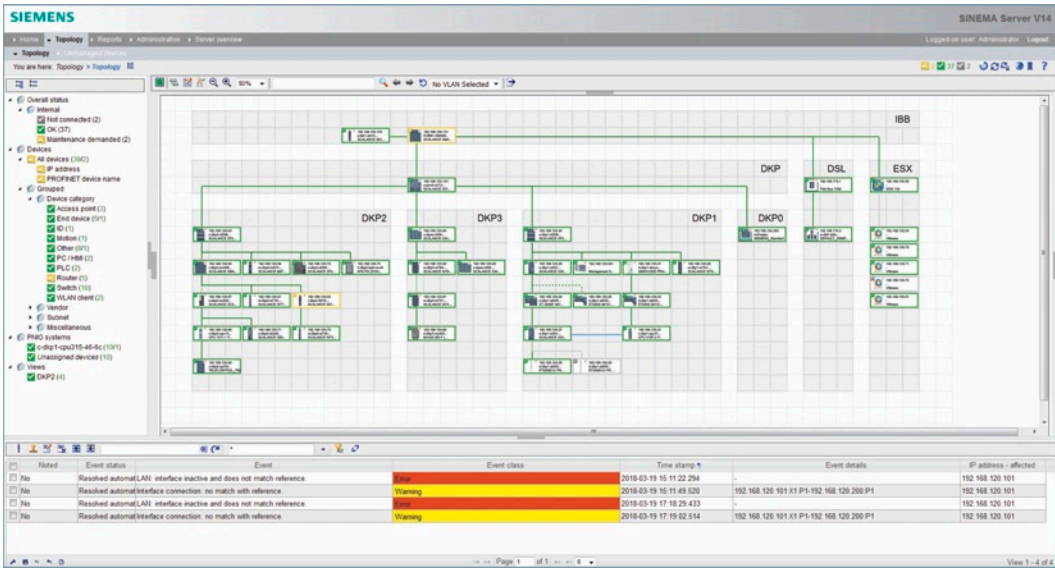
SINEMA Server

Die wichtigsten Funktionen der Netzwerkmanagement-Software



Intuitive Bedienung

SINEMA Server beinhaltet die wichtigsten Funktionen für das industrielle Umfeld. Die übersichtliche Oberfläche ermöglicht eine intuitive Bedienung. Der Benutzer erhält schnell einen Überblick über das gesamte Netzwerk.



Automatische Geräteerkennung und Generierung der Netzwerktopologie

Die Netzwerkmanagement-Software erkennt mit Hilfe von Discovery and Configuration Protocol (DCP) und Simple Network Management Protocol (SNMP) sowie über die PROFINET-Diagnose automatisch PROFINET- und Ethernet-Geräte im Netzwerk. Diese Geräte können über mehrere Netzwerkkarten (NIC) erkannt und grafisch in einem Webbrowser dargestellt werden. Somit kann das Wartungspersonal von Prozess- und Produktionsanlagen ohne aufwändige Konfiguration immer den aktuellen Status der Geräte und deren Verbindungen (Topologie) überwachen. Eine detaillierte Gerätedarstellung ist für Automatisierungskomponenten von Siemens möglich. Dazu gehören z. B. Netzwerkkomponenten wie die Siemens-Produktfamilien SCALANCE und RUGGEDCOM, Steuerungen wie SIMATIC S7-410-5H oder SIMATIC S7-1500 und die entsprechenden Kommunikationsbaugruppen. Weitere Komponenten sind die unterbrechungsfreie DC 24 V-Stromversorgung SITOP PSU8600 sowie Identifikationssysteme und Antriebssysteme wie SIMOTION oder kontinuierliche Gasanalysegeräte wie SIPROCESS GA 700 auf der Feldebene.

Ebenso können Geräte anderer Anbieter und deren Gerätestatus sowie Verbindungen in SINEMA Server dargestellt werden. Über das Geräteprofilkonzept lassen sie sich nahtlos integrieren.

