SIEMENS

Fachartikel

Das industrielle Netzwerk 4.0

Software-Lösungen leisten einen entscheidenden Beitrag zur Kosteneinsparung

Die Digitalisierung generiert eine Vielzahl an Kundenvorteilen, stellt aber auch Herausforderungen an die industriellen Kommunikationsnetzwerke. Auch sicherheitsrelevante Standardisierungen, wie z. B. IEC 62443 oder IEC 61850 spielen eine zunehmend wichtigere Rolle und müssen für ein zukunftsfähiges industrielles Netzwerk berücksichtigt werden. Hierzu leisten Software-Lösungen einen entscheidenden Beitrag, um die Inbetriebnahme-Zeiten und die Wartungsphasen zu reduzieren.

Ein industrielles Netzwerk für unterschiedliche Anwendungen

Um das Ziel zu erreichen, Industrieunternehmen zukunftssicher zu machen, müssen neue Wege und Möglichkeiten geschaffen werden. Diese beginnen mit dem Ausbau der Vernetzung von Sensoren, die Produktiv-Daten für die weitere Verarbeitung an zentrale Datenbanken (z. B. Cloud) übertragen sollen oder auch die Flexibilität (z. B. Daten für unterschiedliche Anwendungen bereitstellen) steigern können. Dies sind nur zwei Beispiele, die sich durch die Digitalisierung entwickelt haben. Auch das Thema Virtualisierung darf in diesem Zusammenhang nicht außer Acht gelassen werden. Die Virtualisierung bietet den wesentlichen Vorteil, dass die industriellen Anlagen und generell die Anwendungen der Zukunft flexibler und skalierbarer werden. So können zum Beispiel neue Anwendungen einfach über weitere virtuelle Instanzen angelegt werden und mit den industriellen Anlagen Daten austauschen. Mit all diesen Themen muss sich auch ein industrielles Kommunikationsnetzwerk in Zukunft auseinandersetzen. Hinzu kommt der Bedarf, dass die industriellen Kommunikationsnetzwerke eine hohe Flexibilität und Anpassbarkeit anbieten müssen, um den Herausforderungen der Zukunft Rechnung zu tragen.

Zusammenwirken zwischen IT- und OT-Welt, so sparen Sie Investitionskosten in Ihren industriellen Anlagen.

Einhaltung der IEC-Standards

Allerdings kommen gerade in den industriellen Kommunikationsnetzwerken noch weitere Anforderungen hinzu. Denn in den unterschiedlichen Branchen existieren zusätzliche Standards (wie IEC 61158 / IEC 62443 im Bereich des Maschinenbaus, der Fertigungs- und Prozessindustrie oder IEC 61850 in den elektrischen Schaltanlagen), die einzuhalten sind. Diese Standards beinhalten auch Vorgaben, die sich gerade auf die Definition der Netzwerkarchitektur auswirken. So zum Beispiel aus der IEC 62443-Norm, wo das Thema strikte Netzwerktrennung zwischen dem Unternehmensnetzwerk (IT-Netzwerk) und dem Produktionsnetzwerk (Operational Technology (OT)-Netzwerk) beschrieben ist. Ein weiteres Beispiel ist die IEC 61850-Vorgabe, die entsprechende Kommunikationsprotokolle (wie MMS zur Datenkommunikation und GOOSE-Telegramme) festgelegt hat.

All diese Themen sind für die Erstellung einer Netzwerkinfrastruktur für ein industrielles Kommunikationsnetzwerk zu beachten. Darüber hinaus darf das Thema „Security" – also Netzwerksicherheit – natürlich nicht außer Acht gelassen werden. In vielen Fällen wird es jedoch vernachlässigt, weil es als zu umständlich und zu kompliziert eingeschätzt wird. Allerdings hat dies Gründe, weshalb derartige, sicherheitsbezogene Ansätze existieren, wie Benutzerverwaltung, verschlüsselte Datenprotokolle und sichere Authentifizierung. Aber im Vordergrund all dieser Security-Vorgaben steht in erster Linie der Schutz der industriellen Netzwerke vor unerlaubtem Zugriff und Manipulation.

Zusammenwirken zwischen IT- und OT-Welt

Ein weiterer Punkt, der auch in den industriellen Kommunikationsnetzwerken berücksichtigt werden muss, sind die zentralen „Unternehmenspolicies". Unternehmenspolicies sind Regeln und Vorgaben (z. B. das gewisse Ports gesperrt sein müssen, das Passwörter gewisse Sicherheitsmerkmale erfüllen, usw.), die durch die zentralen Netzwerkadministratoren für das Unternehmen festgelegt sind und die auch im industriellen Kommunikationsnetzwerk berücksichtigt werden müssen. Hierfür ist es notwendig, sich mit den Netzwerkadministratoren des Unternehmens abzustimmen und die Zuständigkeit der Netzwerkübergänge zwischen den IT- und OT-Netzwerken gemeinsam festzulegen. Security ist dabei ein nicht zu unterschätzender Erfolgsfaktor für die Digitalisierung.

