SIEMENS

Fachartikel

Netzwerkmanagement 4.0 für die digitale Fabrik

Cockpit für das Nervensystem der digitalen Fabrik

Kommunikationsnetzwerke in der Industrie müssen besonders hohe Anforderungen erfüllen. Ein zukunftssicheres und effizientes Netzwerkmanagement wird deshalb für jedes Industrieunternehmen, das langfristig erfolgreich sein will, zu einem unverzichtbaren Kernelement.

Industrielle Kommunikationsnetzwerke in der digitalen Fabrik unterscheiden sich dabei erheblich von gewöhnlichen Netzwerken, wie sie uns aus dem Büroumfeld bekannt sind. Deshalb ist eine Differenzierung zwischen IT (Information Technology)- und OT (Operational Technology)-Netzwerken wichtig. Zwar handelt es sich in beiden Fällen um Kommunikationsnetzwerke mit einer hohen Anzahl an Teilnehmern. Jedoch kommen in der IT-Umgebung eher Endgeräte wie Desktop- und Tablet-PCs, Voice-over-IP-Telefone, Drucker oder Multifunktionsgeräte zum Einsatz, die sich unter gemäßigten Umweltbedingungen in Innenräumen wie Büros oder Hallen befinden. Der Anwendungsbereich bei OT hingegen liegt insbesondere auf Ebene der Produktion und im sogenannten Industrial Backbone bis hin zum sogenannten Field Level (Feldebene) – also in anspruchsvollen Industrieumgebungen mit grundlegend anderen Applikationen. Dafür ist zum einen unabdingbar, dass die Hardware höchst robust, hitze- wie kältebeständig sowie wasser- und staubresistent ist. Zum anderen sind die Maschinen und Anlagen in unterschiedlichen Subnetzen z. B. über Switches, Router oder IWLAN (Industrial Wireless LAN)-Komponenten miteinander verbunden und müssen echtzeitfähige, deterministische, redundante und somit höchst zuverlässige Kommunikation sicherstellen. Vorausschauende Planung und schnelle Reaktionszeiten sind in der Industrie wichtiger als in anderen Bereichen, da bei Störungen oder Ausfällen im Netzwerk die Gefahr besteht, dass die Produktion stillsteht. Das verursacht immense Kosten. Höchste Verfügbarkeit des Netzwerkes hat demnach oberste Priorität.

FCAPS 4.0 mit 5 bestehenden Elementen und zwei umfassenden, übergreifenden Erweiterungen zu „System Administration" sowie „Northbound Interface"

So liegt es auf der Hand, dass solche speziell für die Industrie entwickelten Netzwerkkomponenten auch ein besonderes Netzwerkmanagement erfordern, das exakt auf die Bedürfnisse der Industrie abgestimmt ist.

FCAPS-Modell für mehr System in einer immer komplexeren Welt

Es gibt unterschiedliche Ansätze auf dem Markt, wie man den Herausforderungen der Digitalisierung auf der Netzwerkebene begegnen kann. So finden sich proprietäre Lösungen, branchenspezifische Antworten oder spezielle Bausteine für mehr oder weniger komplexe Netzwerkstrukturen.

