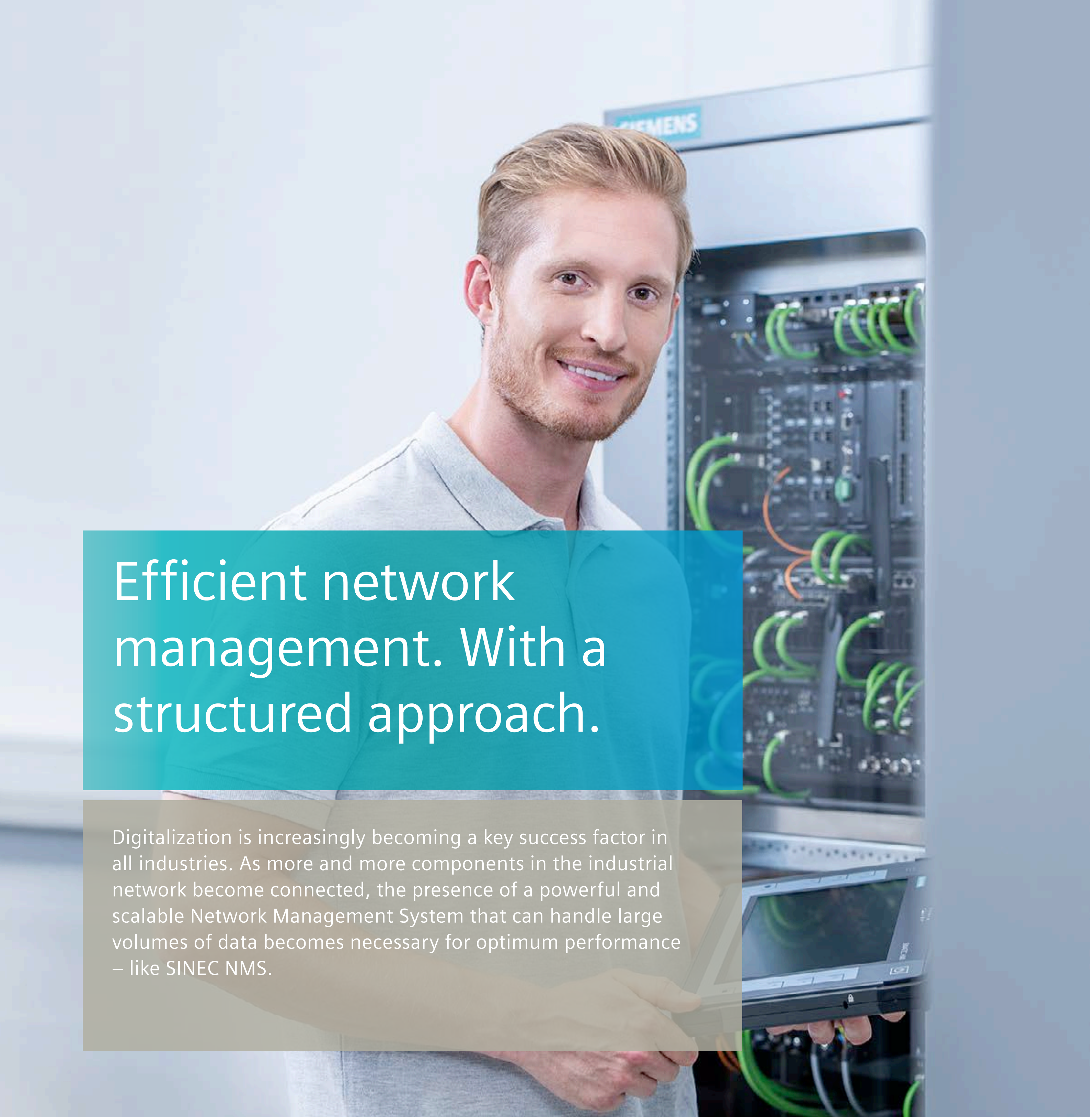
SIEMENS

# Turning insights into outlooks

## SINEC NMS – the all-around Network Management System

siemens.com/sinec-nms



# Efficient network management. With a structured approach.

Digitalization is increasingly becoming a key success factor in all industries. As more and more components in the industrial network become connected, the presence of a powerful and scalable Network Management System that can handle large volumes of data becomes necessary for optimum performance – like SINEC NMS.

