

Industrial Communication

Sigurna i efikasna komunikacija u industrijskom okruženju!"

© Siemens AG 2020

[siemens.com](https://www.siemens.com)

Digitalization and big data address key industry trends



Digitalization

Industrie 4.0



Industrial Internet of Things (IIoT)

Big Data

Different requirements for OT and IT



IT FOCUS:

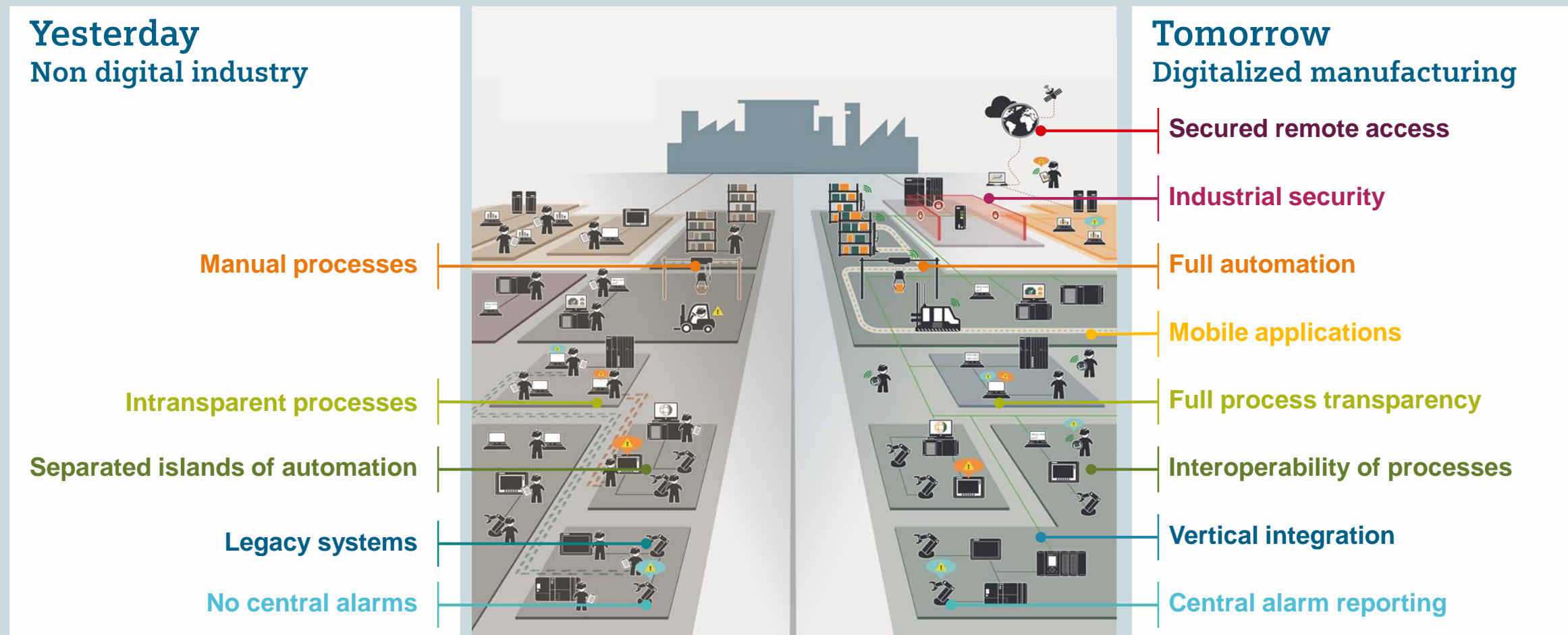
- **User experience:** performance of the transmission of data such as telemetry, location, voice, and video over a common infrastructure

- **Cybersecurity**

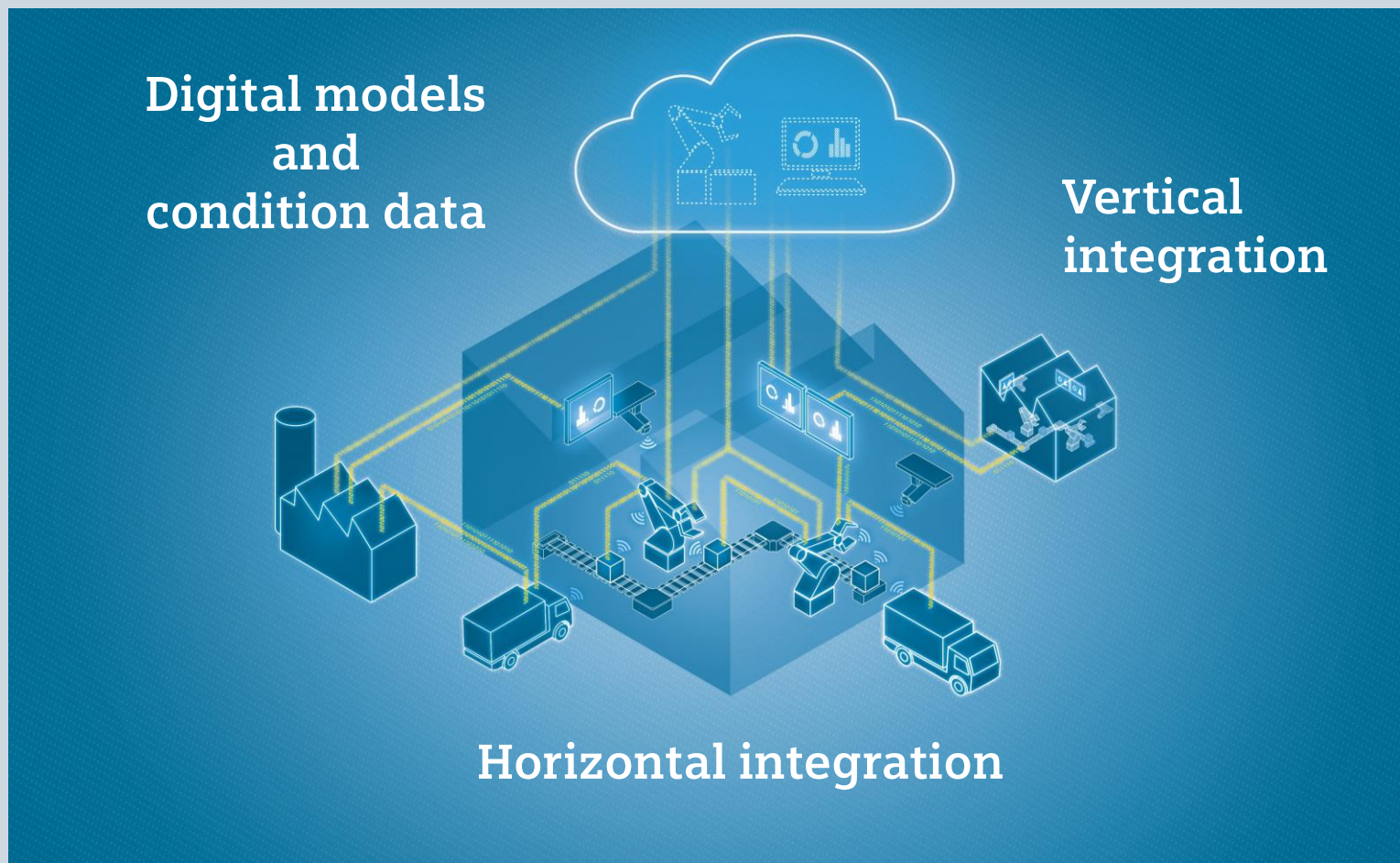
OT FOCUS:

- **Secure operation of plants:** reliable data exchange of time-critical applications – even in harsh environments
- **Constant availability:** 24/7
- <https://new.siemens.com/global/en/products/automation/topic-areas/industrial-communication-networks/ot-it-separation.html>

Digitalization will change the way you work...



...and this requires powerful communication networks in the industrial space



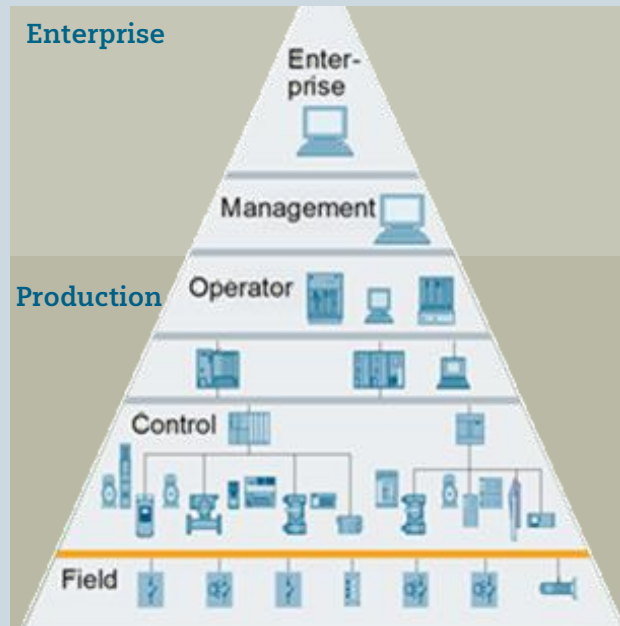
Strong communication networks to handle massive amount of data required

- **High speed:** Real-time communication
- **High data volumes:** Large bandwidth
- **Protect against spying and attacks:** Secure communication
- **Ensured connectivity:** Robust and reliable components and networks
- **Flexibility:** Plug'n'play, on demand and easy (re-)configuration

Digitalization results in enterprise and production layer to get closer connected

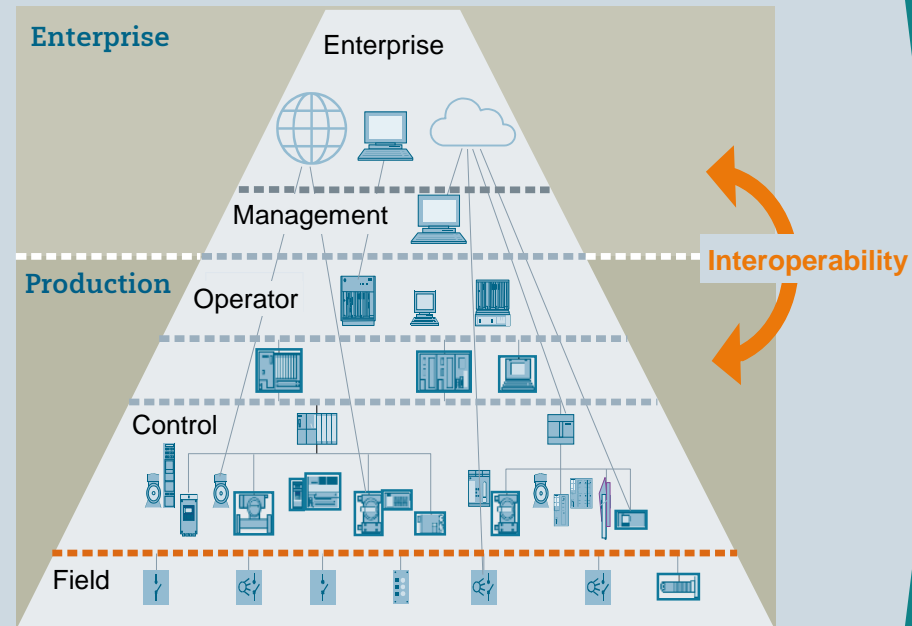
SIEMENS

Yesterday:
Limited interoperability



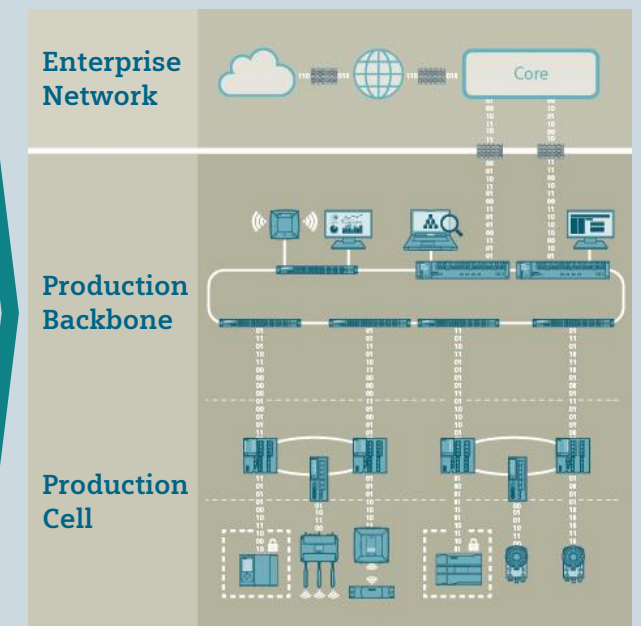
Limited communication between
enterprise and production layer

