APPLICATION OF WIRELESS TECHNOLOGIES IN AUTOMOTIVE PRODUCTION SYSTEMS

Renzo Calcagno
Comau spa
Italy

Fulvio Rusinà
Comau spa
Italy

Franco Deregibus
Comau spa
Italy

Alberto Sangiovanni Vincentelli
University of California, Berkeley

Alvise Bonivento
University of California, Berkeley

Speaker: Renzo Calcagno, Comau spa, Italy (renzo.calcagno@comau.com)

Topic: Robot programming
Keywords: Wireless technologies in automotive systems

Full Paper:

Summary

Wired and wireless

One of the main ingredients of automation is undoubtedly control, which means information being collected, processed and delivered back to each actuator. In this context, telematics plays a key role in the automation industry.

To manage at best the requirements of each environment, several industrial communication standards mushroomed all over the world. To improve the portability and the interoperability of these standards, several attempts are still running to unify and consolidate them into fewer and widely used approaches. In this process, Ethernet (IEEE 802.3), the well known standard of PCs' communication, seems to play a fundamental role, thanks to the capability to integrate the heterogeneous traffics of office and industry automation over a single infrastructure. Furthermore, the idea of applying wireless to automated industrial processes is gaining ground. This raises some questions, such as:

- What are the benefits of the extensive use of wireless technology in process automation?
- What is the best wireless technology for industrial automation?
- Is wireless the suitable next step towards a unified communication interface?

This paper tries to answer these and other questions, collecting ideas and drawing new perspectives.

Fig. 1 – An industrial scenario involving robots

Wireless in the industry: benefits, threats and true restrictions

When considering the introduction of wireless technology into manufacturing plants, different aspects must be considered:

1. Costs. The first reason justifying wireless deployment is always cost saving due to wire replacement; the industrial case is particularly critical due to the high costs of industrial wiring.
2. Resiliency and Safety. The impact of a link failure event over system safety must be minimized: wireless is vulnerable to noise, temporary interferences, fading. A receiver can be "jammed" quite easily. Usually, these are the first objections to wireless: anyway there are several possible solutions preventing such problems and, don't forget it, wires can be cut (and hard to repair) and wired devices (switches, hubs, repeaters) break!
3. Priority. Safety requirements involve the use of a protocol which is reliable and offers real-time guarantees for the most important signals. Not all the protocols are suitable for this. Consider that if, on one hand, you can ensure safety by a simple approach which interrupts processes whenever messages get lost, on the other hand you cannot afford too many interruptions if you do not want to cut down the efficiency of your process.
4. Security. Another threat concerns wireless vulnerability. Anyway this can be considered a thing of the past: several solutions exist to improve security and privacy of wireless transmissions.
5. Mobility. Wireless means mobility. Freedom from wires brings several benefits: you can move around your plant without disrupting connectivity; in case of frequent reconfiguration of your plant involving assembly lines, you do not have to deal with cable bonds. In most cases, an industrial application requires more a nomadic rather than a true mobile solution: this means that you work in quasi-static scenarios on which wireless is particularly effective.
6. Scalability. Intuitively, a wireless solution is more efficient if it allows for an increase of the number of users connected to the same device (overcoming the paradigm of a point-to-point connection), number of active networks, capability to automatic configuration. This will be further discussed in next section.
7. Protocols Inter-operation. Several different industrial communication standards compete and cannot inter-work each other. A wireless protocol can behave as a bridging protocol among them.
8. Fabric-to-Office Integration. A wireless protocol can efficiently transport also office-related and internet-oriented traffic. This would allow to carrying on the evolution started by industrial Ethernet, optimizing network maintenance costs and always-on connection to the office. The integration with the office (the so called "global networking") enables, in perspective, added valued industrial management (automated asset management, supply chain management, customer relationship management).
9. Dynamic Chain Configuration. On the other hand, fabric-to-office integration enables to draw an improved production environment, flexible and dynamically re-configurable according to highly differentiated customer requests recalling data (for instance orders) stored on other systems.

Wireless in robotics: more ingredients

The above considerations are especially true for robotics. This scenario introduces however some further ingredients, with relative requirements and constraints.

