Digitalisierung braucht Netzwerke.

Und damit Netzwerk-Management-Systeme.

Komplexe Netzwerke als Herausforderung

In den Chefetagen der Welt wächst das Bewusstsein, dass Daten eine elementare Ressource für Wettbewerbsfähigkeit und dauerhaften Erfolg in der Industrie sind. Kein Wunder also, dass die Digitalisierung in allen Branchen unaufhaltsam voranschreitet – unabhängig von der Unternehmensgröße. Wer jedoch das ganze Potenzial digitaler Daten voll ausschöpfen will, braucht entsprechende Netzwerke: leistungsstark, sicher, hochverfügbar sowie idealerweise leicht zu konfigurieren und zu überwachen.

Denn mit der Forderung nach umfassender Konnektivität nimmt sowohl die Zahl der kommunizierenden Teilnehmer als auch die Datenmenge zu. Mit anderen Worten: Netzwerke werden immer komplexer. Deshalb wird der Ruf nach effizientem Netzwerkmanagement selbstverständlich immer lauter. Als Wegbereiter für die digitale Transformation in der Industrie treibt Siemens den Fortschritt auf diesem Gebiet kontinuierlich voran – für Lösungen, die den Anforderungen einer digitalen Welt gerecht werden.

Transparenz trotz Komplexität

Mit der zunehmenden Komplexität industrieller Netzwerke wird es für Betreiber immer wichtiger, ein Höchstmaß an Transparenz sicherzustellen: Zu wissen, welche Komponenten wo im Einsatz sind und wie sie arbeiten, ist zwingend erforderlich für effizientes Netzwerkmanagement und essentiell für die Sicherheit und Verfügbarkeit von Daten.
Deshalb sollte ein zeitgemäßes Netzwerk-Management-System (NMS) benutzerfreundlich sein und die Möglichkeit bieten, alle Netzwerkkomponenten auf einen Blick zu überwachen und mit minimalem Aufwand zu verwalten – rund um die Uhr, herstellerübergreifend und unabhängig von der Knotenanzahl, die im Rahmen der Digitalisierung ohnehin stetig weiter zunehmen wird.
Das erklärt auch, warum Skalierbarkeit ein großes Thema ist: NMS-Lösungen müssen in der Lage sein, mit dem Netzwerk zu wachsen. Zudem bieten skalierbare Systeme den großen Vorteil, dass Unternehmen nicht vom Start weg in eine Komplettlösung investieren müssen, sondern mit einer kleinen Lösung einsteigen und diese sukzessive ausbauen können.
Wichtig in diesem Zusammenhang ist das Thema Northbound-Schnittstelle: NMS-Lösungen müssen die Anbindung von Netzwerken an moderne Cloud-Lösungen unterstützen – etwa an MindSphere, dem cloudbasierten, offenen IoT-Betriebssystem von Siemens.

Die Liste an Anforderungen, die ein zukunftssicheres NMS erfüllen muss, ist lang. Dadurch bietet es aber auch eine Fülle von Vorteilen.