Today: Arising challenges through
increasing interoperability



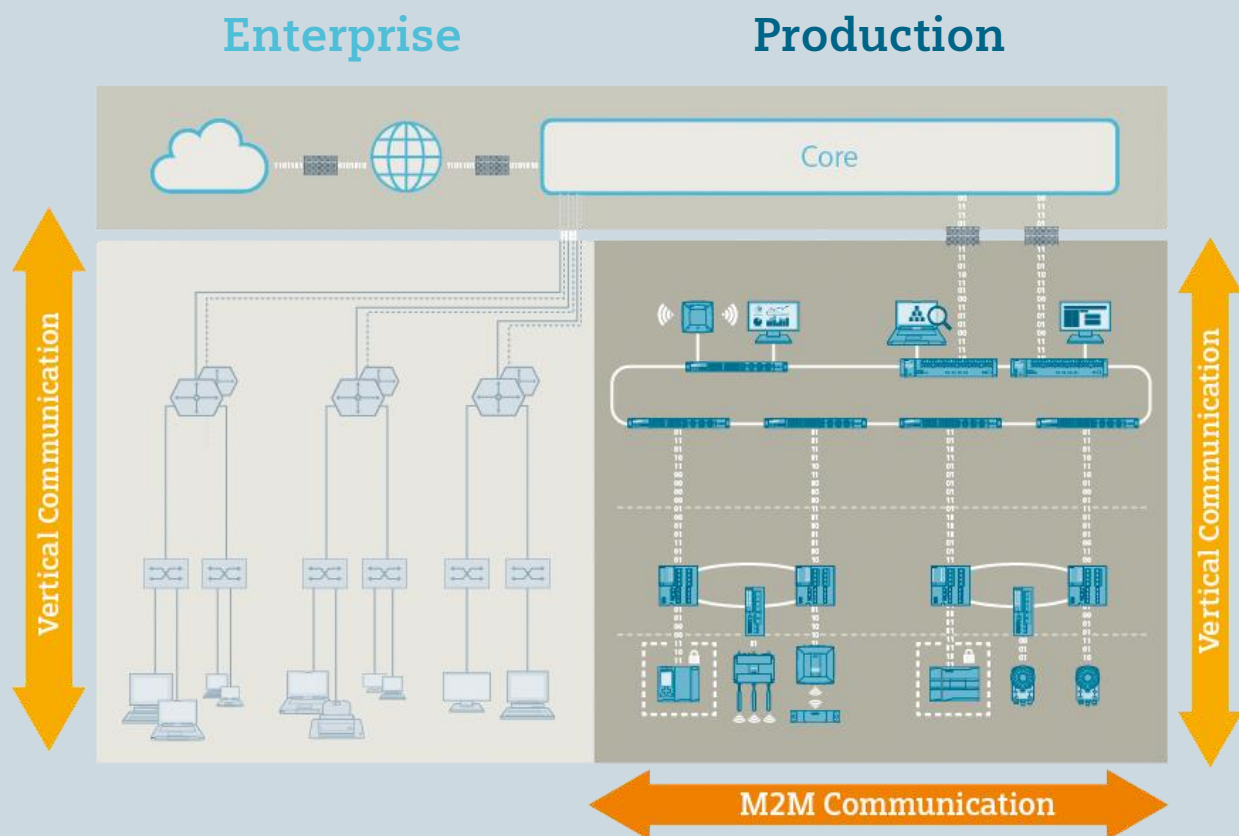
Challenge to handle complexity of
increasing communication

Future: Defined interface to
handle complexity



Two dedicated networks with
defined managed interface

Industrial Networks have critical requirements which need to be addressed



High Availability

To avoid significant economic losses or other damages



Robustness

Extreme temperatures, dusty or corrosive environments



Flexibility

Optimization and innovation causes changing production layouts



Determinism

Real-time requirements of automation tasks



Security

Threat of unauthorized access; secure remote access, e.g. for OEMs



Mobile Applications

Reliable communication, e.g. for automated guided vehicles, monorails



Safety

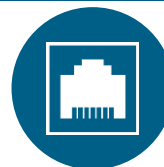
Fail-safe communication to provide safety for operators and assets

SCALANCE – Industrial Communication portfolio

SCALANCE: Industrial Communication proved to enable communication in production

- **High availability**
based on industrial features and industrial design
- **Fast & easy integration**
for new and existing networks based on TIA design
- **Easy to use**
with configuration via Web Based Management or TIA Portal
- **Easy device replacement**
with C-PLUG, also by untrained staff
- **For all Ethernet networks**
local, wireless and remote

Our Portfolio



Wired

- Industrial features
- Industrial design
- Fast & easy integration



Remote

- Different medias (DSL, UMTS, LTE)
- Transparent connectivity
- Easy enrollment with SINEMA RC



Wireless

- Indoor and outdoor applications
- Several country approvals
- Real-time capability



Security

- Firewall & VPN
- Remote access
- Fits to industrial security concepts



Software

- Transparency for the industrial network
- Integration into HMI / SCADA systems



Industrial Networks have critical requirements which need to be addressed



High Availability

To avoid significant economic losses or other damages



Robustness

Extreme temperatures, rugged, e.g., dusty or corrosive environments



Flexibility

Optimization and innovation causes changing production layouts



Determinism

Real-time requirements of automation tasks



Security

Threat of unauthorized access; secure remote access, e.g., for OEMs



Mobile Applications

Reliable communication e.g., for automated guided vehicles, monorails



Safety

Fail-safe communication to provide safety for operators and assets

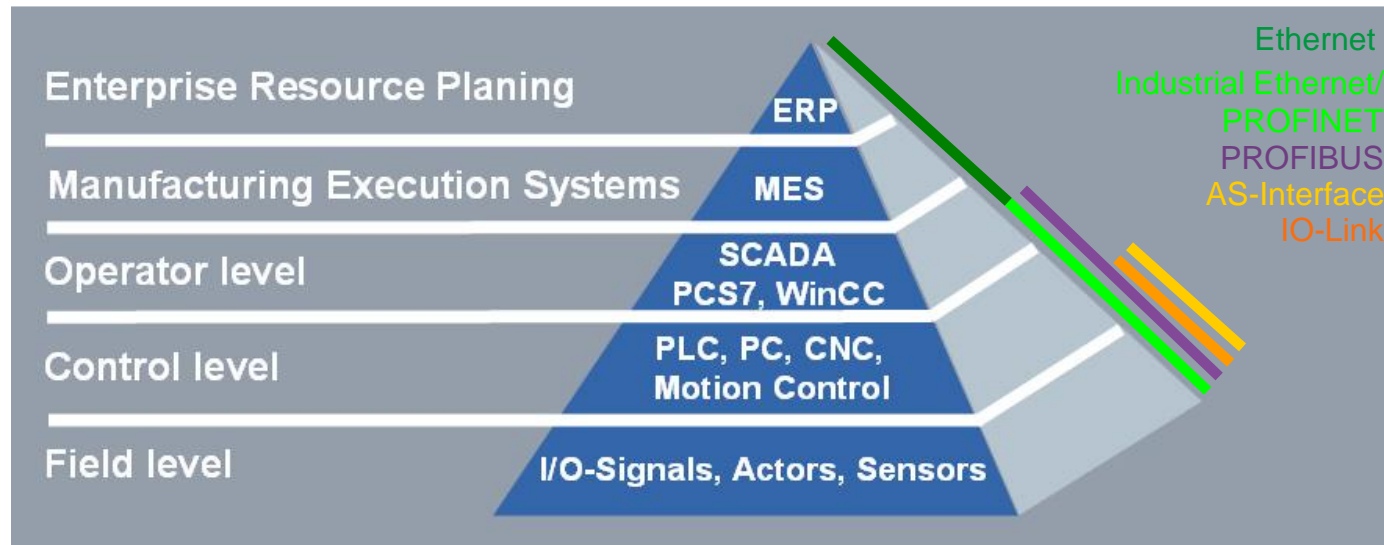
- **Ring redundancy** e.g., with MRP, HSR, PRP,...
- Quick and easy replacement with **C-PLUG**
- **Fanless design** to avoid downtimes
- **FastConnect** cables and plugs
- **Modularity**
- **Different interfaces** for electrical / optical connections
- **Guaranteed switchover** times in case of failures or **deterministic roaming** for wireless applications
- **Security modules** which fit to industrial security concepts
- **IWLAN RCoax Cable** for durable wireless connection during movement
- **Emergency shutdown over PROFINET** (wired as well as wireless)

Bus systems for the industry

PROFINET/Industrial Ethernet	
Industrial Ethernet (IEEE 802.3)	– the industrial standard based on the international Ethernet standard
PROFINET (IEC 61158/61784)	– the open Industrial Ethernet standard for automation
Industrial Wireless LAN (IEEE 802.11)	– the industrial standard for wireless communication based on the international standard
PROFIBUS	
PROFIBUS (IEC 61158/61784)	– the international standard for the field level is the global market leader among fieldbus systems
AS-Interface	
AS-Interface (IEC 62026-2/EN 50295)	– the international standard, which, as an economical alternative to the cable harness, links sensors and actuators by means of a two-wire line
IO-Link	
IO-Link	– the standard for intelligently connecting sensors and actuators from the field level to the MES level

G_IKT10_XX_000002

Operation of industrial bus systems



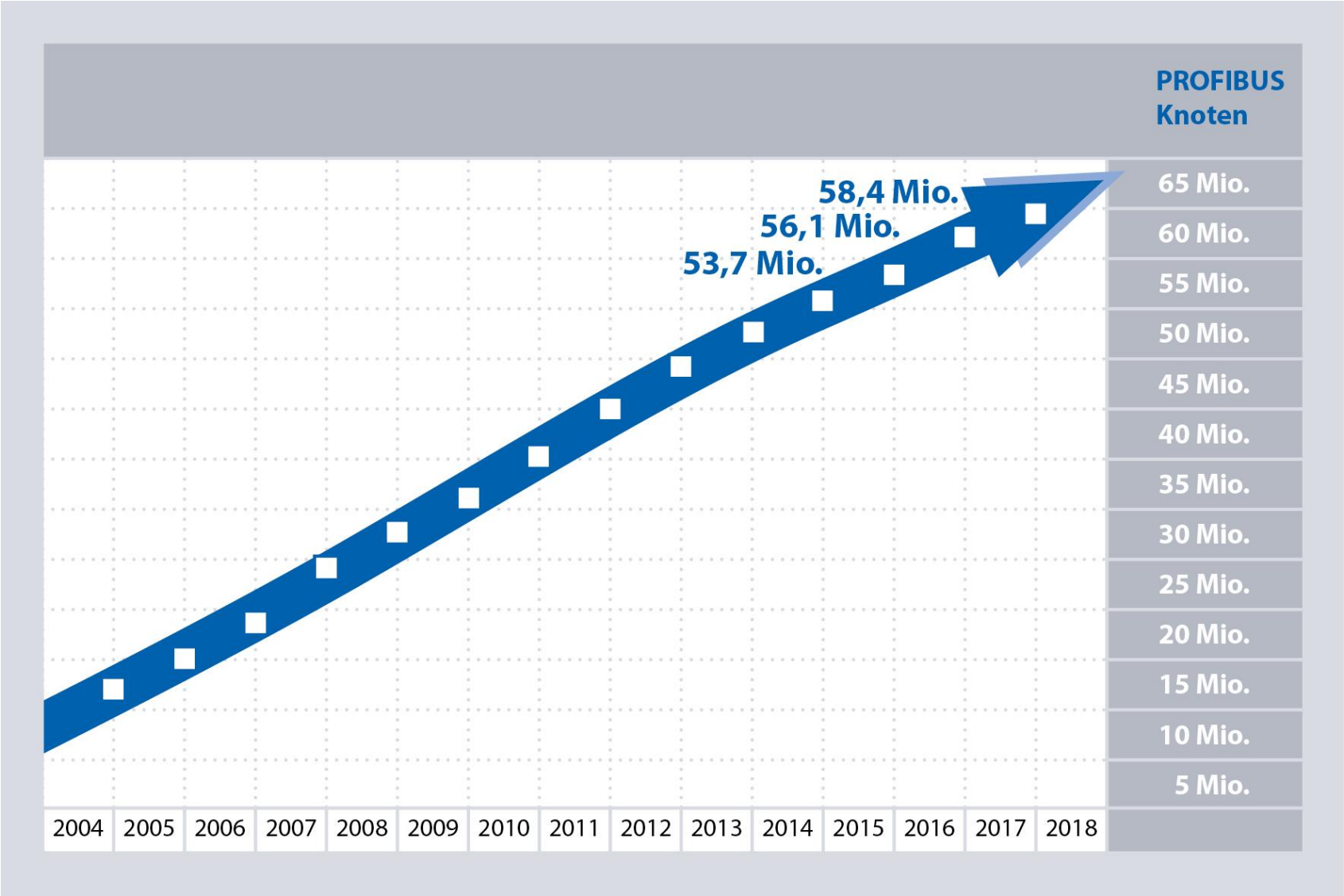
PROFIBUS-/PROFINET nodes



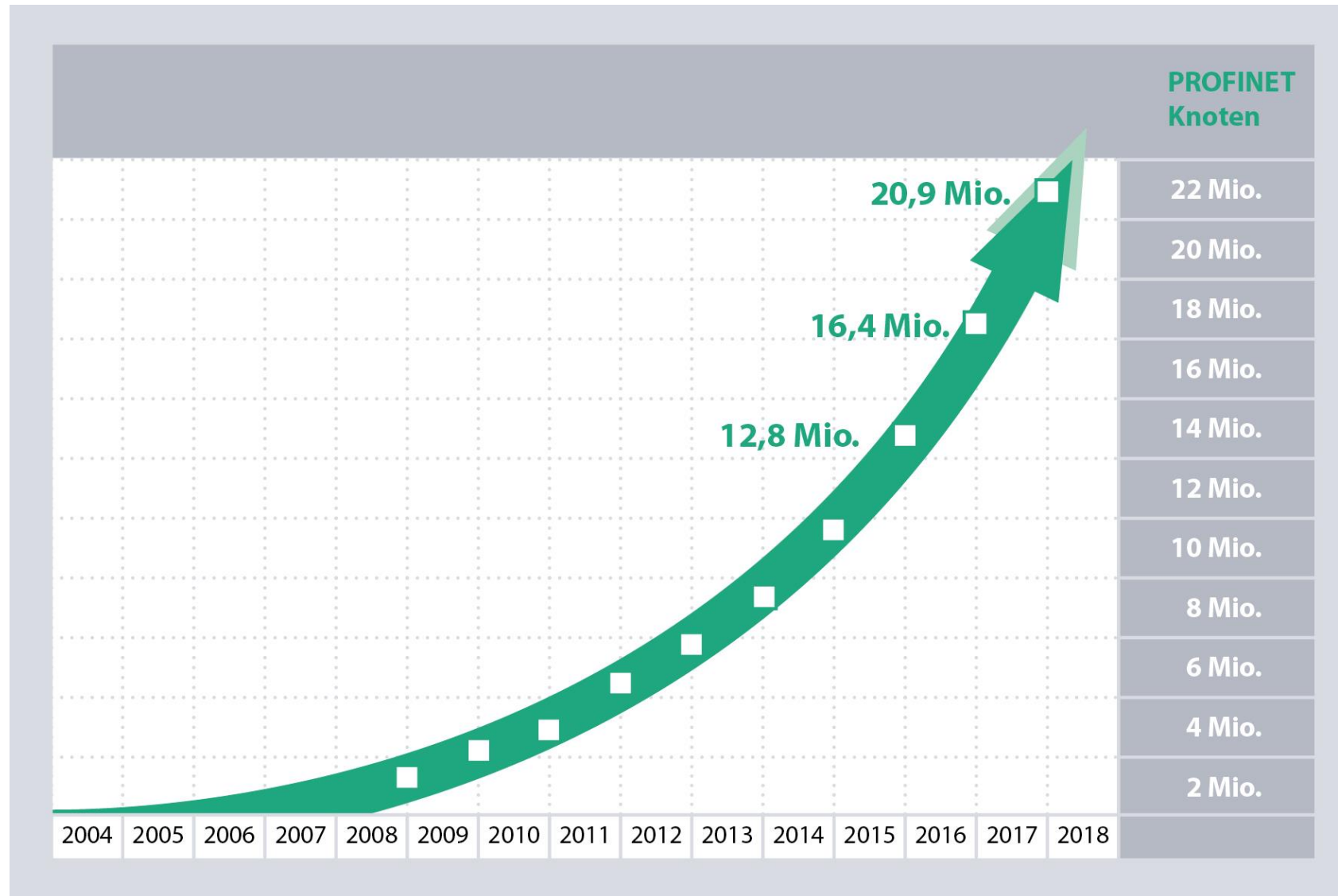
Counting the nodes of PROFIBUS and PROFINET, numbers from various vendors of actually sold nodes are notarized.



