Digitalization requires networks.

And therefore Network Management Systems.

The challenge of complex networks

There is a growing recognition at management levels around the world that data is a fundamental resource for boosting competitiveness and achieving lasting success in the industry. It's thus no surprise that the progress of the digital transformation in all sectors has become unstoppable, regardless of company size. But anyone aiming to take full advantage of the potential offered by digital data needs the appropriate networks: powerful, secure, with high-availability and ideally easy to configure and monitor.

After all, the demand for end-to-end connectivity means an increase in both the numbers of communication participants and the volume of data. In other words, the networks are growing more and more complex. And this of course means that there is also an increasing demand for efficient network management. As a trailblazer for the digital transformation in industry, Siemens is constantly working to drive progress forward in this area, to achieve solutions that fit the needs of a digital world.

Transparency despite complexity

As industrial networks grow more and more complex, it will be increasingly important for operators to ensure maximum transparency: knowing which components are being used where, and how they function, is a vital prerequisite for efficient network management and essential for data security and availability. That's why a contemporary Network Management System (NMS) should be user-friendly and offer the opportunity of monitoring all network components at a glance and managing them with minimum effort – 24/7, regardless of vendor and regardless of the number of nodes, which will certainly continue to increase as the digital transformation progresses. It also explains why scalability is so important: NMS solutions must be capable of growing along with the network. In addition, scalable systems offer the major advantage that businesses do not have to invest in a complete solution right at the outset; they can begin with a small-scale solution and expand it over time. Northbound interfaces are important in this regard: NMS solutions must support the connection of networks to state-of-the-art cloud solutions, for example MindSphere, the cloud-based, open IoT operating system from Siemens.

There is a long list of requirements that a future-proof NMS must satisfy. The result, however, is that it can also offer a wealth of benefits.

Minimize downtimes

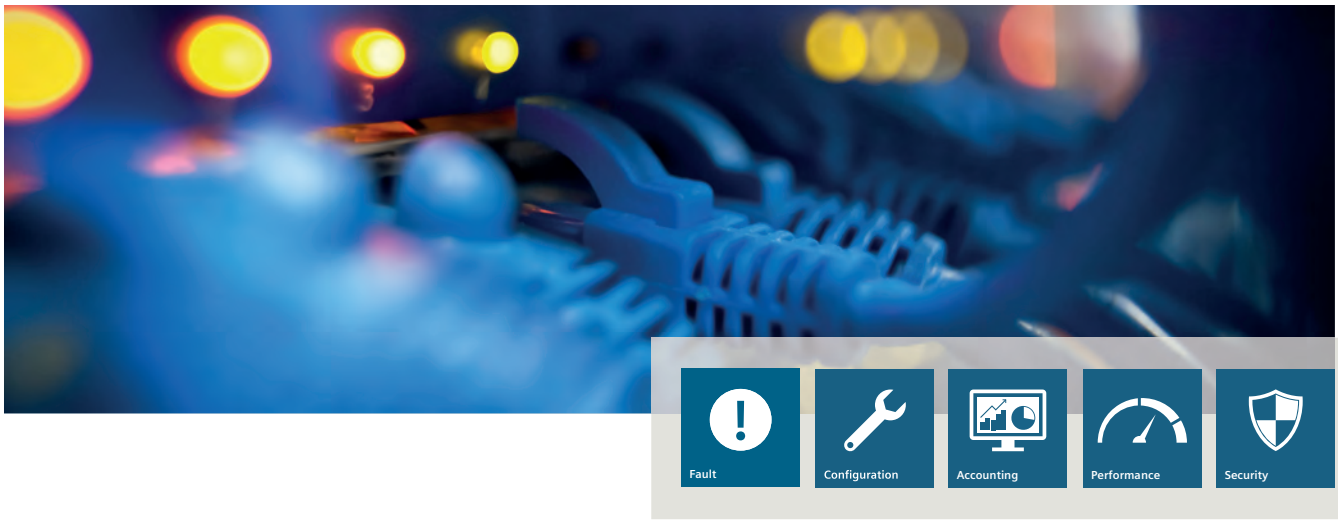
Even if the statistics show that only a small proportion of malfunctions and outages are caused by network components like switches, a worst-case scenario can never be entirely ruled out. And if it happens, the cost-efficient solution is to locate and fix the source of the error as swiftly as possible. An NMS makes this possible, along with error prevention: tracing potential future problems and taking preventive action before any damage occurs. This way, everything stays on the network at all times, and the risk of an unscheduled outage is kept to a minimum.