For more information:
**siemens.com/sinec-nms**

### Paving the way for the digital transformation

SINEC NMS, our new Network Management System, is set up to deal with more and more complex network structures in an increasingly digitalized world. It can be used to centrally monitor, manage, and configure networks with tens of thousands of devices – round the clock. The scalability of SINEC NMS means it can grow in parallel as the network becomes larger and more complex.

# The NMS of the future. And beyond.

SINEC NMS was developed from the ground up including the requirements of industrial networks for Operational Technology (OT) but offers full conformity to the ISO model for network management called FCAPS.

## Fault Management

- Quick and easy location of faults
- Exact status overview enables a fast response if an error occurs
- Network structuring provides maximum transparency
- Reliable diagnostics via central evaluation of network capacity utilization

## Configuration Management

- Central, policy-based configuration and maintenance of the entire network saves time
- Easy and centralized backup and management of device configurations
- Less time and effort wasted in checking and upgrading firmware versions

## Accounting Management

- Complete overview of all network components provides a thorough oversight
- Reliable monitoring of network topology
- Network reports and event documentation improves security

## Performance Management

- Network optimization based on performance evaluation adds flexibility
- Transparency thanks to creation of statistics and data storage
- High level of availability due to constant network monitoring
- Early detection of changes in the network

## Security Management

- Reliable fulfillment of process-based and technical security requirements according to IEC 62443
- Increased network security thanks to central policy-based firewall configuration
- Enhanced security due to defined user management
- Central network documentation via policy-based reports, e.g. for audits

# Refining network management

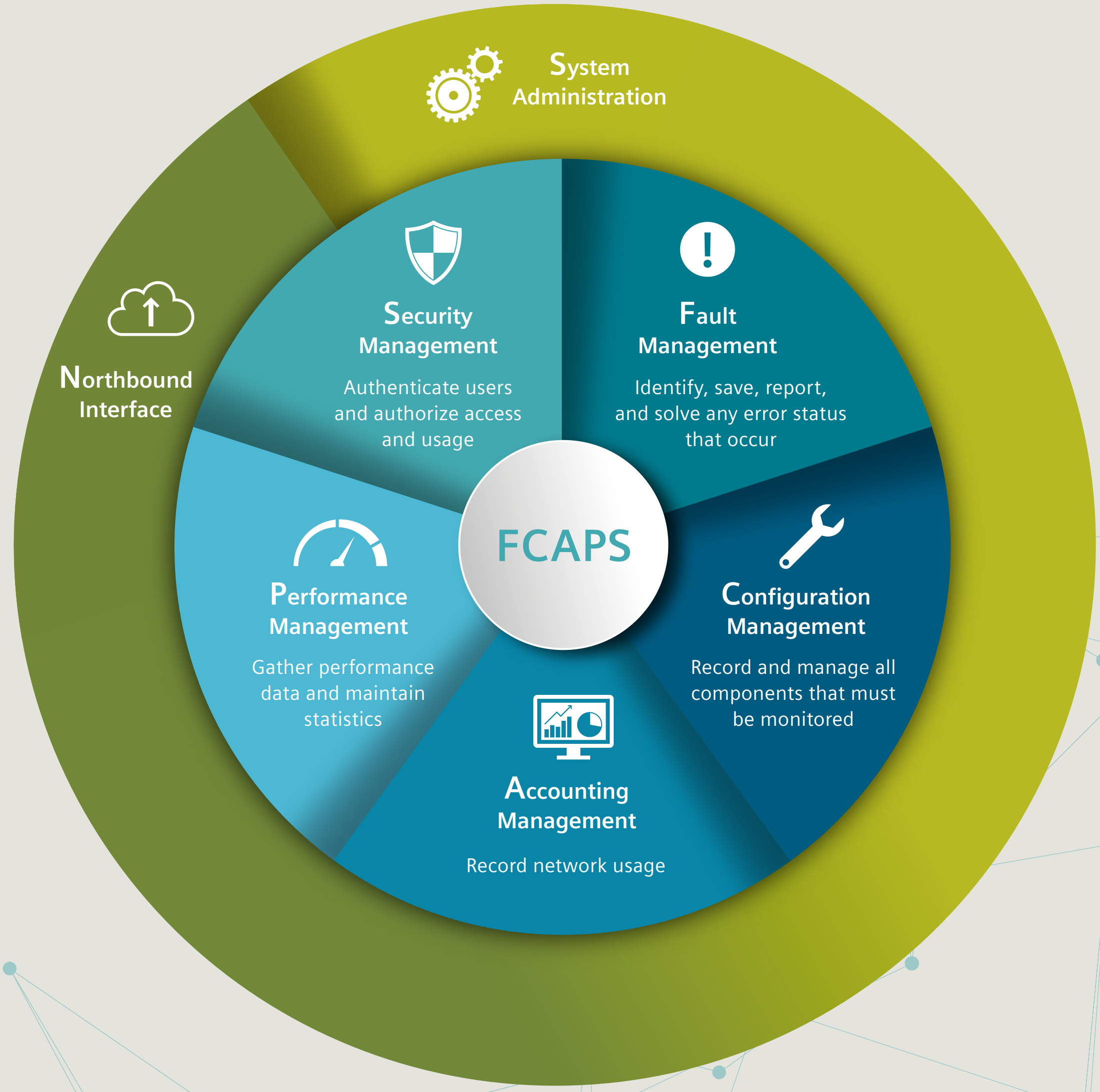
SINEC NMS goes beyond FCAPS, offering two essential system elements specifically addressing the industrial network requirements. This completes our offerings for OT networks.