More in details, industrial solutions using robots, as those traditionally included in Comau's portfolio, foresee a working set, including a robot (see Fig. 2.), and a control unit with its Teach Pendant (Fig. 3), the hand-held device which allows remote control of the robot and simplifies monitoring (it collects signals and provides a smart display of the information).

Fig. 2 – Comau SMART robot range: from 6 up to 800 Kg payload

A careful analysis of the characteristics (timing requirements, resiliency, semantics, etc.) of the signals being exchanged by the units must be the starting point for the design of any wireless solution.
This is a typical point-to-point communication scenario, where expensive cabling forces each Teach Pendant (TP) to be dedicated to a single robot. Wireless connectivity allows to overcoming this paradigm: a single TP can monitor and even coordinate several robot units at the same. This implies the use of a multiple access wireless technology: if the wireless medium can be shared among multiple users, multiple devices can contemporarily talk to each other.

Fig. 3 - Teach Pendant for C4G family

Multiple access wireless means that a single operator can connect several units at the same time, but also that several operators can monitor and collect alarms from the same unit. Furthermore, several units can coordinate at run time; this implements a general purpose scenario which can be called "multipoint wireless" (may mean machine-to-machine, man-to-machine or machine-to-man data communication).

Moreover, with a multiple-access capability, additional data, such as video sequences or sensor measures, could be contemporarily collected. This would significantly improve early fault discovery and diagnosis: monitoring could get more efficient and even a large plant could be potentially monitored by a single location.
This would be a further improvement (in terms of flexibility) but would require also a large capacity channel (that is a *broadband wireless technology*) and a flexible channel able to differentiate among different data profiles (that is a *differentiated* or prioritized *technology*).

Wireless characteristics
The previous sections have argued that the challenge of wireless deployment in an industrial setting goes true several factors and requirements. The selection of the right wireless technology is crucial.
As a matter of fact, a plethora of wireless technologies exists, spanning from narrowband to broadband, from short- to long-range, licensed and unlicensed, standard or proprietary, application-dependant and general purpose, point-to-point or multiple-access.
Because of the strict requirements of automation scenarios a suitable wireless solution should fulfill at least some characteristics:

- resilient and reliable;
- immune to interference from other radio sources;
- multiple-access;
- data- and Internet-oriented;
- priority capable;
- broadband;
- scalable;
- secure.

In next section Comau's approach, based on the previously listed requirements, will be introduced.

Which technologies
The question is then: "Which wireless technology?"
Let's recall the rational towards the final decision:

- The desired wireless solution should be based on a standard. This is fundamental to avoid the nightmare of a new multitude of proprietary incompatible solutions.

- The range of communication is expected to be in personal (WPAN) or local range (WLAN). Wide area (WWAN) and metropolitan area networks (WMAN) seem to be less suitable for several reasons. First, they involve a strategic partnership with some public (licensed) telecom operator. Secondly, they involve higher costs (the costs due to the public services and the higher costs of the devices). Third, they are quite rigid in their configuration with a star topology and a central base station. Furthermore, the bandwidth (with currently deployed solutions) is not large enough.

These points are sufficient do discard WMAN, GSM, UMTS and all proprietary solutions. Furthermore:

- RFID does can not be applied a safety critical solution. It is a low cost and low power solution which offers limited payload and simple functionality. It is suitable to keep track of goods and recognize them throughout an industrial process, but not to pilot an industrial plant and to guarantee flexible and huge data exchange. It can work as an additional collateral technology, not as the main one.
- Bluetooth (2.4 GHz) played an interesting role in the past of WPAN: it offers a good compromise between data rate (about 1 Mbps) and range (about 10 m or 100m with lower data rates). Anyway this trade-off seems to be its main limit: UWB seems to be preferred for higher data rates and Zigbee for lower consumptions and longer battery life.
- Ultra-Wide Band - UWB (3.1-10.7 GHz) is very promising: this technology can handle the bandwidth required to transport multiple real-time services (including audio and videos!) – up to 450 Mbps in short range. It is being investigated as replacement of USB and IEEE Firewire (1394). UWB provides a new paradigm with RF energy spread over several GHz (and such a low power density to appear harmless noise). Studied but not ratified by IEEE yet (in the 802.15.3 family).
- Zigbee (2.4 GHz) is focused on ensuring a very long primary battery life rather than high data rate (low duty cycle). Consequently, nodes are able to remain quiescent for long periods without communications. Based on high-density star and mesh networks and using a DSSS approach (see below), this technology can guarantee low latency but only to low throughput data (about 20-200 Kbps).
- Hyperlan (2.4 GHz) is an effective technology but is an only European standard and is loosing popularity, mainly due to its costs.

