

# Siemens Industrial WIFI

SCALANCE W



## Agenda

- Introduction
- Product offering
- WIFI basics
- Wireless IT vs OT
- Scalance W configuration demo

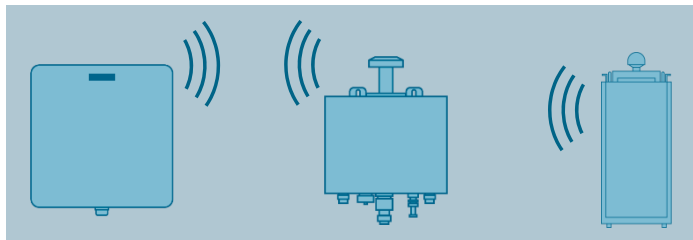


# Overview of Siemens wireless technologies



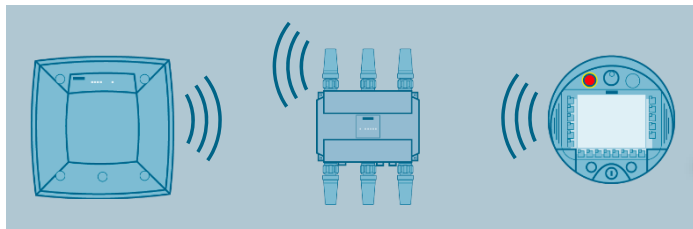
## Wireless Remote Networks

For remote access to distributed systems via mobile radio. This is done with SCALANCE M



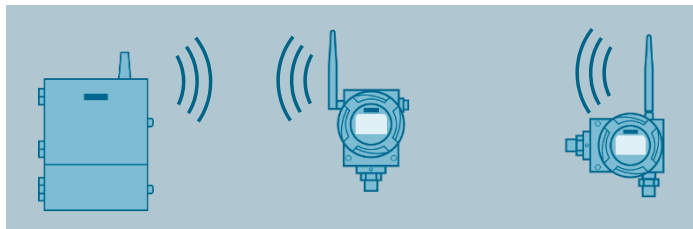
## WiMAX

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



## 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.

# SCALANCE W is successfully operating in a wide variety of demanding **SIEMENS** applications...

*Ingenuity for life*



## Wireless networks in industrial applications

- Overhead monorails
- Automated guided vehicle + Automated mobile robot systems (AGVs + AMRs)
- Intralogistics (rack feeder, shuttle)
- Retrofitting with wireless networks (E.g. PROFIBUS to PROFINET)

Cyclic and reliable communication



## Wireless applications with critical requirements

- Public transport (e.g. train to ground)
- Amusement park rides
- Ski lifts, big wheels, fun rides
- Safety applications (with Safety Integrity up to Level SIL3 according to IEC 61508)

Emergency stop for safety applications



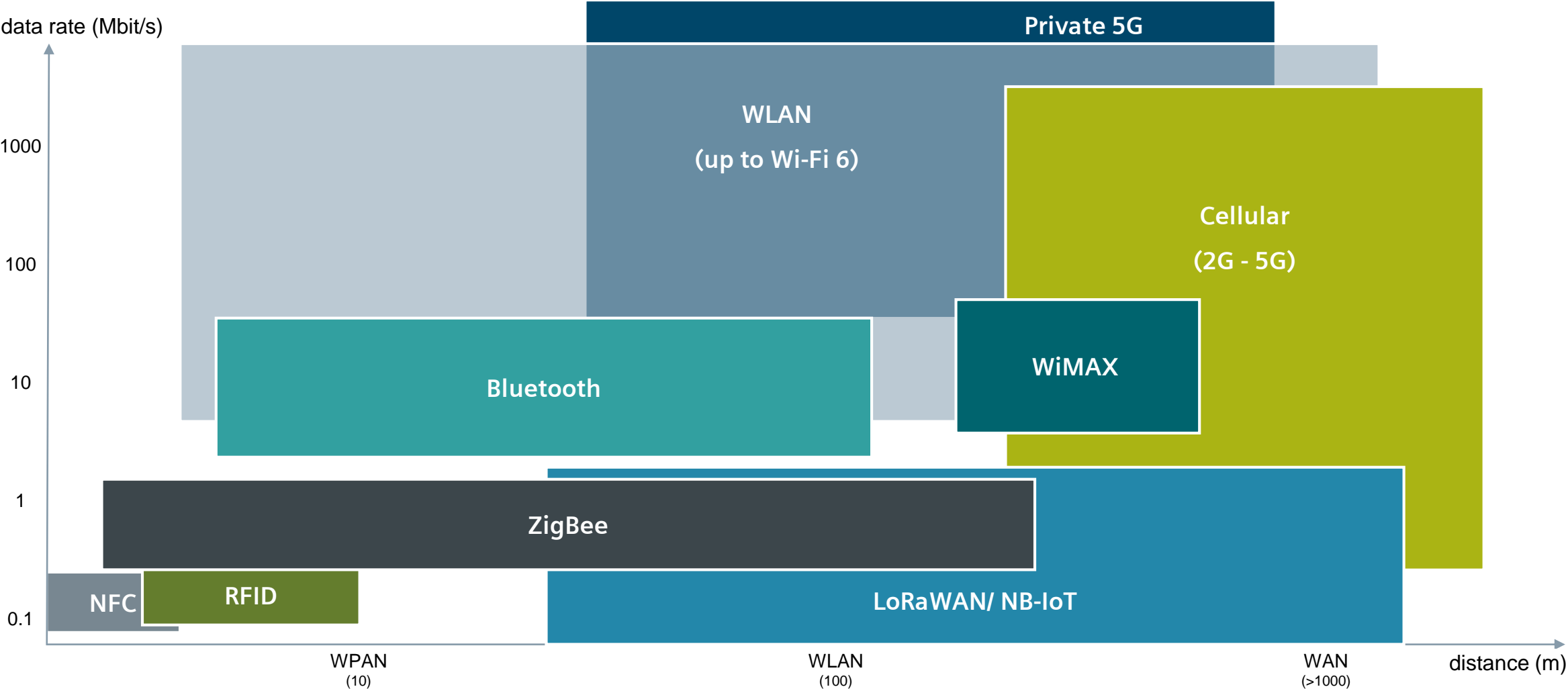
## Portfolio for harsh environments – indoor and outdoor

- Oil & Gas industry
- Seaport applications and container terminals
- Mine shafts and tunnel networks
- Underground mining / mine shafts

Industrial approvals and enhanced environmental conditions (EEC)



# Overview of wireless technologies based on different ranges and data rates (single cell)



# Evolution of the IEEE 802.11 Standard

## Wi-Fi standard is evolving to match new requirements



IEEE 802.11-1997	IEEE 802.11a	IEEE 802.11g	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax
<b>Released:</b> 1997	<b>Released:</b> 2001	<b>Released:</b> 2003	<b>Released:</b> 2009	<b>Released:</b> 2012	<b>Release:</b> 2020
<b>Data rate:</b> max. 2 Mbps	<b>Data rate:</b> up to 54 Mbps	<b>Data rate:</b> up to 54 Mbps	<b>Data rate:</b> up to 600 Mbps	<b>Data rate:</b> up to 6933 Mbps	<b>Data rate:</b> up to 9608 Mbps
<b>Frequency:</b> 2.4 GHz	<b>Frequency:</b> 5 GHz	<b>Frequency:</b> 2.4 GHz	<b>Frequency:</b> 2.4 & 5 GHz	<b>Frequency:</b> 5 GHz	<b>Frequency:</b> 2.4 GHz & 5 GHz Wi-Fi 6E: 6 GHz
	<b>Core features:</b> <ul style="list-style-type: none"> <li>• OFDM (Orthogonal Frequency Division Multiplexing)</li> <li>• Siemens iPCF (Rapid roaming)</li> </ul>	<b>Core features:</b> <ul style="list-style-type: none"> <li>• OFDM (Orthogonal Frequency Division Multiplexing)</li> </ul>	<b>Wi-Fi 4</b> <b>Core features:</b> <ul style="list-style-type: none"> <li>• MIMO (Multiple-Input/Multiple-Output)</li> </ul>	<b>Wi-Fi 5</b> <b>Core features:</b> <ul style="list-style-type: none"> <li>• Channel bonding up to 160 MHz</li> </ul>	<b>Wi-Fi 6</b> <b>Core features:</b> <ul style="list-style-type: none"> <li>• OFDMA (Orthogonal Frequency-Division Multiplexing)</li> </ul>

[802.11 Timelines](#)

## What's not in the standard?

- Scheduling algorithm to trigger frames at the Access Point
  - Fast roaming is not improved and could take up to seconds
- No reliable, predictable worst- case latency for an industrial application!

## iFeatures from Siemens to improve the Standard

- Improvement for fast roaming
  - Reduced latency with deterministic cycles
  - Application-appropriate treatment of all client devices
- Reliable, predictable worst- case latency for an industrial application!



