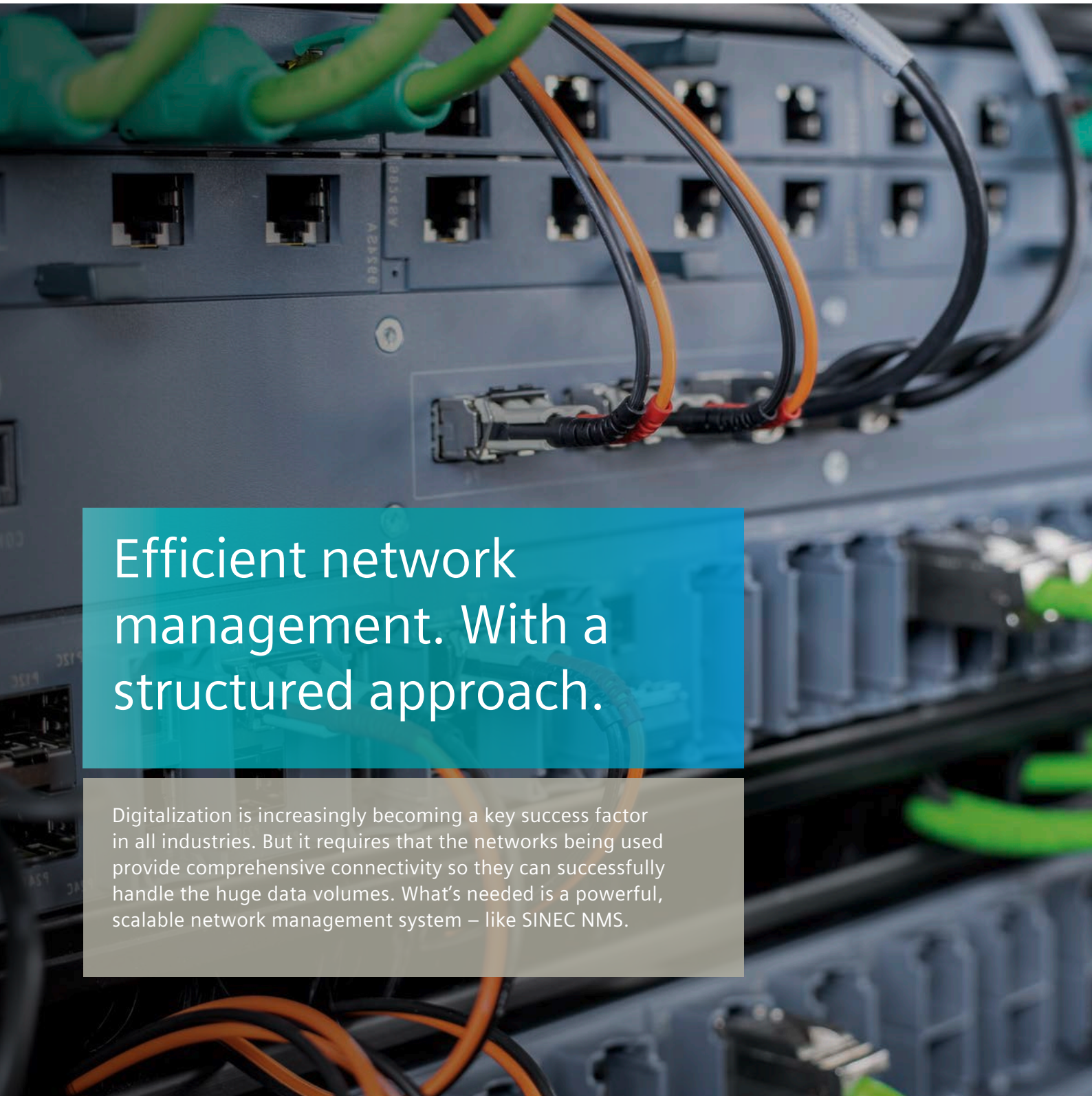

SIEMENS
Ingenuity for life
Turning insights into outlooks
SINEC NMS – the all-around Network Management System
siemens.com/sinec-nms