Consequently, only WLAN survives the required screening process. In next section (which WLAN) it is shown that it fulfills all the requirements previously mentioned and that a WLAN solution in particular seems suitable for the industrial implementation.

Which WLAN

WLAN (or Wi-Fi) is based on a set of well-known standards (the 802.11 family) developed by the IEEE organization: most of them have already been ratified, while new developments, mostly backward compatible, are still being finalized to further improve them. This is a first reason supporting WLANs.

Secondly, WLAN (or Wi-Fi) was designed as a wireless extension of Ethernet, so it can simply guarantee a natural inter-working with internet-like data. This would enable fabric-to-office integration.

Third, several implementations are already available and quite cheap. Furthermore, open source tools and drivers simplify the development of custom solutions.

Fourth, Wi-Fi bandwidth is suitable for data rates required by the industrial application. Available bandwidth ranges from 1 to 11 Mbps in the first releases (802.11 and 802.11b), to 54 Mbps (802.11a and 802.11g) and up to 500 Mbps in the close future (802.11n): each of these standards achieves different performances which will be investigated below.

Fifth: the reach (about 100m; more with directional antennas) is suitable for industrial applications.

Sixth: the wireless medium is shared among multiple users. Consequently, a MAC (Medium Access Control)

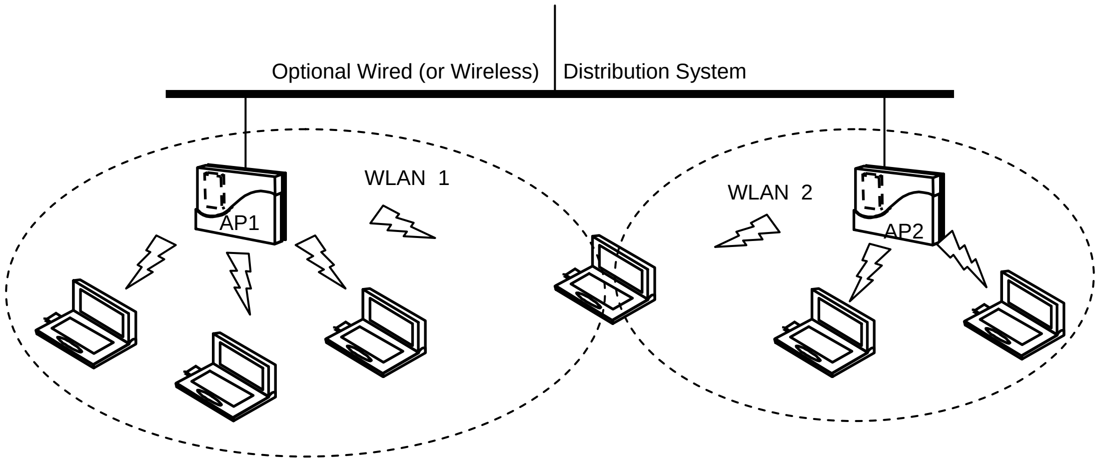

Fig. 4 – Logical architecture of a structured WLAN scenario, with shared wireless medium

protocol allows efficient access to the medium, with low configuration efforts. The simplest solution ("structured mode") foresees a central node (called Access Point – AP) which defines the rules to associate and participate in its network. It would be natural to put an AP in each robot[1].

Seventh: the WLAN standards use Radio Frequency ranges which include portions of the globally allocated Industrial, Scientific, and Medical (ISM) bands in the 2.4 GHz region[2], and of unlicensed bands in the 5 GHz region[3]. This means that no license is required. Although this means complying with regional rules for electro-magnetic emissions and potential external interference, the closed environment typical of a manufacturing plant is a natural shield against these types of attack.

Eighth, Wi-Fi includes solutions to dynamically set the transmission rates (and the redundancy codes) according to the available bit-error rate (BER) and signal-to-noise (SNR) ratios. Transmission is based on "spread spectrum" (SS) techniques, whose common rationale is to expand the digital signal so that the average transmitted spectral power is kept low while maintaining high data rate and reliability performance.