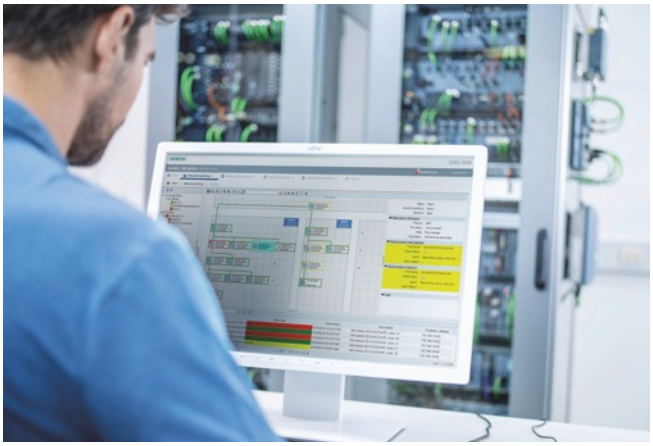
Was die meisten modernen Netzwerk-Management-Systeme (kurz NMS genannt) vereint, sind die fünf von der ISO (International Organization for Standardization) definierten Eckpfeiler des sogenannten FCAPS-Modells. Erstens „Fault Management", für eine einfache und schnelle Fehlerlokalisierung. Zweitens „Configuration Management" für Zeit- und Aufwandsersparnis durch zentrale Konfiguration und Wartung des gesamten Netzwerkes. Drittens „Accounting Management" für Sicherheit durch Prüfung des Netzwerkes und zuverlässige Dokumentation der Ereignisse. Viertens „Performance Management" für Flexibilität durch Netzwerkoptimierung, Transparenz durch Statistikerstellung sowie hohe Verfügbarkeit durch permanente Überwachung des Netzwerkes. Fünftens „Security Management" für erhöhte Netzwerksicherheit, durch die Verwaltung prozessualer und technischer Sicherheitsanforderungen gemäß IEC 62443 (z. B. Definition von Backup-Policies oder UMAC).

Da die verschiedenen Netzwerk-Management-Systeme demnach ähnlich aufgebaut sind, ist es auf den ersten Blick nicht leicht zu erkennen, wodurch sich NMS auszeichnen, die besonders gut für die Herausforderungen der digitalen Fabrik geeignet sind.

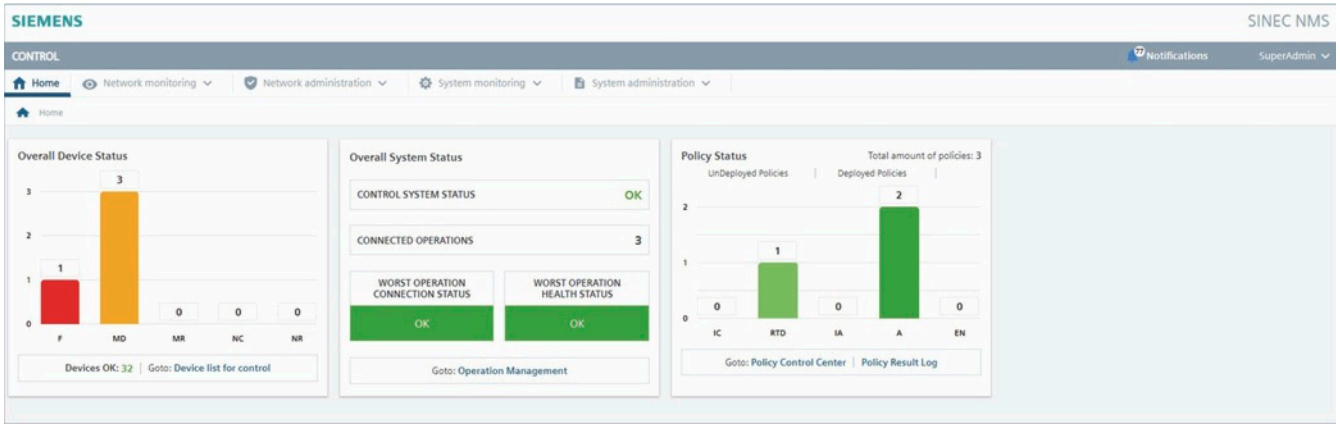
Die neue Lösung von Siemens, SINEC NMS, dient als anschauliches Beispiel zur Erläuterung wesentlicher Merkmale. Denn sie ist Vorreiter, branchenübergreifend in allen Industrien einsetzbar und skalierbar. Dieses NMS vereint in einem System die wichtigsten Aspekte, die im Kontext von Netzwerkmanagement im Umfeld von Industrie 4.0 immer wieder gefordert werden: Man kann damit industrielle Netzwerke jeder Größenordnung vollständig darstellen, zentral und komfortabel überwachen, verwalten und regelbasiert konfigurieren.

