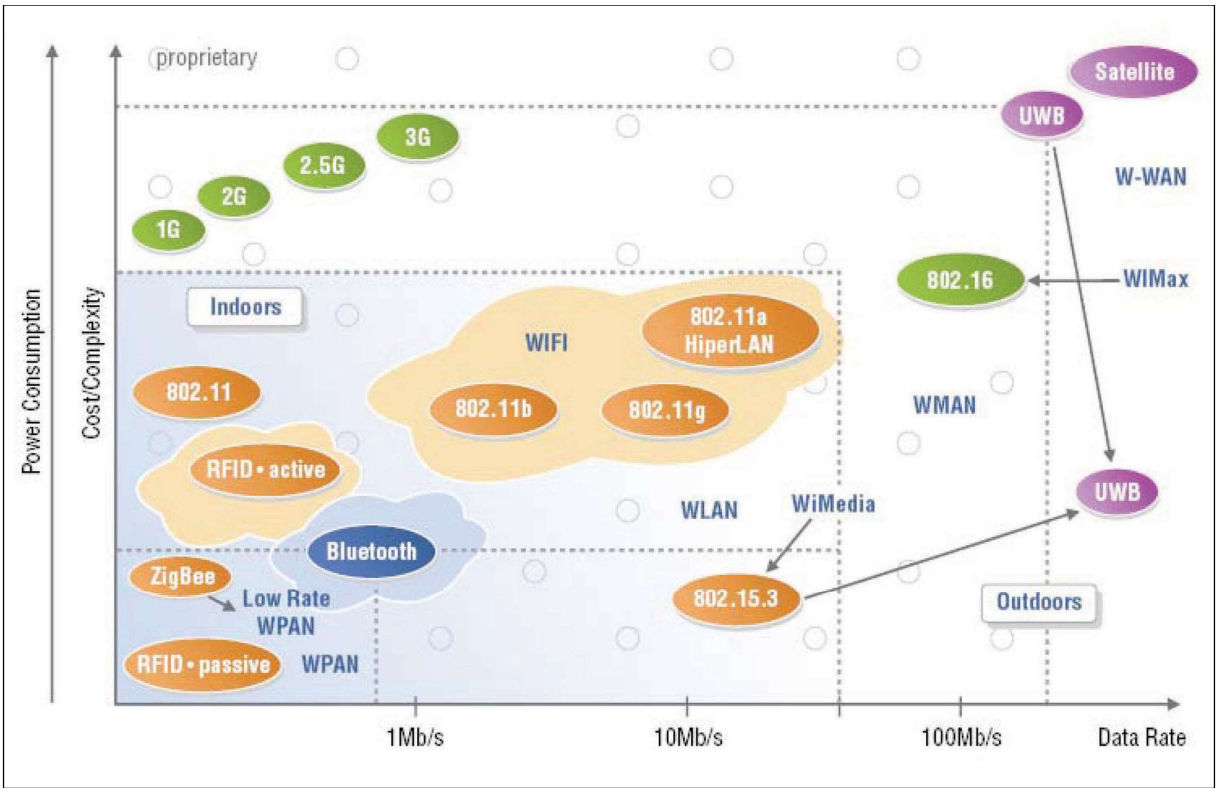
Wireless communication:

Introduction

After the development of fieldbuses, wireless communication between sensors and automation systems has also gained momentum. Wireless communication can be used for short-term solutions: for temporary installations where laying out cabling is too extensive and expensive, for rotating equipment and for applications that need to be set up quickly. For longer-term solutions, wireless communication can be used for complete factories and as operator tools.

Wireless communication using IEEE network standard:

For network standardization, the IEEE 802.x (i.e. the Institute of Electrical Engineers) is used. The 802.11 for WIFI communication is one of the best known. The total IEEE 802.x division of communication techniques can be found in the following figure 1. Here, the power consumption is plotted against the communication speed.