Ninth, security is not a problem. The IEEE standard includes a robust and mature security solution that overcomes the weaknesses of the early "WEP" encryption schemes.

Tenth, power consumption optimization is not a critical for wireless robot control applications. One of the most frequent objection to the use of WLAN (for instance in sensor networks) does not hold for robotics.

There are several possible flavors of WLAN in terms of radio transmission schemes, namely: 802.11, 802.11a, 802.11b, 802.11g, and 802.11n. The IEEE 802.11 existing solutions are shortly recalled below.

- 802.11. The first IEEE 802.11 solutions were designed for the 2.4-2.4835 GHz band and used two different spread-spectrum techniques: Frequency Hopping (FHSS) and Direct Sequence (DSSS). FHSS is not as complicated as DSSS and uses less energy, but DSSS has longer range. DSSS supports higher data rates from individual physical layers, which is why DSSS was chosen for a higher-rate 802.11 physical layer (802.11b). Both FHSS and DSSS reach 2 Mbps line rate and use approximately 30MHz for transmission (one third of the band). This limits the number of non-overlapping access points within coverage distance to a maximum of three.
- 802.11b specifies a physical modulation using DSSS at data rates of 5.5 and 11 Mbps. The frequency bands and

[1] In addition MAC protocol is evolving to support delay-sensitive traffic also in case of data congestion, through prioritization or resource reservation (802.11e) and to support complex topological network configuration self-configuring in meshes (802.11s).

[2] Wireless devices using the ISM bands include portable phones, microwave ovens, garage door openers, security devices, etc. Within the ISM bands, all users share the airwaves and must tolerate interference from one another.

[3] These portions of the spectrum have been set aside specifically for largely unregulated use, in the sense that the individual user does not require a license.

number of channels is the same as for the early IEEE 802.11 standard.

- 802.11a operates in the 5 GHz band (5.150-5.350 GHz and 5.725-5.825 GHz). A technique called OFDM[4] is used to increase 802.11 data rates to 54 Mbps. OFDM increases spectral efficiency and allows greater channel throughput. With OFDM, the high-speed data signal is transported via 64 parallel sub-channels within a 20-MHz channel.
- 802.11g, similarly to 802.11b, operates in the 2.4GHz band, and uses one third of the band per channel. 802.11g mimics 802.11a modulation (OFDM) so that it can reach 54 Mbps data rates. The number of non overlapping channels is 12.
- 802.11n is a future standard yet to be ratified by the IEEE 802.11 Group. It is supposed to allow for a raw throughput of up to 500 Mbps in the 5 GHz band.

Consequently, 802.11a is the only standard which all of the following requirements:

- It is already available.
- It provides high data rates: this means more transmission opportunities for critical (automation) data and potential room for other delay-sensitive (multimedia) or high-volume (internet) traffic.
- Allows for a high number of non-overlapping channels, which means easier network configuration and opportunity to install several AP able to operate without interfering (operating in physically distinct ranges).
- Operates in the 5 GHz range, which not only allows room for more channels, but is quite prone form undesired interference. In the 2.4 GHz range, RF interference from other devices, such as the newer cordless phones microwaves ovens, wireless video, Bluetooth devices is can reach critical values.

Comau’s final decision falls then into IEEE 802.11a standard.

Does it work?

Although IEEE 802.11a is the most suitable existing solution, it was designed for consumer electronics. Consequently, some modifications must be made to enhance safety and reliability performance. Typical issues which arise when moving to a more critical environment, include:

- addition of resiliency mechanisms to prevent holes in safety due to faulty transmissions (including robot stop);
- potential decrease in the efficiency and availability, mainly due to safety improvement;
- indoor radio propagation limitations due to multi-path and undesired scattering;
- interference problems due to other wireless devices (electro-magnetic compatibility issues).

All these issues have been extensively considered by Comau which has performed many tests jointly with its scientific partners (Istituto Superiore Mario Boella in Turin and University of California at Berkeley).
Tested scenarios include:

- propagation measures in laboratory
- propagation measures in industrial environment
- efficiency of wireless transmissions on a real robotic application in the automotive production plants of FIAT Mirafiori (Turin).