Stillstandzeiten minimieren

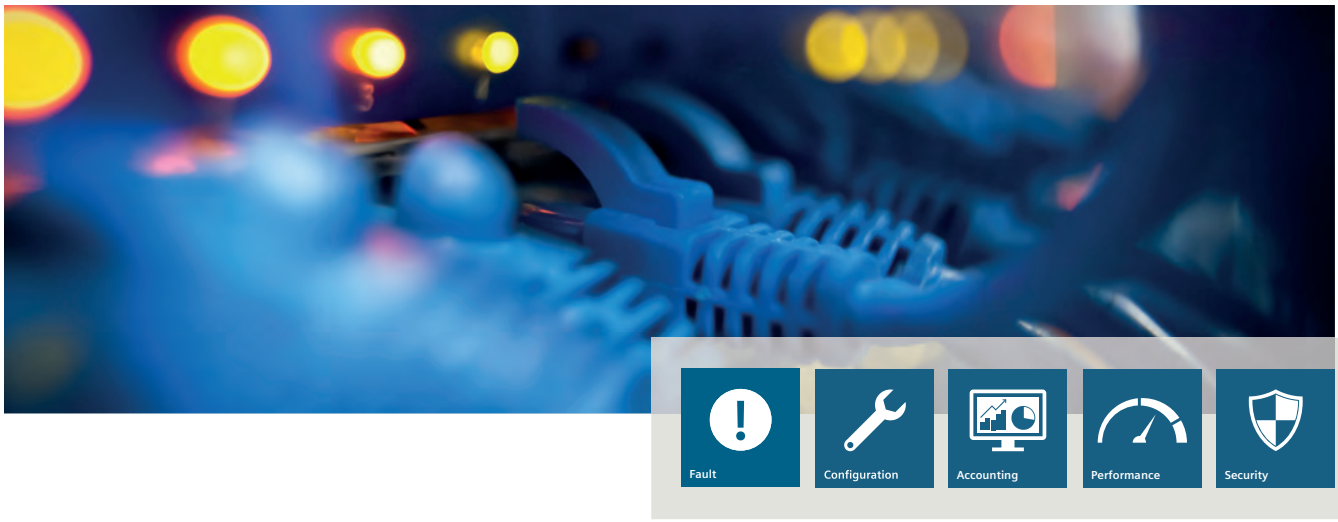
Auch wenn die Statistik sagt, dass Störungen und Ausfälle nur zu einem geringen Anteil von Netzwerkkomponenten wie Switches verursacht werden: Der Fall der Fälle lässt sich nie ganz ausschließen. Tritt er tatsächlich ein, ist es kosteneffizient, die Fehlerquelle so rasch als möglich zu lokalisieren und zu korrigieren.
Genau das ermöglicht ein NMS – ebenso wie die Fehlerprophylaxe: potenzielle, zukünftige Probleme aufspüren und mittels präventiver Maßnahmen beheben, bevor Schaden entstehen kann. Auf diese Weise bleibt immer alles am Netz – und die Gefahr eines unplanmäßigen Stillstands wird minimiert.

Betriebsbereitschaft sicherstellen

Dass die Komponentenlandschaft innerhalb eines Netzwerks in der Regel sehr heterogen ist, liegt nicht nur an den unterschiedlichen Hardwarekategorien von meist mehr als einem Hersteller. Auch hinsichtlich bestehender Softwarekonfigurationen und deren Verteilung gibt es oft große Unterschiede.

Eine Bestandsführung dieser Faktoren ist wichtig. Denn für dauerhaft reibungslosen Netzbetrieb müssen Hardware und Programmierungsänderungen koordiniert werden – gemäß der jeweiligen Firmware-Policy und der branchenspezifischen Besonderheiten. Als Beispiel die Prozessindustrie: Um Regressansprüche von vornherein auszuschließen, werden Systeme vom TÜV abgenommen. Deshalb sind Updates hinsichtlich der Softwareversionen eher selten. Ganz anders in der Fertigungsindustrie, bei der Energieversorgung oder bei öffentlichen Infrastrukturen: Hier kommt prinzipiell nur die neueste Software zum Einsatz, durch die Vorgabe aus den Security-Richtlinien der Betreiber, immer die neuesten Updates zu verwenden.

In jedem Fall ist die Koordination aller Assets in einem Netzwerk sehr anspruchsvoll. Aus diesem Grund finden sich am Markt diverse Tools, die Hilfe versprechen. Dabei handelt es sich aber in der Regel um Insellösungen, die nicht integraler Bestandteil eines umfassenden NMS sind.



Doch genau danach wird verlangt: nach einer ganzheitlichen NMS-Lösung, die die Dokumentation des kompletten Inventars stets aktuell hält – die alle relevanten Netzwerkkomponenten erfasst, neue Hard- und Software hinzufügt sowie bestehende Systeme modifiziert. Am besten ganz einfach per Knopfdruck.