**iFeatures are needed for reliable and real-time automation solutions**

# Industrial Communication and Identification

## Expertise in industrial networks and industrial identification

**SIEMENS**  
*Ingenuity for life*

### Industrial Communication

#### Industrial Ethernet



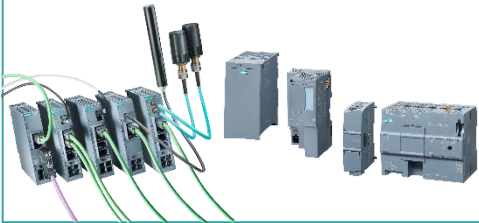
#### Rugged Communication



#### Security



#### Remote



#### Wireless



#### CPs, Profinet and Profibus



#### Software



#### Cabling Technology



### Industrial Identification & Locating

#### Optical Identification



#### RFID



#### RTLS





# Industrial Wireless LAN: SCALANCE W – Powerful, safe and reliable

**SIEMENS**  
*Ingenuity for life*

## Wide-ranging usage

- In the cabinet
- Wall and ceiling mounting
- Outdoor applications

## High reliability

- Industrial-standard hardware
- iFeatures for industrial requirements
- Redundant wireless connection by iPRP

## Powerful

Up to 2x 1733 Mbit/s data rate with Dual Radio and 4 x 4:4 MIMO

## Wireless communication

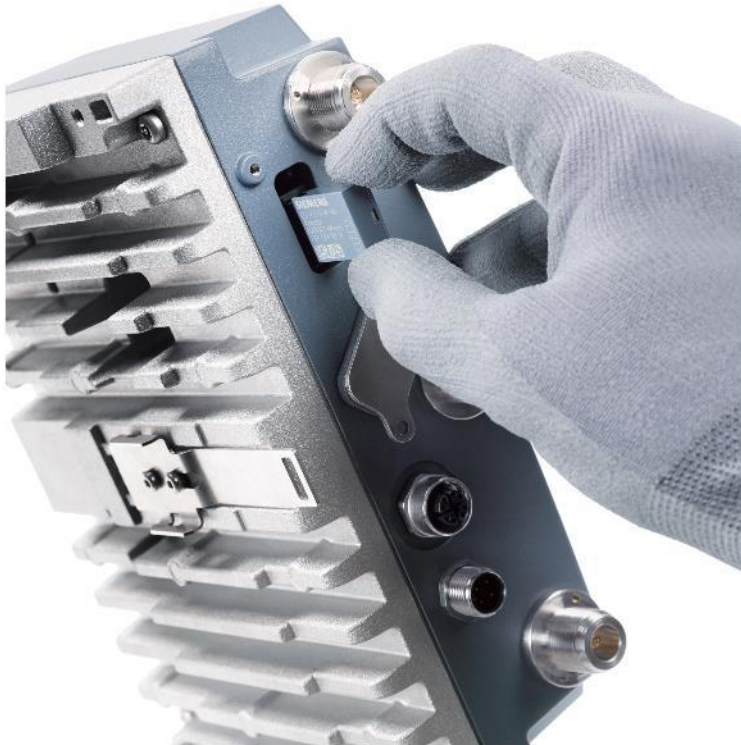
- Connection of mobile devices
- Flexibility without cables

## Easy handling

- Configuration via Web-based Management
- Integration into TIA Portal
- Central configuration and monitoring with SINEC NMS



# Real-time wireless networks: Additional industry features activated by KEY-PLUG



## Feature / Function

- Real-time functionality, PROFINET IO, PROFIsafe, determinism with iPCF
- Wireless communication for free guided roaming subscribers (iPCF-MC)
- Redundancy for wireless communication (iPRP)
- Save and restore functionality
- Blocking and firewall algorithms

## Benefit

- Safety over wireless
- Connectivity to fast moving applications
- Reliable communication also for mobile clients
- Seamless roaming
- High availability and redundant applications possible
- Easy recovery – reduced costs in service and configuration
- Increased network security

# The use of the suitable accessories allows flexible use at different locations

## KEY-PLUG W700

- iFeatures
- Security



### Flexible use of industrial feature set



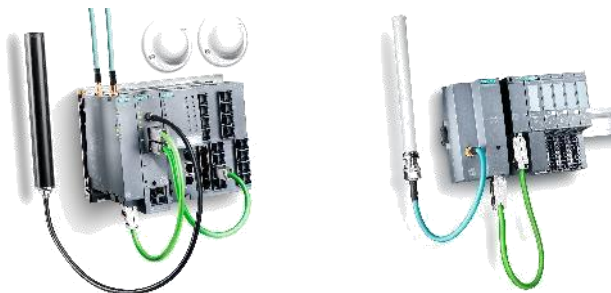
- KEY-PLUG to activate the iFeatures e.g. security features



### Wide accessories portfolio



- Antennas and cables for all kinds of use cases and applications










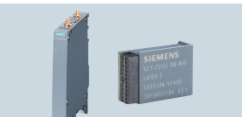




### Seamless integration into cabinet



- Construction of the housing analogous to the SIMATIC components for rail mounting

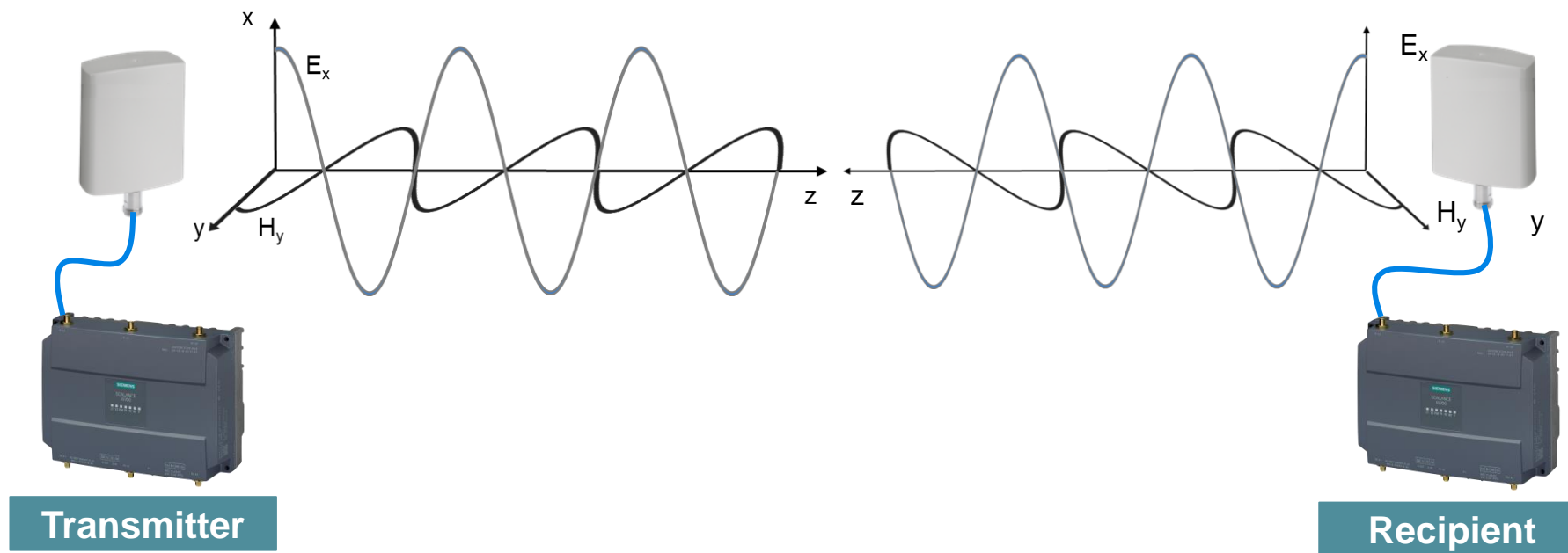
# SCALANCE W products

## Overview

Industry					Outdoor		<div></div> <div>KEY-PLUG</div> <div>In Cabinet</div> <div>Indoor</div> <div>Outdoor</div> <div>* = Transmitting antenna x receiving antenna : spatial streams</div>	
AP		CL		AP		CL		
CL		AP		CL		AP		
AP		CL		AP		CL		
High End	<div></div> <ul style="list-style-type: none"><li>450 Mbit/s</li><li>3 x 3:3*</li><li>1 &amp; 2 radio</li><li>RJ45 &amp; R-SMA</li></ul>	<div></div> <ul style="list-style-type: none"><li>450 Mbit/s</li><li>3 x 3:3*</li><li>1 &amp; 2 radio</li><li>RJ45 &amp; R-SMA</li></ul>	<div></div> <ul style="list-style-type: none"><li>450 Mbit/s</li><li>3 x 3:3*</li><li>1 &amp; 2 radio</li><li>M12 &amp; N-Connect</li></ul>	<div></div> <ul style="list-style-type: none"><li>450 Mbit/s</li><li>3 x 3:3*</li><li>1 &amp; 2 radio</li><li>M12 &amp; N-Connect</li></ul>	<div></div> <ul style="list-style-type: none"><li>450 Mbit/s</li><li>3 x 3:3*</li><li>1 &amp; 2 radio</li><li>RJ45/2SFP &amp; R-SMA</li></ul>			
	<div></div> <ul style="list-style-type: none"><li>300 Mbit/s</li><li>2 x 2:2*</li><li>1 radio</li><li>RJ45/M12 &amp; R-SMA</li></ul>	<div></div> <ul style="list-style-type: none"><li>300 Mbit/s</li><li>2 x 2:2*</li><li>1 radio</li><li>RJ45 &amp; R-SMA</li></ul>	<div></div> <ul style="list-style-type: none"><li>300 Mbit/s</li><li>2 x 2:2*</li><li>1 radio</li><li>M12 &amp; N-Connect</li></ul>	<div></div> <ul style="list-style-type: none"><li>300 Mbit/s</li><li>2 x 2:2*</li><li>1 radio</li><li>M12 &amp; N-Connect</li></ul>				
	<div></div> <ul style="list-style-type: none"><li>150 Mbit/s</li><li>1 x 1:1*</li><li>1 radio</li><li>RJ45 &amp; R-SMA</li></ul>	<div></div> <ul style="list-style-type: none"><li>150 Mbit/s</li><li>1 x 1:1*</li><li>1 radio</li><li>RJ45 &amp; R-SMA</li></ul>						

