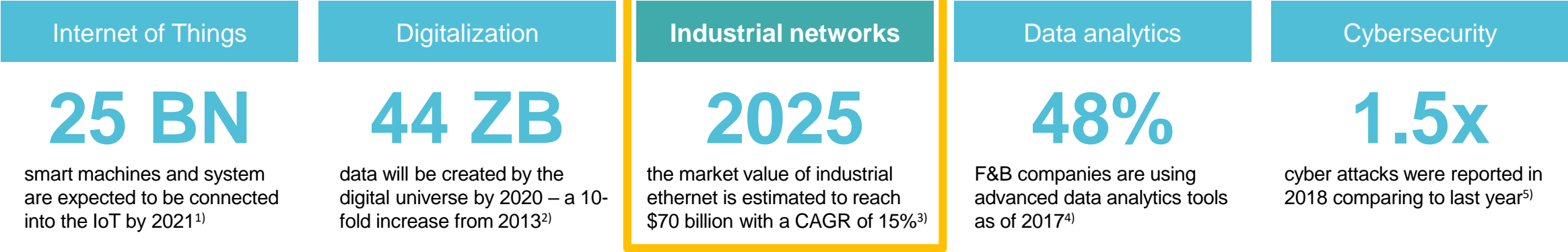


Network Monitoring & Management

A requirement for a successful
digital enterprise

Global trends are creating new challenges for our customers



A comprehensive network management system has become essential



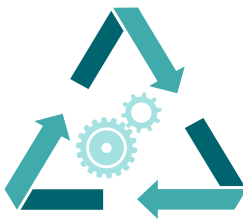
Acceptance



Network reliability



Economic efficiency



Compatibility



Support & warranty

1) Gartner 2) IDC 3) Global Market Insights, Inc 4) Longitude Research & Siemens 5) SiteLock

Increasing demands on Industrial Network Management and monitoring

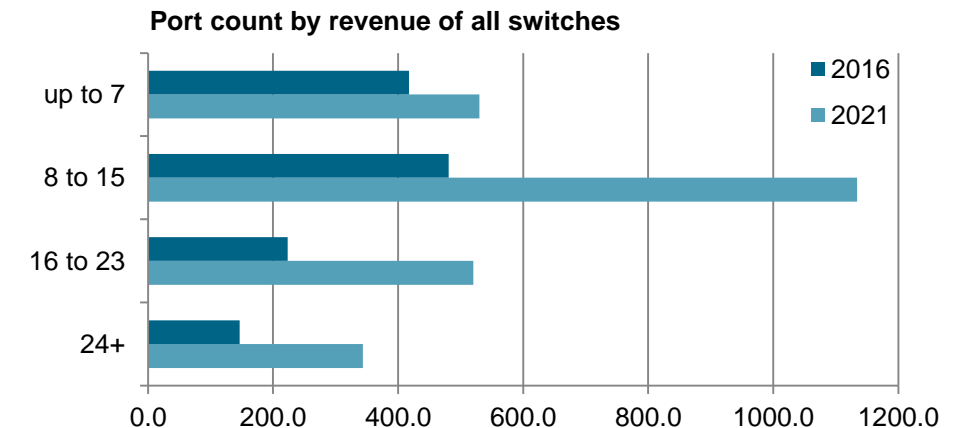
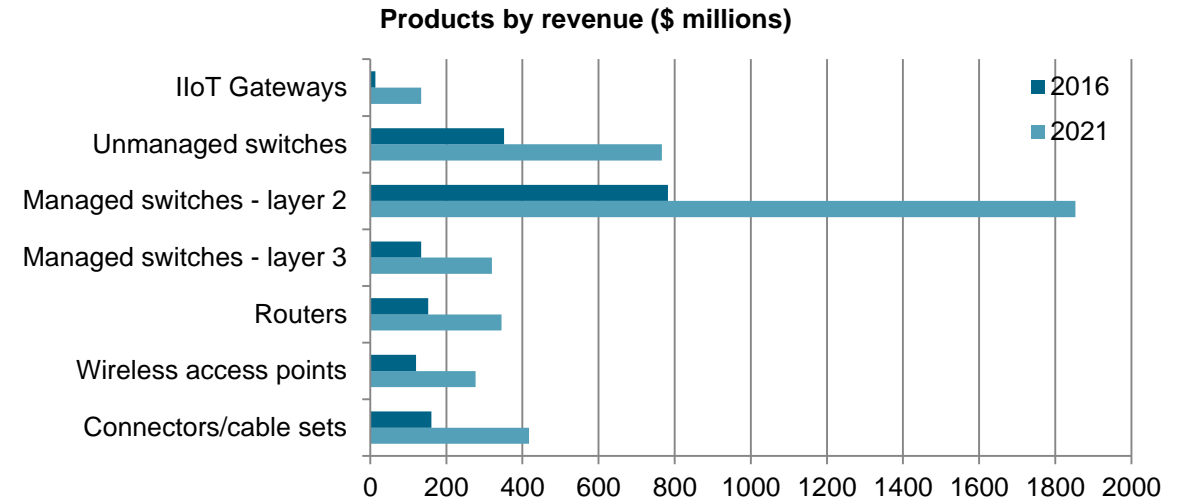
Studies prove:

- World market for Industrial Ethernet networks grows continually
- Number of PROFINET nodes rising
- Increasing number of managed devices
- Growing amount of devices with a small size (fewer port count of each device)

This leads to:

- Size of networks will continue to increase
- Complexity within the network will continue to grow

➤ **This results in an increasing demand for network management solutions**



Source: IHS Technology, *Industrial Ethernet Infrastructure Components Report – 2016 und 2021*

SINEC NMS helps you to face the current challenges: Productivity, Cost Pressure and Regulations

Protect Productivity



Protect
against

- Externally caused incidents through increasing connectivity
- Unauthorized Access
- Outdated firmware versions

Reduce cost



Costs

- Lack of transparency
- Manual monitoring of inventory
- Ageing assets

Comply to regulations



Comply to

- Reporting Requirements
- Security Standards (IEC-62443)

Network Management

Definition – FCAPS (universal) following ISO standard 10040

The term "network management" usually refers to the administration, the operating technology and the monitoring of IT and telecommunication networks.

The International Organization for Standardization (**ISO 10040**) defined five pillars of state-of-the-art network management and developed **FCAPS**, an ISO model.

(F) Fault Management:

- Identify, save, report and solve any error status that occur

(C) Configuration Management:

- Record and manage all components the must be monitored

(A) Accounting Management:

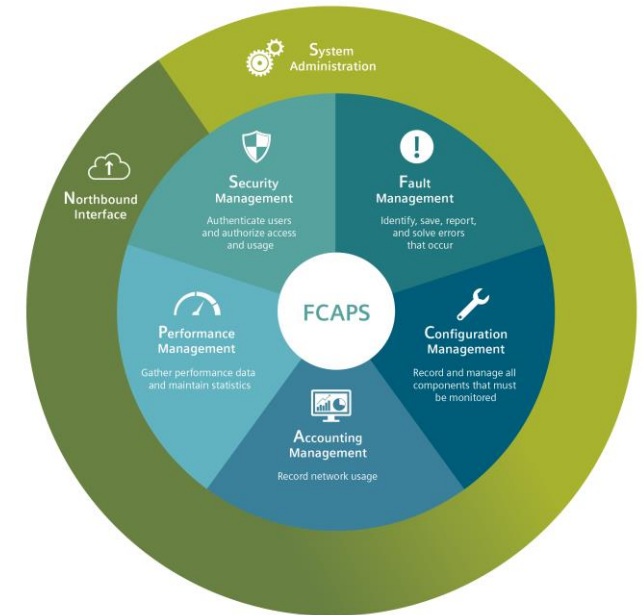
- Record network usage to generate an invoice

(P) Performance Management:

- Gather performance data, maintain statistics and define limit values

(S) Security Management:

- Authenticate users and authorize access and users



**SINEC NMS goes beyond FCAPS, offering two essential system elements specifically addressing the industrial network requirements. They complete the NMS offering necessary for the OT environment:
“System Management” and Northbound Interface”**

