SIEMENS

Technical Article

Network Management for the Digital Enterprise 4.0

Cockpit for the Digital Nervous System

Communication networks in industry must meet exceptionally high standards. Future-proof, efficient network management thus becomes an essential core element for any industrial company striving for success on a long-term basis.

Industrial communication networks in the digital enterprise differ greatly from the conventional networks familiar to us in the office environment. A differentiation between IT (information technology) and OT (operational technology) networks is therefore important. In both cases, these are communication networks with a high number of subscribers. In the IT setting, however, end-user devices employed are more likely to include desktop and tablet PCs, Voice over IP phones, printers, or multifunctional devices, which are located indoors with temperate environmental conditions – such as offices or halls. The scope of OT, in contrast, focuses on the production level – from the so-called industrial backbone to the field level, i.e. fundamentally different applications in demanding industrial environments. On the one hand, this requires hardware that is extremely rugged and resistant to heat, cold, water and dust. On the other hand, the machines and plants in the various subnets are interconnected, e.g. via switches, routers or IWLAN (Industrial Wireless LAN) components that must ensure real-time capable, deterministic, redundant and thus highly reliable communication. Predictive planning and quick response times are more important in industry than in other sectors, as there is a risk of production standstills in the event of network faults or outages – which causes immense costs. Accordingly, a network with maximum availability is a top priority.

FCAPS 4.0 with 5 existing elements and two comprehensive, universal enhancements – „System Administration" and „Northbound Interface"

Of course, such network components developed specifically for industry also necessitate special network management precisely tailored to the needs of industry.

FCAPS model for a more systematic approach in an increasingly complex world

There are different concepts in the market place on how to tackle the challenges of digitalization at the network level. These include proprietary solutions, industry-specific answers, or special building blocks for more or less complex network structures.

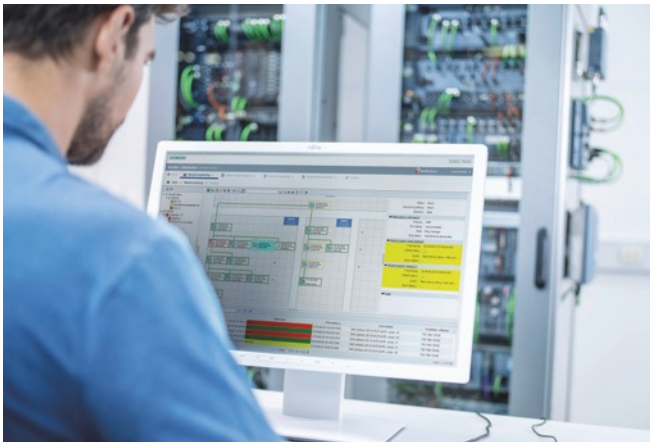
What unites most modern network management systems (NMS for short) are the five cornerstones of the so-called FCAPS model defined by the ISO (International Organization for Standardization). First, „Fault Management" for quick and easy fault localization. Second, „Configuration Management" for saving time and money through centralized configuration and maintenance of the entire network. Third, „Accounting Management" for security by testing the network and reliably documenting events. Fourth, „Performance Management" for flexibility through network optimization, transparency through the generation of statistics, and high availability through the continuous monitoring of the network. Fifth, „Security Management" for increased network security through the management of procedural and technical security requirements according to IEC 62443 (e.g. definition of backup policies or UMAC).

Since the various network management systems are similarly structured, it is difficult to see at first glance what distinguishes an NMS that is particularly well suited to the challenges of the digital enterprise.

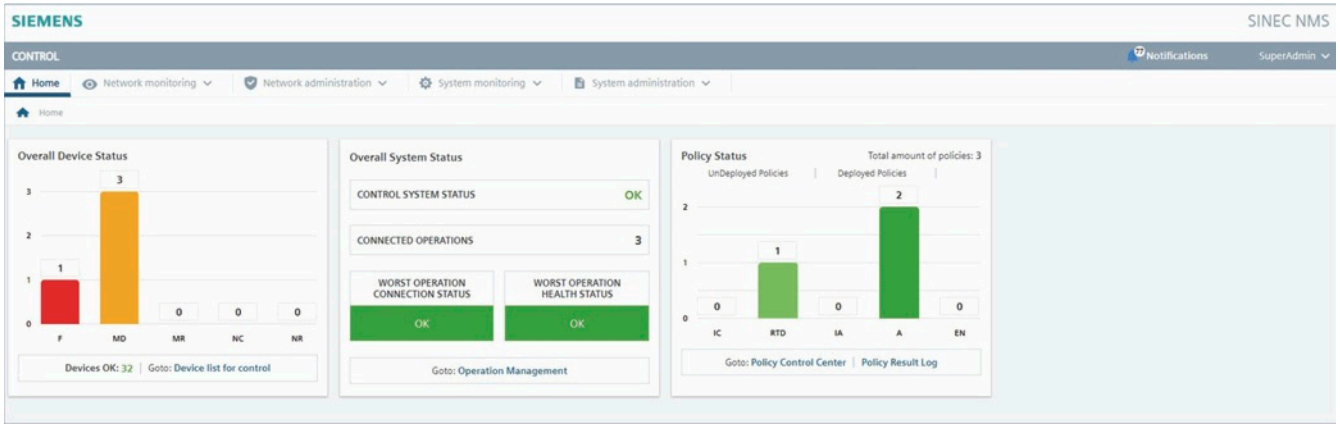
The new solution from Siemens, SINEC NMS, serves as an illustrative example to explain the main features. SINEC NMS is a trailblazer that can be used scalably across industries. This NMS unites in one system the most important aspects repeatedly requested in the context of network management concerning Industrie 4.0: It can fully depict industrial networks of any size, and centrally and conveniently monitor, manage and configure them on the basis of rules.