## Northbound Interface

- Easy data handling thanks to direct access to network information for further processing in other systems and applications, e.g. OPC UA
- Data preprocessing
- Short response times thanks to advanced notification management

## System Administration

- Decentralized approach with a comprehensive view of the network, regardless of its size and complexity
- Central commissioning and administration of distributed SINEC NMS Operations in SINEC NMS Control
- Efficient role and rights administration


System Administration
Northbound Interface
Security Management
Authenticate users and authorize access and usage
Fault Management
Identify, save, report, and solve any error status that occur
FCAPS
Performance Management
Gather performance data and maintain statistics
Configuration Management
Record and manage all components that must be monitored
Accounting Management
Record network usage

# First choice for complex network structures

SINEC NMS makes it easy to integrate new components into your network, and to monitor and configure existing devices. Configuration is policy-based, so it can be applied generically to multiple components. For large-scale networks in particular, this means major time savings when it comes to configuration and troubleshooting, e.g. for SCALANCE and RUGGEDCOM devices.

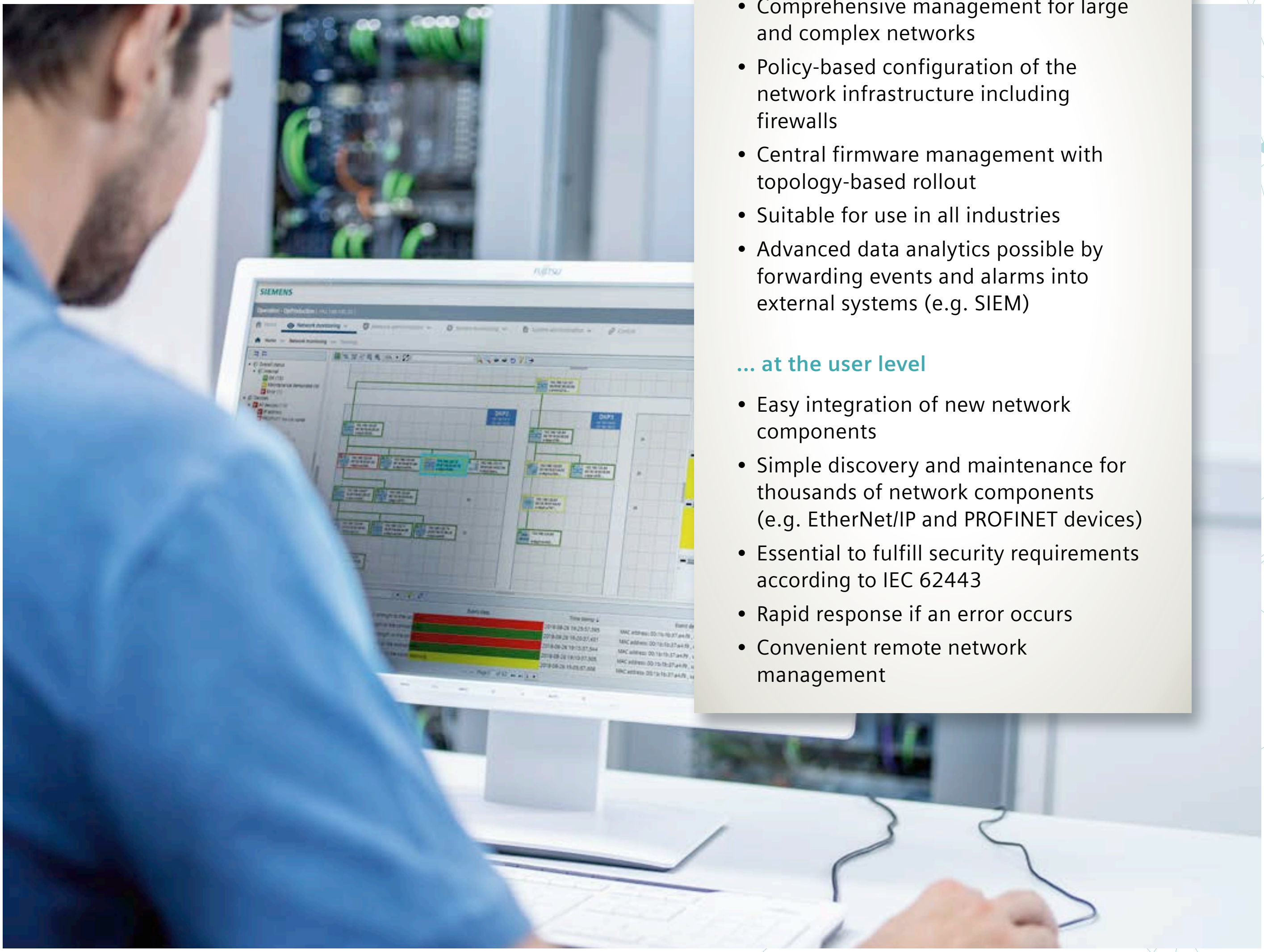
## BENEFITS...

### ... at the enterprise level

- Comprehensive management for large and complex networks
- Policy-based configuration of the network infrastructure including firewalls
- Central firmware management with topology-based rollout
- Suitable for use in all industries
- Advanced data analytics possible by forwarding events and alarms into external systems (e.g. SIEM)

### ... at the user level

- Easy integration of new network components
- Simple discovery and maintenance for thousands of network components (e.g. EtherNet/IP and PROFINET devices)
- Essential to fulfill security requirements according to IEC 62443
- Rapid response if an error occurs
- Convenient remote network management



**Published by**
**Siemens AG**

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

**For the U.S. published by**
**Siemens Industry Inc.**

100 Technology Drive
Alpharetta, GA 30005
United States

Article No.: DIPA-B10076-00-7600
Dispo 06366
WS 11190.0

siemens.com/sinec-nms

Subject to changes and errors. The information provided in this brochure contains descriptions or performance characteristics which, in case of actual use, do not always apply as described or which may change as a result of further development of the products. The desired performance characteristics are only binding if expressly agreed in the contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies, the use of which by third parties for their own purposes may violate the rights of the owners.

**Security information**
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

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.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
**siemens.com/industrialsecurity.**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the 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
**siemens.com/industrialsecurity.**