SIEMENS


Industrial Wireless Communication

# iFeatures – special industrial functions for wireless applications

## Industrial Wireless LAN

Brochure

Edition 03/2019

siemens.com/iwlan

# iFeatures for special demands

Requirements on industrial networks are constantly increasing in the course of digitalization. Wireless communication via Industrial Wireless LAN (IWLAN) is already used in countless solutions, e.g. by mobile network participants in automatic guided vehicles (AGV) or in crane applications.

Not only the hardware, but also the software of the network components must meet special requirements for use in the industry. The SCALANCE W portfolio is perfectly suited for this purpose.

Siemens has developed special iFeatures for use in industrial environments which are enabled by KEY-PLUGs or CLPs inserted into the devices. These smart additional functions can be easily activated as software – also subsequently – on various IWLAN Access Points and Client Modules.

## Advantages of iFeatures at a glance

- Reliable real-time communication with SCALANCE W-700 (even with PROFIsafe)
- High availability thanks to seamless redundancy
- Secure IWLAN communication

| KEY-PLUG (for W-700) or CLP (for W-1700) | iFeatures | For Access Points | For Client Modules (or Access Points in Client mode) |
|---|---|---|---|
| **KEY-PLUG W780 iFeatures** | iPCF<br>iPCF-MC<br>iPRP<br>iREF*<br>Inter AP-Blocking* | • | • |
| **KEY-PLUG W740 iFeatures** | iPCF<br>iPCF-MC<br>iPRP | | • |
| **KEY-PLUG W700 Security** | Inter AP-Blocking | • | |
| **SCALANCE CLP 2GB W1780 iFeatures** | iPRP | • | • |
| **SCALANCE CLP 2GB W1740 iFeatures** | iPRP | | • |

* iREF and inter AP-Blocking in Access Point mode only

# Real-time communication

**Industrial Point Coordination Function (iPCF) and industrial Point Coordination Function Management Channel (iPCF-MC) for required deterministics and fast roaming in PROFINET and EtherNet/IP applications**

In the PROFINET environment, controllers and I/O cannot communicate reliably with each other via the regular IEEE 802.11 WLAN standard because real-time communication and deterministics are lacking. In addition, the roaming times between two radio cells need to be as quick as possible. Our solution enabling use of PROFINET and EtherNet/IP via WLAN for wireless communication with SCALANCE W-700 is the iPCF iFeature for guided applications or iPCF-MC for freely moving network devices.

**iPCF for linear applications**

This supplementary feature is especially relevant for overhead monorails. In such linear structured applications, the use of RCoax radiating cables instead of conventional antennas ensures a reliable and continuous signal quality.

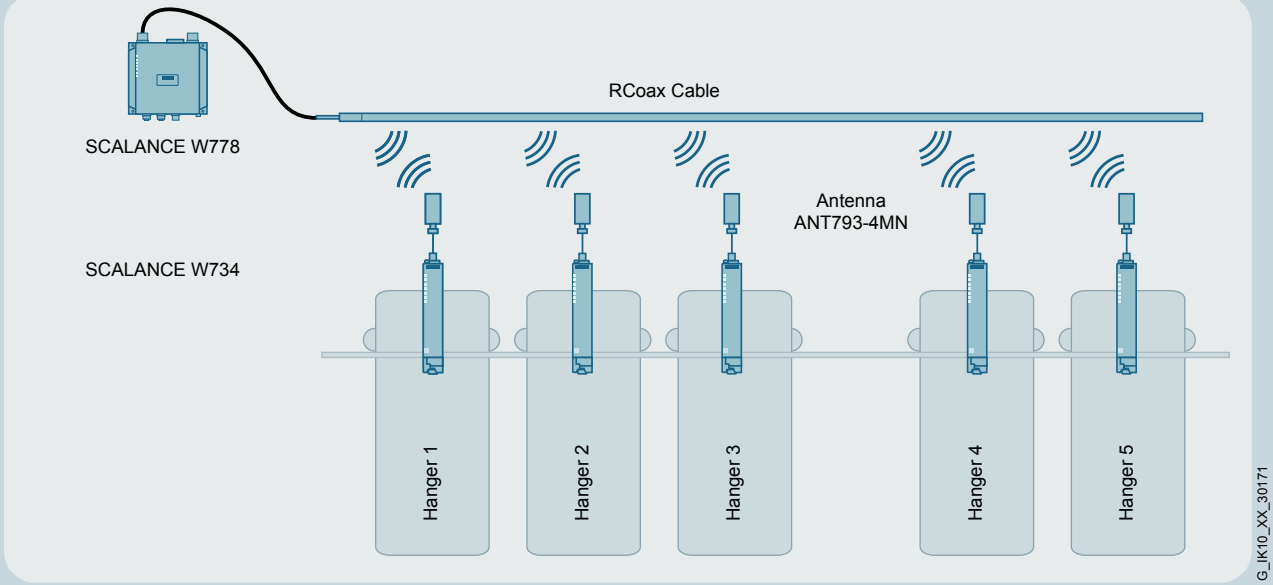
The iPCF iFeature enables the entire data flow of a radio cell to be sorted – making the communication deterministic. This is managed by the Access Point which cyclically polls all the radio cell Clients. iPCF also facilitates fast and reliable switching between two radio cells. Here can be ensured constant roaming times of significantly less than 50 ms.