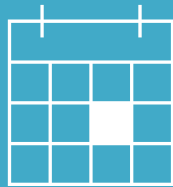
SINEC NMS

Cornerstones of a network management system

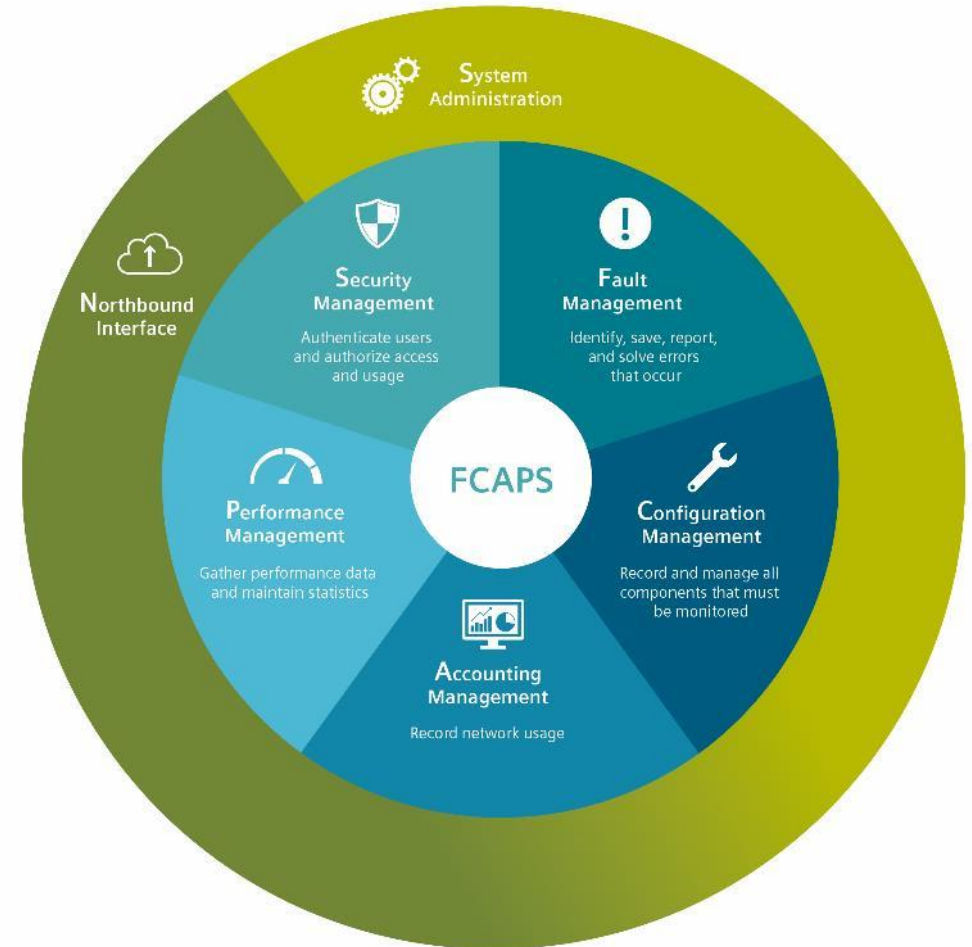
Predictive
Maximum transparency of the
entire network architecture



Preventive
Reduces unplanned
network downtime



Corrective
Policy-based configuration for
networks (up to 12,500 devices)



SINEC NMS Top highlights

Maximum transparency for your industrial network

Graphical representation



- Topological recognition and representation of the network
- Integration into HMI / SCADA systems possible

Monitoring and diagnostics



- SNMP, PROFINET and SIMATIC mechanisms are being used
- Evaluation and presentation of diagnostic conditions

Automatic Documentation



- Permanent inventory and documentation of all network users

Management



- Device configuration via policy-based roll-out
- Firmware management
- Monitoring and management centrally and 24/7

Validation of network parameters



- Repeatedly check and document the essential characteristics of the network

SINEC NMS – a new Network Management System

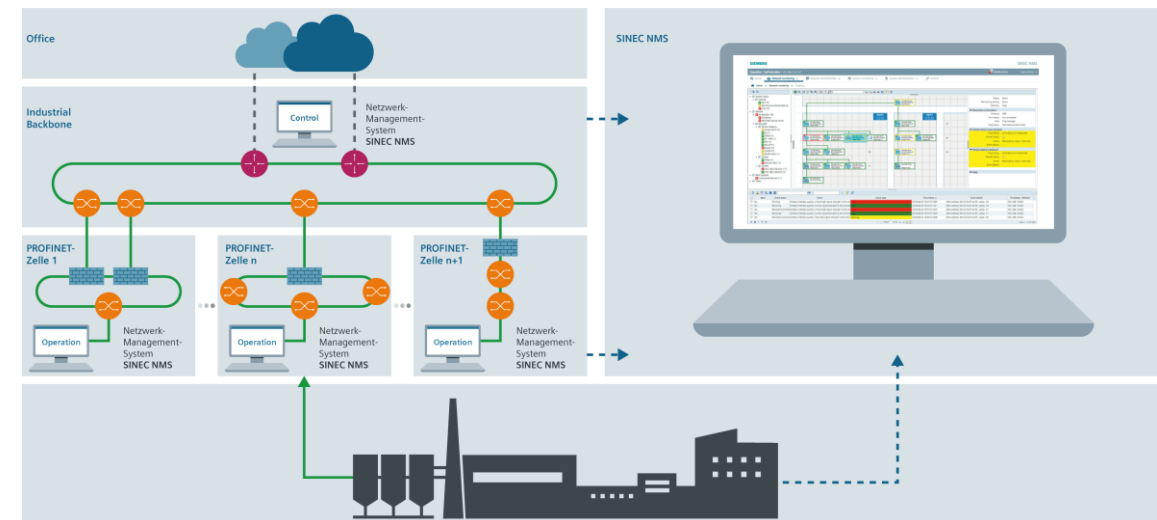
- SINEC NMS is fully web- based network management platform developed to meet today's and tomorrow's challenges
- Operators can monitor and manage their industrial network with a single SINEC NMS installation.
- Thanks to the distributed approach of SINEC NMS, the network management system can be dynamically adopted to your specific network requirements.
- SINEC NMS is divided into two levels:

Control:

The control is the central instance in SINEC NMS, which displays the overall condition of the network. It gives the user an overview of the overall network status. Furthermore, the distributed SINEC NMS Operations are centrally managed in the control.

Operation:

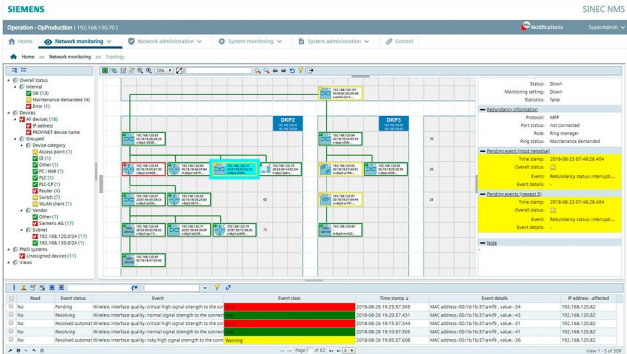
The Operations detects the network devices and reads the respective information from the devices. In addition, the SINEC NMS Operations is distributed throughout the network and implement the configuration parameters (policies) from the Control on the devices.



SINEC NMS Fault Management (FCAPS)



Fault Management



Network monitoring

- In addition to using SNMP (Simple Network Management Protocol), it is also possible to directly access SIMATIC controllers (S7-300/S7-400), or access PROFINET participants via “read data record”.
- Detection and fundamental diagnosis of SIMATIC S7-1200 and S7-1500 via SNMP.
- Port statistics: central evaluation of the network utilization of individual ports in the devices: number of received, sent and rejected telegrams.

Diagnosis management

- A wide range of mechanisms (DCP, ICMP, ARP, SNMP, PROFINET/SIMATIC diagnosis) are used to collect and centrally archive diagnostic data from all network components.
- Diagnostic states are reported as events, assigned to the corresponding devices, and highlighted in the device list and topology. This allows early fault detection.

Topology

- The network topology is automatically discovered, displayed and monitored for changes (reference topology).
- Medium type, redundancy and VLANs are graphically displayed.
- Changing topologies (e.g., tool changers) can be monitored without disruptive error messages.
- By structuring the entire network topology into different views, topological hierarchies can be created for the convenient localization.