Nodes - PROFIBUS



Nodes - PROFINET



Industrial Communication

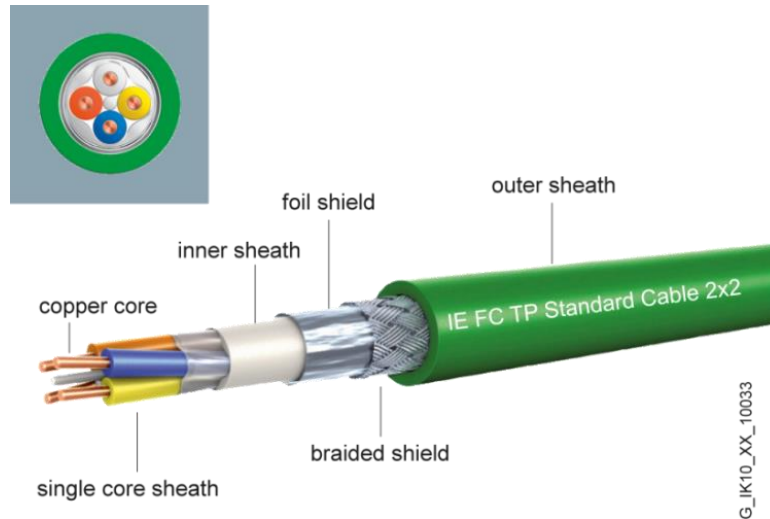
Passive network components

Transfer media - comparisons

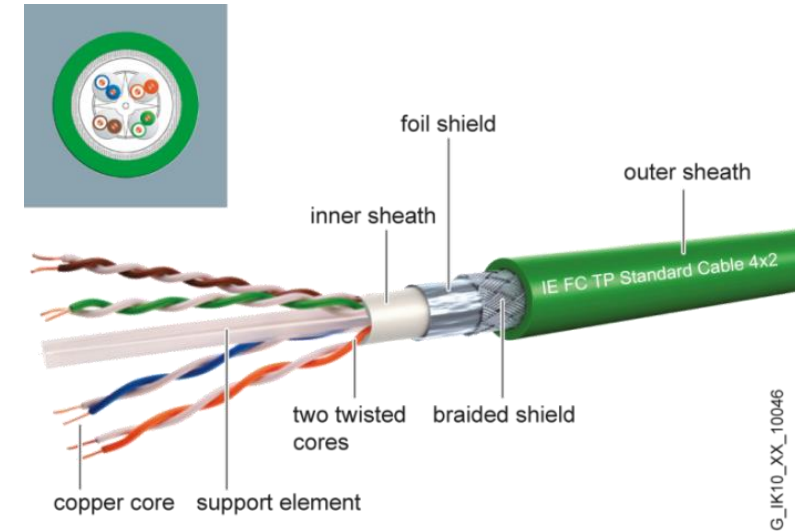
	Twisted pair network	Fiber optic network	Wireless link
Max. network expansion	5000 m ⁴⁾	Up to 150 km: over 150 km, consider signal propagation time	1000 m per segment ⁵⁾
Max. distance between two network nodes / Access Points	100 m	50 m POF 100 m PCF 3000 m multimode 70,000 m single mode	30 m indoors per segment 100 m indoors per segment
Max. connecting cable length	100 m	50 m POF 100 m PCF 3000 m multimode 70,000 m single mode	100 m feeder cable to the Access Point
Pre-assembled cables	Yes	Yes	—
Assembly on site	without special tool; FastConnect technology	Special tool required	with specialist personnel
Integrated diagnostics support	LED indicators; signaling contact; SNMP network management; Web-based management, PROFINET diagnostics	LED indicators; signaling contact; SNMP network management; Web-based management, PROFINET diagnostics	LED indicators; SNMP network management; Web-based management
Redundant network structures	Electrical ring or doubling of the infrastructure (linear, star, tree)	Optical ring or doubling of the infrastructure (linear, star, tree)	Multiple illumination or use of different frequency bands (2.4 and 5 GHz)
<div> <div> 1) suitable for 10 Mbit/s, 100 Mbit/s and 1000 Mbit/s 2) Safeguard against subnetwork failure by means of redundant voltage supply 3) no effect in the case of ring structure 4) if there are 50 switches in the ring 5) depending on antenna used </div> <div> ● ● ● ● suitable ● ● ● ○ partly suitable ● ● ○ ○ ○ ○ ○ ○ not applicable </div> </div>			

Design of the Industrial Twisted Pair cable

4-Core, CAT5e for 10/100 MB/s Ethernet:



8 Core, CAT6 for Gigabit Ethernet:

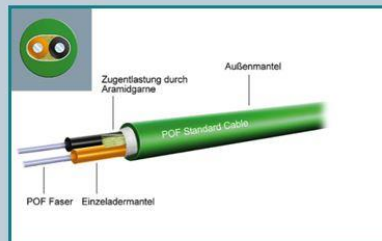


- Standard, flexible, train, marine and TP cables
- Sold by the meter
- Not pre-assembled

Fiber-optic cables for Industrial Ethernet/PROFINET

POF cables

- Up to 50 m cable length (980/1000)
- SC RJ plug for PROFINET standardized
- Quick and easy assembly on site
- POF diagnostics in SCALANCE X devices
- Type of delivery: Sold by the meter



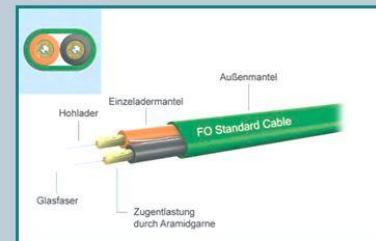
PCF cables

- Up to 100 m cable length (200/230)
- SC RJ plug for PROFINET standardized
- Pre-assembled cables for easy laying of cables
- Quick and easy assembly on site
- Type of delivery: Sold by the meter and pre-assembled



Standard fiber-optic cables

- Long cable lengths:
SM: 200 km MM: 5 km
(9/125) (50/125)
- Pre-assembled cables for easy laying of cables
- Fiber monitoring in SCALANCE X204-2FM
- Type of delivery: Sold by the meter and pre-assembled



FC fiber-optic cables

- Long cable lengths:
MM: 3 km
(62.5/200/230)
- Quick and easy assembly on site
- Suitable for SC, ST/BFOC and LC plugs
- Type of delivery: Sold by the meter



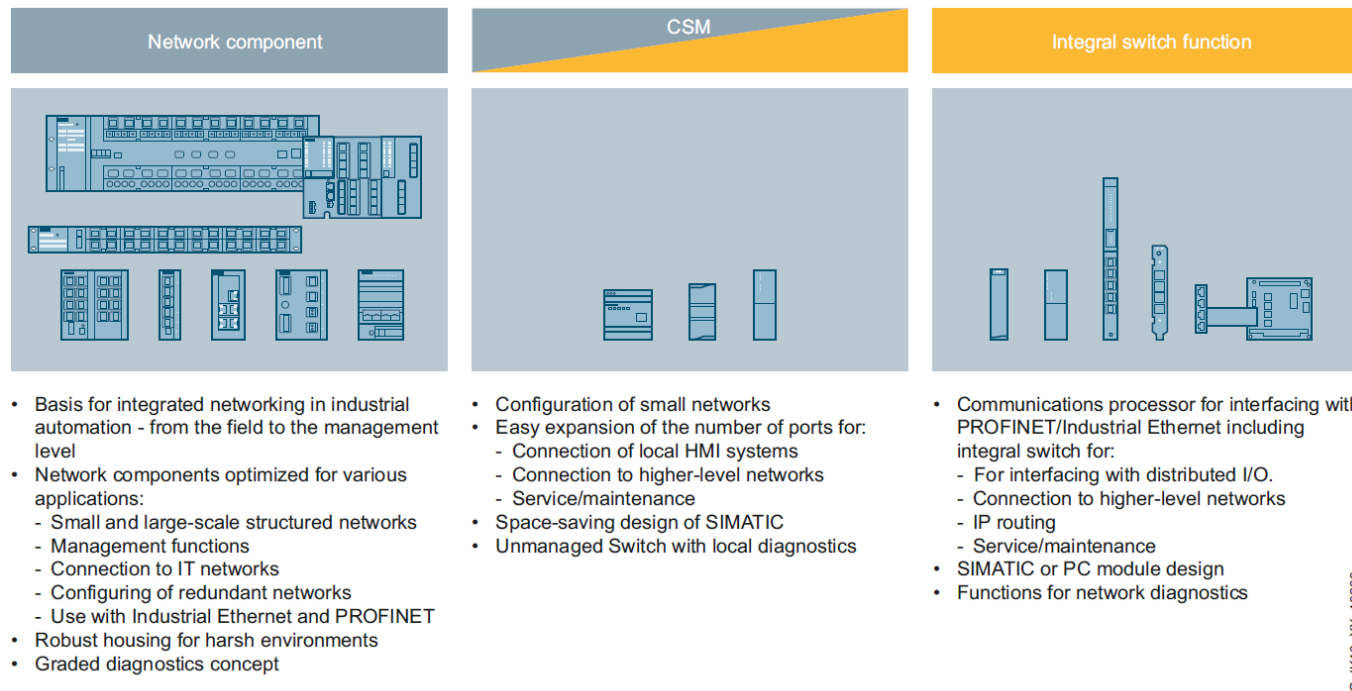
Industrial Communication

SCALANCE X - Portfolio

The suitable switch for every application

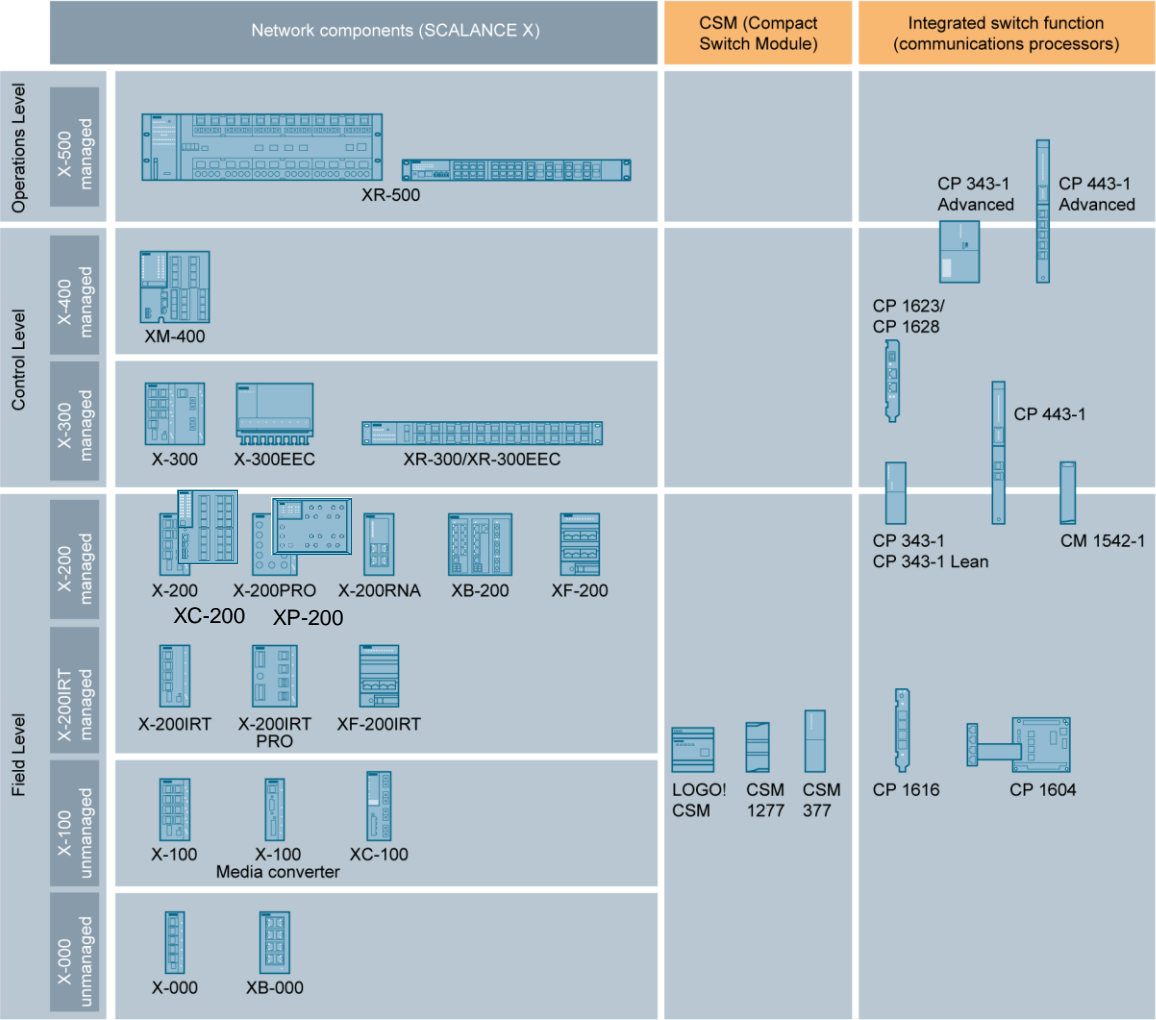
There are three characteristic types of Industrial Ethernet switch

- Stand-alone network components (SCALANCE X)
- Modules in a control module or I/O module (CSM)
- Integrated into a communications processor (CP with integral switch)