**iPCF-MC for applications with free-moving Clients**

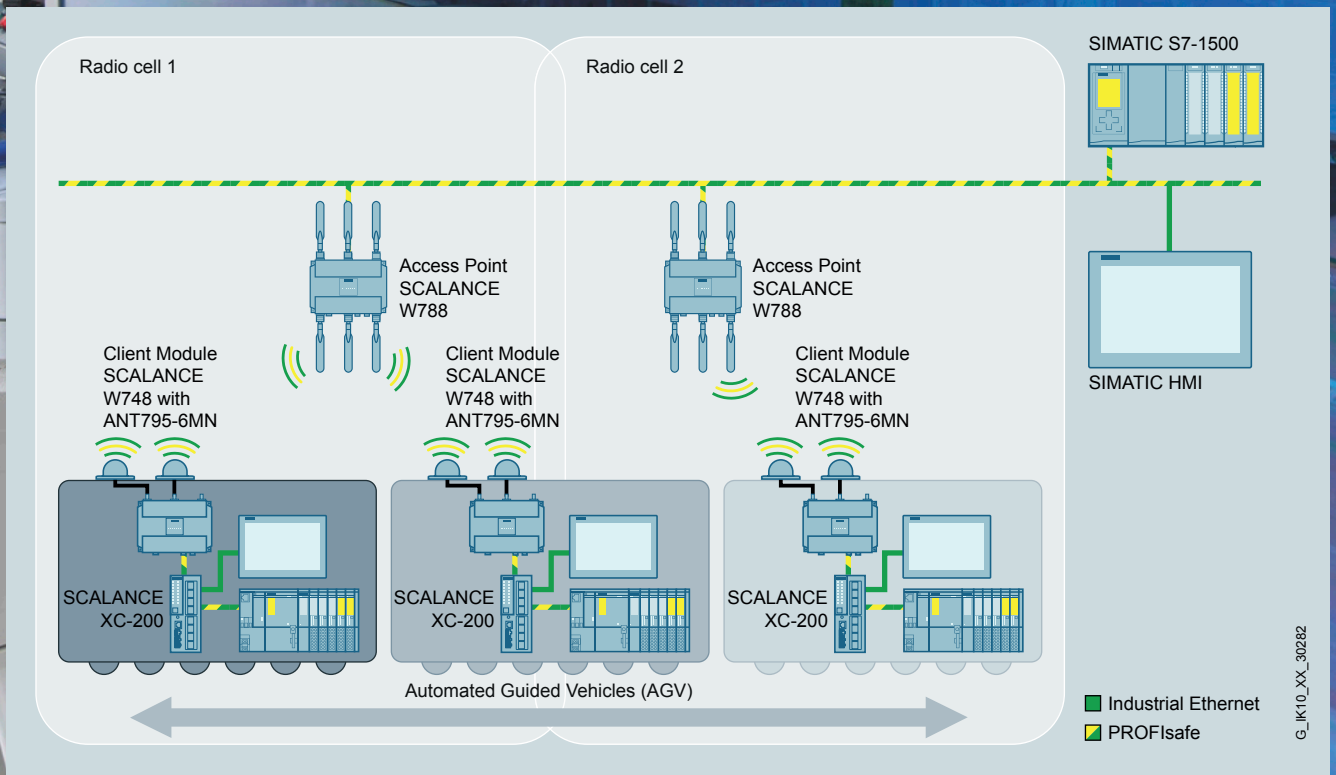
iPCF-MC is particularly suitable for applications involving mobile Clients which move freely in the field and which communicate with the controller via PROFINET (and even PROFIsafe) or EtherNet/IP. iPCF-MC provides the necessary deterministics and real-time communication. Although rarely required, applications with RCoax and directional antennas are also possible.