SINEC NMS – Network Management System – Method and phases

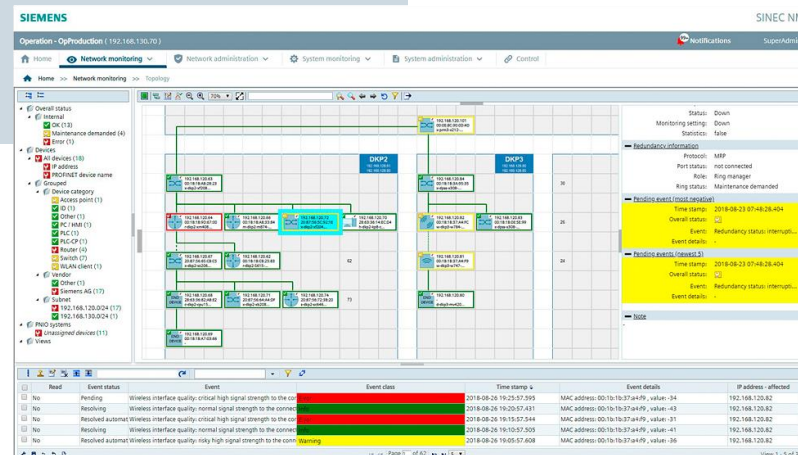
Network scan

- Determination of IP address ranges that are to be searched
- SCAN is done with the following protocols:
 - Discovery Configuration Protocol (DCP)
 - Internet Control Message Protocol (ICMP)

Filtering possibilities

Monitoring

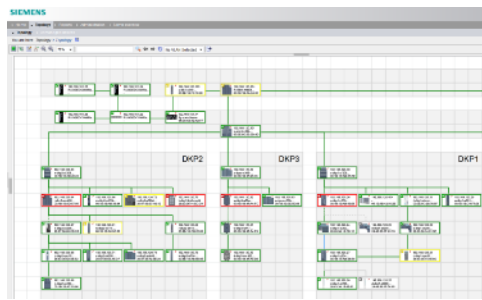
- Recognition of the IP addresses in the network
- Identification of network participants via
 - DCP
 - SNMP
 - PROFINET
- Reading of device and diagnostical information
 - SNMP
 - PROFINET read record
 - SIMATIC S7 Protocol
- Reading of the network topology with SNMP via LLDP-MIB



SINEC NMS – Fault management

Visualization and monitoring information

Topology (LLDP, Bridge)



LAN Ports (Utilization, Error, Discarded)

Port	Status	Monitoring	Admin	Port MAC address	Connection type	Speed in Mbps
fe-2-1	Down	Down	Up	94:b8:c5:12:a8:41	Unknown	100
fe-2-2	Down	Down	Up	94:b8:c5:12:a8:42	Unknown	100
fe-2-3	Down	Down	Up	94:b8:c5:12:a8:61	Unknown	100
fe-3-2	Down	Down	Up	94:b8:c5:12:a8:62	Unknown	100
fe-1-3	Up	Up	Up	94:b8:c5:12:a8:63	Unknown	100
fe-3-4	Down	Down	Up	94:b8:c5:12:a8:64	Unknown	100
fe-2-5	Down	Down	Up	94:b8:c5:12:a8:65	Unknown	100
fe-3-6	Down	Down	Up	94:b8:c5:12:a8:66	Unknown	100
fe-om-1	Up	Up	Up	94:b8:c5:12:a8:7d	Unknown	100
ge-1-1	Up	Up	Up	94:b8:c5:12:a8:21	Unknown	100
ge-1-2	Down	Down	Up	94:b8:c5:12:a8:22	Unknown	1000

VLAN's (Incl. highlighting in Topology)

Filter data:				
Max. possible VLANs: 255		Currently used VLANs: 2		
VLAN #	Name	Status	Untagged ports	Tagged ports
1	vswitch.0001	Static	-	-
2	vswitch.0002	Static	-	-

I&M data for asset management

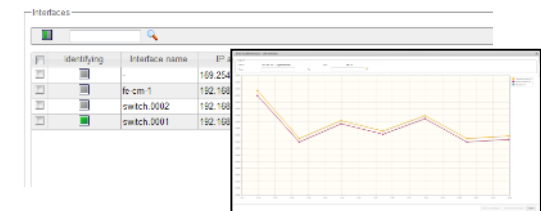
Firmware	ROX 2.11.2 (2017-12-08 11:23)
Hardware version	rx1510
Vendor	Siemens AG
Serial number	30140102-0012-003A040017

Redundancy Information RSTP, MRP, HRP (redundant path shown in topology)

Port	Protocol	Status	Additional information	Role
fe-2-1	RSTP	broken	enabled	-
fe-2-2	RSTP	broken	enabled	-
fe-3-1	RSTP	broken	enabled	-
fe-3-2	RSTP	broken	enabled	-
fe-3-3	RSTP	forwarding	enabled	-
fe-1-4	RSTP	broken	enabled	-

Trend Charts

Historical values (Availability, workload, discarded packets...)



SINEC NMS

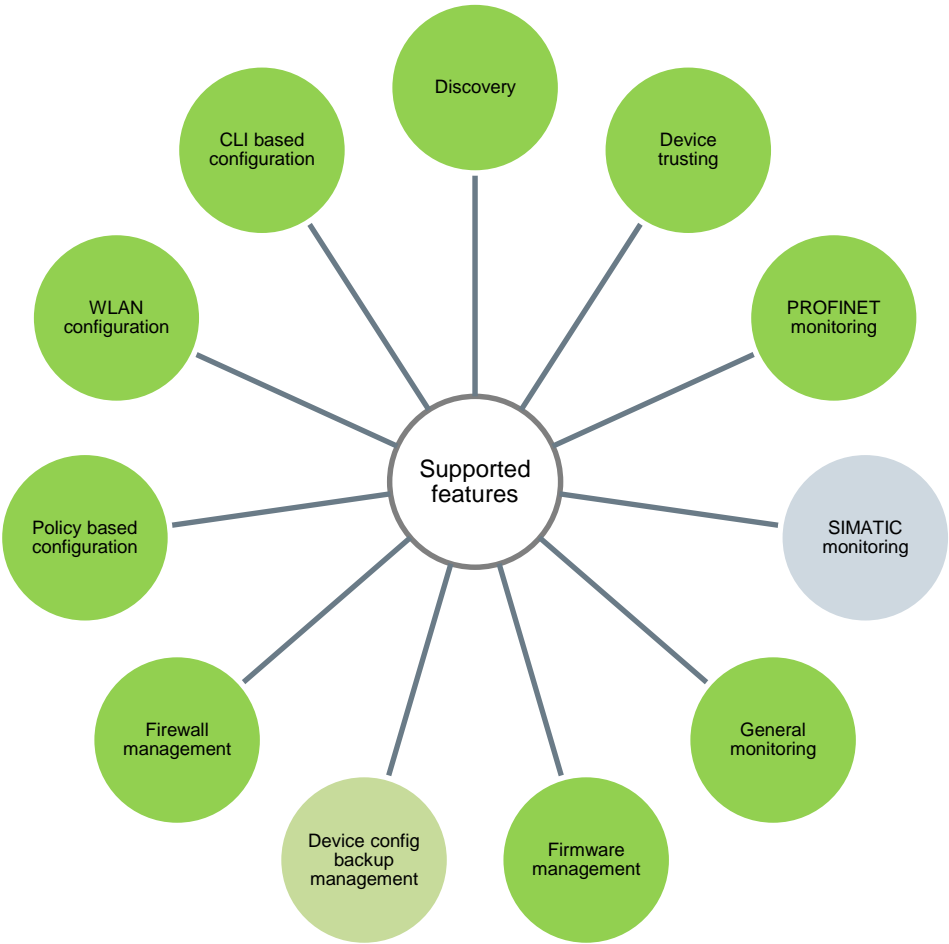
Supported products



SCALANCE product family



All SCALANCE devices are supported by SINEC NMS. The more recent hardware, the better representation you get. However configuration is depending on device firmware and device capabilities.