Ensure availability

The component landscape in any given network tends to be non-uniform, not only because network components represent a range of hardware categories, usually from more than one manufacturer but also because there are often major differences in terms of the existing software configuration and the way it is distributed. It is very important to document these factors.

After all, if networks are to operate smoothly for the long term, hardware and configuration changes must be coordinated – in accordance with the firmware policy and the specific characteristics of the industry in question. Take the process industry, for example: To avoid the risk of claims for compensation, systems are approved by the technical inspection authority TÜV. That's why updates to software versions tend to be infrequent. The opposite is the case with the manufacturing industry, power supply, and public infrastructure, where in principle only the latest software is utilized, since the operators' security guidelines insist that the latest updates must be used at all times.

In any case, coordinating all the assets in a network is highly demanding, which is why there are many tools on the market that promise to help. In most cases, however, these are standalone solutions that are not an integral part of an end-to-end NMS. But that is precisely where the demand lies: for an end-to-end NMS solution



that keeps the documentation of the entire inventory up to date at all times, records all the relevant network components, adds new hardware and software, and modifies existing systems. Preferably with just the push of a button.

User management

Network expansion is usually accompanied by an increase in the number of participants. That means information on all aspects of how the network resources are used is also increasingly important: who used which resource, when, and for how long? An NMS must provide robust answers to these questions and make it possible to allocate roles and tasks through the issue of authorizations. The possibility of providing the various users with specific rights rules out the possibility of abuse of access authorizations at the network configuration stage.

Optimize performance

The performance of a network directly affects the quality of business processes and thus a company's competitiveness. That's why it is tremendously important to make constant improvements to general network performance using a sophisticated NMS: to maximize throughput, avoid bottlenecks, and identify potential risks. The objective in all cases is to achieve maximum performance gains. The first step involves determining and analyzing network capacity utilization. This means gathering and evaluating vast amounts of statistical data.

The knowledge gained in this way makes it possible to assess the performance of the facilities and make planned improvements by putting appropriate actions in place.

Minimize cyber risks

Given the importance of industrial networks for corporate performance as a whole, successfully protecting them against potential cyber threats must be given top priority. The list of potential sources of risk is a long one. Criminal attacks by hackers, unauthorized access, or physical and electronic sabotage: all these incidents can potentially result in huge losses, and every effort must be made to avoid them. A functioning NMS plays a key role here, too: It ensures maximum data security, and its protective measures include all components involved in the communication process. To this end, an NMS saves all access data for device authentication, like user IDs and passwords, logs all operator actions, and ensures central administration of all security functions.

The NMS of the future

For an NMS to achieve all of the above, it must perform all the associated functional tasks. The cornerstones of state-of-the-art network management are defined by FCAPS, a model created by the ISO (International Organization for Standardization).

FCAPS stands for:

- **F**ault Management: Identify, save, report, and solve any error status that occur
- **C**onfiguration Management: Record and manage all components that must be monitored
- **A**ccounting Management: Record network usage
- **P**erformance Management: Gather performance data and maintain statistics
- **S**ecurity Management: Authenticate users and authorize access and usage

The trend toward digitalization and Industrie 4.0 highlights the importance of having a powerful and future-proof NMS – especially with regard to the functions described in the **FCAPS** model. What's more, Siemens has set itself the goal of utilizing its innovations to adapt the concept of network management to meet the needs of automation and further optimize it.

Published by
Siemens AG 2018

Process Industries and Drives
P.O. Box 48 48
90026 Nürnberg
Germany

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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit

www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under **http://www.siemens.com/industrialsecurity**

More informationen:
www.siemens.com/network-management