Mehr als ein Standard-Netzwerkmanagement

Speziell für die hohen Ansprüche von Netzwerken in der digitalen Fabrik hat Siemens das FCAPS-Modell erweitert. Das unterscheidet SINEC NMS bedeutend von anderen NMS. Das übergreifende Element „System Administration" umfasst die drei Aspekte: Operation-Management, Systemskalierbarkeit und Benutzerverwaltung. Kernaspekt ist hier der verteilte, dezentrale Ansatz mit ganzheitlicher Sicht auf das Netzwerk, unabhängig von dessen Größe. Dieser ermöglicht, dass das Netzwerkmanagement flexibel auf die Komplexität sowie die individuellen Bedürfnisse des jeweiligen Anlagennetzwerkes angepasst werden kann. Das System wächst skalierbar mit dem Netzwerk, von 50 bis zu 12.500 Teilnehmern. Hierfür ist SINEC NMS in die übergeordnete Ebene Control und mehrere verteilte, unterlagerte Operations aufgeteilt. Control ist die zentrale Instanz in SINEC NMS, die übersichtlich und schnell den Gesamtstatus des Netzwerkes anzeigt. Im Control werden die untergeordneten SINEC NMS Operations-Ebenen zentral in Betrieb genommen und verwaltet. Mit der zentralen Benutzerverwaltung lassen sich Rollen und Zugriffsrechte effizient einrichten, bearbeiten und verwalten. Beispielsweise in einer lokalen Benutzerverwaltung. Alternativ können bestehende Nutzer aus einer zentralen Benutzerverwaltung wie RADIUS oder Active Directory über User Management Component (UMC) übernommen werden. Die SINEC NMS Operations wiederum sind im Netzwerk verteilt und haben die Aufgabe, die Netzwerkgeräte zu erkennen sowie die jeweiligen Informationen aus ihnen auszulesen. Sie setzen zudem die Konfigurationsvorgaben aus der Control-Ebene auf alle Teilnehmer um.



Zentrales Firmware-Management mit Topologie-basiertem Rollout spart enorm viel Zeit und ist kein Problem mehr mit SINEC NMS



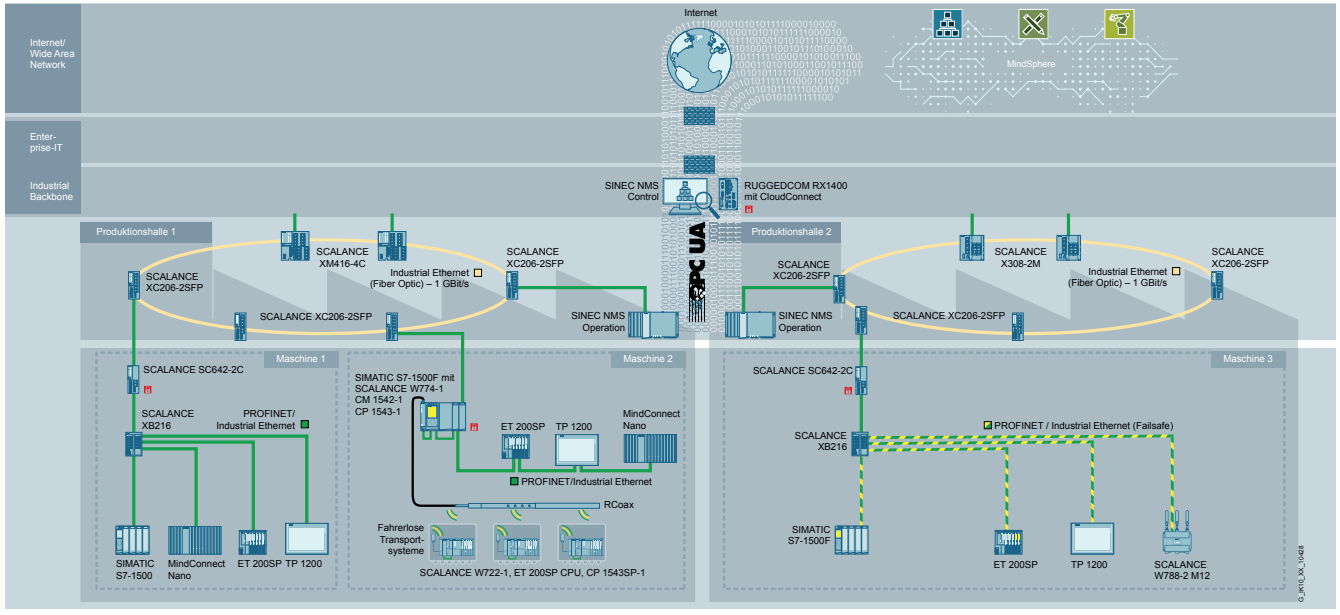
Mit SINEC NMS Control hat man den Gesamtstatus des Netzwerkes immer im Blick