G_1K10_XX_10238

Positioning of Industrial Ethernet Switches



G_K10_XX_10237

General explanations of terminology

Unmanaged Layer 2 Industrial Ethernet Switches

SIEMENS

Feature / function

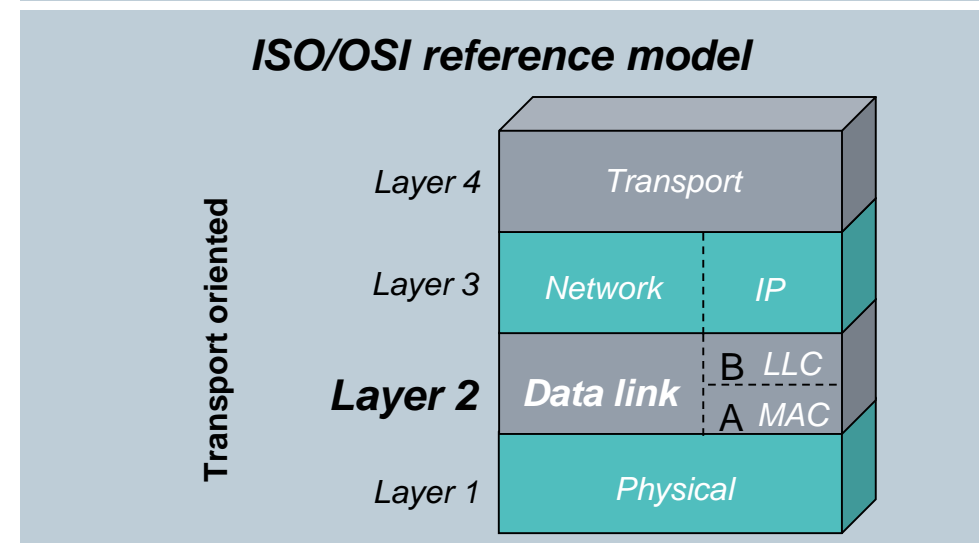
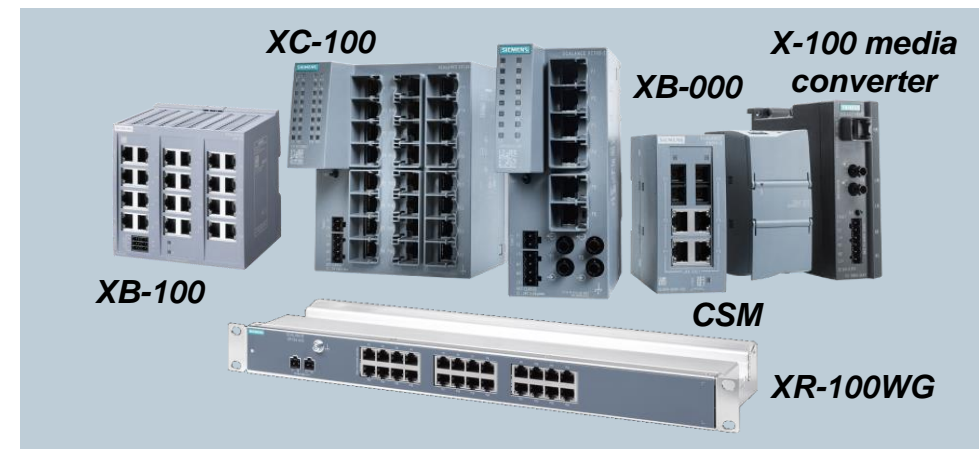
- Simple connection to the network (Plug&Play)
- Local monitoring and control is possible with LED display and signaling contact
- Use typically in small networks

Benefits

- Cost-effective solution for setting up electrical and optical line bus and star structures (optical up to 26 km)
- Space-saving installation due to compact design
- Simple expansion of Industrial Ethernet networks
- Fast commissioning without configuration
- High data rate up to 1 Gbps
- Suitable for building automation (XB-000, XB-100 with AC 24 V)

SCALANCE product lines

X-000, XB-000, XB-100, XC-100, XR-100WG, media converter X-100, Compact Switch Modules (CSM)



Note: Link to technical slides „unmanaged Switches“

General explanations of terminology

Managed Layer 2 Industrial Ethernet Switches SCALANCE X

SIEMENS

Feature / function

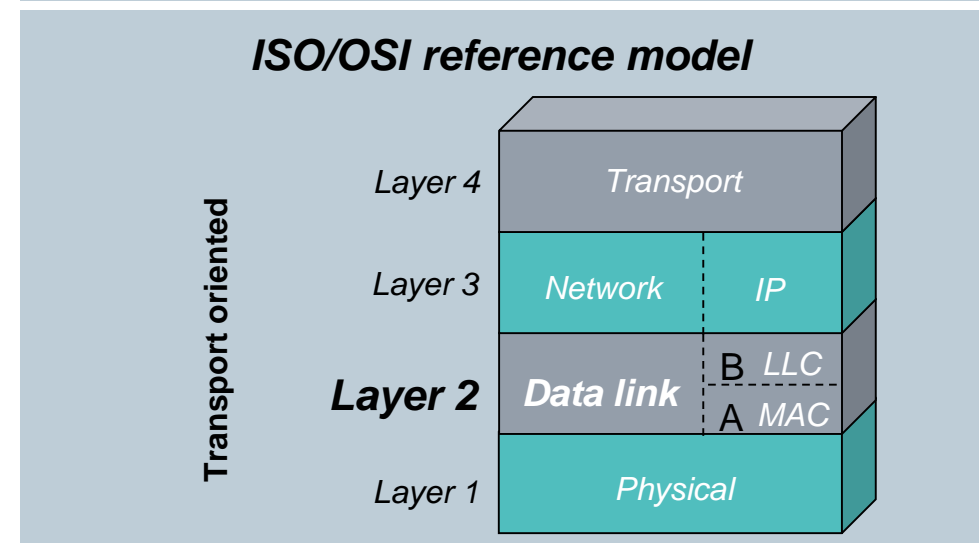
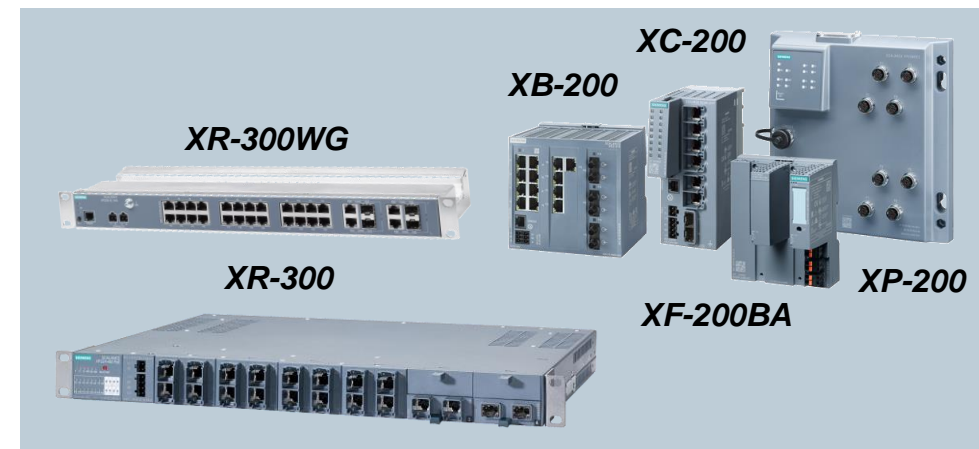
- Support SNMP (Simple Network Management Protocol) via integrated agents and have CLI command lines (Command Line Interface) that can be accessed via serial console, Telnet and Secure Shell
- Often configured / managed as a group of several switches
- Structuring of large networks using virtual LANs (VLANs)
- Configuration and diagnostics also possible via the network management software SINEC NMS

Benefits

- High availability due to redundancy functions
- Simple monitoring and diagnostics with signaling contact, SNMP, digital inputs, SINEC NMS and PROFINET diagnostics
- Simple adaptation to different network structures
- Reduction of storage costs due to modularity
- Simple device replacement with C-PLUG plug-in exchangeable medium

SCALANCE product lines

X-200¹⁾, XB-200, XC-200, XF-200, XF-200BA, XP-200, X-300, XR-300, XR-300WG, XM-400, XR-500



¹⁾ Except X-200RNA

General explanations of terminology

Managed Layer 3 Industrial Ethernet Switches SCALANCE X

SIEMENS

Feature / function Communication beyond the boundaries of subnets

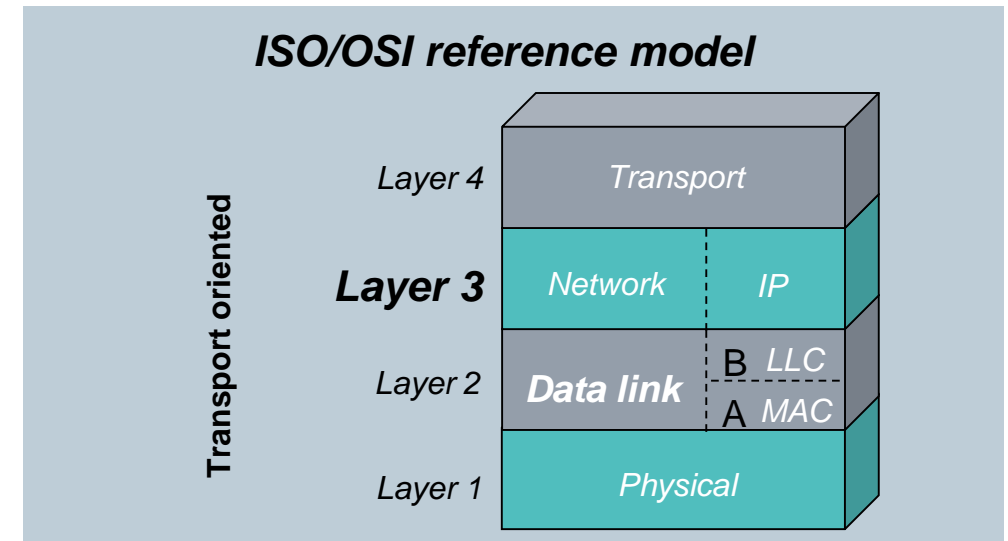
- Connection of subnets
- Routing
- Limitation of broadcast domains
- Support all layer 2 functionalities

Benefits

- Offer all the advantages of layer 2 managed switches
- Simple networking and structuring of high performance industrial networks
- Connection of Industrial Ethernet networks to IT networks
- Increase of network availability by routing

SCALANCE product lines

XM-400, XR-500



TIA Selection Tool

To support the selection of Industrial Ethernet Switches and the configuration of the modular variants, the **TIA Selection Tool** may be used:

<http://w3.siemens.com/mcmts/topics/en/simatic/tia-selection-tool/Pages/tab.aspx>

The screenshot displays the TIA Selection Tool interface, which is used for configuring industrial communication components. The main window shows the configuration of a SCALANCE X-500 switch, with a focus on the 'Gerätekonfiguration' (Device Configuration) tab. The configuration is organized into a tree structure on the left, including sections like 'Anlagenkonfiguration', 'Steuerungen', 'IO Systeme', 'Panels', 'Industrie PCs', 'Motoren und Antriebe', 'Industrielle Schaltungstechnik', 'Software', 'Industrielle Kommunikation', 'Stromversorgung', and 'SIMATIC Ident'.

The central part of the interface shows the 'Gerätekonfiguration' (Device Configuration) for the SCALANCE X-500 switch. It includes a visual representation of the switch's modular architecture, showing various ports and modules. Below this, a table lists the available modules and their specifications:

Artikelübersicht	Eigenschaften	Meldungen	Baugruppe	Baugruppenträger	Steckplatz	Bestellnummer
SCALANCE XR552-12M, Ports hinten, IP-Routing (Layer 3) vorbereitet				SCALANCE XR552-12M, Ports hinten		6GKS552-0AA00-2HR2
MM992-4CuC, 4 x 10/100/1000 Mbit/s RJ45-Ports, elektrisch				SCALANCE XR552-12M, Ports hinten	1	6GKS992-4GA00-8AA0
MM992-4CU, 4 x 10/100/1000 Mbit/s RJ45-Ports, elektrisch				SCALANCE XR552-12M, Ports hinten	2	6GKS992-4SA00-8AA0
MM992-4PDEC, 4 x PoE 100/1000Mbit/s RJ45-Ports, elektrisch				SCALANCE XR552-12M, Ports hinten	3	6GKS992-4RA00-8AA0
MM991-4, 4 x 100 Mbit/s BFOC-Ports, optisch, Multimode, Glas, bis max. 5 km				SCALANCE XR552-12M, Ports hinten	4	6GKS991-4AR00-8AA0
MM991-4LD, 4 x 100 Mbit/s BFOC-Ports, optisch, Singlemode, Glas, bis max. 26 km				SCALANCE XR552-12M, Ports hinten	5	6GKS991-4AC00-8AA0
MM992-4, 4 x 1000 Mbit/s SC-Ports, optisch, Multimode, Glas, bis max. 750 m				SCALANCE XR552-12M, Ports hinten	6	6GKS992-4AL00-8AA0
MM992-4SFP, für SFP-Stecktransceiver, 1 x 100 oder 1 x 1000 Mbit/s Multimode oder Singlemode, Glas				SCALANCE XR552-12M, Ports hinten	7	6GKS992-4AS00-8AA0
MM992-4LD, 4 x 1000 Mbit/s SC-Ports, optisch, Singlemode, Glas, bis max. 10 km				SCALANCE XR552-12M, Ports hinten	9	6GKS992-4AM00-8AA0
MM992-4SFP, für SFP-Stecktransceiver, 1 x 100 oder 1 x 1000 Mbit/s Multimode oder Singlemode, Glas				SCALANCE XR552-12M, Ports hinten	10	6GKS992-4AS00-8AA0

On the right side of the interface, there is a 'Katalog' (Catalog) section with a search bar and a list of available modules. The list includes various optical and electrical modules, such as MM992-4PDEC, MM991-4, MM991-4LD, MM992-4, MM992-4LD, MM992-4SFP, and MM991-1. The 'Zubehör' (Accessories) section lists items like POWER SUPPLY PS598-1 and KEY Plug Layer 3.