More than a standard network management system

Siemens has enhanced the FCAPS model especially for the high demands of networks in the digital enterprise. This greatly distinguishes SINEC NMS from other network management systems. The overarching „System Administration" element covers the three aspects of operation management, system scalability and user administration. The core aspect here is the distributed, decentralized approach with a holistic view of the network, regardless of its size. This approach makes it possible for network management to be flexibly adaptable to the complexity and individual needs of the respective plant network. The scalable system grows with the network, from 50 to 12,500 subscribers. For this, SINEC NMS is divided into the superordinate „Control" level and several distributed, subordinate "Operations". „Control" is the central instance in SINEC NMS which clearly and quickly displays the overall status of the network. In „Control", the subordinate SINEC NMS operation levels are centrally put into operation and managed. With central user administration, roles and access rights can be efficiently set up, edited and managed. For example, in a local user administration system. Alternatively, existing users can be taken from a central user administration system such as RADIUS or Active Directory by means of User Management Component (UMC). In turn, the SINEC NMS operations are distributed across the network and are tasked with recognizing the network devices and reading out the respective information from them. They also apply the configuration parameters from the control level to all subscribers.



Central firmware management with topology-based rollout saves a lot of time and is easily handled with SINEC NMS



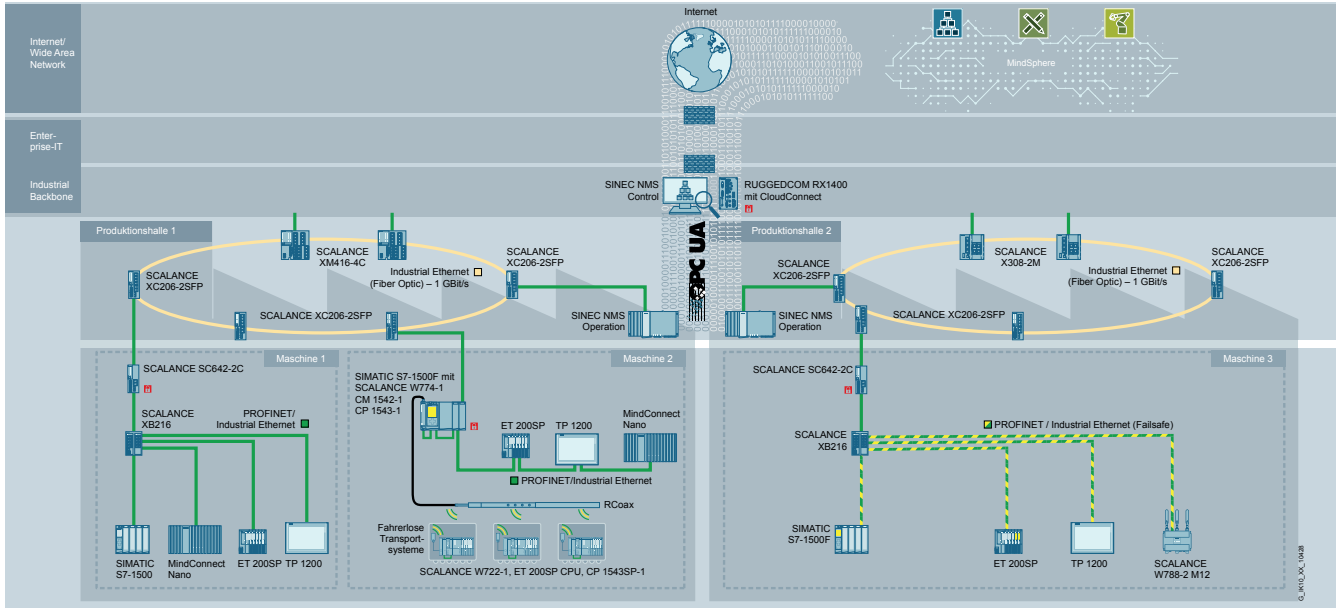
With SINEC NMS Control, the overall status of the network is always in sight

