
SIEMENS
Ingenuity for life
Verwandelt Einsichten in Aussichten.
SINEC NMS – das umfassende Netzwerk-Management-System
siemens.de/sinec-nms

Effizientes Netzwerkmanagement. Mit System.

Digitalisierung wird in allen Branchen mehr und mehr zum zentralen Erfolgsfaktor – vorausgesetzt, die eingesetzten Netzwerke erfüllen die Forderung nach umfassender Konnektivität und meistern die damit verbundenen enormen Datenmengen. Verlangt wird ein leistungsstarkes und skalierbares Netzwerk-Management-System – wie SINEC NMS.

Mehr Informationen unter:
siemens.de/sinec-nms

Wegbereiter für die digitale Transformation

SINEC NMS, unser neues Netzwerk-Management-System, ist auf immer komplexer werdende Netzwerkstrukturen in einer zunehmend digitalen Welt vorbereitet. Mit ihm lassen sich Netzwerke von 50 bis 12.500 Teilnehmern zentral und rund um die Uhr überwachen, verwalten und konfigurieren. Dank seiner Skalierbarkeit wächst SINEC NMS mit, wenn das Netzwerk größer und komplexer wird.

Das NMS von morgen. Und übermorgen.

SINEC NMS unterstützt die fünf Eckpunkte für modernes Netzwerkmanagement – wie sie in FCAPS, einem Modell der ISO definiert sind – und erweitert es um die Anforderungen der Operational Technology (OT).

Fault Management

- Einfache und schnelle Fehlerlokalisierung in Anlagen
- Schnelle Reaktion im Fehlerfall durch klare Statusübersicht
- Übersichtlichkeit durch Strukturierung des Netzwerks
- Zentrale Auswertung über Netzwerkauslastung für zuverlässige Diagnose

Configuration Management

- Zeitersparnis durch zentrale Konfiguration und Wartung des gesamten Netzwerks
- Einfaches und zentrales Sichern und Verwalten von Gerätekonfigurationen
- Reduzierter Aufwand für das Überprüfen und Hochrüsten von Firmware-Versionen

Accounting Management

- Umfassender Überblick durch Gesamtübersicht aller Komponenten im Netzwerk
- Zuverlässige Überwachung der Netzwerktopologie
- Erhöhte Sicherheit durch Prüfung des Netzwerks und Dokumentation der Ereignisse

Performance Management

- Flexibilität durch Netzwerkoptimierung auf Basis von Leistungsauswertungen
- Transparenz durch Statistikerstellung und Datenspeicherung
- Hohe Verfügbarkeit durch ständige Netzwerküberwachung
- Frühzeitiges Erkennen von Veränderungen im Netzwerk

Security Management

- Verbesserte Sicherheit durch definierte Benutzerverwaltung
- Erhöhte Netzwerksicherheit durch zentrales Netzwerkmanagement
- Zuverlässige Erfüllung prozessualer und technischer Sicherheitsanforderungen gemäß IEC 62443

Netzwerkmanagement weitergedacht

SINEC NMS geht weiter als FCAPS – und bietet zusätzlich zwei übergreifende Elemente, die speziell auf die industriellen Ansprüche an Netzwerke ausgerichtet sind und unser NMS funktional abrunden.

Northbound Interface

- Einfaches Datenhandling durch direkten Zugriff auf Netzwerkinformationen zur Weiterverarbeitung in anderen Systemen und Applikationen (z.B. OPC UA)
- Vorverarbeitung der Daten
- Kurze Reaktionszeiten durch ausgereiftes Benachrichtigungs-Management

System Administration

- Dezentraler Ansatz mit ganzheitlicher Sicht auf das Netzwerk – unabhängig von dessen Größe und Komplexität
- Zentrale Inbetriebnahme und Administration der verteilten SINEC NMS Operations im SINEC NMS Control
- Effiziente Rollen- und Rechteverwaltung

Erste Wahl für komplexe Netzwerkstrukturen

Mit SINEC NMS lassen sich neue Komponenten einfach ins Netzwerk integrieren, sowie bestehende überwachen und konfigurieren. Die Konfiguration erfolgt regelbasiert, kann also übergreifend auf mehrere Komponenten angewendet werden. Das sorgt vor allem bei großen Netzwerken für deutliche Zeitgewinne bei Konfiguration und Fehlersuche.