SINEC NMS

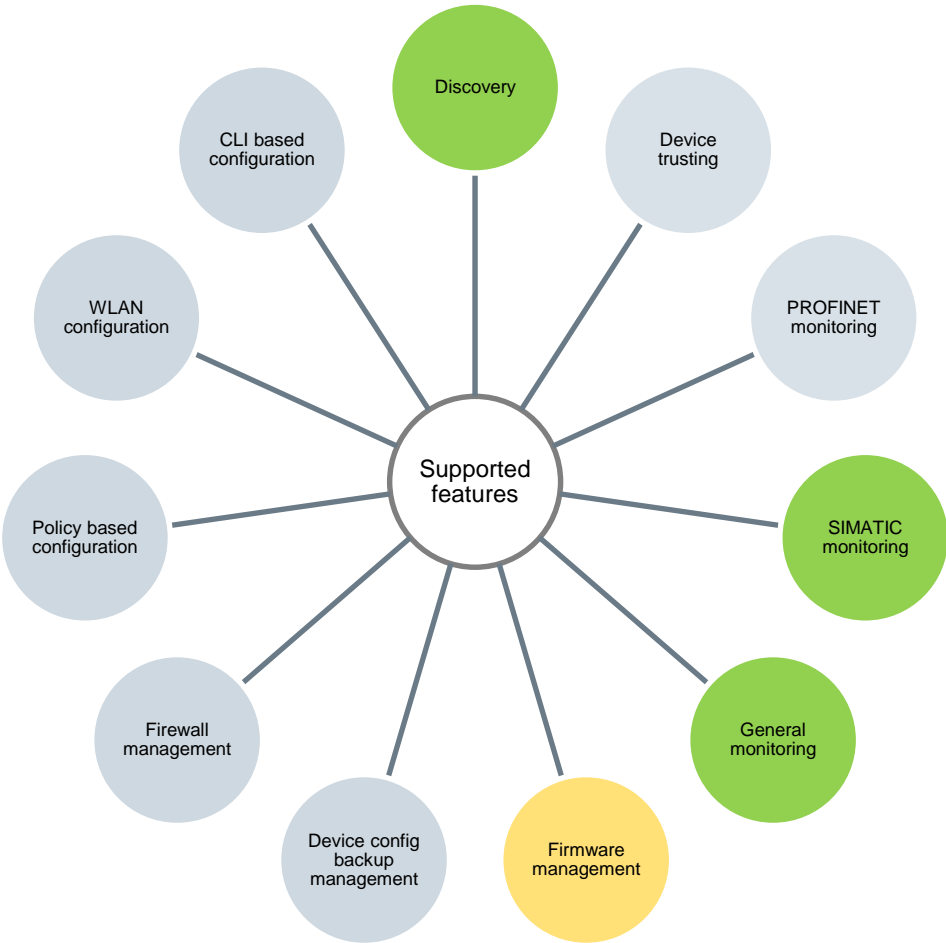
Supported products



PROFINET capable SIMATIC S7-300 / S7-400



SIMATIC S7-300 / S7-400 is fully integrated into monitoring of SINEC NMS. This includes that also PLC specific information (cycle time, connected devices, Alarms & Events) can be read and get monitored.



Supported but depending on device specific capabilities Supported but depending on device firmware Not supported Not applicable as device is not supporting

SINEC NMS

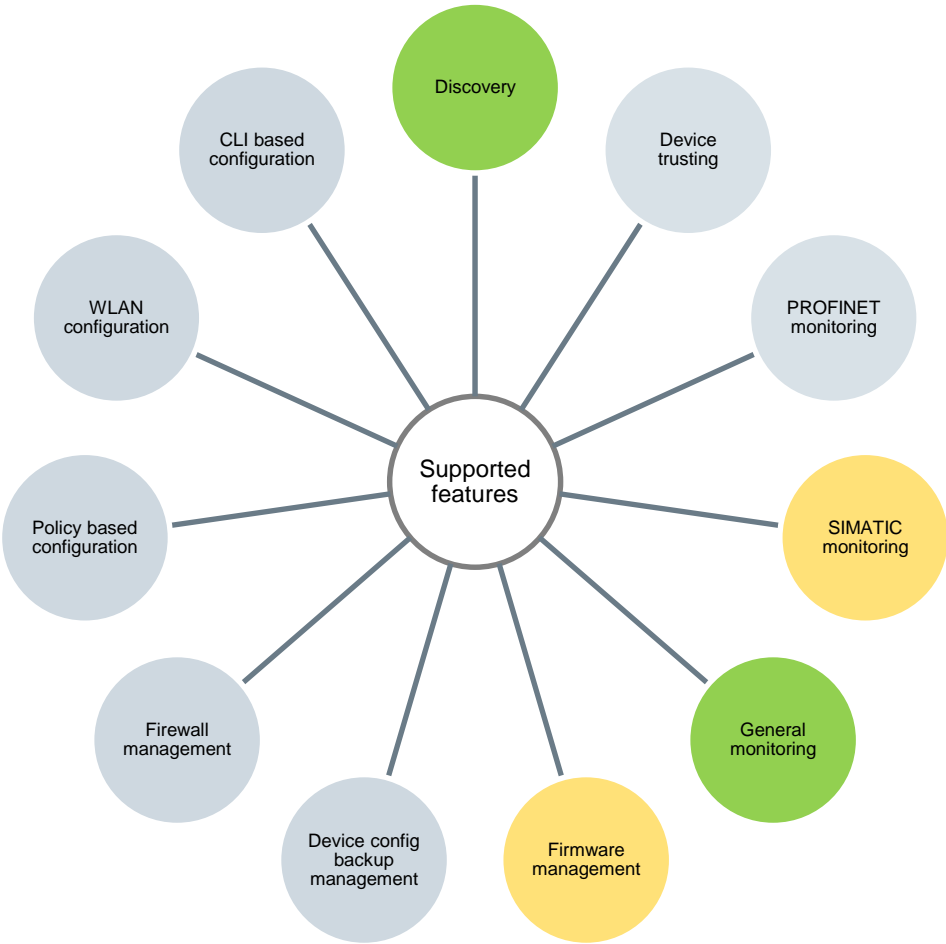
Supported products



PROFINET capable SIMATIC SITOP / S7-1200 / S7-1500



SITOP, SIMATIC S7-1200 and S7-1500 PLCs can be discovered and monitored. This includes I&M data, topology, device reachability and port statistics that get read and displayed within SINEC NMS.



SINEC NMS

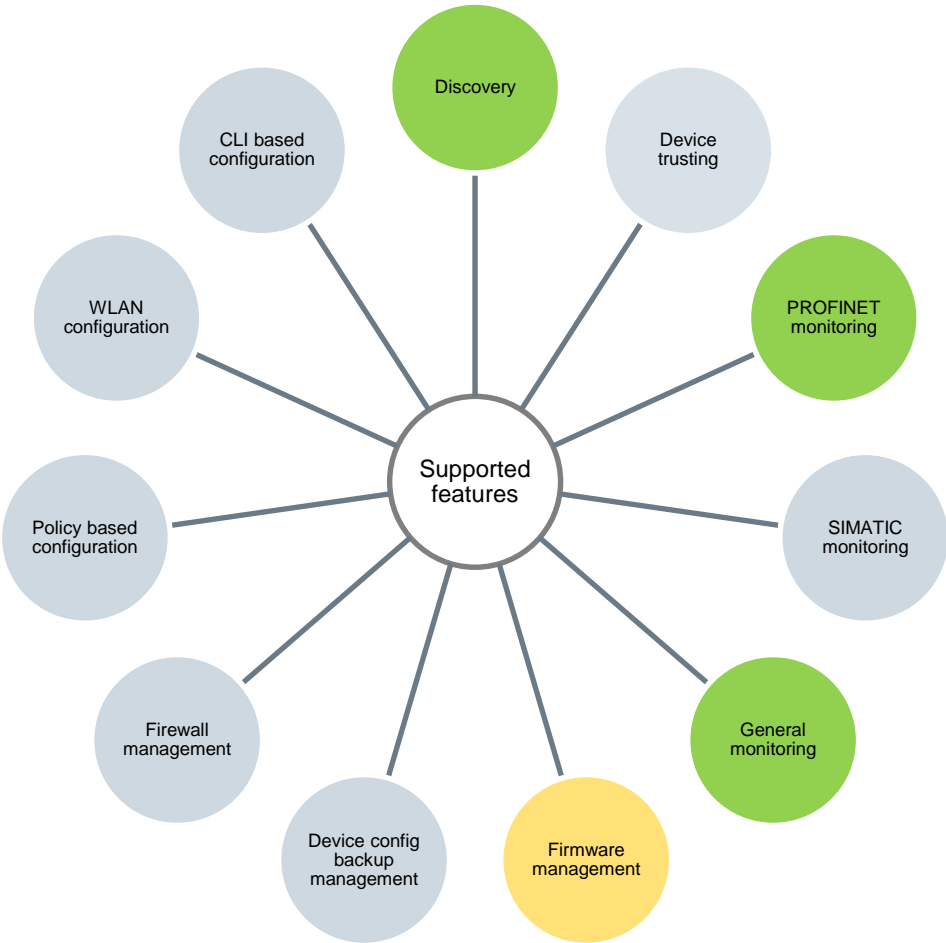
Supported products



PROFINET capable devices (vendor independent)



PROFINET devices can be properly discovered, and monitored based on PROFINET. This includes I&M data, topology, device status, port statistics and channel diagnostics that get read and displayed within SINEC NMS