SIEMENS
Ingenuity for life

IS
for life

Industrial Communication

SCALANCE X – Redundancy and VLAN

Network availability - Requirement

Reliable networks capable of withstanding failures are achieved by:

- Reliable devices
- Fault-tolerant systems
- **Redundancy**

The network should have a topology that allows fast convergence following a fault.

Requirements:

- Automatic reconfiguration following line failure
- Automatic reconfiguration following port deactivation
- Automatic reconfiguration following component failure
- Load distribution
- Monitoring of redundancy mechanisms

Network availability– Redundancy methods

Layer 2 - Redundancy:

- **Media Redundancy Protocol (MRP - IEC 62439-2)**
- **High Speed Redundancy Protocol (HRP - SIEMENS)**
- **Standby-Connection (SIEMENS)**
- **Spanning Tree Protocol (STP - IEEE 802.1d)**
- **Rapid Spanning Tree Protocol (RSTP - IEEE 802.1d-2004)**
- **Passive Listening (Siemens)**
- **RSTP Big Network Support (IEEE 802.1d-2004 - SIEMENS)**
- **Link-Aggregation (LACP)**
- **Multiple Spanning Tree Protocol (MSTP - IEEE 802.1s)**
- **Media Redundancy Protocol Duplication (MRPD - IEC 61158)**
- **Redundant Network Access (RNA - SIEMENS)**
 - **Parallel Redundancy Protocol (PRP - IEC 62439-3)**
 - **High Availability Seamless Redundancy (HSR / HaSaR - according to IEC 62439-3)**

Layer 3-Redundancy

- **Dynamic Routing (RIP, OSPF)**
- **Redundant-Router (HSRP/VRRP)**

What are VLANs?

Virtual Local Area Network (VLAN) are **logical networks**, which operate based on **physical network infrastructure**.

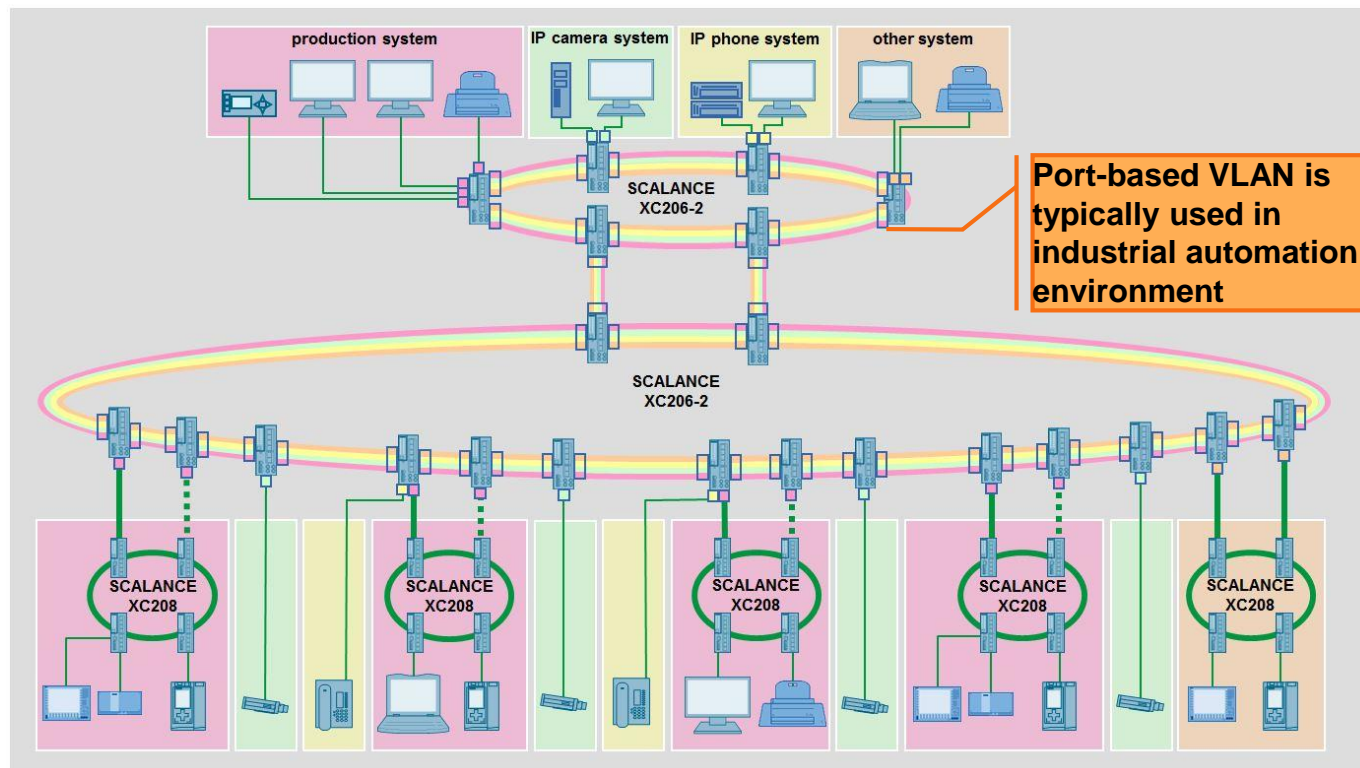
VLANs separate the data traffic of the network devices and allow:

- to build **flexible network structures** independent of the physical network aspects and fixed infrastructure.
- to **separate application and user** of the network based on organisational aspects.
- to generate **broadcast-domains** which limit the distribution of broadcast.
- to generate virtual workgroups with respect to **security** and **access**, but no authentication or encryption.

VLAN – Types

There are different type of VLAN:

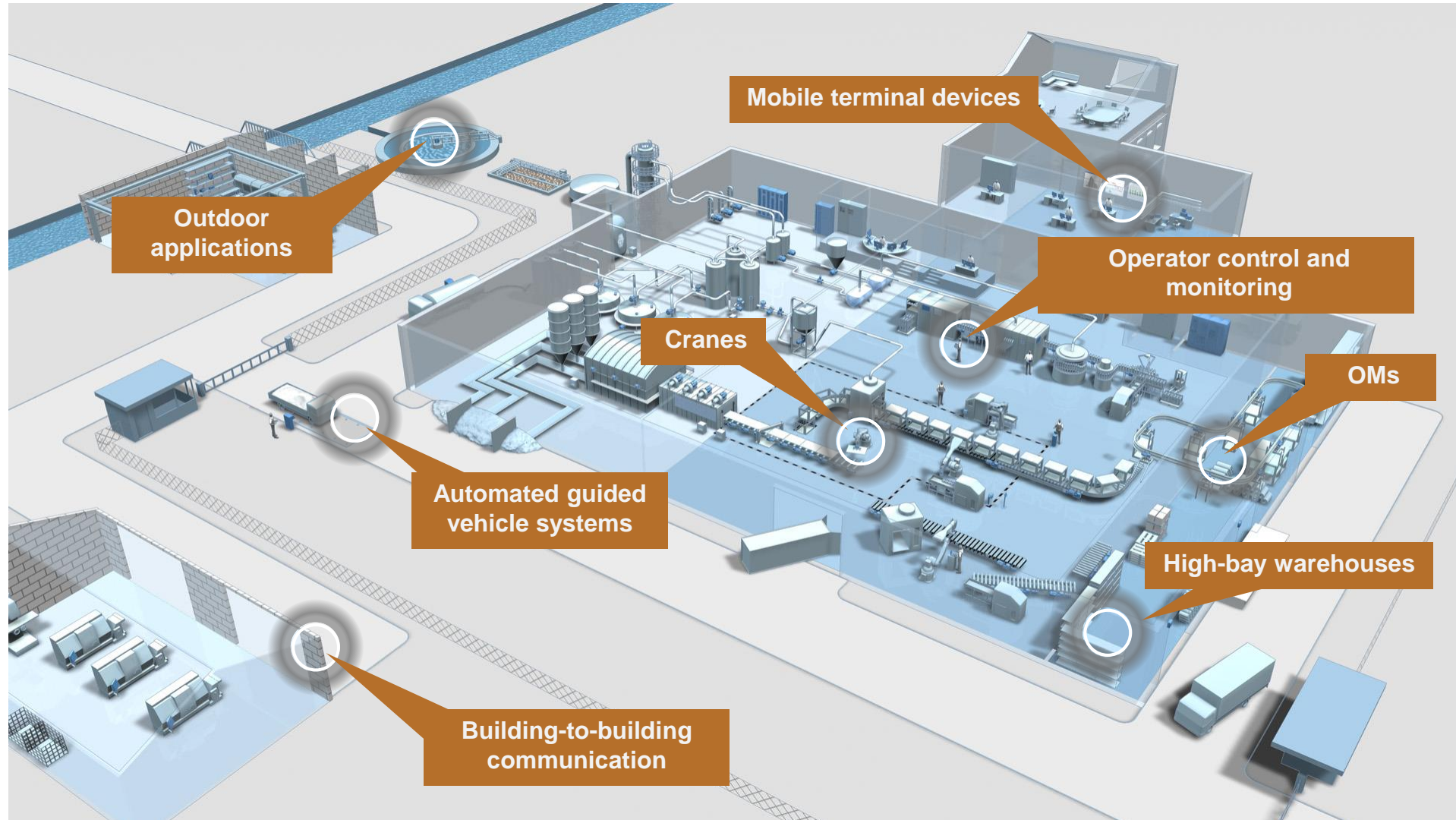
- Port-based VLAN (Layer 2)
- MAC-address-based VLAN (Layer 2)
- IP-address-based VLAN (Layer 3)
- Protocol-based VLAN (Layer3)



Industrial Communication

IWLAN Overview

Applications

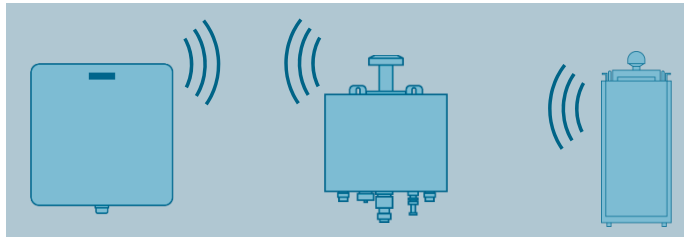


Overview of wireless technologies



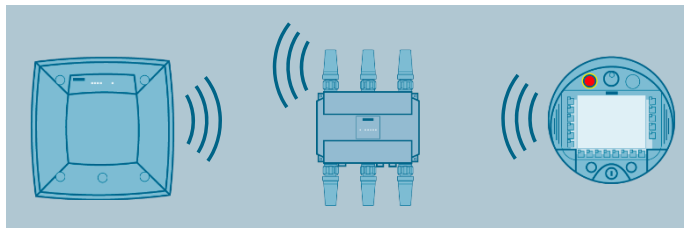
Wireless Remote Networks

For remote access to distributed systems via mobile radio.



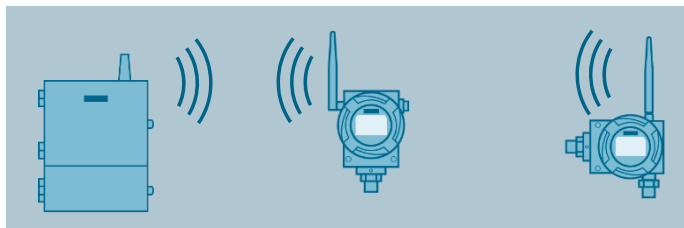
WiMAX

Used for longer ranges as per IEEE 802.16e-2005.



IWLAN - Industrial Wireless LAN

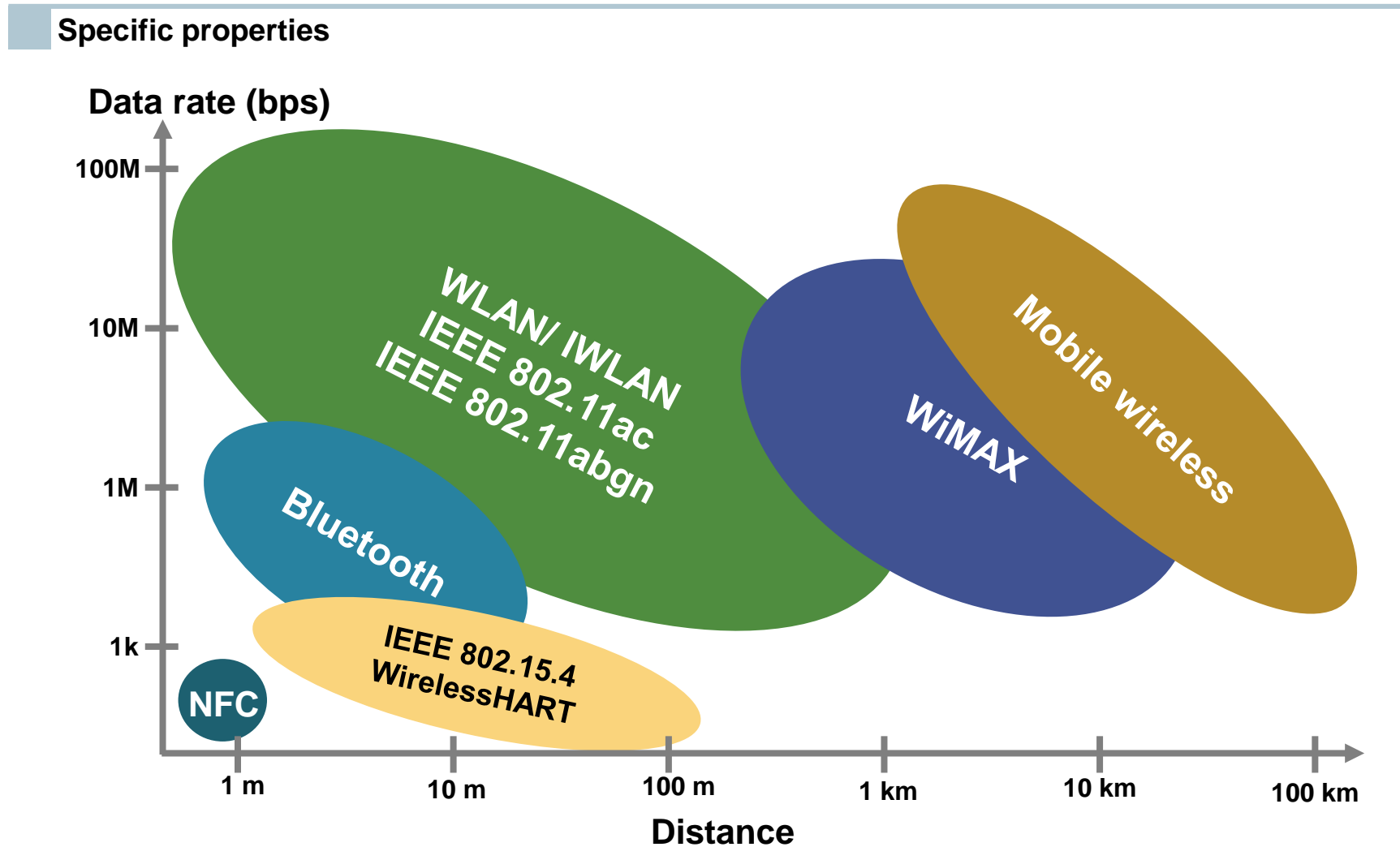
For local wireless networks for communication between controllers, HMI and peripheral systems as an expansion or alternative to cables, sliding contacts, and data light barriers



WirelessHART

For flexible, wireless connection of field devices in process automation.