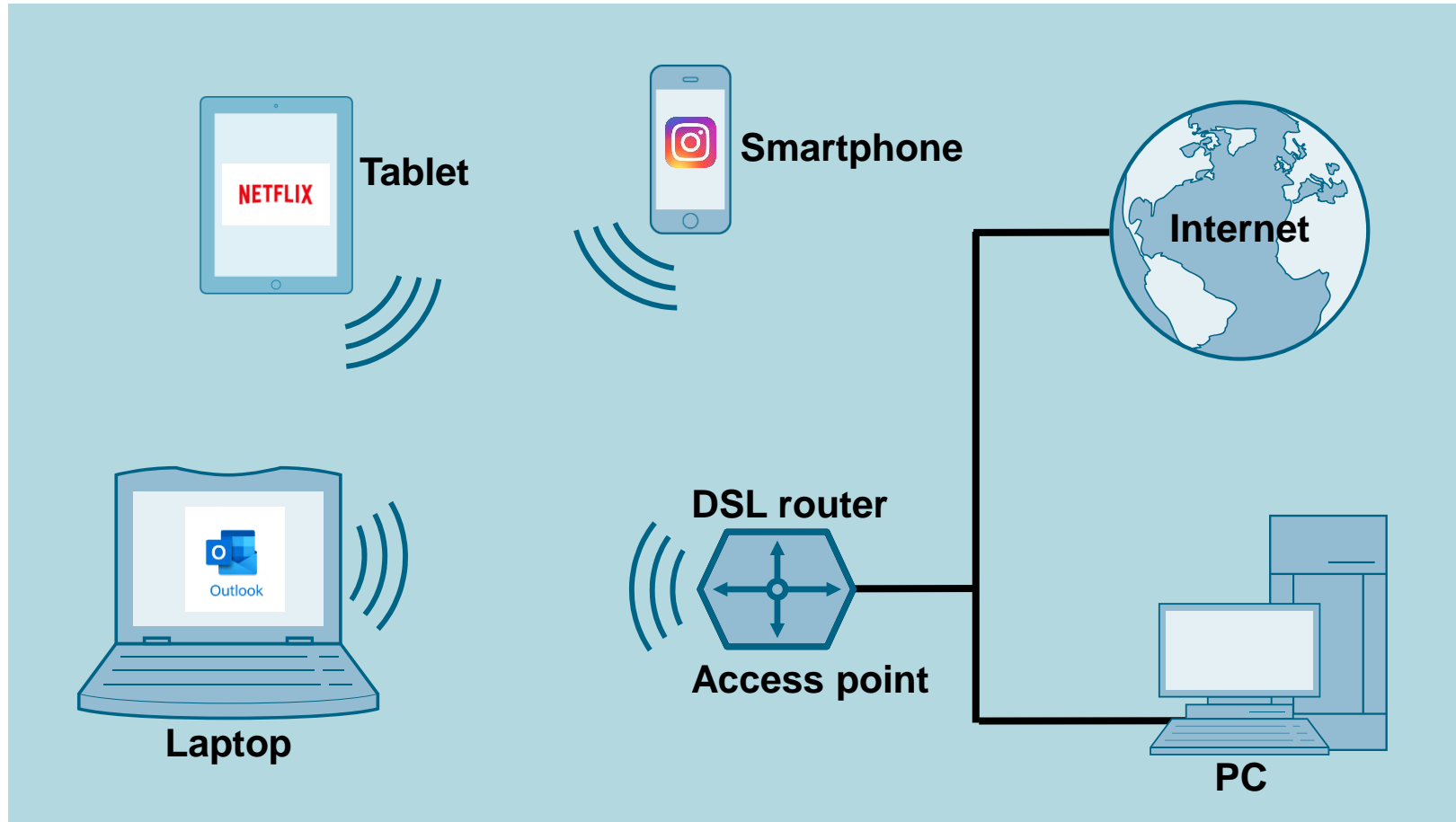


# WIFI Basics...

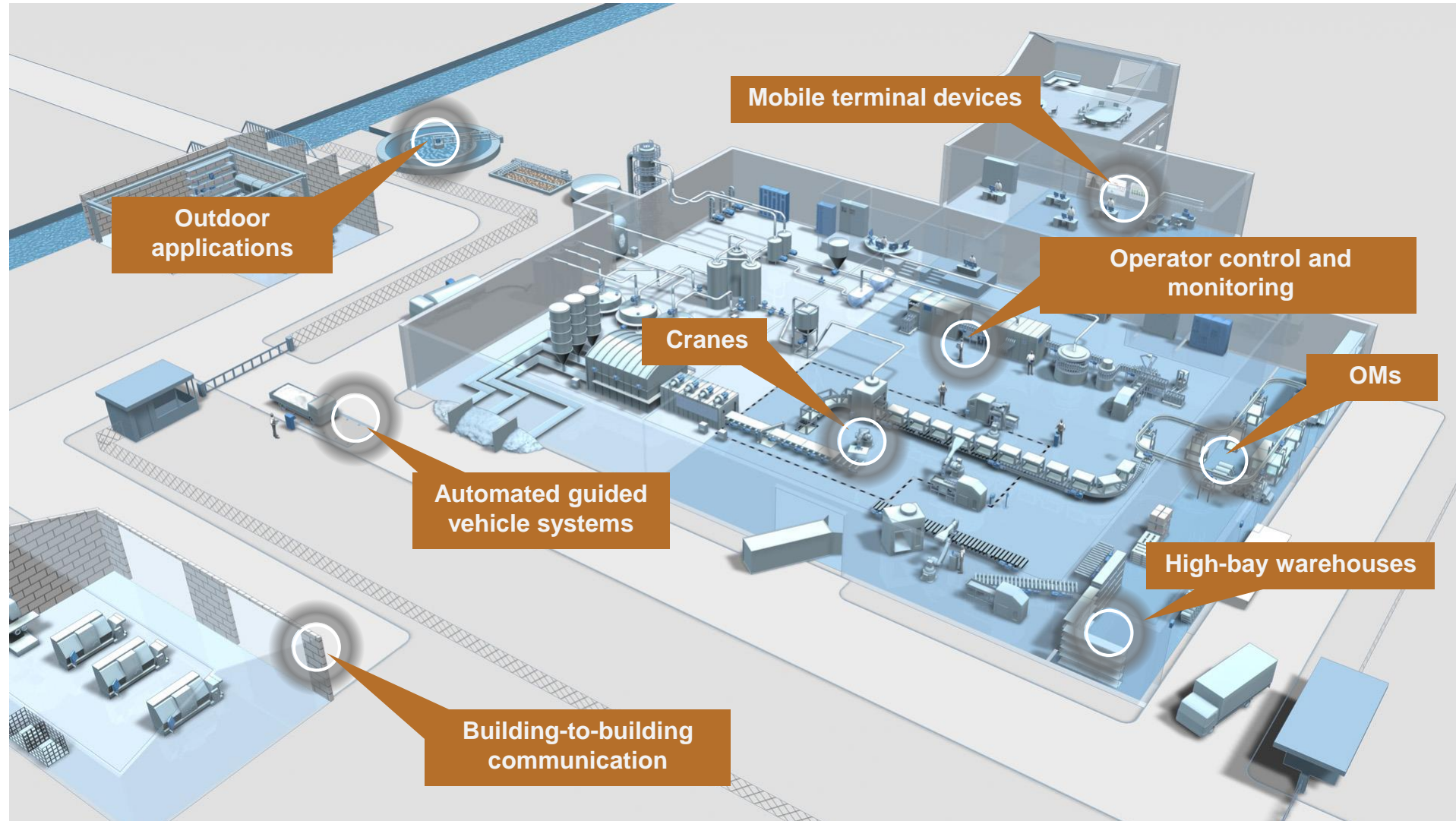


# Application in the standard WLAN

WLAN permits mobile access to the LAN or the Internet, e.g. at the office or at home























# Industrial wireless Applications



# Antenna overview

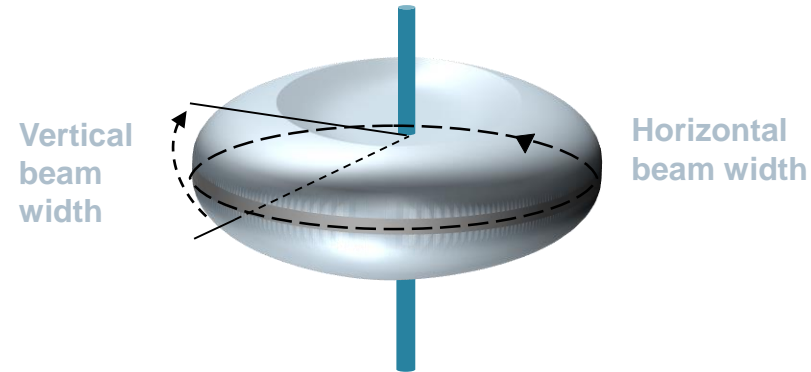


Type of antenna	Frequency (GHz)	Antennas			SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	Type of antenna	Frequency range (GHz)	Antennas			SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65
directional	2.		ANT792-8DN		●			omnidirectional	2,4		ANT792-6MN		●	●	●
	5		ANT793-8DP		●	●					ANT795-4MA		●	●	
			ANT793-8DJ		●	●					ANT795-4MB		●	●	
			ANT793-8DK		●	●					ANT795-4MC		●		●
			ANT793-8DL		●	●					ANT795-4MD		●		●
RCoax	2.4		RCoax radiating cables 2.4 GHz		●	●	●	Sector	2,4 and 5		ANT795-4MX		●		●
			ANT792-4DN		●	●	●				ANT795-6MN		●	●	●
	5		RCoax radiating cables 5 GHz		●	●	●				ANT795-6MT		●		
											ANT795-6MP		●	●	●
			ANT793-4MN		●	●	●		5		ANT795-6DC		●	●	●
											ANT793-6DG		●	●	●