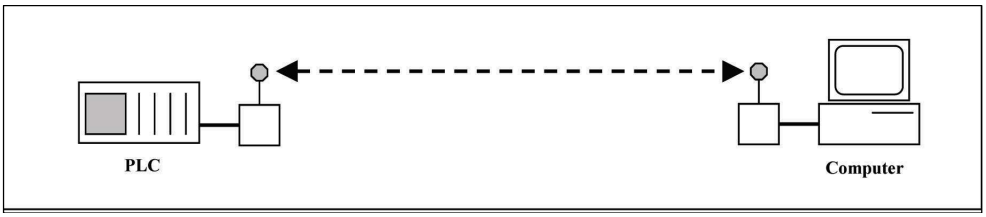
• Figure1Communication techniques according to IEEE802.x

Communication topologies:

There are different types of communication options

Point to point:

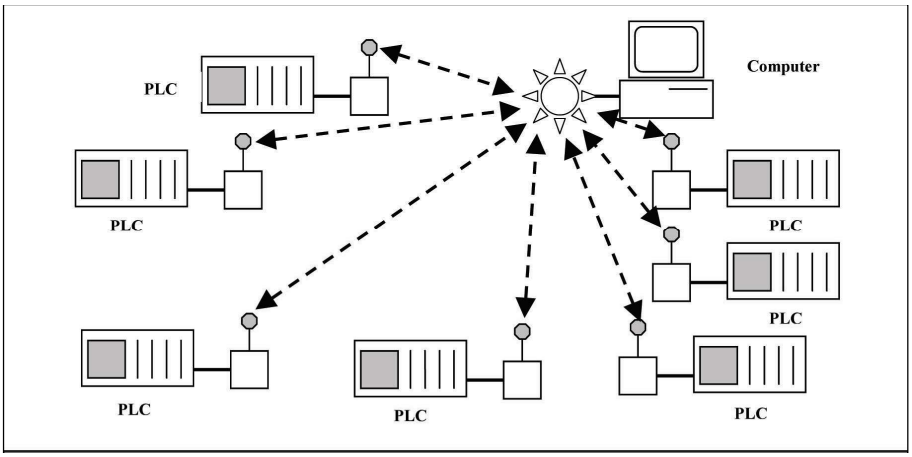
This replaces a direct cable between transmitter and receiver with a wireless connection. Reliable communication is only possible if the transmitter and receiver are close enough to each other so that the transmit-receive path is not interrupted and there is no RF (Radio Frequency) interference.



• Figure2Point to point communication

Point to multipoint or star topology:

Here a base station is used that communicates with multiple stations (in English called a node, i.e. a network node). The reliability of this system depends on the quality of the RF signal between the base station and the node. It is often difficult to find a point for the base station from which all nodes can be reached.

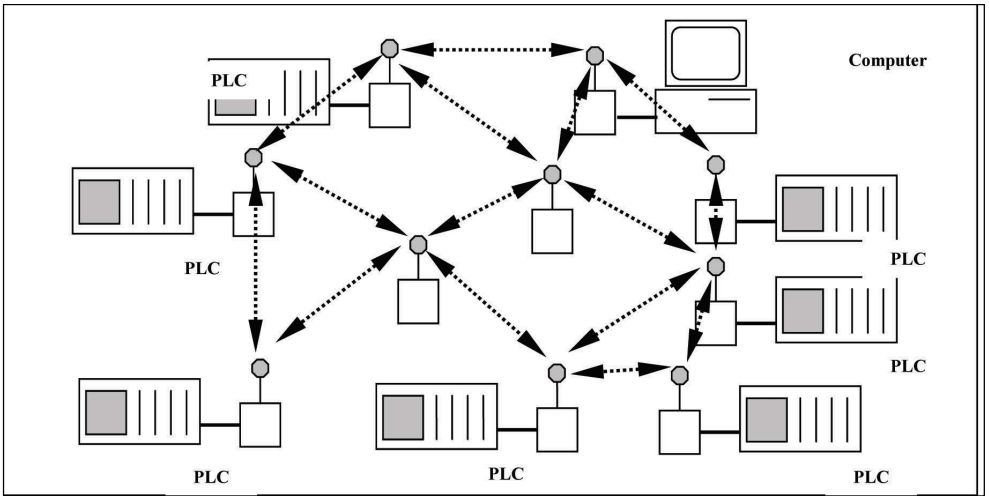


• Figure3Point to multi point communication

Peer to peer or mesh network:

Here, each node can receive and send messages and each node can also function as a router to forward signals from neighboring nodes. If a node fails, the message can be forwarded via another node - so via a different path. This so-called mesh network has the following advantages:

- The more nodes, the greater the reliability.
- The network configures and repairs itself by re-routing without human intervention (so-called 'self organizing')
- The network is redundant and can be made 'more redundant' by adding more nodes.
- The network can be easily upscaled because it does not depend on a central control point.



• Figure4Peer to peer communication

A combination of star and mesh network is also possible.

The reliability of a network therefore depends on the following factors: the accessibility of the transmit/receive path, RF interference and the availability of transmit power.

The following conclusion can now be drawn:

Topology	Reliability	Adaptability	Scalability
Point to point	High	Low	No
Star	Low	Low	Limited
Mesh	High	High	High

Standardization:

Globally, there are two initiatives for standardization of wireless sensor networks i.e. wireless HART and the ISA SP100. The ISA SP100 is the most promising standard and is supported by many end users; it is built in classes 0-5.

Safety	Class 0: Emergency action ; always critical (eg safeguarding systems)
` Control	Class 1: Closed loop regulatory control ; often critical (eg regular control loops)
	Class 2: Closed loop supervisory control (usually non-critical) (eg set point adjustment for control loop optimisation)
	Class 3: Open loop control (human in the loop)
Monitoring	Class 4: Alerting
	Class 5: Logging & downloading/uploading

Classes 3-5 wireless communication is already used by end customers and has proven itself in practice. Classes 0-2 are not (yet) considered suitable for wireless communication because of the unreliability of the signal transmission. The network standard is IEEE 802.15.4-2006 (WPAN, see fig.1) with a speed of 2.4 GHz. The network can be implemented as a star or mesh. The ISA SP100 is an open standard that will use only one application layer of a network protocol.

Security

Security is the most important topic in wireless communication. How can a malicious person ('hacker') be prevented from receiving the signal and how can he be prevented from manipulating a signal and/or putting a wrong signal on the network. There are a few security techniques available for this:

1. Securing the data using encryption: by encrypting the signal, only a recipient who knows the encryption key can interpret the message.
2. Network security through authentication: only pre-verified customers can access the network.
3. Protection by anti-jamming: this allows a signal that is obstructed by EMI (Electro Magnetical Interference) to be received correctly. This can be done by frequency hopping. By changing the frequency, EMI can be suppressed.
4. Security through code management: Items 1 and 2 above only work if the encryption and authentication are only known to the real (verified) users, in other words, they must handle this with care.

Power supply

The wireless components can be supplied with energy in the field in the following ways:

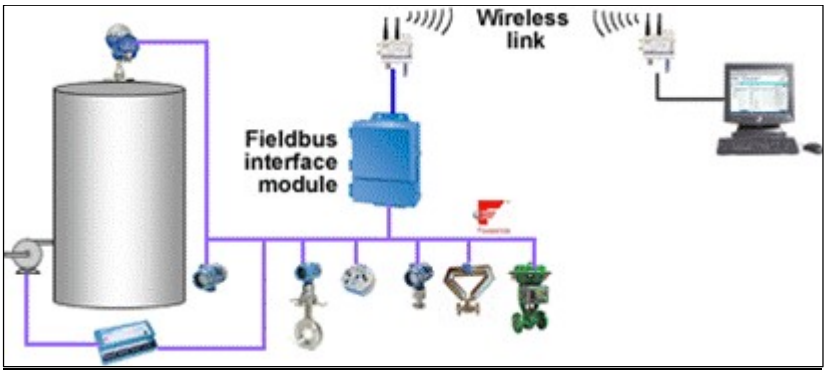
1. Locally available energy sources that are particularly useful when energy consumption is high.
2. Batteries; these are mainly used for low energy use or in hard to reach places
3. Energy 'scavenging'; this means: converting environmental energy into electrical energy. There are a number of possible sources for this, such as: solar energy, vibration energy and thermal energy

By using 'measurement on demand', so only supplying energy when it is needed, a lot of energy can be saved. This is closely related to the scan time - so the update time - of the wireless component; the lower the scan time, the higher the energy consumption. A scan time of 1 s. is already possible. An optimal point between scan time and energy consumption will have to be found.