SINEC NMS

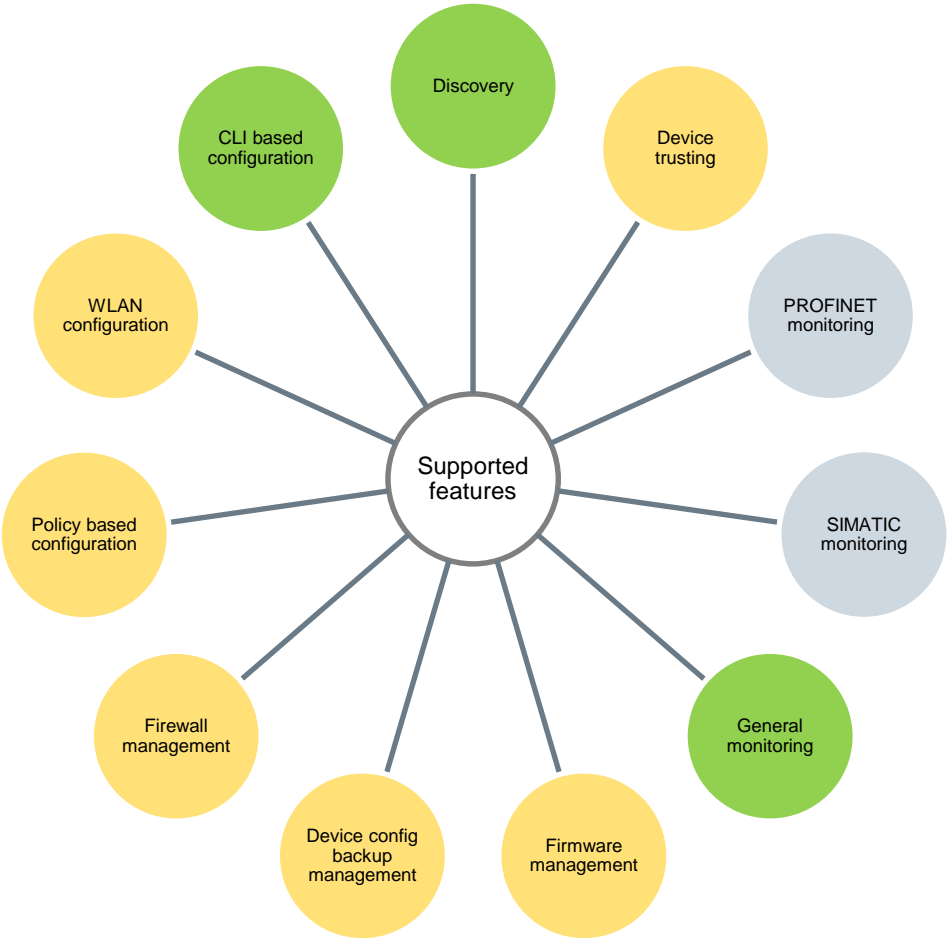
Supported products



3rd party SNMP devices (Vendor independent)

SNMP

SNMP capable network components are supported in terms of monitoring and management. Scope of monitoring depends on capabilities of the device (supported standard MIBS)
Device configuration can be done based on CLI scripts that are rolled out based on policies.



Supported but depending on device specific capabilities Supported but depending on device firmware Not supported Not applicable as device is not supporting

SINEC NMS Fault management – Comprehensive and cross-system diagnostic options

SNMP

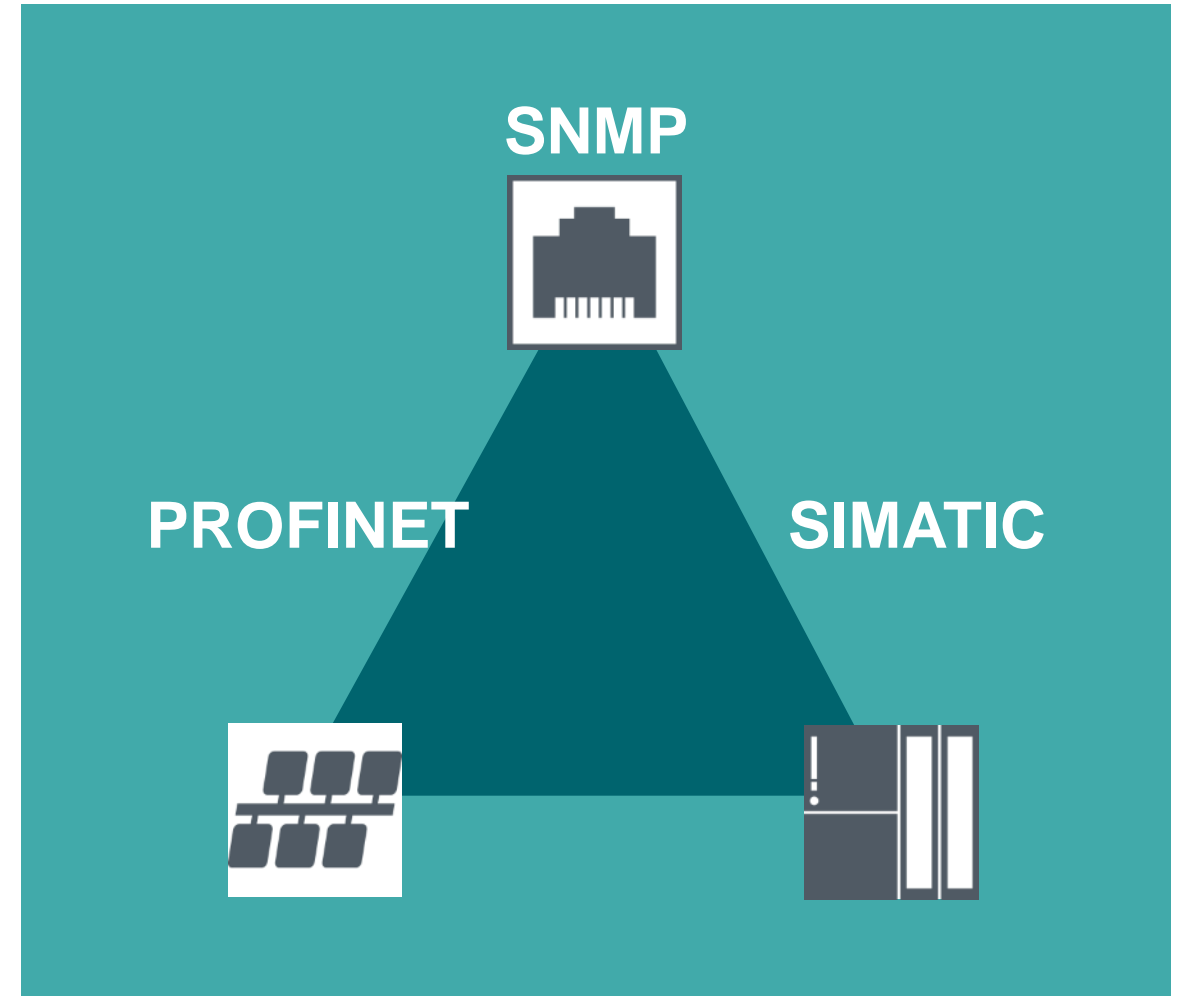
- Standardized diagnostics of networks
- Remote control and configuration
- Notification in the event of faults (TRAPs)

PROFINET

- Open Industrial Ethernet standard of the PNO
- Cross-manufacturer data evaluation
- Standardized diagnostics

SIMATIC (S7-300, S7-400, S7-400H, S7-410-5H)

- Diagnostics of SIMATIC-enabled CPUs and the assigned devices
- Seamless connection to the reporting system of the CPU



Configuration Management



Configuration Management

SIEMENS

Home Network Monitoring Network Administration System Monitoring System Administration

Home Network Administration Configuration Management

Configuration Repository

View Compare Lock Unlock Delete Restore

	Unlock / Lock	Tags	Created Timestamp	System Name	PNIO Name	MAC	Order Number	FW Version
<input type="checkbox"/>	Unlocked	-	12/15/2017 14:18	DKP1-XM408	Not set	28.80.23.D8.EC.6F	66K3 408-80500-2MA0	4.1
<input type="checkbox"/>	Unlocked	Custom:	12/17/2017 13:11	DKP1-XM408	Not set	30.E1.71.86.FB.30	66K3 408-80100-2MA0	2.0
<input checked="" type="checkbox"/>	Unlocked	After Commissioning	12/17/2017 02:22	DKP1-XM408	Not set	80.5A.0A.50.AD.0A	66K3 408-80100-2MA0	2.2
<input type="checkbox"/>	Locked	-	12/18/2017 22:06	DKP1-XM408	DKP1-XM408	28.80.23.D8.EC.6F	66K3 408-80500-2MA0	4.1



Policy-based configuration

- Automated execution of regular tasks, e.g., creation of backups of SCALANCE components every two weeks.
- Configuration of the network via function-based rules, e.g., “set VLAN”, “lock open ports”.