Benutzer verwalten

Mit der Ausdehnung eines Netzwerks steigt meist auch die Anzahl der Teilnehmer. Damit werden Informationen rund um die Nutzung der Netzwerkressourcen immer wichtiger:
Wer hat wann und wie lange welche Ressource verwendet? Ein NMS muss hierauf verlässliche Antworten liefern und die Zuteilung von Rollen und Aufgaben durch die Vergabe von Berechtigungen ermöglichen.
Durch die Möglichkeit, die verschiedenen Benutzer spezifisch mit Rechten auszustatten, ist ein Missbrauch der Zugriffsberechtigungen bei der Netzwerkkonfiguration ausgeschlossen.

Leistung optimieren

Die Leistungsfähigkeit eines Netzwerks hat direkten Einfluss auf die Qualität der Geschäftsprozesse – und damit auf die Wettbewerbsfähigkeit eines Unternehmens. Deshalb ist es von immenser Bedeutung, die allgemeine Leistung im Netzwerk mittels eines ausgereiften NMS kontinuierlich zu optimieren: den Durchsatz zu maximieren, Flaschenhälse zu vermeiden und potenzielle Probleme zu identifizieren. Ziel ist es in jedem Fall, maximale Performancegewinne zu erzielen.

Hierzu wird in einem ersten Schritt die Netzauslastung ermittelt und analysiert. Das bedeutet: Unmengen statistischer Daten werden gesammelt und ausgewertet. Auf Basis der so gewonnenen Erkenntnisse lässt sich das Leistungsverhalten der Betriebsmittel bewerten und letztlich planvoll mittels gezielter Maßnahmen zu optimieren.

Cybergefahren minimieren

Angesichts ihrer Bedeutung für die gesamte Unternehmensperformance hat es oberste Priorität, industrielle Netzwerke zuverlässig vor potenziellen Cyberbedrohungen zu schützen. Dabei ist die Liste möglicher Gefahrenquellen lang. Ob kriminelle Hackerangriffe, unautorisierter Zugriff oder physische und elektronische Sabotage: In jedem Fall droht enormer Schaden, der unter allen Umständen vermieden werden muss. Auch hierbei spielt ein funktionierendes NMS eine zentrale Rolle:
Es sorgt für höchste Datensicherheit und bezieht dabei alle an der Kommunikation beteiligten Komponenten in die Schutzmaßnahmen ein.
Hierzu speichert ein NMS sämtliche Zugangsdaten zur Geräteauthentifizierung, wie User-IDs und Passwörter, protokolliert alle Operator-Aktionen und sorgt für eine zentrale Verwaltung aller Sicherheitsfunktionen.

Das NMS von morgen

Damit ein NMS all das Genannte leisten kann, muss es entsprechende funktionale Aufgaben erfüllen. Die Eckpunkte des heutigen Netzwerkmanagements definiert FCAPS, ein Modell der ISO (International Organization for Standardization).

FCAPS steht für:

- **F**ault Management: auftretende Fehlerzustände erkennen, protokollieren, melden und beheben
- **C**onfiguration Management: alle zu überwachenden Komponenten erfassen und verwalten
- **A**ccounting Management: die Netznutzung erfassen
- **P**erformance Management: Leistungsdaten sammeln und Statistiken führen
- **S**ecurity Management: Nutzer authentifizieren sowie Zugriff und Nutzung autorisieren

Der Trend zu Digitalisierung und Industrie 4.0 zeigt die Bedeutung eines leistungsstarken und zukunftssicheren NMS auf – vor allem im Hinblick auf die im **FCAPS**-Modell beschriebenen Funktionalitäten. Mehr noch: Siemens hat es sich zum Ziel gesetzt, mit seinen Innovationen das Thema Netzwerkmanagement speziell auf die Bedürfnisse der Automatisierung hin anzupassen und weiter zu optimieren.

Herausgeber
Siemens AG 2018

Process Industries and Drives
Postfach 48 48
90026 Nürnberg
Deutschland

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 Up-dates 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

Weitere Informationen unter:
siemens.de/netzwerkmanagement