Steht erst einmal das Netzwerkkonzept, dann geht es darum, sich über den Einsatz von Software- und Hardware-Produkten Gedanken zu machen. Es existiert eine Vielzahl von Herstellern am Markt, die Hardware-Komponenten (wie Switches, Router, Modems, Firewall, Wireless LAN Access Points) bis hin zu Software-Produkten (wie Netzwerk-Management-Systeme z. B. SINEC NMS zur Verwaltung der Hardware, RADIUS-Server für Geräte-Authentifizierung im Netzwerk oder Syslog-Server zur Transparenz der Vorkommnisse im Netzwerk) anbieten.

Bezogen auf die Hardware muss man erwähnen, dass zwischenzeitlich alle Hersteller ein umfassendes Produktportfolio mit einem sehr umfangreichen Feature-Set anbieten. Das heißt, dass sich die Hardware-Produkte kaum noch funktional voneinander unterscheiden. Vielmehr werden die Software-Lösungen in der Zukunft den Unterschied ausmachen.

Netzwerkmanagement für industrielle Netzwerke

Gerade zur Verwaltung der Netzwerke spielen insbesondere die Einfachheit der Bedienung (Reduzierung der Netzwerkkomplexität) und die Reduzierung der Betriebskosten (Operational Expenditure) eine nicht zu unterschätzende Rolle. Für die industriellen Kommunikationsnetzwerke ist nicht nur das Netzwerk selbst von Bedeutung, sondern vor allem auch die Endgeräte sind sehr wichtig. Denn nur zusammen mit den Endgeräten bekommt man einen gesamtheitlichen Überblick über die industriellen Anlagen und kann durch die zusammenhängenden Informationen einen frühzeitigen Ausfall erkennen und auch vorbeugen. Dies erreicht man, indem man die Netzwerkinformationen zusammen mit den Endgeräteinformationen in der Auswertung korreliert.

Allerdings gibt es gerade bei industriellen Anwendungen noch viele weitere Aspekte, die in diesem Zusammenspiel sehr wichtig sind. Zum einen wachsen industrielle Anlagen immer wieder, indem neue Maschinen installiert werden. Diese hat zur Folge, dass auch diese neuen Maschinen eingebunden und geprüft werden müssen: Wurde die Maschine nach den Vorgaben (wie IP-Adressen, Gerätenamen, richtige Firmware-Versionen installiert, ...) entsprechend konfiguriert? Der Aufwand der Prüfung ist heute teilweise sehr aufwändig und mit viel manueller Arbeit verbunden. Hier besteht immer häufiger der Wunsch, dass derartige Maschinen oder Anlagen automatisiert über ein Abnahmeprotokoll geprüft und dokumentiert werden können. Dazu kommt auch noch der Bedarf an Skalierbarkeit in den Software-Produkten: Damit auch im operativen Betrieb ohne große Aufwände weitere Maschinen eingebunden werden können.

Ein anderer wichtiger Punkt ist, eine komplette Inventarliste aller Geräte per Knopfdruck zu erhalten, das heißt eine zentrale Übersicht, welche Komponenten (z. B. Netzwerkkomponenten und Endgeräte) verbaut sind und welcher Firmware-Stand auf der jeweiligen Komponente installiert ist. Dies gilt nicht nur für einen einzelnen Hersteller, sondern herstellerübergreifend für alle Komponenten im industriellen Netzwerk.

Auch das Thema zentrales Firmware-Management darf man hier nicht außer Acht lassen. Hat man die Übersicht, welche Komponenten welche Firmware-Stände haben, kann man sehr schnell identifizieren, ob unerlaubte Firmware-Stände in den industriellen Anlagen im Einsatz sind oder wo Geräte auf den aktuellen Firmwarestand umgerüstet werden müssen.

SINEC NMS kann flexibel skalierbar industrielle Netzwerke jeder Größenordnung darstellen, zentral verwalten und regelbasiert konfigurieren – auch sicherheitsrelevante Aspekte.

Mit SINEC NMS erhöhen Sie die Produktivität ihrer industriellen Anlagen.

Aber bereits eine Phase früher, also vor dem laufenden Betrieb eines industriellen Netzwerkes, ändern sich bei den durch die fortschreitende Digitalisierung immer komplexer werdenden Netzwerken die Anforderungen. So wird im Bereich der industriellen Anlagen die Grundinitialisierung von Geräten immer mehr zur Herausforderung, weil die ersten erforderlichen Basiseinstellungen aufwändig einzeln für jedes neue Gerät vorgenommen werden. Das umfasst z. B. Vergabe von IP-Adresse, Gerätename, Aktivieren sowie Deaktivieren von SNMP oder Diensten (wie DHCP-Client, NTP-Client). Hier wünscht man sich kleine kompakte Helfer-Tools, die intuitiv zu bedienen sind und mit denen man schnell mehrere Geräte gleichzeitig parallel in Betrieb nehmen kann.