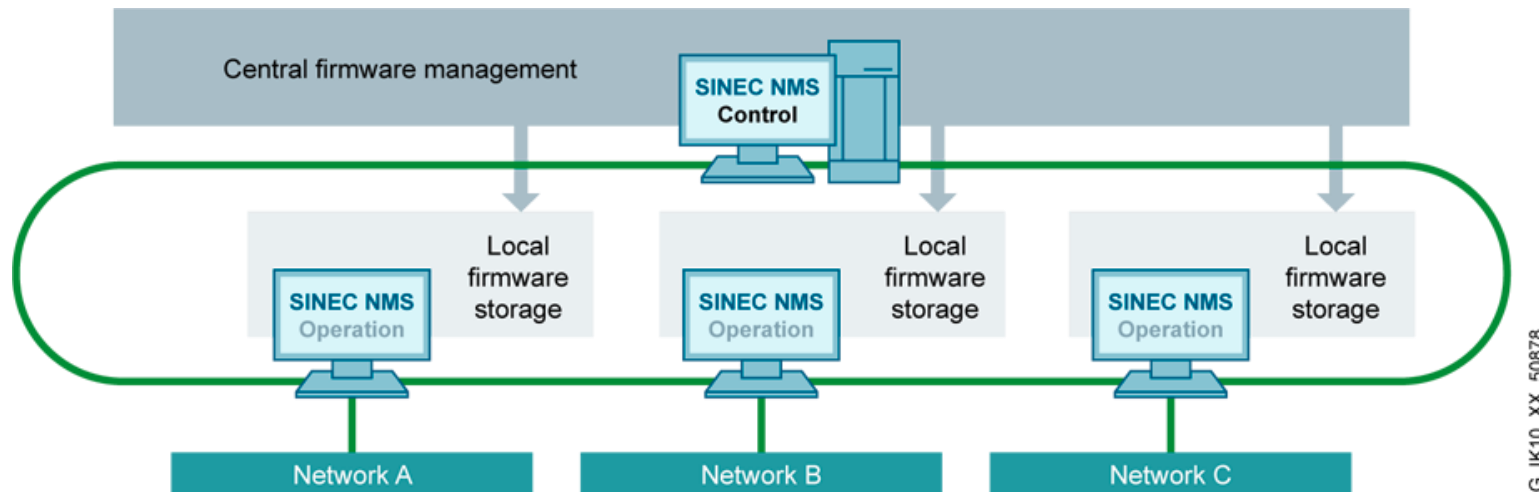
Firmware management

- Central management of the firmware versions for the different device families (SCALANCE X, W, S, M).
- Firmware update function for upgrading the firmware version of single or multiple SCALANCE components (also taking the topology into consideration).

Device Config management

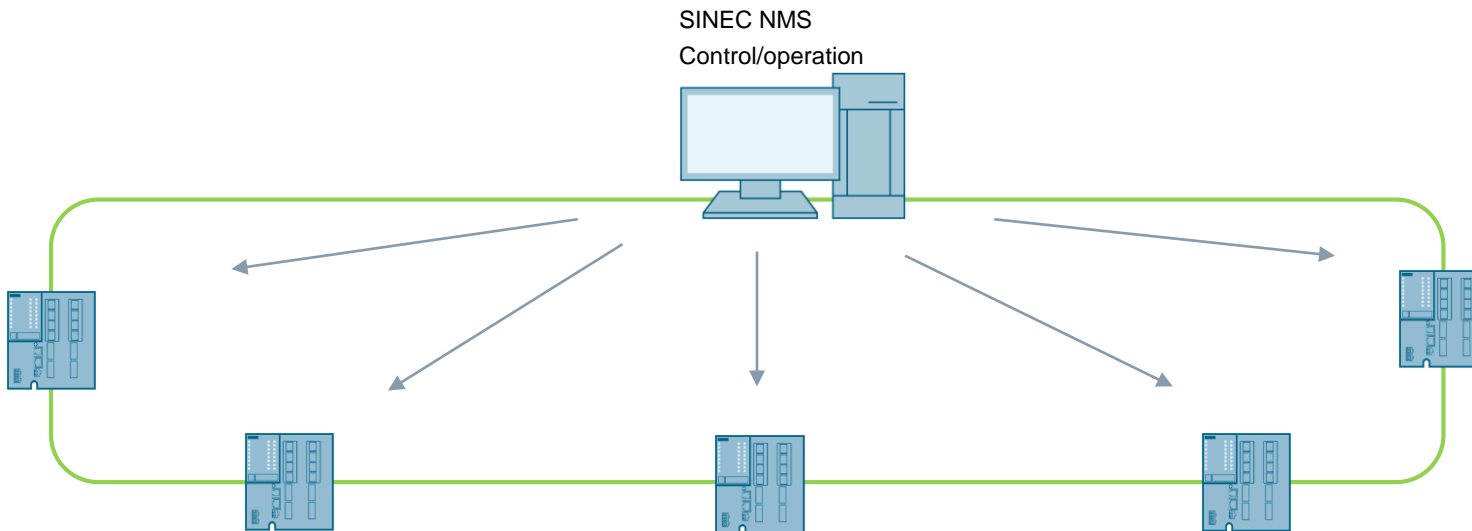
- Backup / restore of the device configuration of SCALANCE components for single or multiple devices.
- Comparison function to detect changes in the configuration of SCALANCE components.
- Definition of individual network parameters for single or multiple SCALANCE components.

SINEC NMS – Firmware Management – Central management of the firmware files



- Firmware files are stored in SINEC NMS
- Firmware files are synchronized with distributed instances
- Firmware can be loaded onto a device either manually or by a scheduled policy

SINEC NMS – Save / restore / edit and compare config files



Config file management in operation:

1. **Saving** to the clipboard
2. **Edit** (Adjust configuration)
3. **Restore** to device
4. **Comparison** of two configurations

- Device config backups get stored and managed on operation level
- Backups can be saved manually or automatically based on policy
- Backups can be compared (summary) in order to detect differences
- Backups can be edited and then restored

Accounting Management



Accounting Management



Inventory

- SINEC NMS detects all devices on the network and displays them either as device list or interface list, generating a complete, up-to-date overview of all components in the network, including their essential properties.

Topology

- The plant topology is automatically discovered, displayed and monitored for changes.
- Medium type (such as WLAN, copper, optical), redundancy and VLANs are graphically displayed.

Validation

- Configurable test patterns enable examination and documentation of essential network properties .
- The validation result is stored together with all underlying data as a PDF .

Performance

- Availability of devices and interfaces
- Performance data such interface utilization
- Inventory and manufacturer lists of devices in the network
- Event classes on number of events with status of “Error”, “Maintenance” or “OK”

Security Management



Security Management

According to IEC 62443



User role management

- User access and privileges/rights can be precisely controlled via the user administration.

Secure system

- Encrypted data communication between SINEC NMS Control and SINEC NMS Operation instances (via certificates and passwords) .
- Encrypted data communication between SINEC NMS and the network components (via SNMP V3).

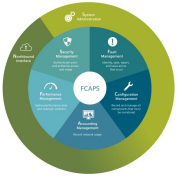
Firewall management

- Central Firewall management for SCALANCE S-615, SC600 and RUGGEDCOM RX1400/1500 devices
- NAT (Network Address Translation) configuration in the firewall editor

Audit trail

- Network documentation with asset information via mouse click
- Documentation and traceability of configuration changes via policy based reports or audit trail

SINEC NMS Northbound Interface



Northbound Interface



System notifications

- Centrally displayed notifications inform the user about currently pending problems. Via quick links, the user is guided to the appropriate place.

OPC UA

- Network information is provided to other OPC UA applications via the OPC UA server interface.

E-mail notifications

- E-mails or any Windows application can be triggered based on events.

URL access

- Higher-level HMI systems can conveniently and directly access the monitored network and diagnostic data by means of URL accesses.