Comparison of wireless technologies



Industrial Communication

Security Basics

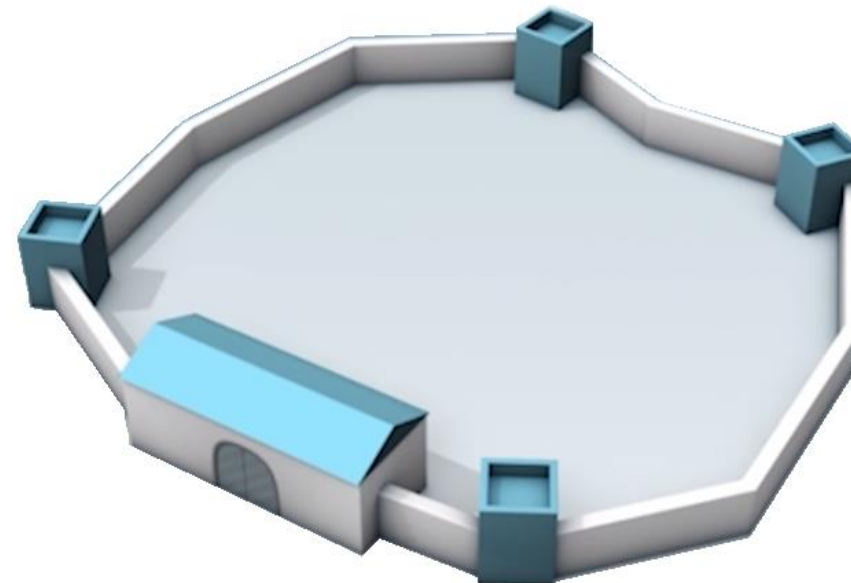
Comprehensively protecting productivity



Single-layered protective measures

A wall as a protective measure

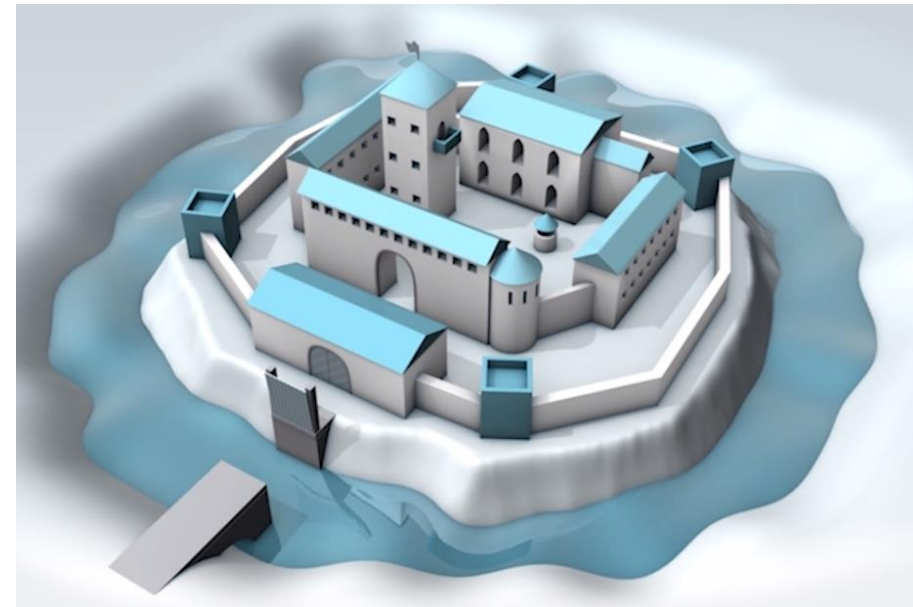
- Single-layered protection
- A point of attack
- One-time investment of time and effort



Multi-layered protective measures

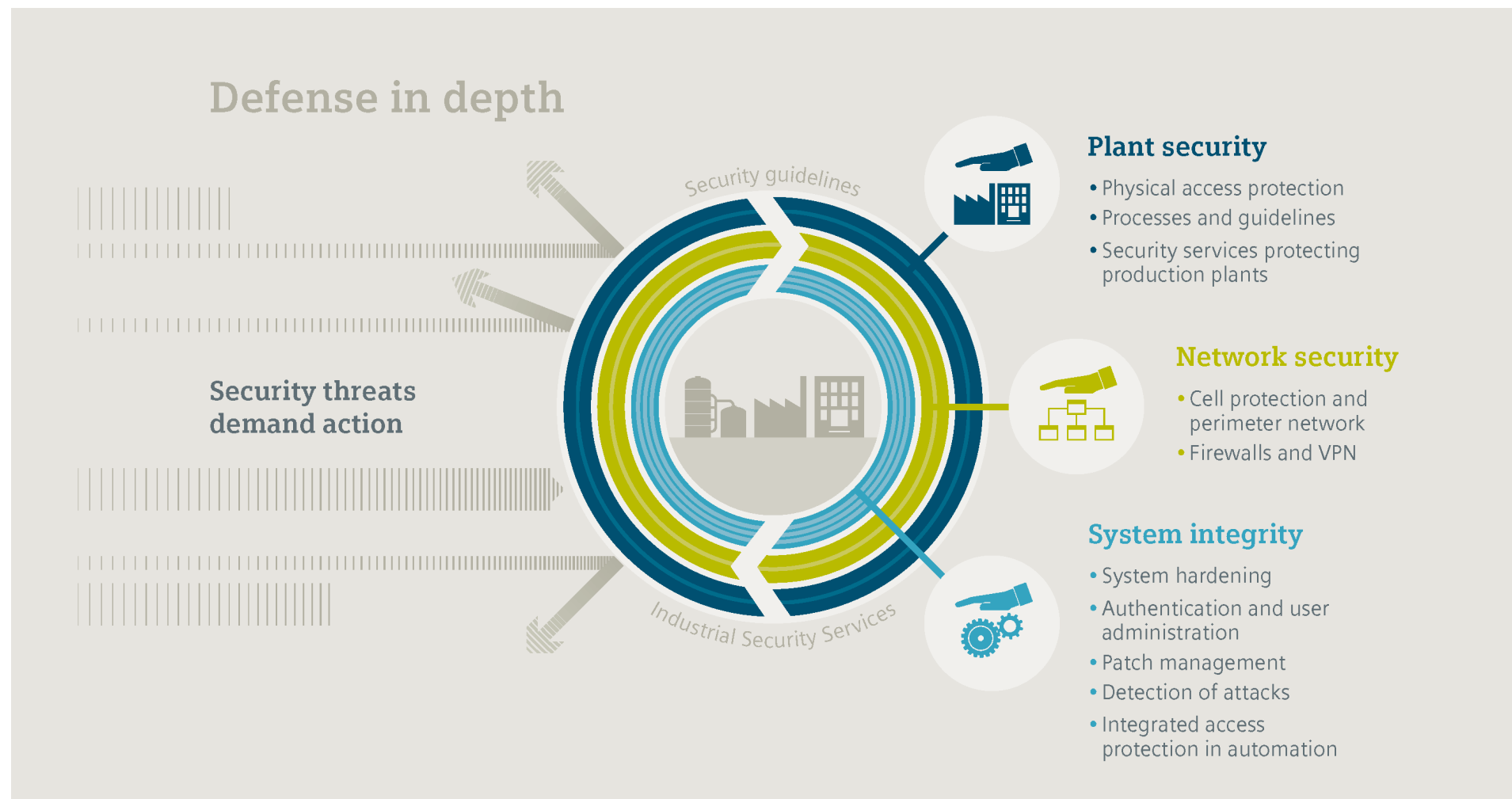
Protective measures of a castle

- Multi-layered protection
- Each layer supports the others
- Breaking each transition requires renewed investment of time and effort



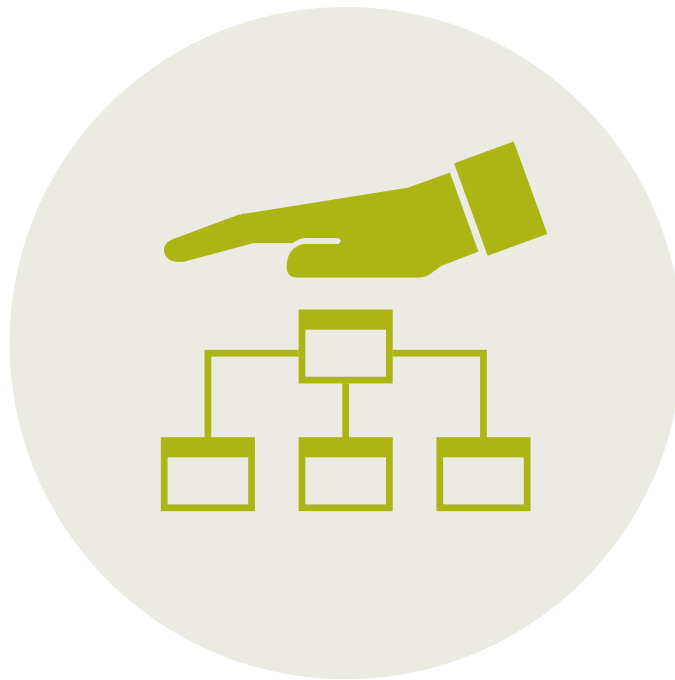
Defense in Depth

Multi-layered protective measures



Defense in Depth

Multi-layered protective measures



Network security

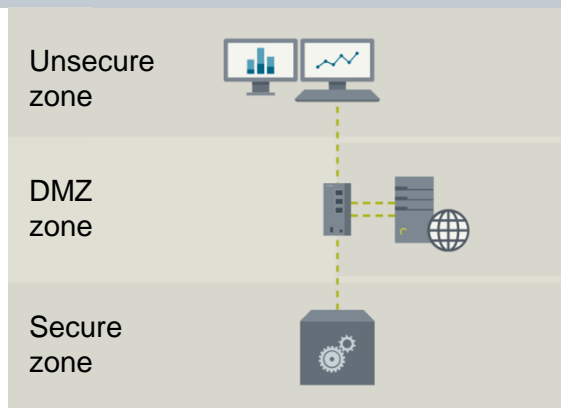
- Cell protection and perimeter network
- Firewalls and VPN

Industrial Security – Essential Network Security use cases

DMZ

Increased protection through data exchange via DMZ by avoiding direct access to the automation network

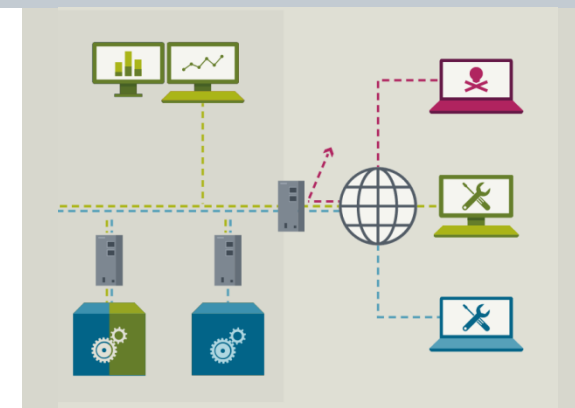
→ A Firewall controls all data traffic between the different networks and DMZ.



Remote access

Secured remote access via the Internet or mobile networks avoiding espionage and sabotage.

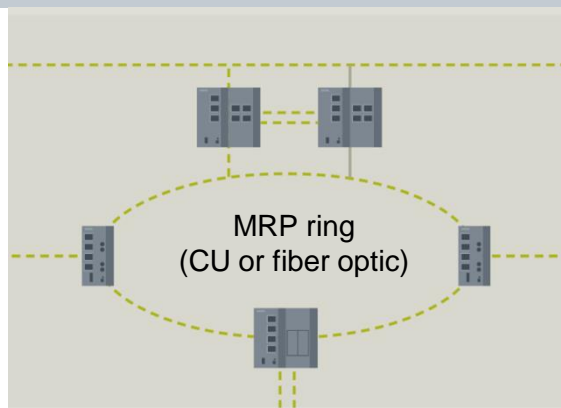
→ Encryption of data transmission and access control via Security modules or Internet- and mobile wireless routers



Secure redundancy

Higher reliability and availability and securing of redundant network structures

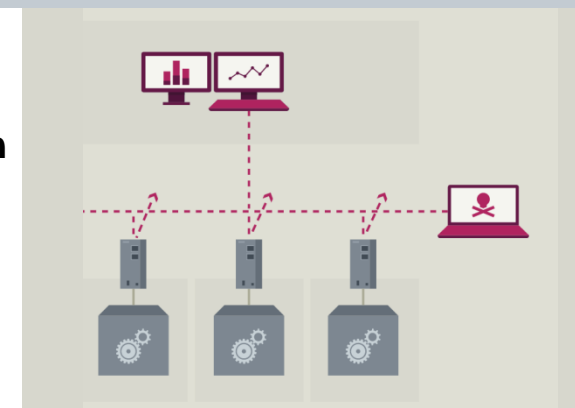
→ Security modules in synchronized standby mode and integrated in redundant rings.