Das Tool SINEC PNI (Primary Network Initialization bzw. Netzwerkgrundeinstellungen) vereinfacht und reduziert die Zeitaufwände für die Erstinbetriebnahme von Netzwerkkomponenten in industriellen Netzwerken.

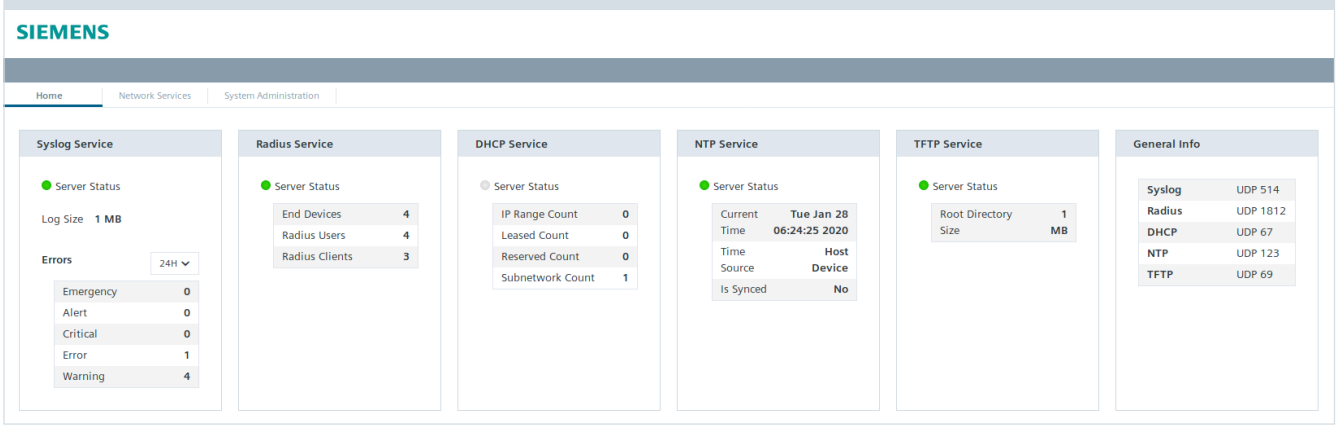
Einfache und schnelle Installation aller erforderlichen Services

Eine zunehmend wichtigere Rolle in den heutigen Security-Konzepten spielt auch ein sicherer Netzwerkzugang. Für den Zugang in das industrielle Netzwerk sollte sichergestellt werden, welche Anwendungen und Geräte überhaupt einen Zugriff erhalten sollen. Zum einen lässt sich der Zugriff von Anwendungen und Geräten über Firewalls zwischen den Netzwerksegmenten schützen oder man verwendet die Vorgaben aus dem Standard IEEE 802.1X, um den Zugriff von Geräten direkt in den industriellen Netzwerken zu regeln.

Ein ebenso wertiger Punkt aus Security-Sicht ist, die Ereignisse in den industriellen Anlagen zu verfolgen, um eventuelle Unregelmäßigkeiten in den industriellen Netzwerken zu identifizieren. Hierfür nutzt man vor allem „Syslog Messages“. Jede Komponente schickt Ihre Ereignisse (z. B. User A hat sich am Gerät B angemeldet am tt.mm.yyyy hh:mm:ss) an einen zentralen Syslog-Server. Dort werden alle Ereignisse gespeichert und können zur weiteren Analyse verwendet werden.

Hinzu kommt, dass man während des gesamten Lebenszyklus für die Instandhaltung und Pflege des Netzwerkes immer wieder bestimmte Netzwerkdienste für einen gesamtheitlichen Netzwerkansatz benötigt. Ein zentraler Infrastruktur-Server, der unterschiedliche Services in einer Instanz vereint, wäre hier optimal.

SINEC INS (Infrastructure Network Services bzw. Netzwerkinfrastrukturdienste) vereinfacht die Installation und Verwaltung aller erforderlichen Services eines industriellen Netzwerkes in einem Tool.



SINEC INS beinhaltet alle erforderlichen Services in einer Oberfläche und reduziert Aufwände für Installation und Verwaltung.

Fazit

Siemens hat mit der neuen Software-Familie SINEC die passende Antwort auf alle diese Themen in den unterschiedlichen Phasen rund um das industrielle Netzwerk parat. Von der Erstinbetriebnahme neuer Geräte bis zur Überwachung und dem Management eines komplexer werdenden Netzwerkes, einschließlich aller benötigten Software-Dienste, die für einen effizienten Netzwerkbetrieb notwendig sind. Besonders komfortabel ist hier, dass die Produkte skalierbar sind und miteinander interagieren. Das leistet einen wesentlichen Beitrag zur Reduzierung der OPEX (z. B. Einsparungen bei Wartungskosten) und macht Industrieunternehmen fit für die digitale Zukunft.

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 einen Bestandteil eines solchen Konzepts. Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **https://www.siemens.de/industrialsecurity**

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

PDF
Fachartikel
DI PA-1920-13
PDF 0420 5 De
Produced in Germany

siemens.de/sinec