The results reveal satisfactory performance often beyond expectations. The bandwidth and resilience protocol available in 802.11a are definitely enough to overcome all restrictions.

Conclusion

The introduction of wireless technology in industrial environments is a challenging goal with huge potential benefits on cost and increased flexibility and this is particularly true for robotics. Several solutions are available and IEEE 802.11a seems to be the only available standard meeting most of the constraints of the robotics scenario.

Since IEEE 802.11 is a consumer electronics technology, Comau has performed extensive studies and tests to verify its performance. The relevant results are being collected and submitted to TÜV to achieve "Functional Safety FS" certification according to EN954-1 (up to cat.4).
Once more Comau is committed to the development of new technologies and to the enhancement of manufacturing

[4] Orthogonal Frequency Division Multiplexing (OFDM), which utilizes multiple carriers (referred to as subcarriers), technically is not a spread spectrum technique (the subcarriers remain stationary and are not spread) but it serves the same purpose of spreading the signal power over a large band: a fast transmission is sent as many slow transmissions, simultaneously, on many different frequencies.

process. Wireless is considered an additional tool which can enable greater efficiencies and is being tested to ensure that all environmental safeguards are in place.

Comau works closely with scientific and academic partners and with its business partners to develop and test new solutions.

Applications
1. Wireless Teach Pendant (WiTP).
Comau Robotics has pleasure in presenting the new product WiTP: a Wireless Teach Pendant, the first important application of wireless technology in the industrial robotics sector, maintaining and implementing the typical operations of traditional networks (wiring fitted) but with no need for physical connection between the robot control unit C4G and the programming unit.
With the wireless Teach Pendant all the traditional data communications/robot programming activities can be carried out without the restriction caused by the cable connected to the control unit, but, at the same time, absolute safety is ensured.

Fig. 5 – Wireless Teach Pendant for C4G family

The main characteristics of WiTP are listed in the following table:

Technical features	WiTP
Wireless technology	802.11 a/b/g
Communication protocol (IEC61508 standard)	Property of Comau (Comau Patent Pending)
Safety certification	EN954-1 category 4
Safe connection to C4G procedure	Pairing/Un-Pairing (Comau Patent Pending)
Range of action in industrial environment	Up to 100 metres
Independent communication channels (as per standard 802.11 a)	19 EU / 24 USA
Autonomy	6 hours
Battery recharging time	2.5 hours
Control electronics	Intel PXA 270 – 520 MHz processor
User serial line	USB 1.1

<u>Safe connection</u> (see Fig. 2.): the connection between the new Teach Pendant and Robot Control Unit is made by "Pairing/UnPairing" safety procedure (Comau patent pending). The safe connection procedure can be carried out on every C4G fitted with wireless technology, therefore one teach Pendant is sufficient for many Control Units.

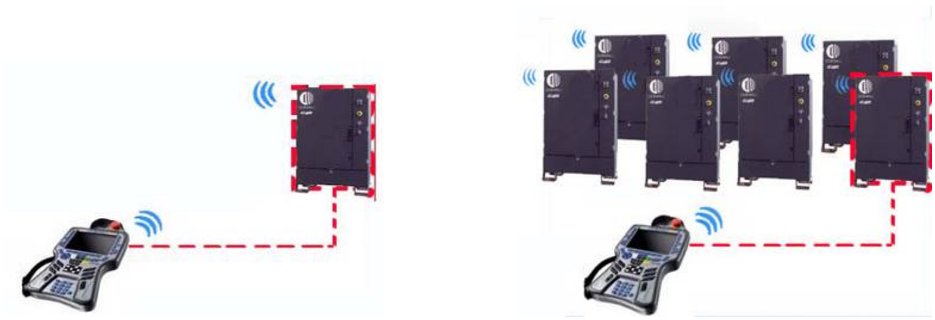

Fig. 6 – Point-to-point and point-to-multipoint safe connection for CG4

2. Factory control architecture (Step 2006).
Comau Power train develops factory layouts. Here there is an example where several modules are connected together with a Plant Ethernet in order to exchange data.