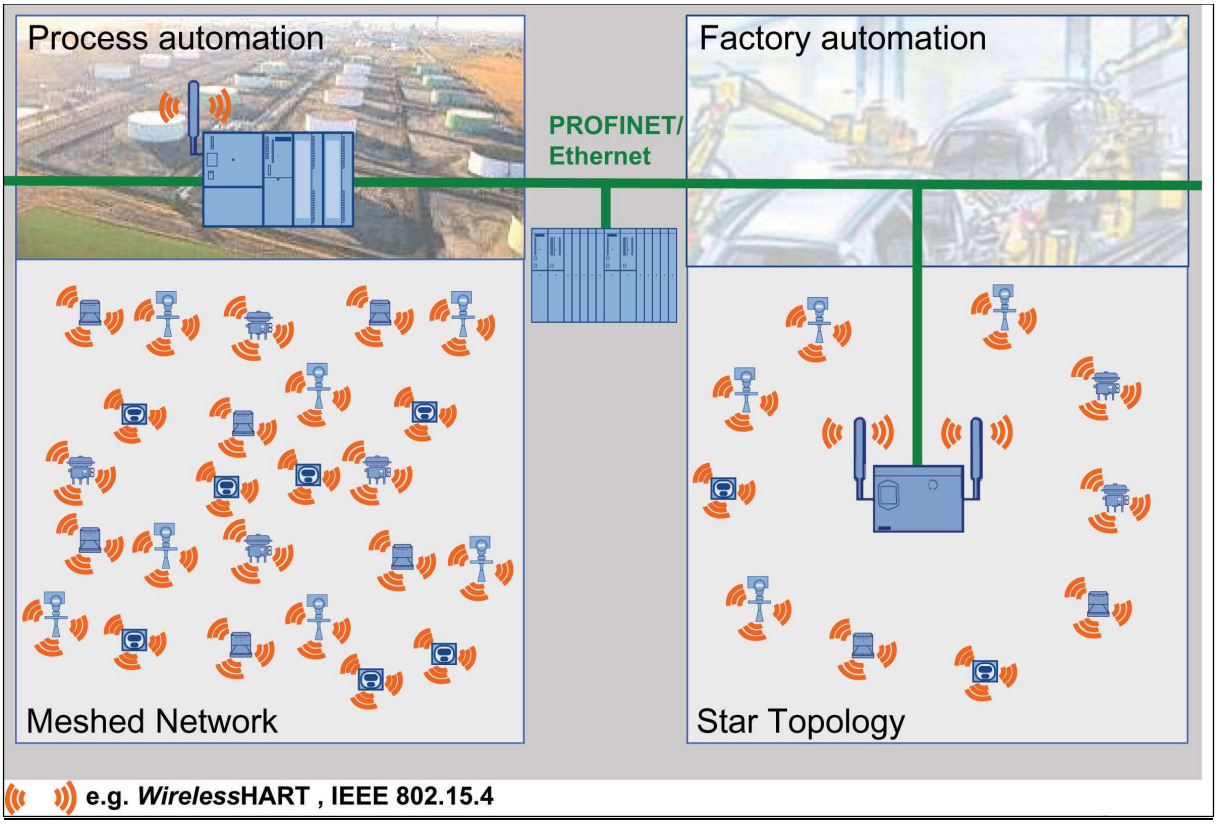
Also, aligning communication between the different network components at the right time, the so-called synchronization, can save energy. This can be done with TDMA (Time Division Multiple Access).

• Figure5Transmitter with solar cell for energy supply.

Examples:



• Figure6Connection of fixed fieldbus via 'wireless gateway' with remote PC.



• Figure7Network structures in industrial environment.