Cell protection

Devices without own network security functionality can be protected within the automation cells

→ Access to cell is secured by firewall mechanisms



Industrial security appliances – SCALANCE S

Use case "Demilitarized zone (DMZ)"

Task

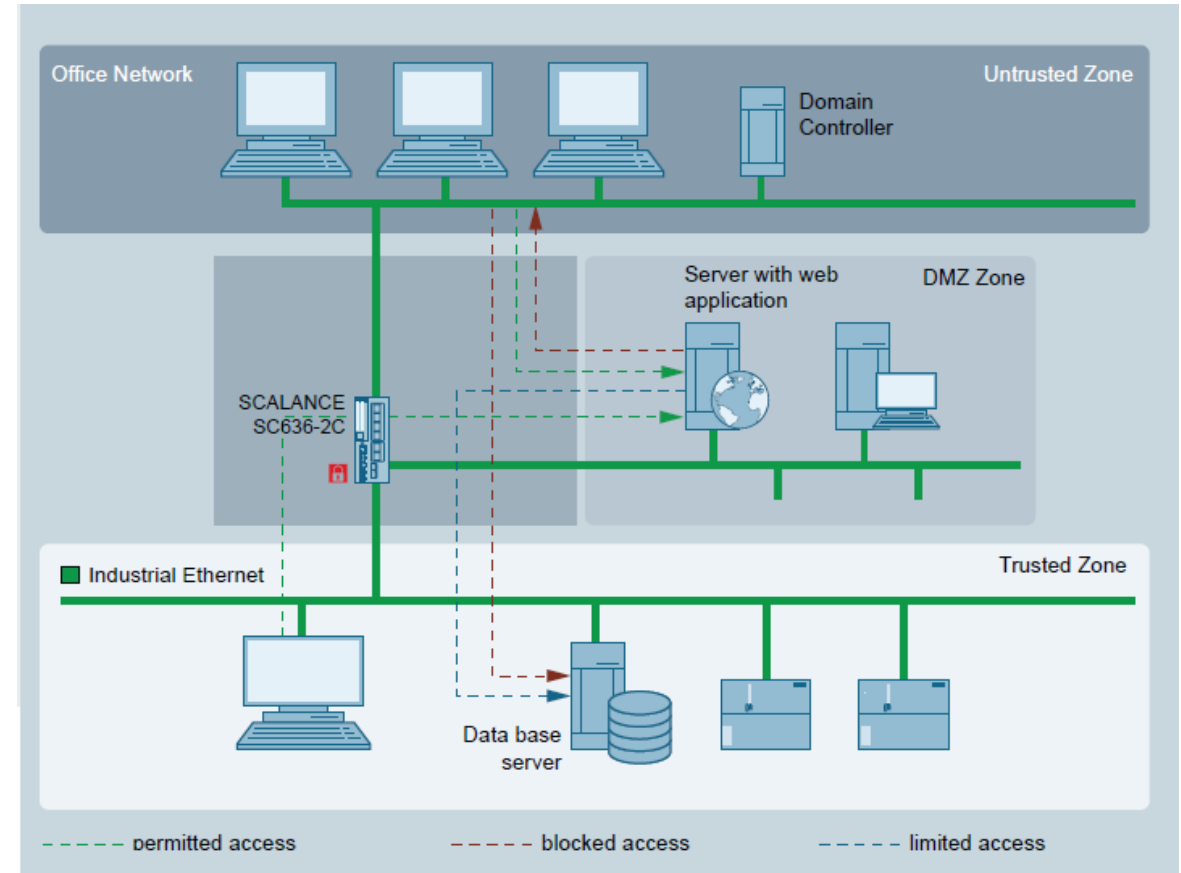
The security concept of an industrial network should be divided into several security zones.

Solution

A flexible security zone concept can be implemented with the cyber security appliance SCALANCE S.

Benefits

- Different security zones such as DMZ, network separation, etc., can be implemented
- Remote access only to specific, selected sections of the industrial network
- Firewall with 600 Mbps and VPN with 120 Mbps
- NAT/NAPT support (series machines)



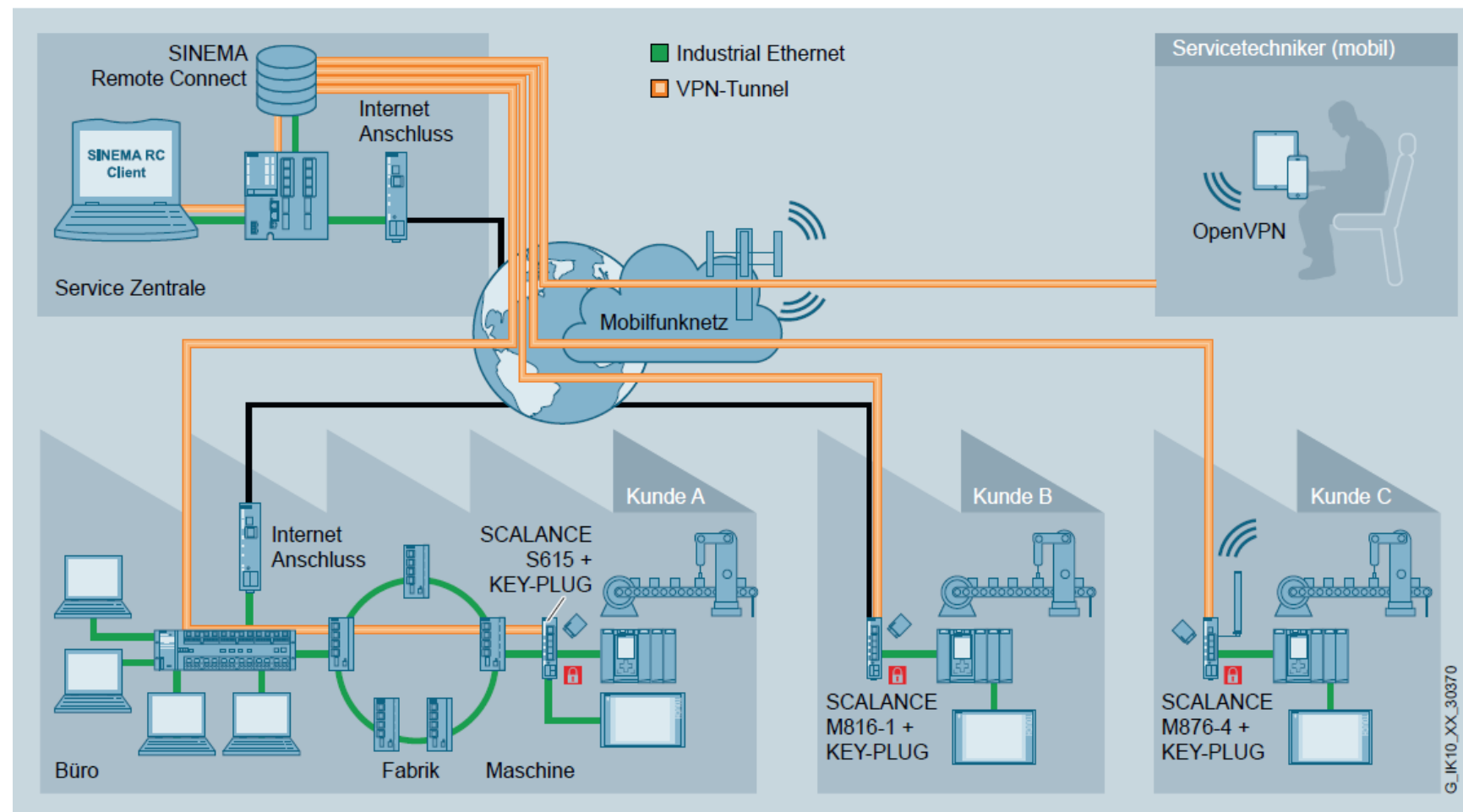
Secure access to remote plants with SINEMA Remote Connect and SCALANCE S615 / SCALANCE M

Task

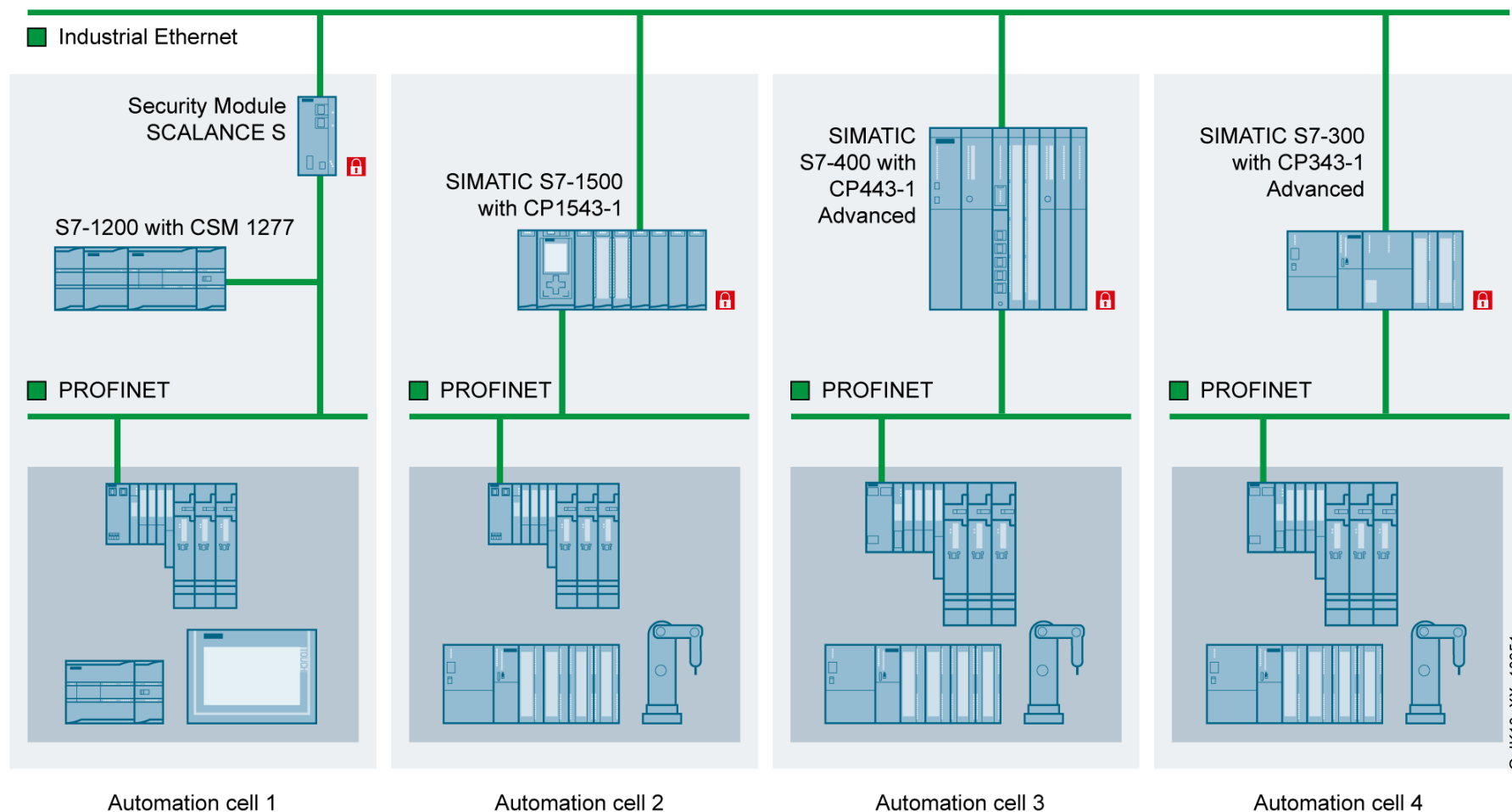
- Remote maintenance for series machines and larger plants with identical subnets
- Remote access to special-purpose machines and sensitive areas
- Central management of the connections needed to acquire status/maintenance data
- User-friendly creation of the devices

Solution

- Central management of machines and service technicians in SINEMA Remote Connect
- Assignment and management of user rights and access authorizations



Cell protection concept



Industrial Communication

TeleControl with SIMATIC NET

IRC - TeleControl

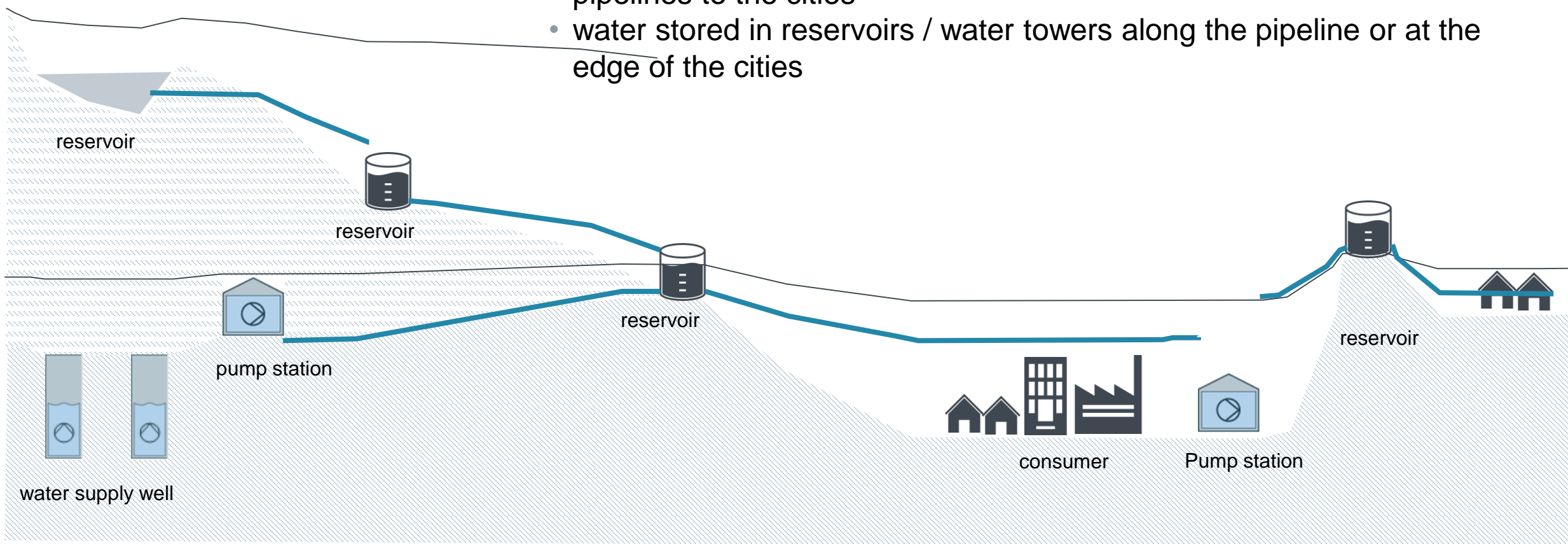
TeleControl

- Monitoring and Control of widely distributed automation processes
- Permanent or spontaneous communication
- Low bandwidth requirement
- Optimized data throughput