Remote Syslog

- Forwarding of Secure Events to a central Syslog Server or SIEM System, MES or SCADA over Syslog messages

SINEC NMS

License concept

Software Purchase

One-Time Payment

Targeting customers with one-time-investment budget

- One-time payment for the use of the software
- Upgrading to new versions via paid upgrade packages

Software Update Service

Annual Maintenance Fee

For customers wanting continuous update automatically

- Annual fee
- Automatic and free delivery of software updates and upgrades

Software Migration

Power Pack

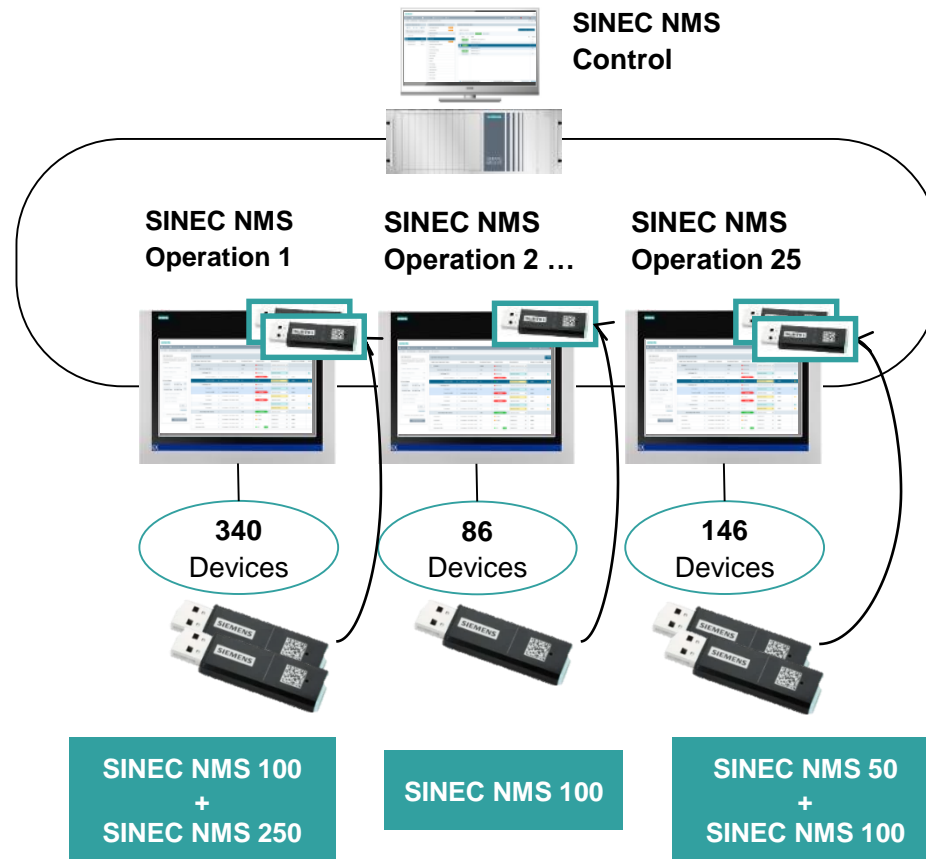
E.g. for SINEMA Server customers

- One-time payment for license migration to the new system
- No data migration; new system will be built

Available for 50, 100, 250 and 500 nodes; 1000 and 5000 nodes on request

SINEC NMS

Licensing concept



SINEC NMS licensing concept

Only SINEC NMS Operations and the amount of devices to be monitored are licensed

License keys are transferred via the supplied Automation License Manager (ALM)

For each SINEC NMS Operation, a max. of **500 devices** is possible

There are 4 license package sizes:

- SINEC NMS 50 for 50 devices
- SINEC NMS 100 for 100 devices
- SINEC NMS 250 for 250 devices
- SINEC NMS 500 for 500 devices

The different license packages can be combined with each other so that the existing number of supported devices can be increased up to max. 500 devices per SINEC NMS Operation

SINEC NMS

Use case – Reducing downtimes in industrial networks



Task

Identifying changes in industrial networks early on and preventing failures – to ensure the productivity of industrial plants and minimize downtimes.

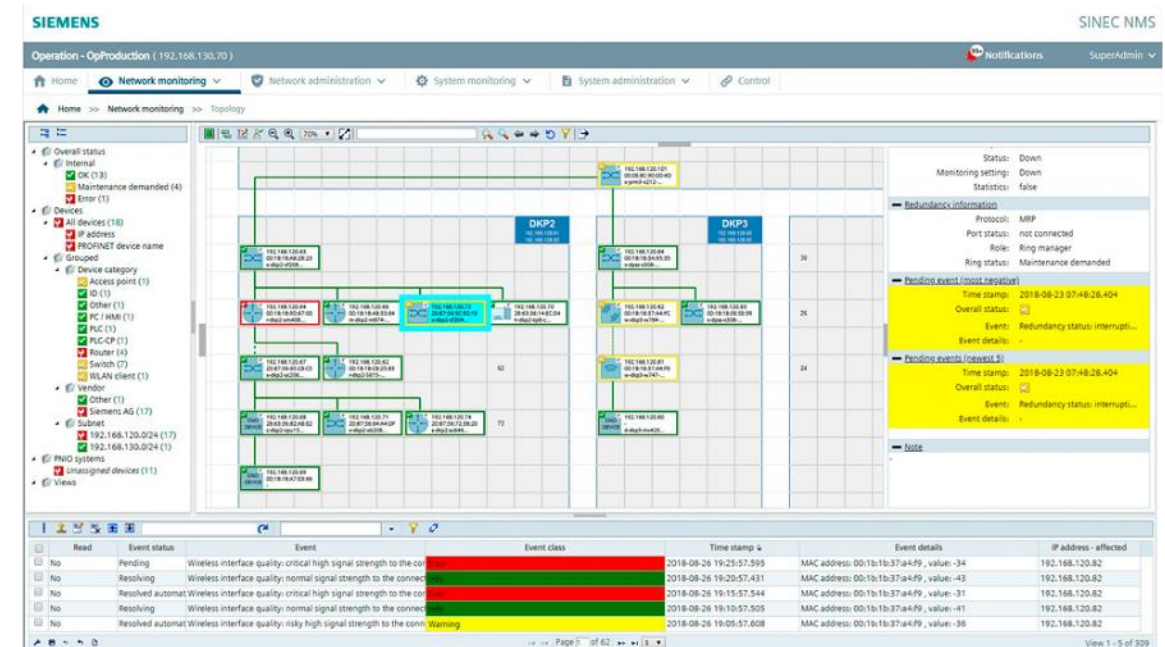
Solution

SINEC NMS constantly monitors the network, 24/7, and depicts the diagnostic states of the network devices live. Furthermore, statistics over any period of time can be displayed and evaluated.

Benefits

- Color diagnostic display to identify undesired failures early on
- E-mail notification to be promptly informed about changes

Topology view



SINEC NMS V1.0

Use case – Local HMI integration

Task

In an existing HMI / SCADA / PCS 7 / PCS Neo or WinCC solution the condition of the network is to be displayed.

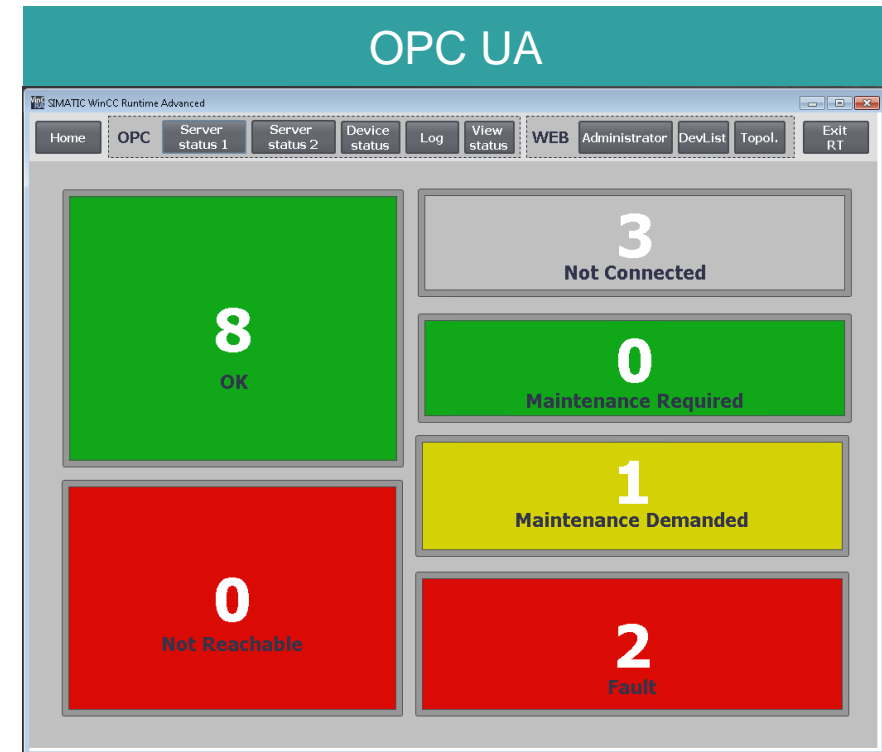
Solution

The network information of SINEC NMS can be easily integrated into HMI / SCADA systems via OPC UA.

Benefits

Seamless integration of network information into an HMI system.