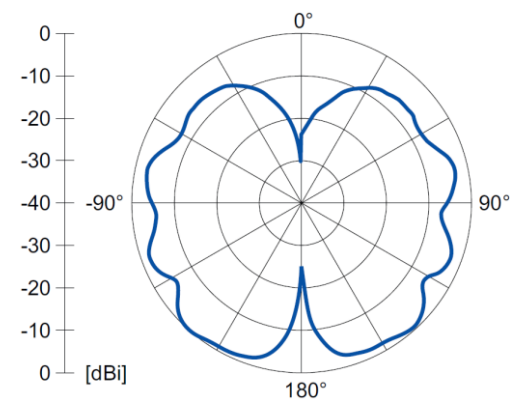
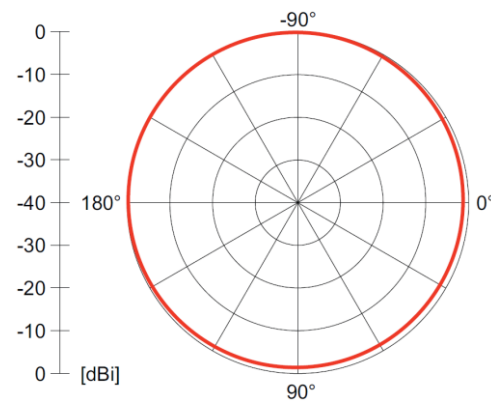


# Omnidirectional antennas

## Omnidirectional antennas (ideal representation)



## Horizontal (left) and vertical (right) antenna diagram



2.5dBi

# Omnidirectional antennas

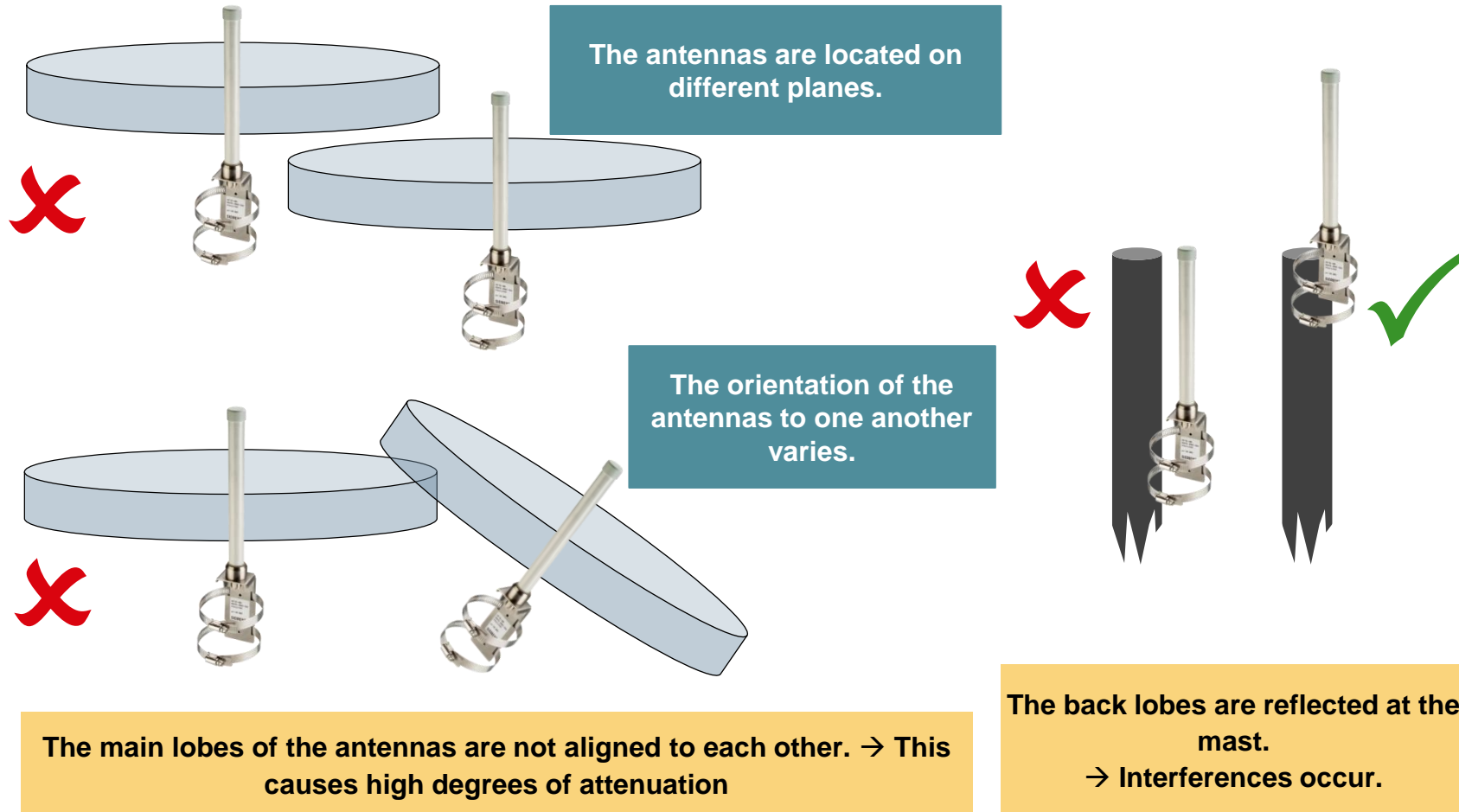
## Typical applications with omnidirectional antennas

- Coverage of halls and open areas
- Coverage of office environments
- Free-moving nodes (due to large radio field coverage)
- Applications with short distances  
(typically up to 100 m)



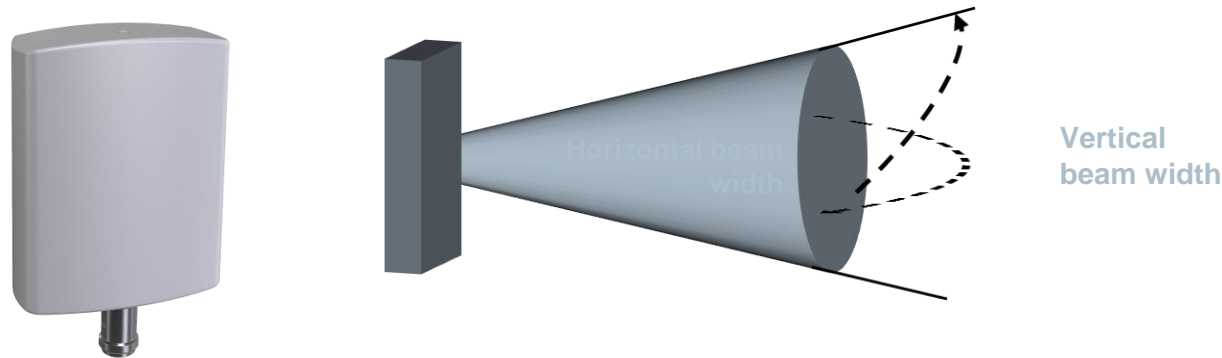
# Omnidirectional antennas

## Alignment and mounting of omnidirectional antennas (ideal representation)

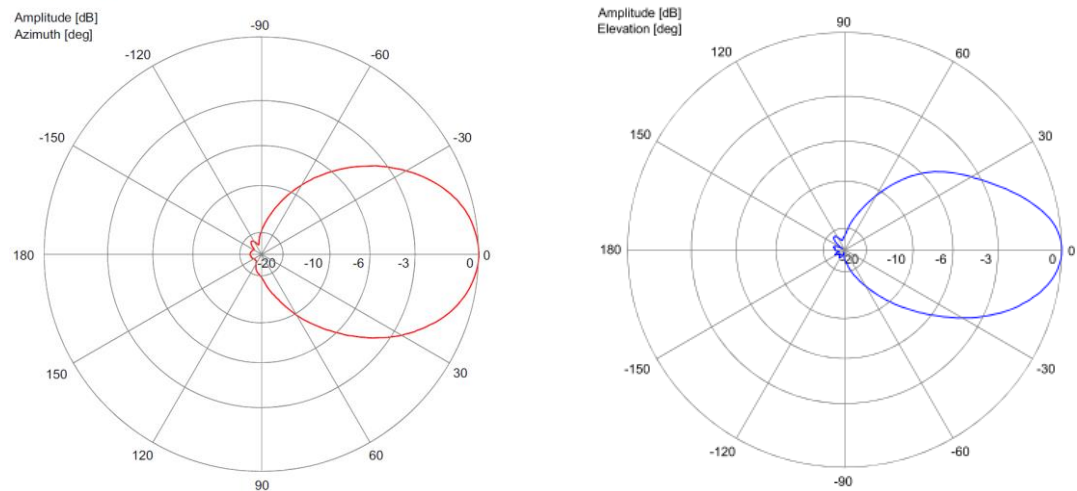


# Directional antennas

## Directional antennas



## Horizontal (left) and vertical (right) antenna diagram





# Directional antennas

## Typical applications with directional antennas



- Crane applications
- Building to building
- Coverage of high-bay warehouses
- Nodes with static positions
- Nodes with one-dimensional movement
- Applications with long distances (up to 1000+ m) at fixed positions

Additionally for sector antennas:

- Applications with medium distances (up to a max. of 500 m) and limited radius



# TIA Selection Tool

To support the selection of Industrial Wireless LAN components the **TIA Selection Tool** can be used:

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

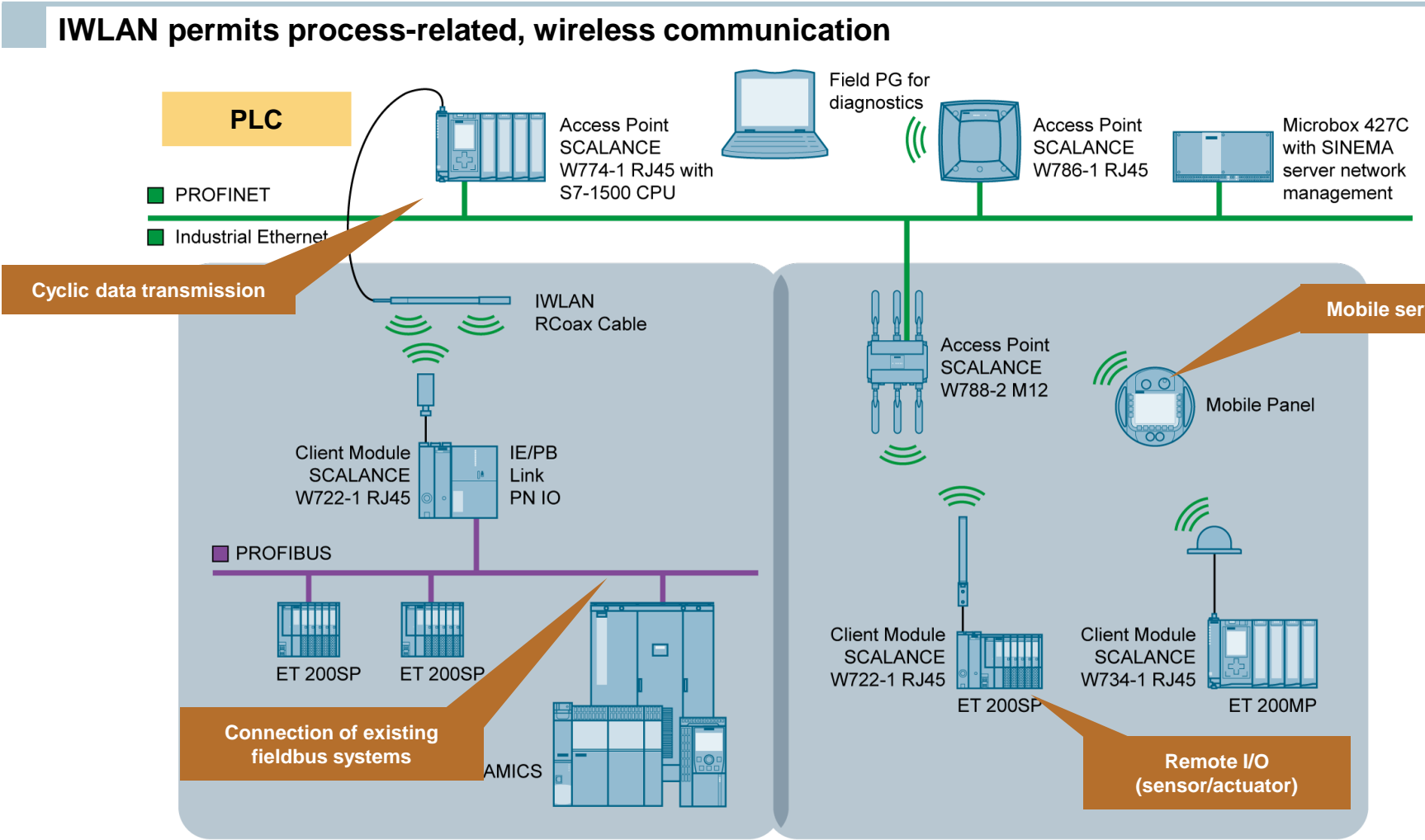
The screenshot displays the TIA Selection Tool interface, which is used for configuring industrial wireless LAN components. The interface is divided into several sections:

- Start**: Includes buttons for "Neues Gerät", "Geräte konfigurieren", "Bestellliste", and "Produkt Suche".
- Neues Gerät**: A sidebar menu with options like "Gerätfamilie auswählen", "Gerät auswählen", and "Gerät anlegen".
- Gerätfamilie auswählen**: A tree view showing various industrial components such as "Anlage", "Steuerung", "Dezentrale Peripherie", "Panels", "Industrie-PC", "Antriebstechnik", "Schalttechnik", "Software", "Kommunikation", "Stromversorgung", and "Industrielle Identifikationssysteme".
- Industrielle Kommunikation**: A section for selecting communication components, including "Industrielle Ethernet", "Industrial Ethernet", "Industrial Wireless", "Telecontrol Auswahl", "Network Security", "Netzübergänge", "Optical Link Modul", and "AS-Interface".
- Gerät**: A section for selecting the device, showing "SCALANCE W788-1 M12 (ROW)" with parameters like "Max. Transmit Power", "Signalstärke", and "Anzahl Streams".
- Antenne**: A section for selecting the antenna, showing "Antenne ANT793-8DK" with parameters like "Anzahl Antennen", "Schaltschrankdurchführung", and "Blitzschutz".
- Strecke**: A section for selecting the cable, showing "15 MBit/s" and "Antennenabstand in Metern".
- Diagramm**: A visual representation of the network setup, showing the distance between the antenna and the device, and the resulting signal strength.
- Ergebnis**: A summary of the configuration, showing the "Strecke von Teilnehmer 1 zu Teilnehmer 2" and "Strecke von Teilnehmer 2 zu Teilnehmer 1", along with the "Empfangenes Signal" and "Signalstärke in Ordnung".

# IT vs OT Wireless networks..

What makes a WIFI network “Industrial” apart from ruggedized hardware?

# Industrial use case with IWLAN



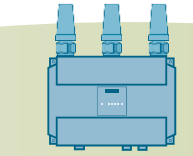


# Standard WIFI example (Distributed approach) Distributed Coordination Function (DCF)

All of the nodes share the available medium = shared medium

The wireless cell uses a specific frequency and channel

5Ghz  
149

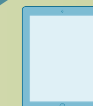


Accesspoint

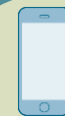
Data is transmitted sporadically



Sender 2



Sender 1



Sender 3

Collisions occur

Wireless cell

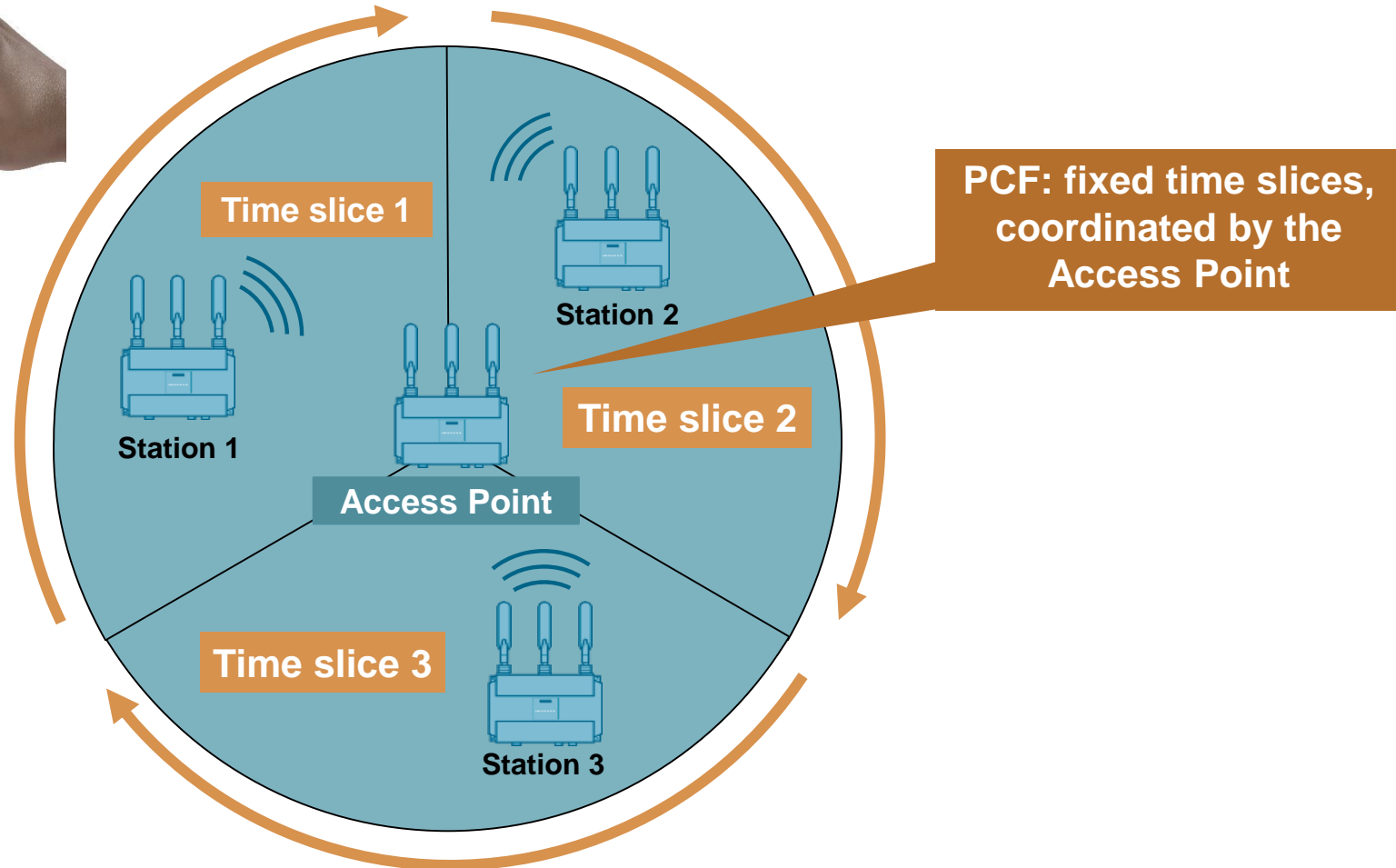
Only one node can transmit at any one time. If two nodes transmit simultaneously, collisions occur