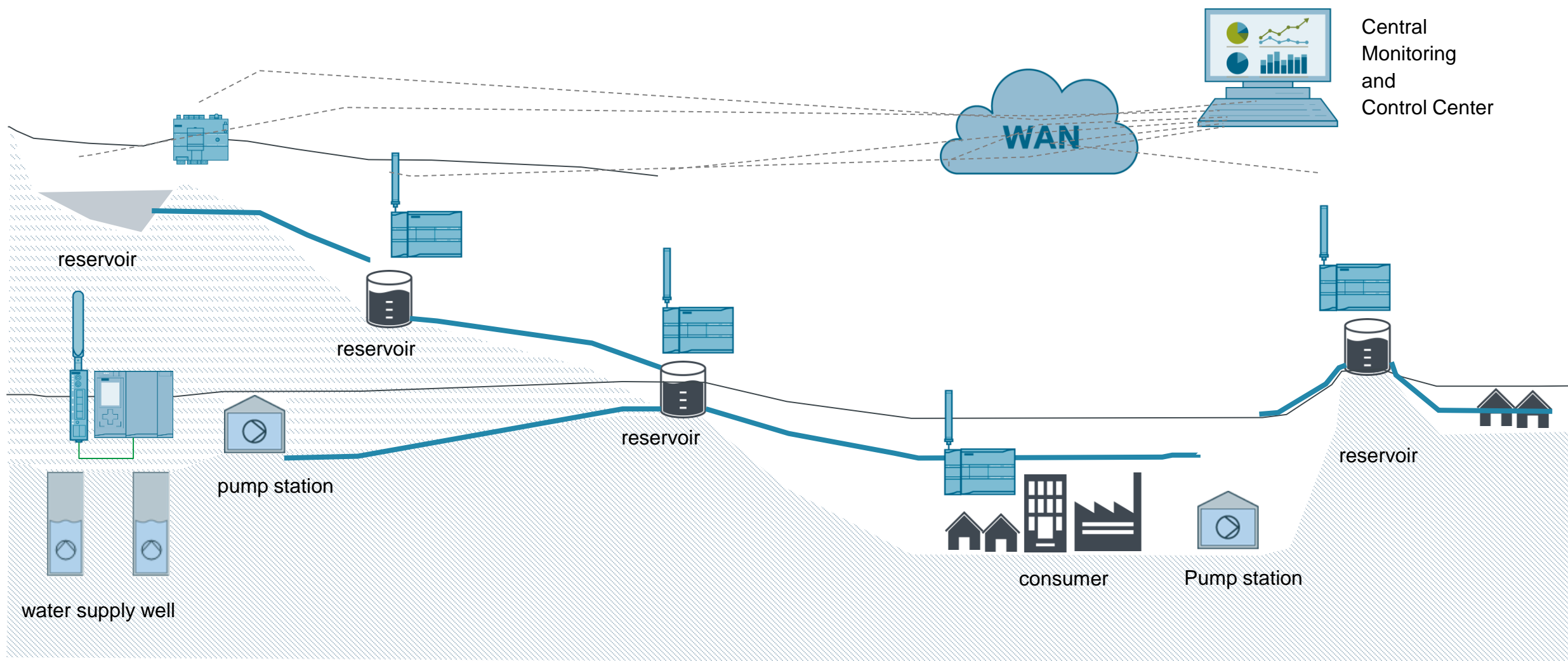


Water supply

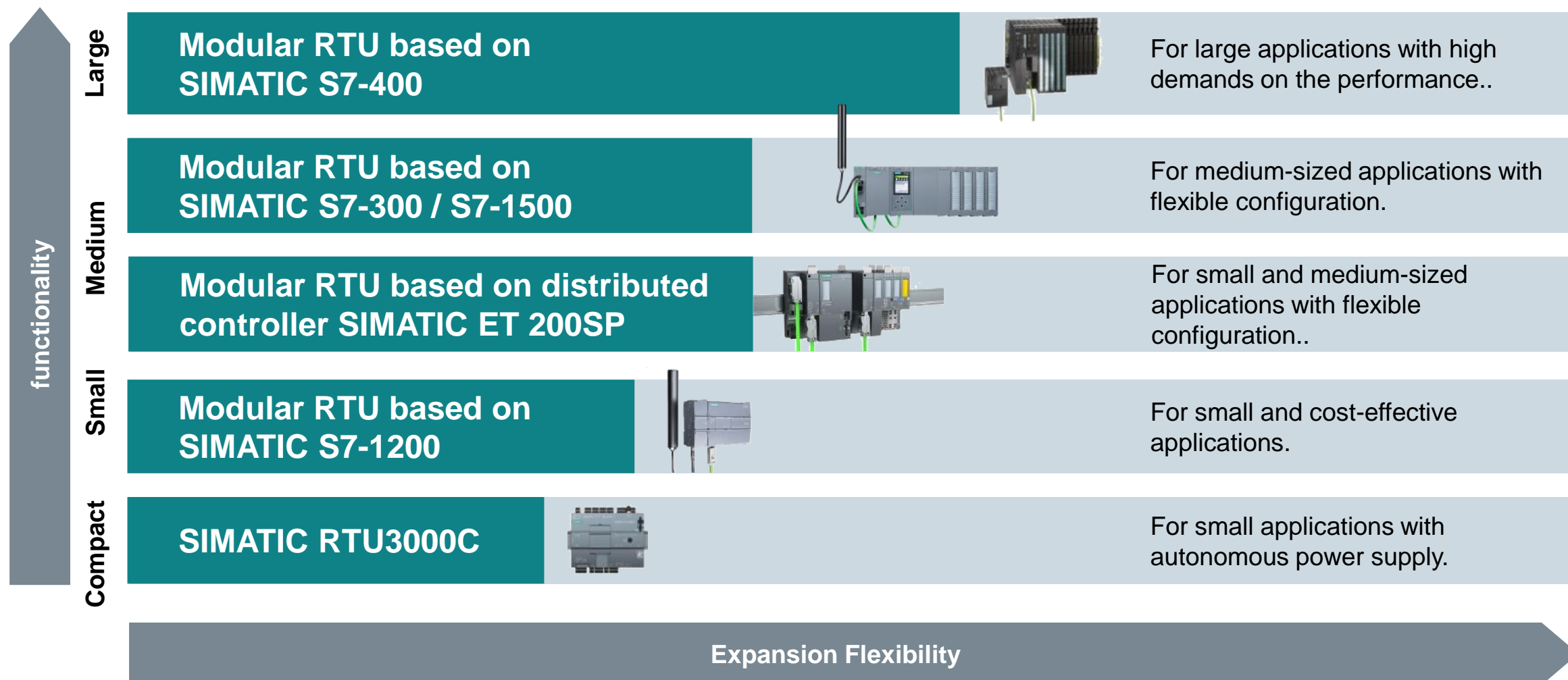
- Water procurement at water wells far outside the cities
- After water purification pumping stations transport the drinking water in pipelines to the cities
- water stored in reservoirs / water towers along the pipeline or at the edge of the cities



Water supply



Positioning - Telecontrol RTU Portfolio





SIEMENS
Ingenuity for life

NS
for life

Industrial Communication

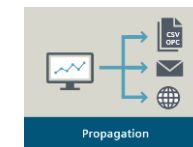
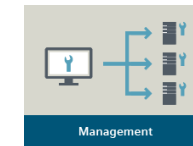
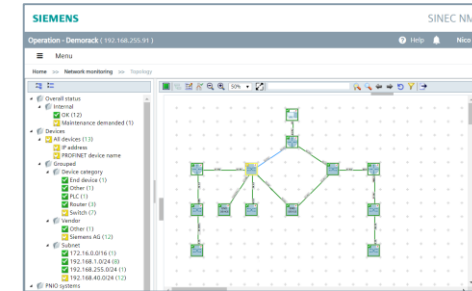
SINEC NMS

SINEC NMS

24/7 Network monitoring and management

Key features

- Centralized operation and User-Management with UMC
- **Server-Client architecture** with Web GUI
- **Automatic/manual device detection**
- **Automatic** generation of the network **topology** (user-defined views possible)
- **Policy-based network configurations**
- **Topology based SCALANCE Firmware-Update**
- **Device Config File Management** (Save/Restore, Edit, Compare)
- Combining of **SNMP** network and **PROFINET/SIMATIC** system diagnosis
- Generation of **alarms** on **events**
- Comprehensible network statistics **reports**, e.g. availability, network performance...
- Adaptable device profiles for e.g. **third party device monitoring**
- Integration into higher-level **HMI/SCADA/PCS 7** systems
- Platform independent data transfer via **OPC UA**
- Creation of **network validation reports (.pdf)**
- e.g. Validation of **network performance**, **availability**, **duplicate PN-Names/IP-address**

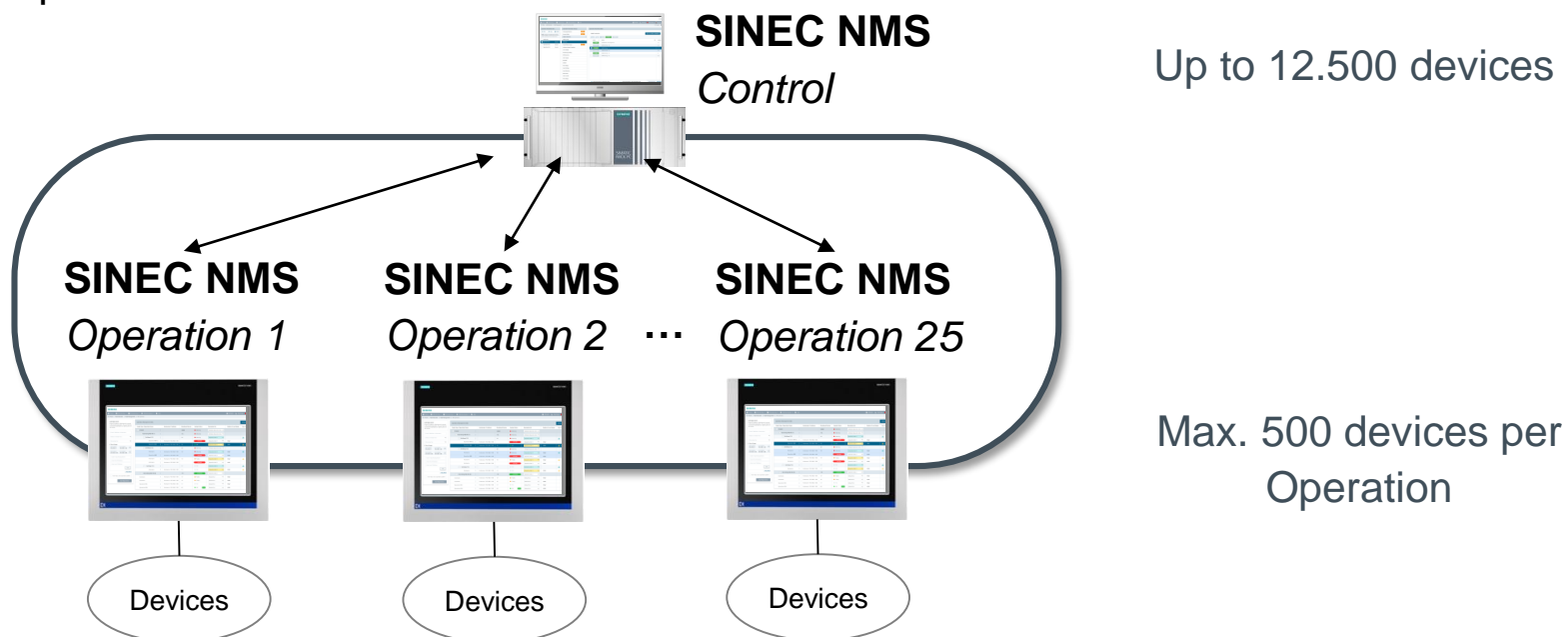


SINEC NMS

Configuration limits

SINEC NMS **decentralized approach** (distributed Control and Operation) enables the customer to connected **up to 25 Operations** to **one SINEC NMS Control**.

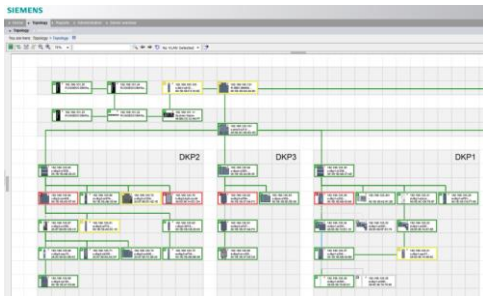
One SINEC NMS Operation supports the monitoring of big networks with up to **500 nodes**. More nodes can be monitored by adding more SINEC NMS Operations. Altogether, one “central” SINEC NMS Control can create a complete inventory list of up to 12.500 devices.



SINEC NMS

Use-Case: Monitoring functions

Topology (LLDP, Bridge)



LAN Ports

Incl. **statistics**
(Utilization, Error, Discarded)

LAN ports						
Port	Status	Monitoring	Administrative	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-3-1	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-3-3	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-3-5	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-cm-1	Up	Up	Up	94 b8 c5 12 a9 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

Including highlighting in Topology

Basic data

Max. possible VLANs 255

Currently used VLANs 2

VLANs

VID	Name	Status	Untagged ports	Tagged ports
1	switch.0001	Static	-	-
2	switch.0002	Static	-	-

Page 1 of 1

I&M for asset management

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

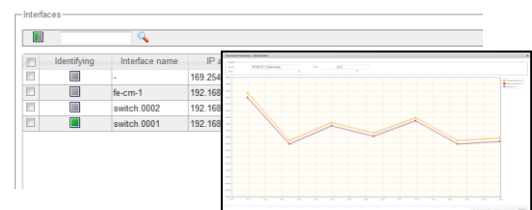
Redundancy Information

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

Redundancy					
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	MRP	broken	enabled	-	-

Interfaces

Incl. statistics (Utilization, Error, Discarded)



Contact



Vladimir Slavojević

Phone: +385 (91) 6105 - 031

E-Mail:

vladimir.slavojevic@siemens.com