HMI / SCADA



SINEC NMS

Use case – PCS 7 / PCS Neo

Task

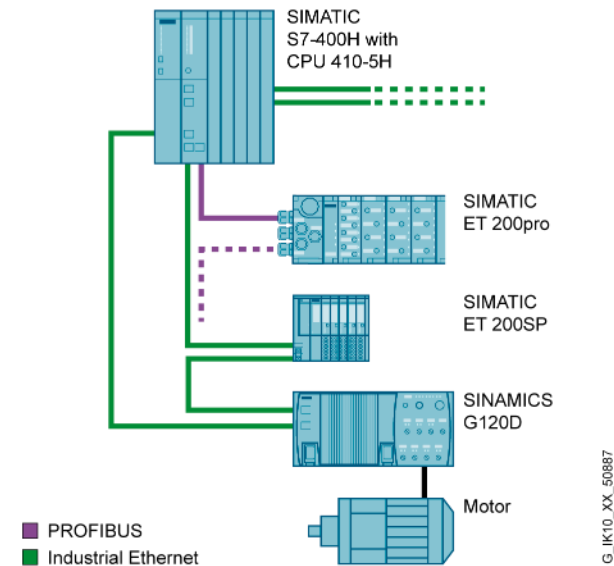
SINEC NMS as central instance for monitoring PCS 7 / PCS Neo environments.

Solution


SINEC NMS can assume the monitoring of SIMATIC S7-300¹⁾, S7-400, S7-400H, and S7-410-5H. SINEC NMS represents a suitable solution for seamless network and system diagnostics in PCS 7 / PCS Neo environments.

Benefits

- One comprehensive tool for diagnostics
- Long-term network monitoring and management
- Full integration with the system platform



Device details (172.20.29.16 / CPU 410-5H)

Summary	Status	Description	SIMATIC	Config.	LAN ports	Events	IP Interfaces	Expert
<div> ✓ OK</div>								
Device identification								
IPv4 address	172.20.29.16			Name	CPU 410-5H			
Device category	PLC			Device type	CPU 410-5H F (5HX08-0AB0)			
MAC	00:1B:1B:74:AA:70			System location	sysLocation not set			

¹⁾ Also ET 200S CPU and ET 200pro CPU

SINEC NMS

Use case – Network Validation for systems integrators and solution providers

Task

Minor modifications are to be made to a plant. The contractor must ensure that the new network solution meets the local network requirements on site when the work is done.

Solution

SINEC NMS can validate networks (including validation reports). The condition of the network can be checked, validated and documented. The system integrator can then with confidence sign off the solution to the end customer.

Benefits

Repeatable validation of networks.

Verifiable parameters

Configuration settings

Basic settings

Export topology as image

Device properties

White list for firmware versions

Different firmware versions

IP address parameters

Device name

Duplicate IP addresses

Duplicate MAC addresses

PROFINET

Duplicate PROFINET device name

PROFINET IO devices without assigned controller

Performance (devices)

Device availability

Performance (LAN ports)

Half duplex

Port speed

Interface utilization

Interface error rate

Discarded packets

Power margins of POF ports

Length-dependent power margins of POF ports

Events

Network events

Report as PDF

Validierungsübersicht..... **BESTANDEN**

Mitarbeiter Abteilung / Unternehmen

Geräteigenschaften:

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
White List für Firmware-Versionen	Nein	-	-	-	-
Unterschiedliche Firmware-Versionen	Nein	-	-	-	-
IP-Adressparameter	Ja	Ja	19(20)	-	Bestanden
Gerätenamen	Ja	Ja	10(20)	-	Bestanden

PROFINET:

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
PROFINET IO-Geräte ohne zugeordneten Controller	Nein	-	-	-	-

Leistungsfähigkeit (Geräte):

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
Geräteverfügbarkeit	Ja	Ja	20(20)	-	Bestanden

Leistungsfähigkeit (Ports):

Validierung	Validiert	Obligatorisch	Geprüft	Betroffen	Ergebnis
Halbduplex	Nein	-	-	-	-
Portgeschwindigkeit	Nein	-	-	-	-
Schnittstellen-Auslastung	Ja	Ja	29(69)	-	Bestanden
Schnittstellen-Fehlerrate	Ja	Ja	29(69)	-	Bestanden
Verwerfene Pakete	Ja	Ja	29(69)	-	Bestanden
Dämpfungsrreserven von POF-Ports	Ja	Ja	2(68)	-	Bestanden
Längenabhängige Dämpfungsrreserven von POF-Ports	Ja	Nein	2(68)	2	Fehlgeschlagen

Ereignisse:

Validierung	Validiert	Obligatorisch	Betroffene Ereignisse	Ergebnis
Ereignisse	Ja	Nein	0	Bestanden

Anmerkungen:

Ort, Datum

Unterschrift

Get started with SINEC NMS!

Take the first step to gain full control over your network

Application example / Getting started guide

Web: <https://support.industry.siemens.com/cs/gb/en/view/109762792>

- Setting up SINEC NMS
- Initial Commissioning
- Network Monitoring
- Topology configuration
-

Use and
Understanding of
SINEC NMS

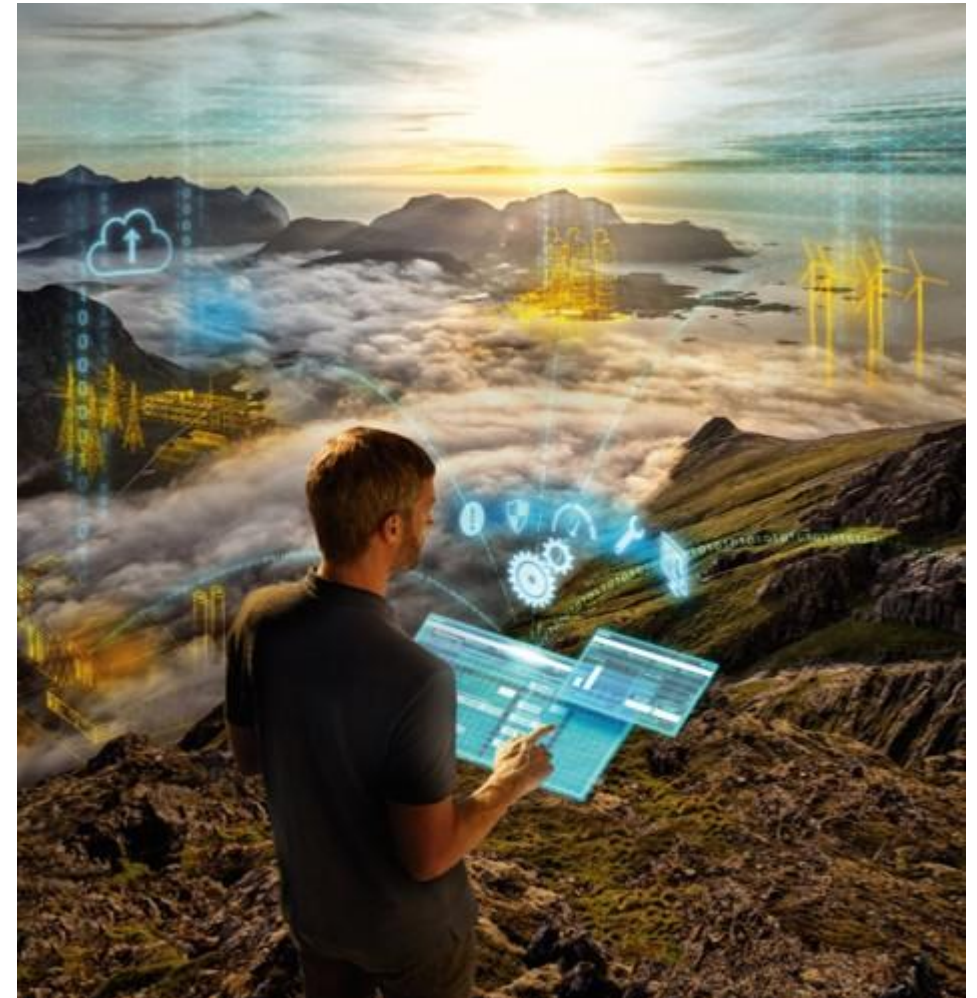
Free 21-day trial licence



Start now!

Download:

<https://support.industry.siemens.com/cs/de/de/view/109762387>



• Questions?

Thank you



Christoffer Karlsson
Product manager
Industrial Communication
+61437584211

Christoffer.karlsson@siemens.com

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations, product names, etc. may contain trademarks or other rights of Siemens AG, its affiliated companies or third parties. Their unauthorized use may infringe the rights of the respective owner.

More information:

[siemens.com/sinec-nms](https://www.siemens.com/sinec-nms)