SIEMENS

# 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. Immer mehr Komponenten sind in industriellen Netzwerken miteinander vernetzt und machen deshalb ein leistungsstarkes, skalierbares Netzwerk-Management-System – wie SINEC NMS – unverzichtbar. Nur so kann man die enormen Datenmengen meistern und das Netzwerk optimale Leistung bringen.

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 mit mehreren Zehntausend Geräten 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

- Schnelle und einfache Fehlerlokalisierung
- Exakte Statusübersicht für schnelle Reaktion im Fehlerfall
- Maximale Transparenz durch Strukturierung des Netzwerks
- Zuverlässige Diagnose dank zentraler Auswertung der Netzauslastung

## Configuration Management

- Zeiteinsparung durch zentrale, regelbasierte Konfiguration und Wartung des gesamten Netzwerks
- Einfaches und zentrales Sichern und Verwalten von Gerätekonfigurationen
- Reduzierter Aufwand für das Überprüfen und Aktualisieren von Firmware-Versionen

## Accounting Management

- Umfassender Überblick durch Gesamtübersicht aller Netzwerkkomponenten
- Zuverlässige Überwachung der Netzwerktopologie
- Erhöhte Sicherheit dank Netzwerk- und Ereignisdokumentation

## Performance Management

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

## Security Management

- Zuverlässige Erfüllung prozessualer und technischer Sicherheitsanforderungen gemäß IEC 62443
- Erhöhte Netzwerksicherheit aufgrund zentraler, regelbasierter Firewall-Konfigurationen
- Verbesserte Sicherheit durch definierte Benutzerverwaltung
- Zentrale Netzwerkdokumentation mit regelbasierten Reports, z. B. für Audits

# Netzwerkmanagement weitergedacht

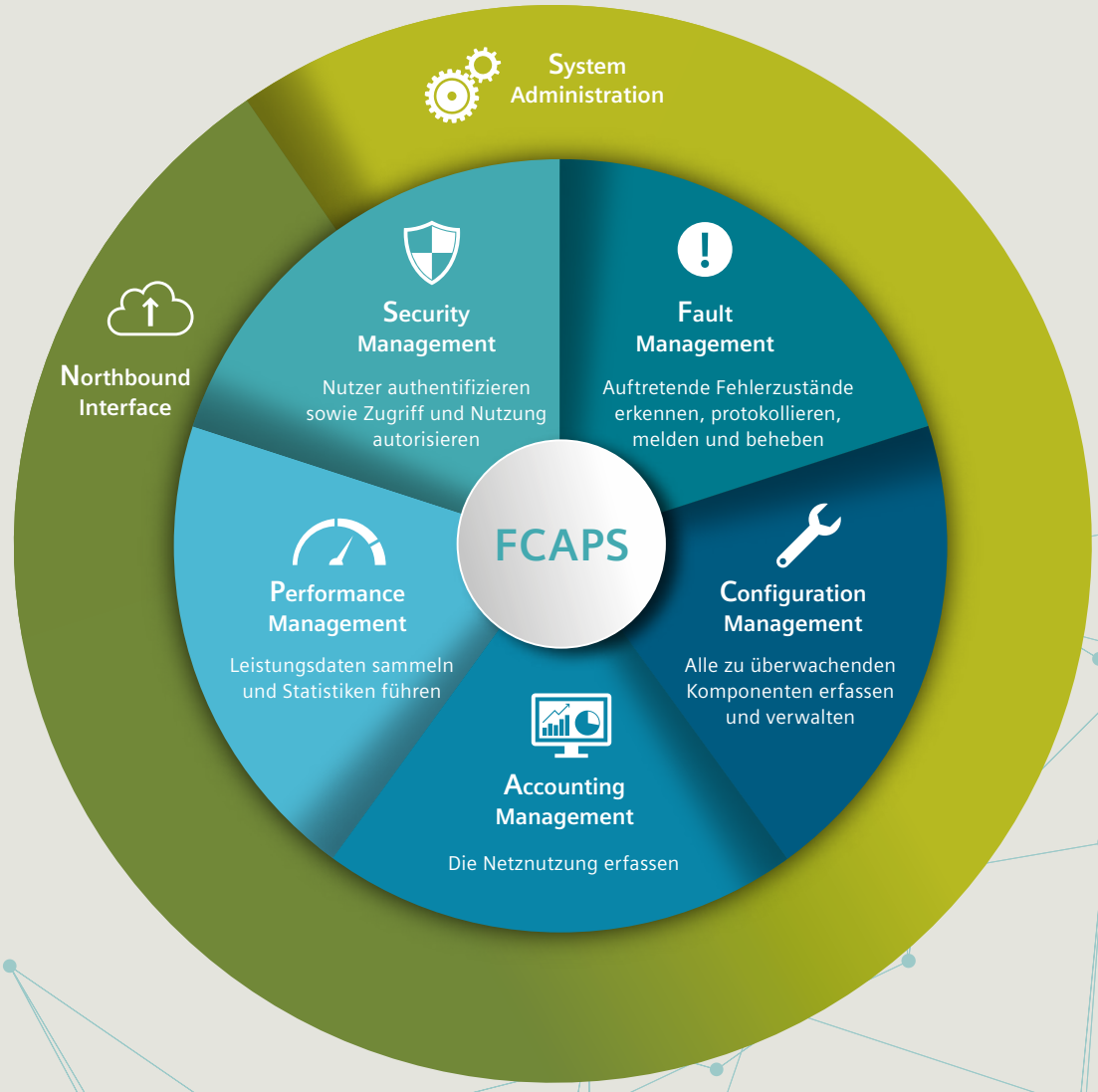
SINEC NMS bietet noch weit mehr als FCAPS: Denn mit zwei essenziellen Systemelementen adressiert es explizit die speziellen Anforderungen an industrielle Netzwerke. Damit wird unser Angebot für OT-Netzwerke vervollständigt.