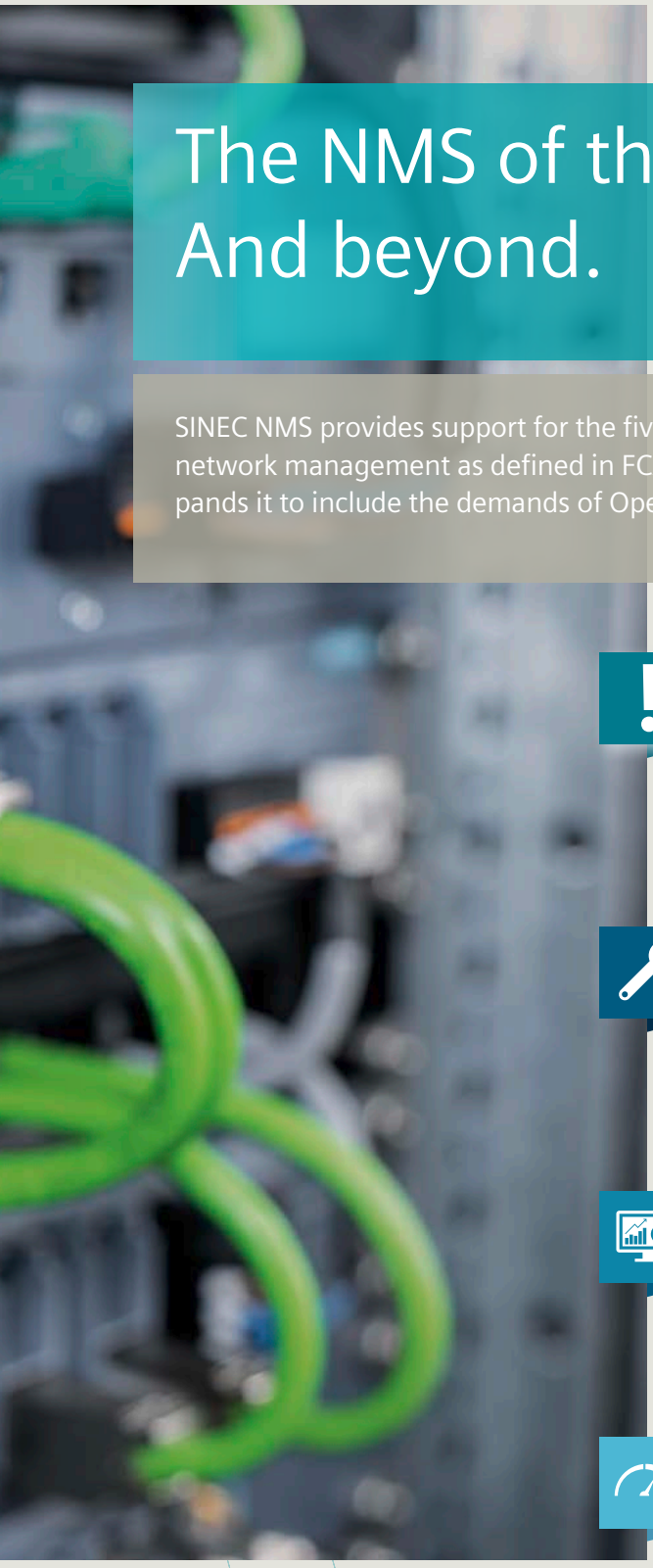
Efficient network management. With a structured approach.

Digitalization is increasingly becoming a key success factor in all industries. But it requires that the networks being used provide comprehensive connectivity so they can successfully handle the huge data volumes. What's needed is a powerful, scalable network management system – 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 50 to 12,500 participants – around 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 provides support for the five pillars of state-of-the-art network management as defined in FCAPS, an ISO model, and expands it to include the demands of Operational Technology (OT).

Fault Management

- Easy and fast location of faults in plants
- Quick response if an error occurs thanks to an exact status overview
- Transparency thanks to network structuring
- Central evaluation of network capacity utilization for reliable diagnostics

Configuration Management

- Central configuration and maintenance of the entire network saves time
- Easy and centralized backup and management of device configurations
- Less time and effort needed to check and upgrade firmware versions

Accounting Management

- Complete overview of all network components provides a thorough oversight
- Reliable monitoring of network topology
- Improved security thanks to network reports and documentation of events

Performance Management

- Flexibility thanks to network optimization based on performance evaluations
- Transparency thanks to creation of statistics and data storage
- High level of availability thanks to constant network monitoring
- Early detection of changes in the network

Security Management

- Improved security thanks to defined user management
- Increased network security thanks to central network management
- Reliable fulfillment of process-based and technical security requirements according to IEC 62443

Refining network management

SINEC NMS goes further than FCAPS, and also offers two overarching elements focused especially on industrial requirements on networks and rounding out the functions of our NMS.

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

First choice for complex network structures

SINEC NMS makes it easy to integrate new components into your network, and to monitor and configure existing components. 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.