Die intelligente Konfiguration der Netzwerkinfrastruktur und -geräte, die die Erfordernisse der Automatisierungslösung optimal abbildet, spielt eine entscheidende Rolle, um bei der Produktion wertvolle Zeit einzusparen und die Produktivität zu steigern. Insbesondere bei Netzwerken mit einer hohen Anzahl an Komponenten kostet es enormen Aufwand, die einzelnen Netzwerkteilnehmer zu konfigurieren und Anomalien im Netzwerk ausfindig zu machen. SINEC NMS arbeitet mit einer regelbasierten Konfiguration der Netzwerkinfrastruktur. Das bedeutet, dass sich z. B. bestehende Geräte im Netzwerk ausgehend von definierten Regeln, die durch den Administrator individuell eingestellt werden können, kontinuierlich konfigurieren und warten lassen. Das spart erheblich Zeit und Kosten. Die sogenannten Policies werden dabei übergreifend auf eine bestimmte Auswahl an Komponenten angewendet. Konfigurationen lassen sich mit diesem regelbasierten Ansatz geräteübergreifend und unabhängig von Gerätetypen vornehmen. Beispielsweise können Nutzer auf diese Weise komfortabel die Passwörter für den Zugriff auf die Geräte verändern.

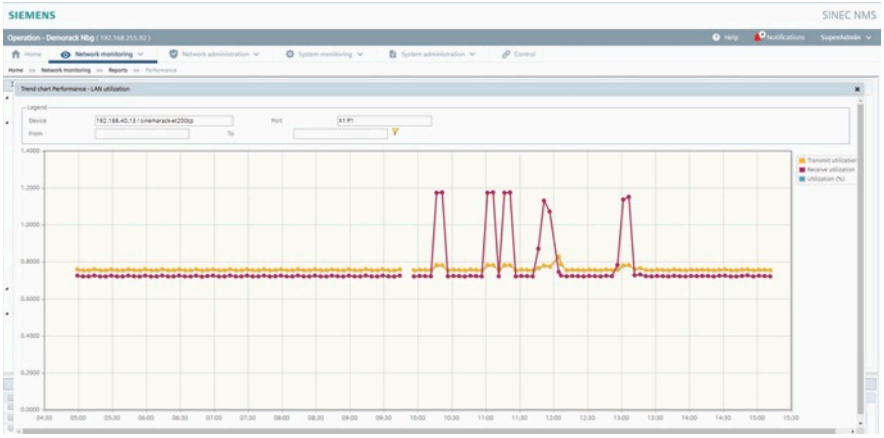
Auch neue Komponenten lassen sich mithilfe von zuvor festgelegten Regeln einfach und schnell ins Netzwerk integrieren. Mithilfe von regelmäßigen Back-ups der Gerätekonfigurationen werden Konfigurationsänderungen schnell erkannt. Das erleichtert erheblich die Fehlersuche. Durch die regelbasiert umgesetzten Massenkonfigurationen lassen sich fehlerhafte Konfigurationen außerdem verringern. Auch für Updates der Firmware sind Massenkonfigurationen hilfreich. In SINEC NMS ermöglicht ein zentrales Firmware-Management mit Topologie-basiertem Rollout beispielsweise, zentral ein Firmware-Update in der Netzwerkinfrastruktur auszurollen, wahlweise für einzelne oder mehrere Netzwerkkomponenten.