## 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 des Netzwerks – unabhängig von dessen Größe und Komplexität
- Zentrale Inbetriebnahme und Verwaltung der verteilten SINEC NMS Operations im SINEC NMS Control
- Effiziente Rollen- und Rechteverwaltung



# Erste Wahl für komplexe Netzwerkstrukturen

Mit SINEC NMS lassen sich neue Geräte einfach ins Netzwerk integrieren sowie bestehende überwachen und konfigurieren. Die Konfiguration erfolgt regelbasiert, kann also übergreifend auf mehrere Teilnehmer angewendet werden. Das sorgt vor allem bei großen Netzwerken für deutlichen Zeitgewinn bei Konfiguration und Fehlersuche, z. B. für SCALANCE- und RUGGEDCOM-Geräte.

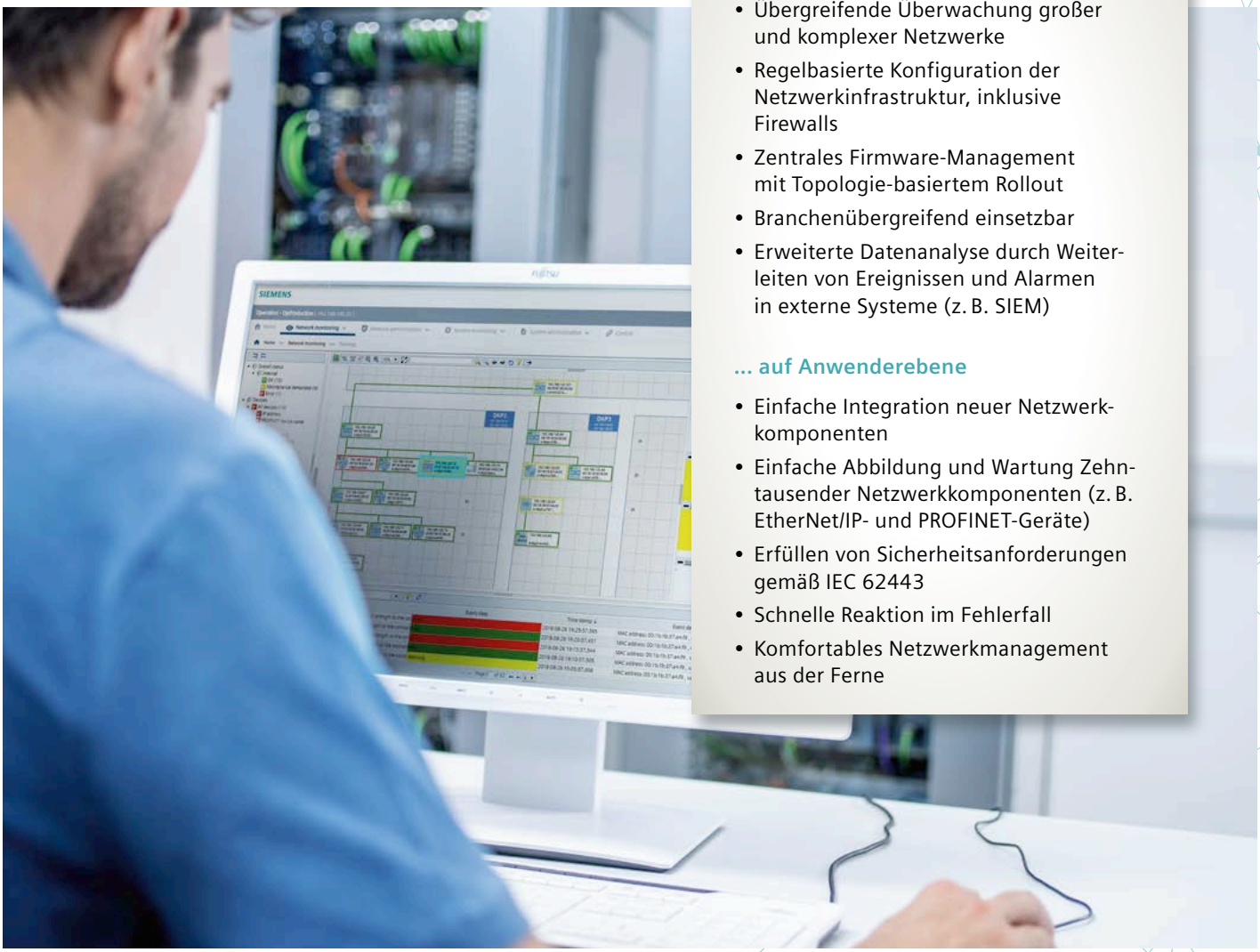
## VORTEILE ...

### ... auf Unternehmensebene

- Übergreifende Überwachung großer und komplexer Netzwerke
- Regelbasierte Konfiguration der Netzwerkinfrastruktur, inklusive Firewalls
- Zentrales Firmware-Management mit Topologie-basiertem Rollout
- Branchenübergreifend einsetzbar
- Erweiterte Datenanalyse durch Weiterleiten von Ereignissen und Alarmen in externe Systeme (z. B. SIEM)

### ... auf Anwenderebene

- Einfache Integration neuer Netzwerkkomponenten
- Einfache Abbildung und Wartung Zehntausender Netzwerkkomponenten (z. B. EtherNet/IP- und PROFINET-Geräte)
- Erfüllen von Sicherheitsanforderungen gemäß IEC 62443
- Schnelle Reaktion im Fehlerfall
- Komfortables Netzwerkmanagement aus der Ferne



**Herausgeber**
**Siemens AG**

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Deutschland

Artikel-Nr.: DIPA-B10076-00
Dispostelle 06366
WS 11190.0
© Siemens 2019
siemens.de/sinec-nms

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 **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 **siemens.com/industrialsecurity.**