# Siemens Industrial WIFI example (Centralized approach)

## Industrial Point Coordination function (iPCF)

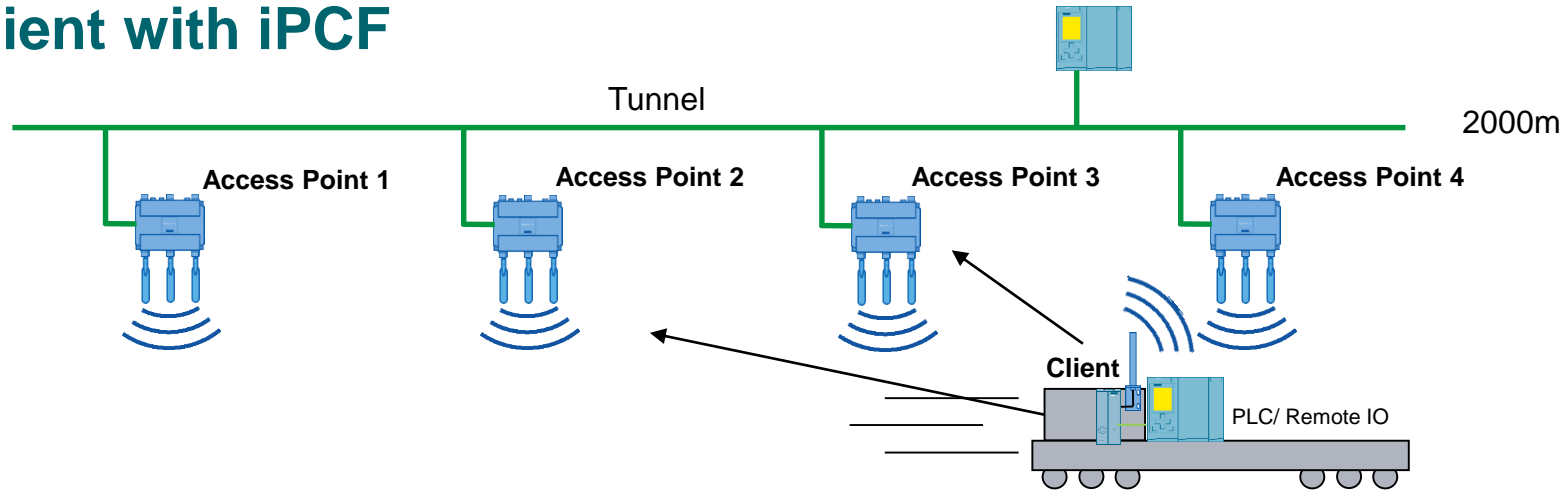
### Basic sequence of the centralized media access

- SCALANCE W iFeature (enabled with Key-plug)
- All participants on the wireless network must Support iPCF
- Access Points poll their clients in the radio cell at very short intervals (about 2ms per client)
- The clients can signal their requirement to send longer data telegrams, they only transmit with permission of AP
- Real-time telegrams such as PROFINET or Ethernet/IP are transmitted with priority
- Due to the short polling times, a client very quickly determines if the connection to the AP is still alive or not, this leads to very quick handover times or roaming of well below 50ms



# Siemens Industrial WIFI example (Roaming)

## Moving client with iPCF



The hand-over of a client from one Access Point to another is called “roaming”.

**"Standard roaming"** needs up to **several hundred milliseconds**.

During that time not data can be transferred!

iPCF alone needs a **maximum of 50 ms** to handle the handover of the client.

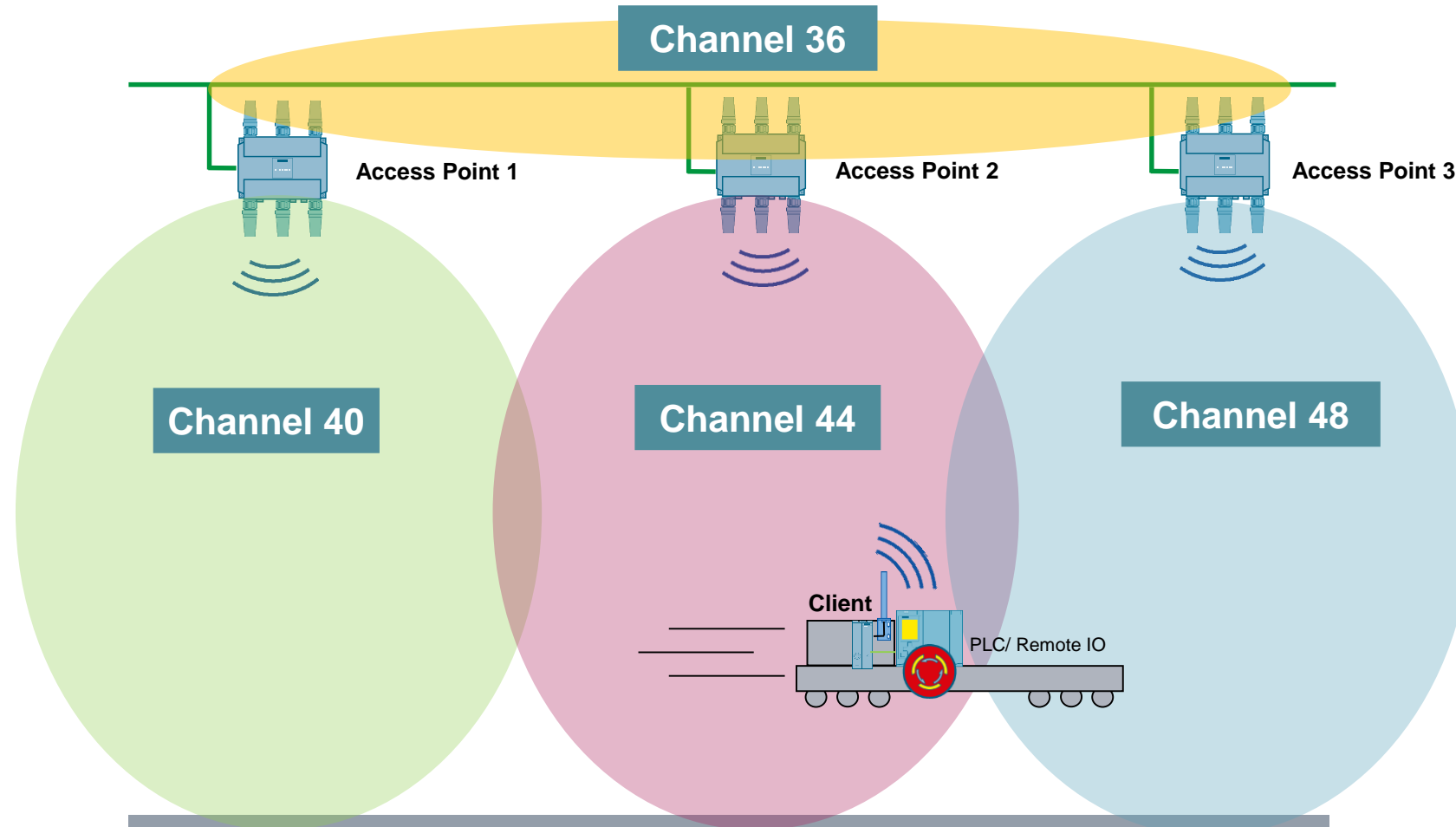
Rapid roaming works only with **iPCF** enabled clients.

The WLAN-client can detect connection-errors quickly, because of the missing polling telegrams. Because of that he can perform the roaming to another AP faster.

Roaming based on iPCF allows the operation of mobile applications without interruption to the automation solution.

# Siemens Industrial WIFI example (Roaming)

## Moving client with iPCF- MC (Management channel)



Roaming based on iPCF-MC allows for even faster roaming times, this method is ideally suitable for AGV applications where the client is moving without a fixed track combined with safety.

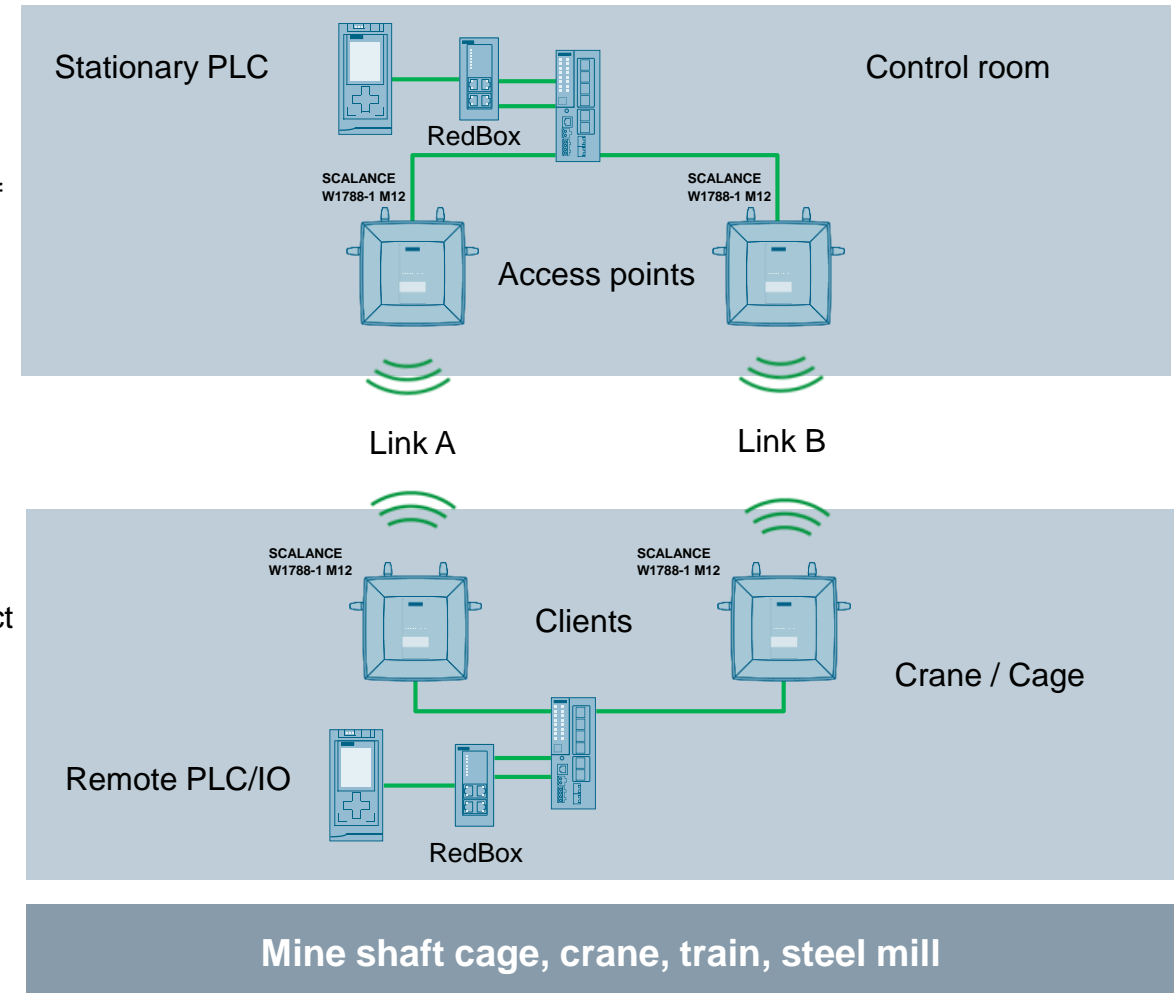
# Siemens Industrial WIFI example (Seamless roaming)