As with iPCF, the Clients are cyclically polled (deterministics). With the iPCF-MC iFeature, the Client scans its environment continuously for alternative Access Points. Should the radio quality deteriorate, a change to another Access Point can be implemented planned and very quickly. This is possible by using two wireless interfaces of the Access Point simultaneously in different ways: While one interface transmits a cyclic signal (beacon), the other is used for data transfer.

## iPCF for linear applications




## iPCF-MC for applications with free-moving Clients



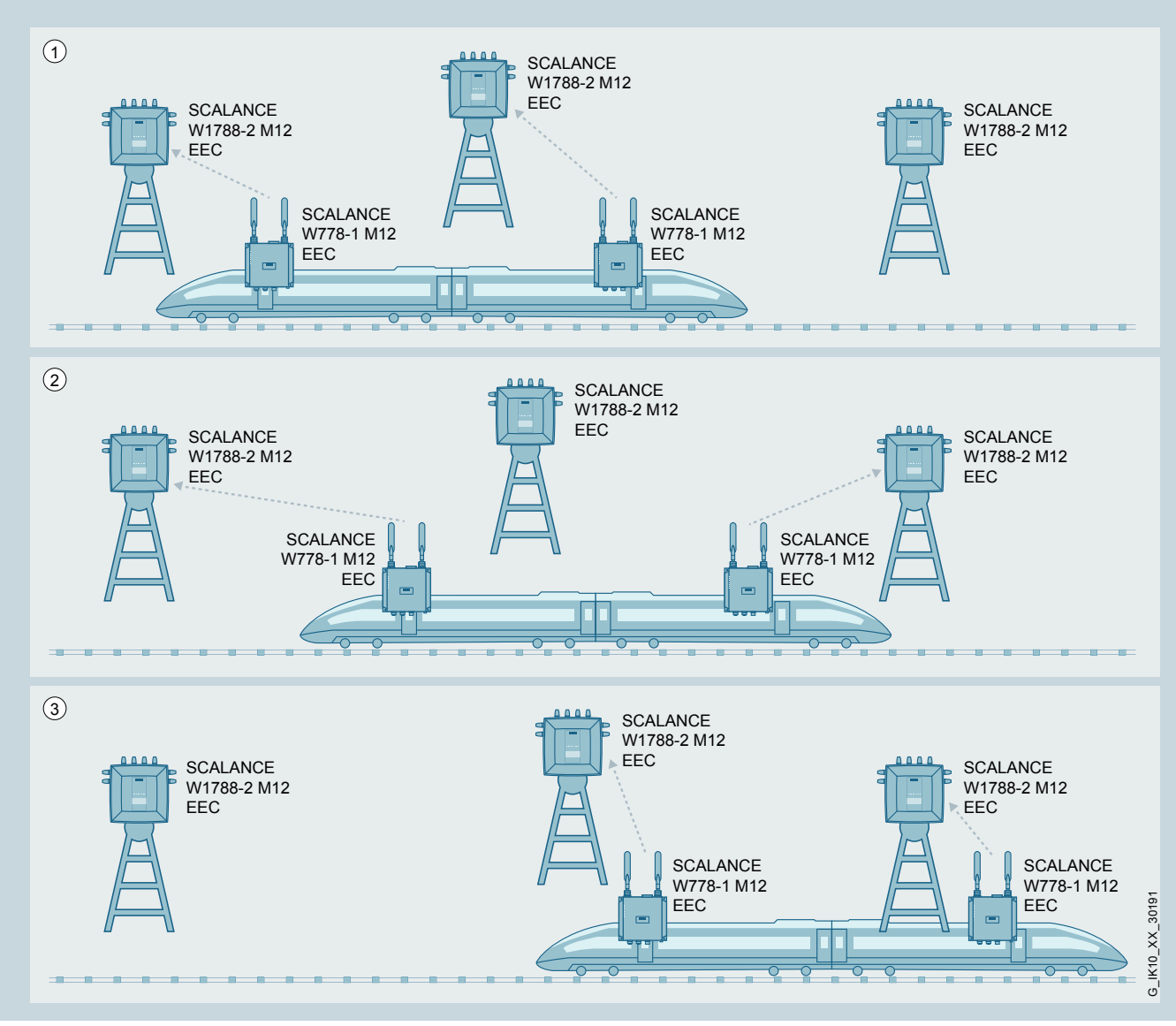
# Redundancy

**Industrial Parallel Redundancy Protocol (iPRP) for redundant, reliable IWLAN communication**

Spatial barriers, poor wireless coverage or interferences often lead to disturbances. Also the duration of a roaming process cannot generally be predicted. All these factors can often lead to a breakdown in communications.