The intelligent configuration of the network infrastructure and devices, which optimally maps the requirements of the automation solution, plays a decisive role in saving valuable time during production and increasing productivity. In particular when it comes to networks with a high number of components, it requires enormous effort to configure the individual network subscribers and to trace anomalies in the network. SINEC NMS works with a policy-based configuration of the network infrastructure. This means that existing devices in the network, for example, can be continuously configured and maintained on the basis of defined rules, which can be individually set by the administrator. This saves considerable time and money. In doing so, the so-called policies are universally applied to a specific selection of components. Using this policy-based approach, configurations can be carried out across devices regardless of device type. For example, users can conveniently change the passwords for accessing the devices in this way. Even new components can be quickly and easily integrated into the network by means of the previously defined rules.

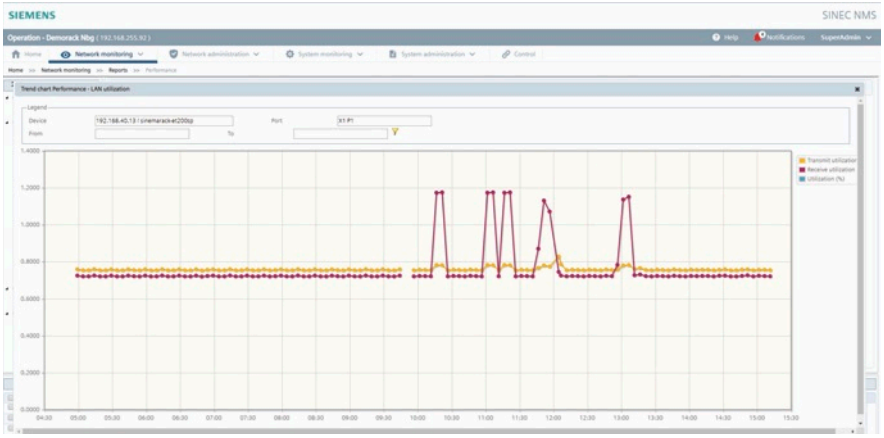
With the aid of regular backups of the device configurations, configuration changes can be quickly recognized. This greatly facilitates troubleshooting. Rule-based bulk configurations also help to reduce incorrect configurations. For firmware updates, too, bulk configurations are helpful. For example, in SINEC NMS, central firmware management with topology-based rollout enables the central rollout of a firmware update in the network infrastructure, either for single or multiple network components.

Gateway between two worlds

The second enhancement setting SINEC NMS apart from other network management systems is the so-called „Northbound Interface“. Like „System Administration“, it universally covers the entire network management system. The „Northbound Interface“ creates the link between the two worlds: OT production network and IT network. Via the „Northbound Interface“, the data from the production preprocessed on the OT level by the industrial NMS can be conveniently transmitted to the IT level for further processing.



„Northbound Interface“ links the production network with IT and cloud applications for seamless data exchange



SINEC NMS operation: Through the „Performance Management" area, performance data can be collected and evaluated via statistics – for the continuous monitoring and thus optimization of the network

In this way, the information from the network diagnostics of the production network can be seamlessly integrated into various HMI and SCADA systems as well as applications such as WinCC or SIMATIC PCS 7.

Technically, on the one hand, this is carried out via the OPC UA server interface. In doing so, network information is provided to other OPC UA applications via the Ethernet-based and thus platform- and manufacturer-independent communication standard OPC UA (Open Platform Communications Unified Architecture). Alternatively, higher-level HMI systems can conveniently and directly access the monitored network and diagnostic data by means of URL access.

Add to that the sophisticated notification management system of SINEC NMS. As a result, response times can be substantially shortened, since occurring events are immediately reported. A distinction can be made between system and email notifications. The former informs the user directly in the system's user interface about currently pending problems in the network. The user is then guided directly to the corresponding location by means of quick links. Alternatively, notifications can also be sent by email triggered on the basis of previously defined events.

Conclusion

These features clearly demonstrate what characterizes a powerful and future-proof industrial network management system. It is a pioneer for the digital transformation in industry and thus a prerequisite for a successful digital enterprise in all industrial sectors.

To ensure the long-term security and availability of the data there, not only professional network planning and implementation are required, but also trained personnel. As an experienced solution provider, Siemens offers comprehensive solutions for industrial networks by combining components, software, training courses, service and support.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept. For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity

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

PDF
Technical Article
FAV-IEE-219
BR 0219 / 4 En
Produced in Germany

siemens.com/sinec-nms