## Moving client with iPRP (Industrial Parallel redundancy protocol)



### Parallel Redundancy Protocol

- An established redundancy technology well established in wired ethernet Networks to achieve redundancy
  - The data is transmitted synchronously between two or more devices on on physically different paths. This leads to **0ms** reconvergence time in case of failure on one of the links due to frame duplication.
  - In order to make the principle of PRP available with radio links and paths of of different speeds, Siemens offers a solution with the proprietary iFeature iPRP
- 
- If the roaming process is delayed, interference or disruptions crop up, Communication continues reliably via a second path.
  - The unique feature is that the two clients on the moving part will never connect to the same Access Point.
  - The two clients will never scan simultaneously for available Access Points, this means that at least one connection is always stable
  - The iPRP solution is particularly suitable for trains, Mine shafts, AGV's and steel mills to mention a few examples



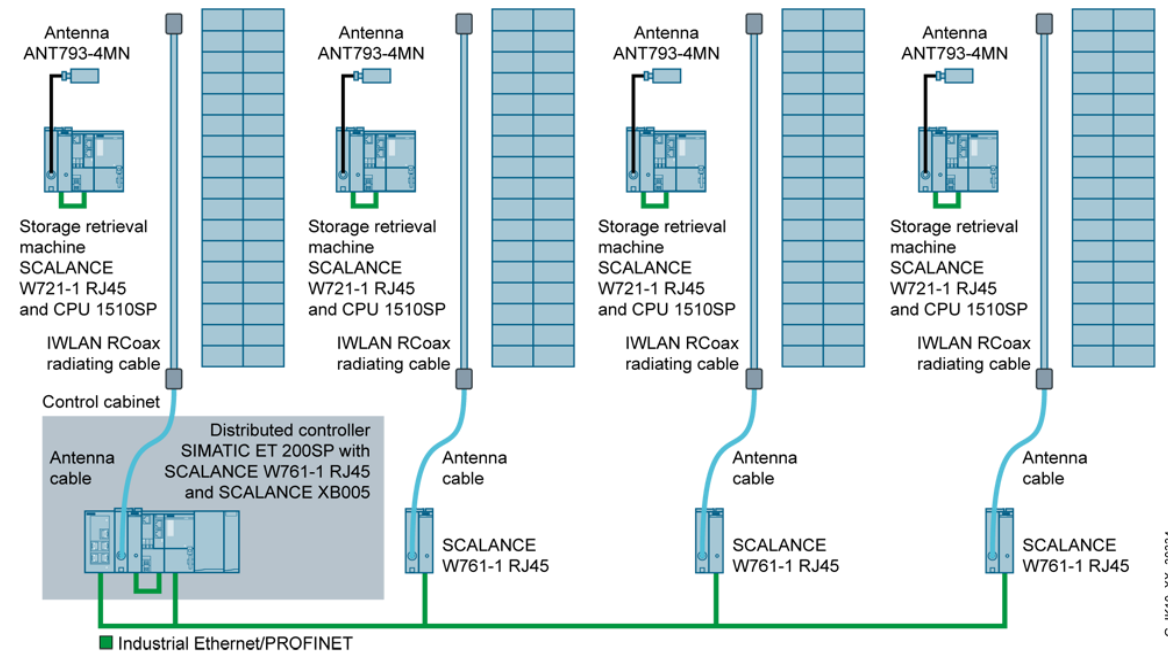


# RCoax – Radiating cable

## Introduction

Whether for cranes, elevators or rail vehicles: the RCoax radiating cables enable reliable wireless connections where conventional antenna technology would be difficult to install.

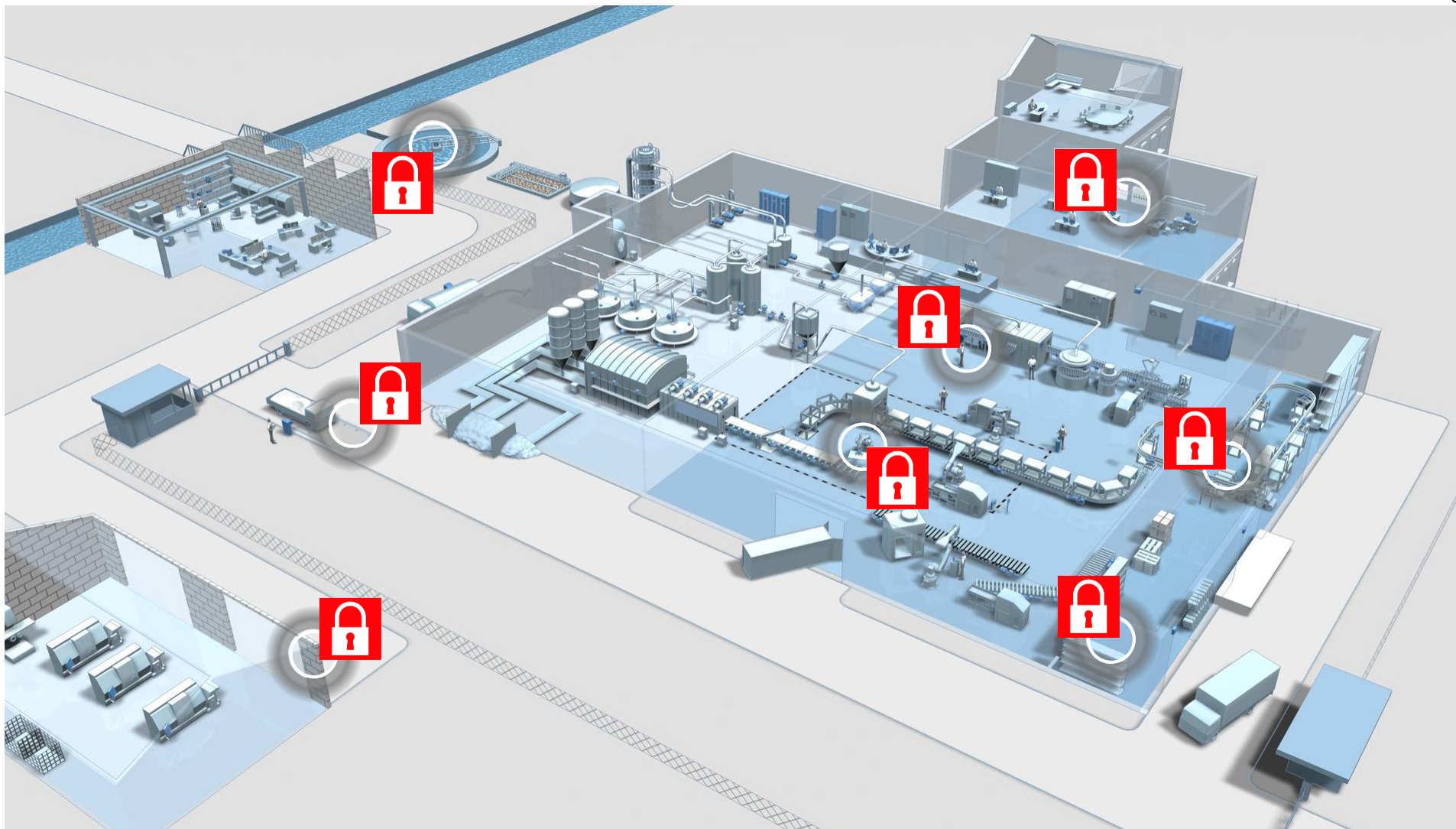
- Operated as antennas of SCALANCE W Access Points, the RCoax radiating cables ensure reliable wireless connections.
- The coaxial cable is robust and easy to install. For Industrial Wireless LAN applications in the 2.4 GHz and 5 GHz frequency bands two variants are available.
- The connection to SCALANCE W-700 Access Points is made as an external antenna.
- Mobile devices are connected via SCALANCE W-700 client modules.



**Maximum reliability thanks to controlled and defined radio field**  
**Non-contact data transfer, so non-wearing and low-maintenance**

# WLAN Security

**SIEMENS**  
*Ingenuity for life*



# WLAN Security

## Siemens Security Advisory by Siemens ProductCERT



Siemens Security Advisory by Siemens ProductCERT

---

### **SSA-901333: KRACK Attacks Vulnerabilities in Industrial Products**

Publication Date: 2017-11-09  
Last Update: 2019-04-09  
Current Version: V1.6  
CVSS v3.0 Base Score: 6.8

#### **SUMMARY**

Multiple vulnerabilities affecting WPA/WPA2 implementations were identified by a researcher and publicly disclosed under the term "Key Reinstallation Attacks" (KRACK). These vulnerabilities could potentially allow an attacker within the radio range of the wireless network to decrypt, replay or inject forged network packets into the wireless communication.