Tor zwischen zwei Welten

Die zweite Erweiterung, wodurch sich SINEC NMS von anderen Netzwerk-Management-Systemen abhebt, ist das sogenannte „Northbound Interface“. Dieses umfasst gleichermaßen wie „System Administration“ übergreifend das gesamte Netzwerk-Management-System. Das „Northbound



„Northbound Interface“ verknüpft Produktionsnetzwerk mit IT und Cloud-Applikationen zum nahtlosen Datenaustausch



SINEC NMS Operation: Über den Bereich „Performance Management“ können Leistungsdaten gesammelt und über Statistiken ausgewertet werden – zur kontinuierlichen Überwachung und damit Optimierung des Netzwerkes

Interface“ schafft die Verknüpfung zwischen den zwei Welten: OT-Produktionsnetzwerk und IT-Netzwerk. Die auf OT-Ebene durch das industrielle NMS vorverarbeiteten Daten aus der Produktion können über „Northbound Interface“ komfortabel an die IT-Ebene zur Weiterverarbeitung übermittelt werden. So lassen sich die Informationen aus der Netzwerkdiagose des Produktionsnetzwerks nahtlos in verschiedene HMI- und SCADA-Systeme sowie Applikationen wie WinCC oder SIMATIC PCS 7 integrieren.

Technisch erfolgt dies zum einen über das OPC UA-Serverinterface. Netzwerkinformationen werden dabei via Ethernet-basierten und somit plattform- und herstellerunabhängigen Kommunikationsstandard OPC UA (Open Platform Communications Unified Architecture) für andere OPC UA-Anwendungen bereitgestellt. Alternativ können überlagerte HMI-Systeme komfortabel über URL-Zugriffe direkt auf die überwachten Netzwerk- und Diagnosedaten zugreifen.

Hinzu kommt das ausgereifte Benachrichtigungs-Management von SINEC NMS. Dadurch lassen sich die Reaktionszeiten erheblich verkürzen, da auftretende Ereignisse unmittelbar gemeldet werden. Dabei kann zwischen System- und E-Mail-Benachrichtigungen unterschieden werden. Erstere informieren den Anwender direkt im System auf der Benutzeroberfläche über aktuell anstehende Probleme im Netzwerk. Mittels Quick-Links wird der Anwender dann direkt zur entsprechenden Stelle geführt. Alternativ lassen sich Benachrichtigungen auch via E-Mails versenden, die basierend auf zuvor definierten Ereignissen ausgelöst werden.

Fazit

Diese Merkmale zeigen anschaulich, was ein leistungsstarkes und zukunftssicheres industrielles Netzwerk-Management-System kennzeichnet. Es ist Wegbereiter für die digitale Transformation in der Industrie und somit Voraussetzung für eine erfolgreiche digitale Fabrik in allen Branchen.

Um dort langfristig Sicherheit und Verfügbarkeit der Daten zu gewährleisten, ist nicht nur eine professionelle Netzwerkplanung und -realisierung, sondern auch geschultes Personal notwendig. Siemens bietet als erfahrener Lösungsanbieter umfassende Gesamtlösungen für industrielle Netzwerke im Zusammenspiel aus Komponenten, Software, Schulungen, Service und Support an.

Security-Hinweise

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. Weitergehende Informationen über Industrial Security finden Sie unter **https://www.siemens.com/industrialsecurity**

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

PDF
Fachartikel
FAV-IEE-219
BR 0219 / 4 De
Produced in Germany

siemens.de/sinec-nms