These problems can occur in all mobile applications, such as in automatic guided vehicles (AGV), for example. Railway applications in which Client Modules in the moving train communicate with the Access Points on the trackside must also meet special requirements.

The iPRP iFeature facilitates the use of redundancy technology for parallel utilization of two radio links in wireless networks. This supplementary function enables redundant communication over two IWLAN connections, even for moving applications. Disruptions to data transfer on one radio link are compensated by parallel transmission on a second link: Whenever the roaming process is delayed or interference occurs, communication continues running reliably via this second path.



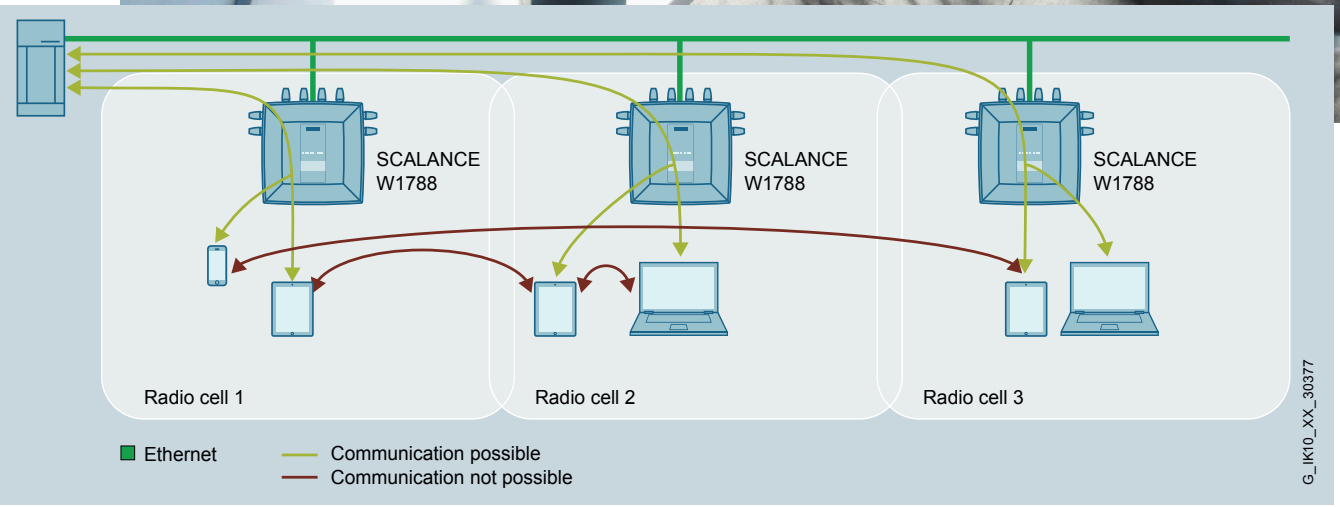
# Secure communication

**Inter AP-Blocking for secure IWLAN communication**

Inter AP-Blocking prevents cross-communication between WLAN Clients. By defining secure communication partners and gateways, the security risk in a network environment with unknown participants is reduced.

Normally, the Clients connected to an Access Point can communicate with all the participants of the layer 2 network. This constitutes a potential security risk, because unknown and unsafe network participants can also access your devices. Communication to others in the network is therefore prohibited in security related applications in order to avoid data manipulation and theft or other failures.

With the Inter AP-Blocking iFeature, the communication of the Clients connected to the Access Point can be restricted. This additional security function ensures that Clients within the network infrastructure only connect with the pre-defined, secure Access Points. Only those devices whose IP addresses have been configured on the Access Point as allowed addresses can be reached by the Clients. Communication with other network participants is prohibited and is blocked.



## Get more information

Wireless approvals:
**www.siemens.com/wireless-approvals**

PLUGs for network components:
**www.siemens.com/plugs**

Services:
**www.siemens.com/industrial-networks-services**

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


PDF (6ZB5530-0CX02-0BA1)
BR 0319 6 En
Produced 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.**