Umfassende, systemübergreifende Diagnosemöglichkeiten

SINEMA Server verfügt über verschiedene Diagnosemöglichkeiten:

- SNMP: für die standardisierte Diagnose von Netzwerkkomponenten beliebiger Hersteller
- PROFINET: der offene Industrial Ethernet-Standard für die herstellerübergreifende Datenauswertung
- SIMATIC: für die baugruppeninterne Auswertung zur Integration in die durchgängige Systemdiagnose ins TIA Portal (nahtlose Anbindung an das Meldewesen der CPU)

Zentrales Firmware- und Konfigurationsmanagement

Über ein zentrales Firmware- und Konfigurationsmanagement per CLI können alle Geräte in einem überwachten Netzwerk gleichzeitig konfiguriert werden. SINEMA Server bietet die Möglichkeit Firmware-Updates für SCALANCE-Geräte von zentraler Stelle aus durchzuführen. Dies kann manuell angestoßen oder in gewünschten Zeitfenstern eingeplant werden.

Anwenderspezifische Topologiedarstellung des Netzwerkes

SINEMA Server ermöglicht, neben der automatisch generierten Topologiedarstellung auch die Netzwerkteilnehmer in jeder beliebigen anderen Anordnung darzustellen. Zusätzlich lassen sich zusammenhängende Geräte in der Topologie gruppieren. Diese anwenderspezifischen Topologien können mit Hintergrundbildern (z. B. Gebäude- oder Anlagenplänen) ergänzt werden. Für eine verständlichere Übersicht ist es möglich zwischen einer funktionellen oder gerätespezifischen Icon-Darstellung auszuwählen. Im Fehlerfall können somit die jeweiligen Netzwerkkomponenten schneller gefunden und ausgetauscht oder repariert werden.

Alarmierung bei Events

Zur lückenlosen Überwachung des Netzwerkes ohne Zeitverzögerung müssen Netzwerkmeldungen sofort erkannt und die Anwender umgehend informiert werden. Deshalb erfasst und verarbeitet SINEMA Server alle Meldungen von Vorfällen und versorgt so den Benutzer mit allen wichtigen Event-Informationen über das Netzwerk.

Benutzerdefinierte Darstellung

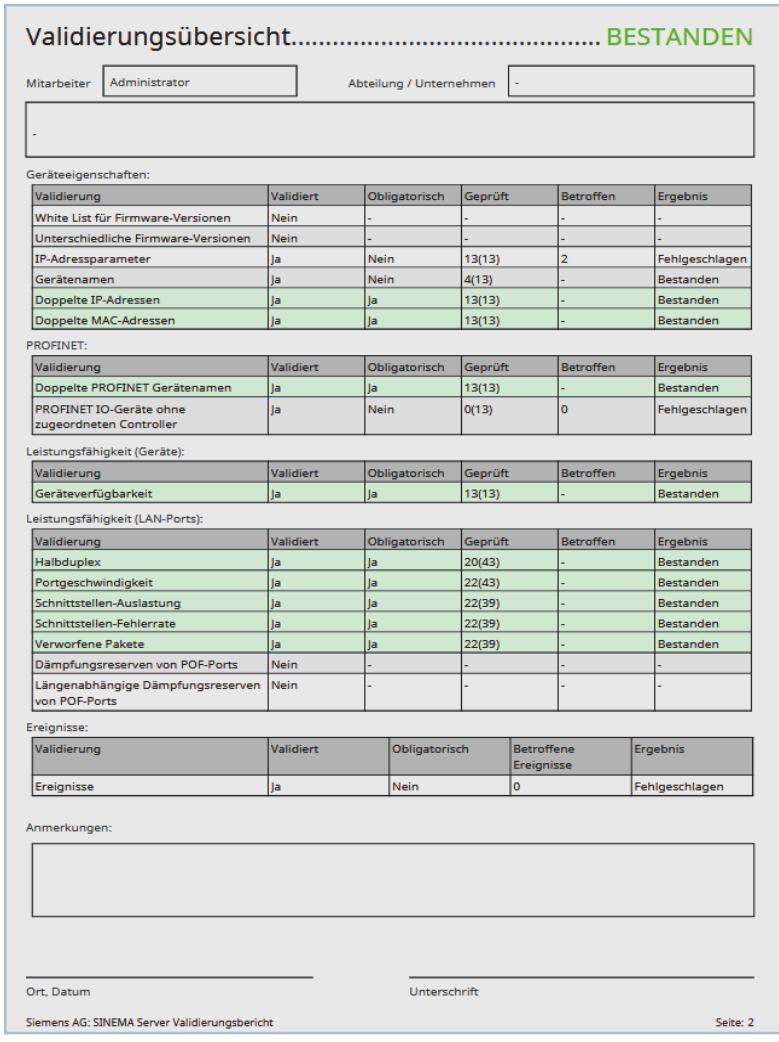
SINEMA Server ermöglicht es, den Anwendern verschiedene Rollen zuzuweisen (z. B. Administrator, Wartungspersonal, etc.). Dafür definiert der Administrator verschiedene Gruppen, denen entsprechende Rechte und topologische Ansichten zugeordnet werden. Damit ist es möglich, dass mehrere Personen mit unterschiedlichen Aufgaben gleichzeitig in einem SINEMA Server-System arbeiten können.