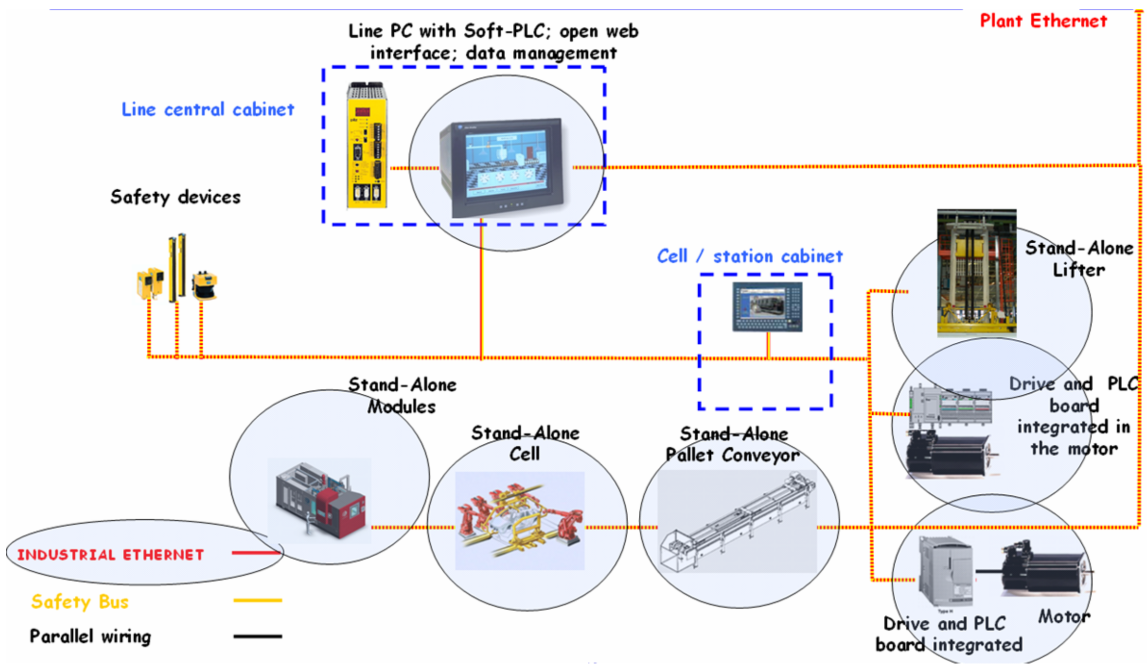

Fig. 7 – Factory control architecture

Using the Wireless technology replacing the "Industrial Ethernet" have the following advantages:

- Reduction of wiring and connections between cabinet and components
- Cabinet volume reduction due to hand-held HMI
- Reduction of assembly time of the station/line
- Opportunity for new functionalities and cost reductions

Other applications of networking or HMI. The wireless technologies are used to connect devices like:

- Teach Pendant
- Welding timer
- PLC
- HMI
- Other PC

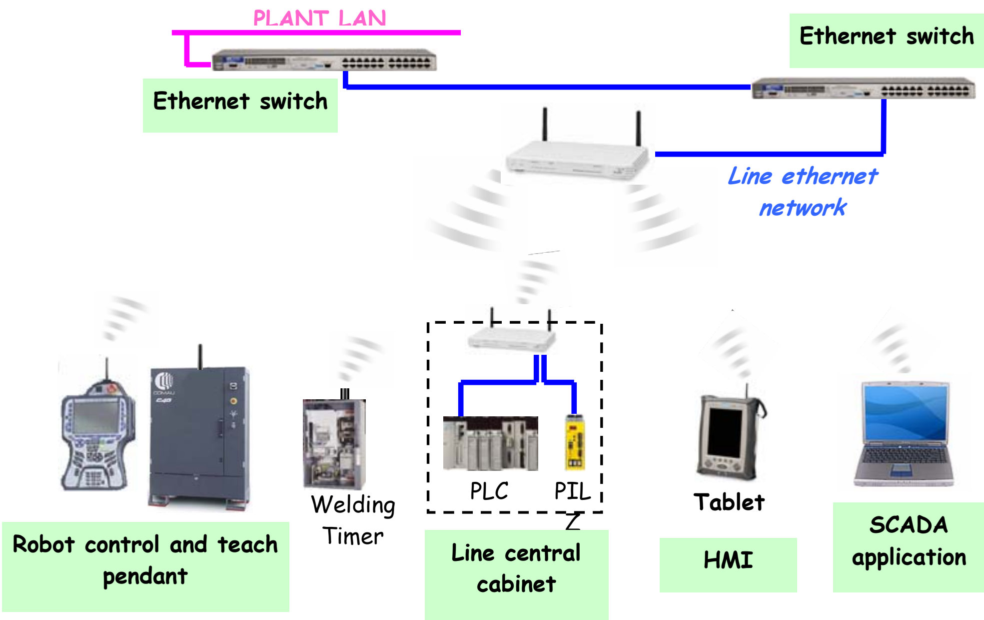

Fig. 8 – Application of wireless technologies- Networking and HMI

Other wireless application foreseen for over the 2006.