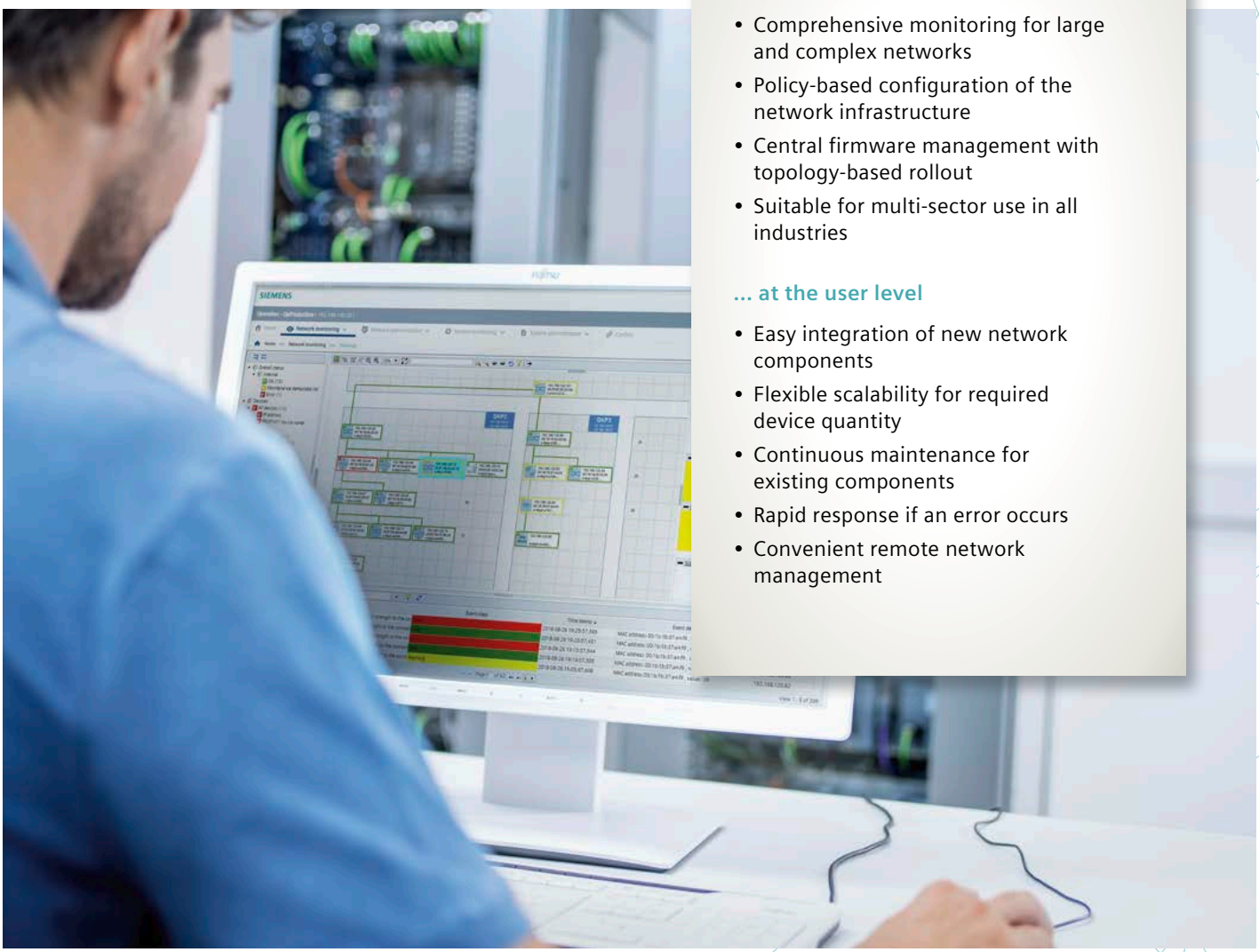
BENEFITS...

... at the enterprise level

- Comprehensive monitoring for large and complex networks
- Policy-based configuration of the network infrastructure
- Central firmware management with topology-based rollout
- Suitable for multi-sector use in all industries

... at the user level

- Easy integration of new network components
- Flexible scalability for required device quantity
- Continuous maintenance for existing components
- Rapid response if an error occurs
- Convenient remote network management



Published by
Siemens AG 2018

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

Article No.: PDPA-B10449-00-7600
Dispo 06366
WS 11182.0
Printed in Germany

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
https://www.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
https://www.siemens.com/industrialsecurity.