Benutzerfreundliche Reports

Die Diagnose umfasst nicht nur den aktuellen Zustand des Netzwerkes, sondern auch die Analyse der vergangenen Daten. SINEMA Server speichert alle aus den Netzwerkkomponenten ausgelesen Werte. Diese können dann in benutzerfreundlichen Reports zeitlich gefiltert und ausgewertet werden. Das Risiko zukünftiger Ausfälle lässt sich damit minimieren. Über einen Validierungsreport erfolgt ein Soll-Ist-Vergleich der Qualitätskriterien im Netzwerk, z. B. bei doppelten IP-Adressen.

Diagnose von Anlagen mit identischen IP-Adressen

Vor allem der Serienmaschinenbauer konfiguriert seine Anlagen häufig mit gleichen IP-Adressen. Diese Serienmaschinen werden in den Industrieanlagen über NAT-Router integriert. SINEMA Server kann auch diese Netzwerke, die hinter einem NAT-Router liegen, überwachen und diagnostizieren.



Validierungsübersicht..... BESTANDEN

Mitarbeiter: Administrator — Abteilung / Unternehmen: -

-

Geräteeigenschaften:

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
White List für Firmware-Versionen	Nein	-	-	-	-
Unterschiedliche Firmware-Versionen	Nein	-	-	-	-
IP-Adressparameter	Ja	Nein	13(13)	2	Fehlgeschlagen
Gerätenamen	Ja	Nein	4(13)	-	Bestanden
Doppelte IP-Adressen	Ja	Ja	13(13)	-	Bestanden
Doppelte MAC-Adressen	Ja	Ja	13(13)	-	Bestanden

PROFINET:

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
Doppelte PROFINET Gerätenamen	Ja	Ja	13(13)	-	Bestanden
PROFINET IO-Geräte ohne zugeordneten Controller	Ja	Nein	0(13)	0	Fehlgeschlagen

Leistungsfähigkeit (Geräte):

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
Geräteverfügbarkeit	Ja	Ja	13(13)	-	Bestanden

Leistungsfähigkeit (LAN-Ports):

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
Halbduplex	Ja	Ja	20(43)	-	Bestanden
Portgeschwindigkeit	Ja	Ja	22(43)	-	Bestanden
Schnittstellen-Auslastung	Ja	Ja	22(39)	-	Bestanden
Schnittstellen-Fehlerrate	Ja	Ja	22(39)	-	Bestanden
Verworfene Pakete	Ja	Ja	22(39)	-	Bestanden
Dämpfungsreserven von POF-Ports	Nein	-	-	-	-
Längenabhängige Dämpfungsreserven von POF-Ports	Nein	-	-	-	-

Ereignisse:

Validierung	Validiert	Obligatorisch	Betroffene Ereignisse	Ergebnis
Ereignisse	Ja	Nein	0	Fehlgeschlagen

Anmerkungen:

Ort, Datum — Unterschrift

Siemens AG: SINEMA Server Validierungsbericht — Seite: 2

Weitere Informationen

Netzwerkmanagement mit höchster Transparenz
www.siemens.de/sinema-server

Professional Services für industrielle Netzwerke
www.siemens.de/industrial-networks-services

Siemens AG
Process Industries and Drives Division
Process Automation
Postfach 48 48
90026 Nürnberg
Deutschland

Artikel-Nr.: 6ZB5530-1BB01-0BA8
W-FPN8Z-PD-PA262 / Dispo 26000
BR 0618 2.5 WÜ 8 De
Printed in Germany

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z. B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter
http://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter
http://www.siemens.com/industrialsecurity.