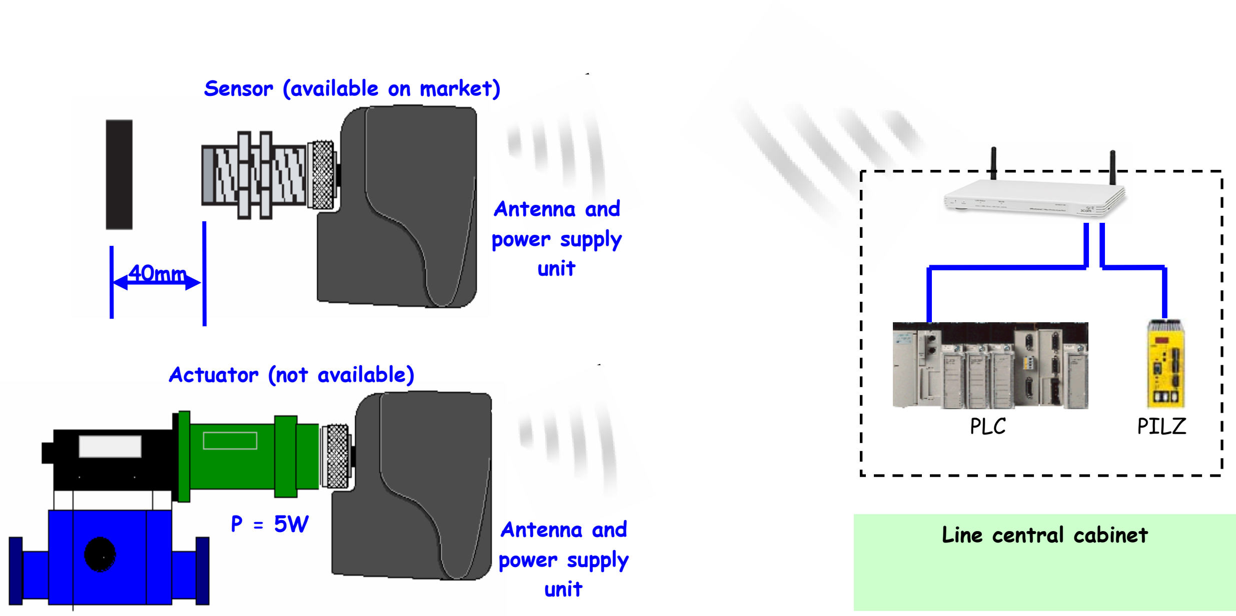

Fig. 9 – Sensors and actuators

References

[1] IEEE Std 802.11, 1999 Edition (R2003) (ISO/IEC 8802-11: 1999) IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[2] IEEE P802.11REV-ma/D3 Unapproved Draft Standard (This document reflects the combining of the 2003 Edition of 802.11 plus the 802.11g, 802.11h, 802.11i and 802.11j Amendments).

[3] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks", Proceedings of the IEEE, vol. 93, no. 6, pp. 1130-1151, June 2005

[4] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a Wireless Link in an Industrial Environment using an IEEE 802.11-Compliant Physical Layer", IEEE Transactions on Industrial Electronics, vol. 43, no. 6, pp. 1265-1282, December 2002

[5] A. Bonivento "Digital Channel Estimation for wireless Sensor Network", Internal Report, Berkeley Wireless Research Center and Computer Sciences, University of California, Berkeley, Fall'04 http://www.eecs.berkeley.edu/

Contacts

For more information, please contact:

Comau - Robotics & Final Assembly
Via Rivalta, 30
10095 Grugliasco Torino (Italy)
Tel. +39-011-0049111
www.comau.com