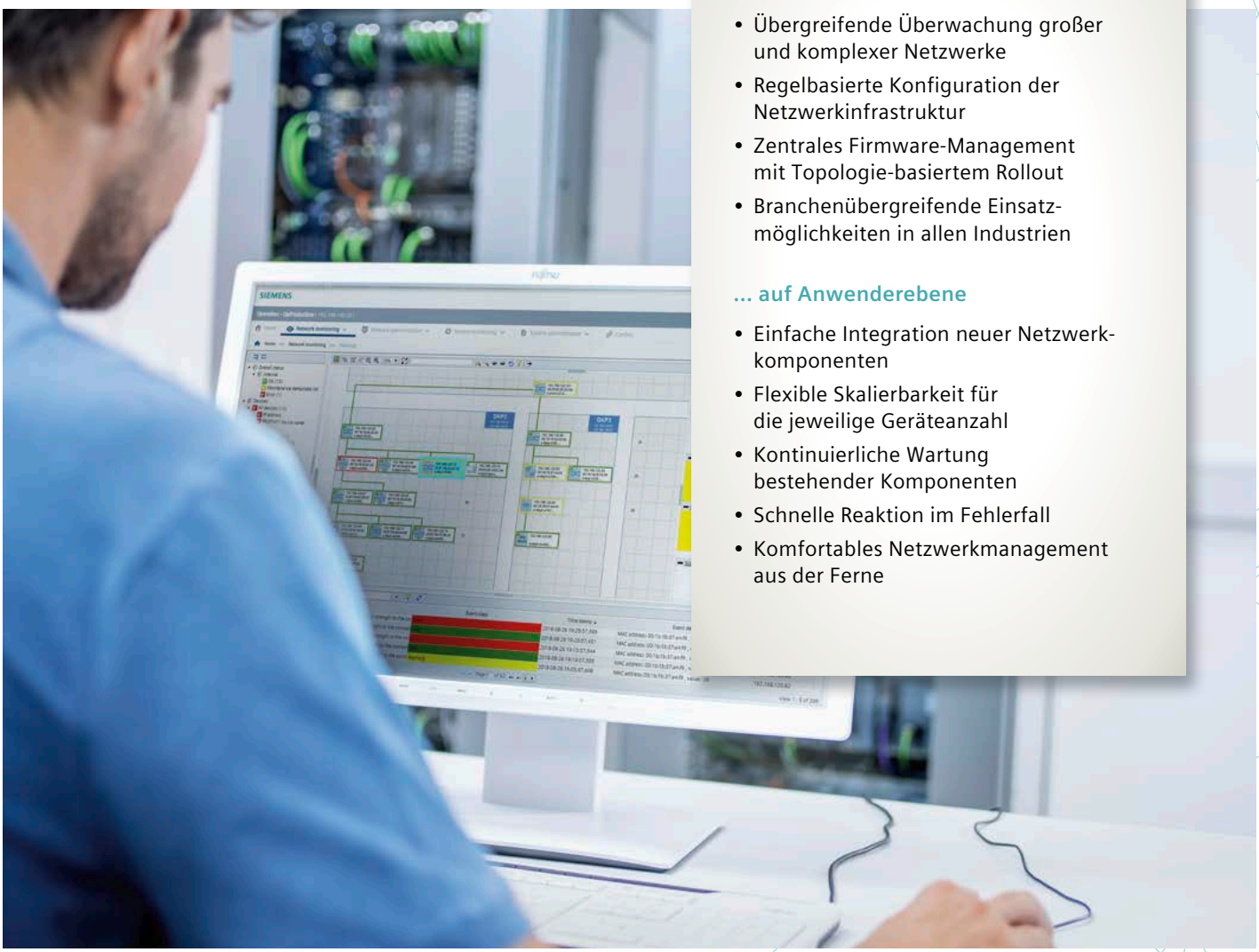
VORTEILE ...

... auf Unternehmensebene

- Übergreifende Überwachung großer und komplexer Netzwerke
- Regelbasierte Konfiguration der Netzwerkinfrastruktur
- Zentrales Firmware-Management mit Topologie-basiertem Rollout
- Branchenübergreifende Einsatzmöglichkeiten in allen Industrien

... auf Anwenderebene

- Einfache Integration neuer Netzwerkkomponenten
- Flexible Skalierbarkeit für die jeweilige Geräteanzahl
- Kontinuierliche Wartung bestehender Komponenten
- Schnelle Reaktion im Fehlerfall
- Komfortables Netzwerkmanagement aus der Ferne



Herausgeber
Siemens AG 2018

Process Industries and Drives
Postfach 48 48
90026 Nürnberg
Deutschland

Artikel-Nr.: PDPA-B10449-00
Dispostelle 06366
WS 11182.0
Gedruckt in Deutschland

Änderungen und Irrtümer vorbehalten. Die Informationen in dieser Broschüre enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden. Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle Erzeugnisbezeichnungen können Marken oder Erzeugnisnamen der Siemens AG oder anderer, zuliefernder Unternehmen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

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 einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **https://www.siemens.com/industrialsecurity.**

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie 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 **https://www.siemens.com/industrialsecurity.**