Several Siemens Industrial products use WPA/WPA2 and are therefore affected by some of the vulnerabilities.

#### **WORKAROUNDS AND MITIGATIONS**

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- The attacker must be within radio range of the affected devices. The attacker must trigger the start of a new WLAN handshake in order to perform the attack. If WPA2- CCMP (AES) is configured on the devices, then attacks are limited to decryption and replay of parts of the network traffic. The attacker cannot join the Wireless network, or obtain the WPA2 key.
- SCALANCE WLC711 and WLC712 are only affected by the vulnerabilities related to the group key in the default configuration. An attacker is therefore not able to access unicast traffic. The devices are only affected by CVE-2017-13082 if they have 802.11r functionality activated. IEEE 802.11r is deactivated by default. The devices are only affected by the remaining vulnerabilities if the functions "MeshConnex" or "Client Bridge Mode" are active. Both functions are disabled by default. If these modes have been activated and are not required for the operation of a wireless environment, then customers can deactivate the functionality to reduce the risk.
- SCALANCE W-700 devices that are operated in Client mode, SIMATIC Mobile Panel 277F IWLAN, and SIMATIC ET200 WLAN are not affected if the iPCF, iPCF-MC, or iPCF-HT features are enabled.
- SCALANCE W-700 devices operated in Access Point mode are only affected if WDS with WPA2 encryption is configured. If iPCF, iPCF-MC, or iPCF-HT is active on all interfaces, then SCALANCE W-700 devices are not vulnerable.
- RUGGEDCOM RX1400 and RS9xxW are not vulnerable if operated in Access Point mode.
- SCALANCE W1750D devices are not vulnerable to these vulnerabilities in the default configuration. Only customers that enabled the "Mesh" or "WiFi uplink" functionality are affected by the vulnerabilities. Disabling these functionalities will completely mitigate the vulnerabilities.
- Ensure multiple layers of security, do not depend on the security of WPA2 alone.
- Use WPA2-CCMP (AES) instead of WPA2-TKIP or WPA-GCMP, if supported by the WLAN clients to reduce the risk of potential attacks
- Apply Defense-in-Depth: <https://www.siemens.com/cert/operational-guidelines-industrial-security>

## IEEE 802.11i offers comprehensive security mechanisms

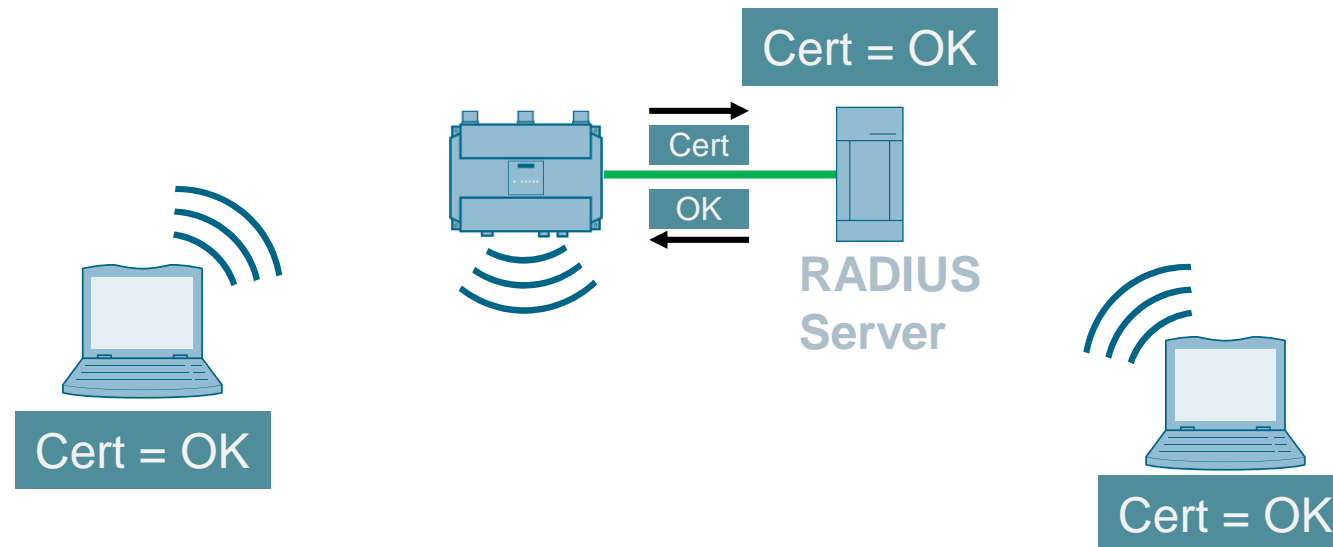
- **TKIP = Temporal Key Integrity Protocol**
  - Transitional solution for downward compatibility with older encryption mechanisms
- **CCMP = Counter-Mode/CBC-MAC Protocol**
  - Based on AES = Advanced Encryption Standard with 128-bit encryption
- **AKM = Authentication and Key Management**
  - Authentication of the radio network via 4-way handshake
  - Automatic key management with cyclical change of the keys





## Wi-Fi security mechanisms

- In response to IEEE 802.11i, the Wi-Fi Alliance launched WPA2 = Wi-Fi Protected Access
- WPA2 uses AES-CCMP and implements the important parts of 802.11i
- WPA2 can be used with pre-shared key (PSK) or with an authentication server (e.g. RADIUS server)





# Typical Weaknesses in wireless networks..

Unencrypted  
Communication

Transmit power to  
high

Reading of data -  
sniffing

Default passwords

Obsolete firmware

Automatic IP address  
assignment

Insufficient  
encryption

Spoofing – using  
false identity

.....

# Application example: SINEC NMS and IWLAN – Centralized WLAN Management



Separate live demo will be provided in coming Webinars



Easy central and policy-based configuration and management of Siemens network components, including Wireless LAN Access Points and Clients with the network management system SINEC NMS. ✓

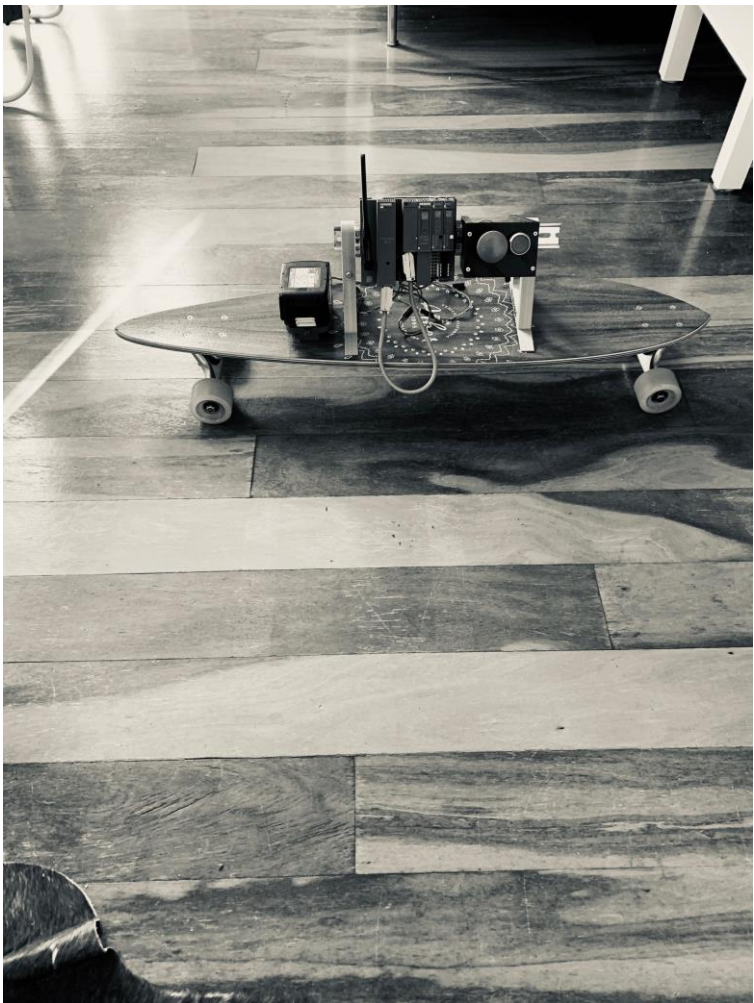
- Easy management of wireless LAN deployments of any size. ✓
- Just one system that can be easily maintained by OT technicians.
- Management of different industrial applications – including critical applications with safety requirements – over wireless.

# Live Demo

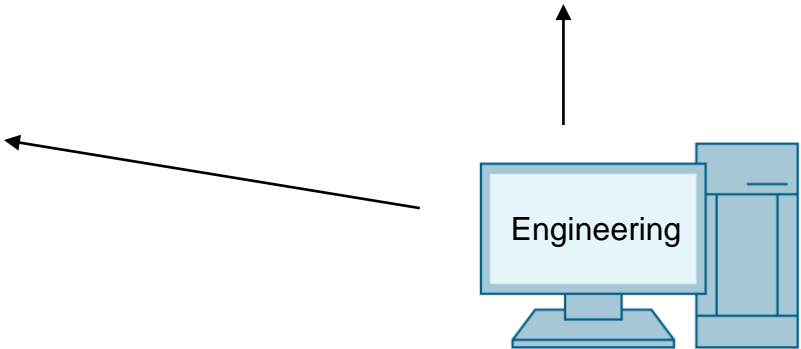
- Configuration of SCALANCE W Access Point
- SCALANCE W Client connection establishment
- Configuration overview

# Wireless Battery powered AGV demo..

AGV



Central controls cabinet





Thank you!



Christoffer Karlsson  
Product manager  
Industrial Communication / Identification

Siemens Ltd.  
885 Mountain Highway  
3153 Bayswater  
+61 437584211

[Christoffer.karlsson@siemens.com](mailto:Christoffer.karlsson@siemens.com)