Roaming in Wireless Factory Automation Networks

Markus Rentschler, Senior Member IEEE
Business Unit Networking
Balluff GmbH
73765 Neuhausen, Germany
Markus.Rentschler@balluff.de

***Abstract*—Factory automation applications operating on wireless communication systems may exceed the coverage area of a single base station, requiring the capability of device movement between multiple base stations. Roaming is a feature that allows such wireless device mobility between base station cells, but cyclic process data communication between PLC on the one side and the roaming wireless device on the other side gets usually interrupted during the handover process, not allowing real-time operation during this handover phase. It is shown that this is not an obstacle in factory automation applications when the handover process is kept under supervision of the PLC control program. This roaming concept is adopted with PNO's new "IO-Link wireless" standard.**

***Keywords*— Actuator, Factory automation, Handoff, Handover, IO-Link wireless, Industrial wireless, Roaming, Sensor, WSAN**

I. Introduction

The suitability of wireless communication systems for industrial automation strongly depends on the requirements of the specific application areas. Figure 1 gives a structural overview of established wireless systems. On the sensor level, the wireless technologies are usually sub-divided into the application domains of process automation (e.g. chemical industry) and discrete factory automation (e.g. assembly line production), due to significantly different performance requirements [1].

Cellular communication systems on the WAN level are utilized almost only in remote service applications or alert systems [2]. Field level wireless systems are often used in monitoring and open-loop control applications [3], e.g. the IWLAN system of Siemens.

In process automation (PA), lower performance requirements on the sensor level exist and wireless communication systems are well established. IEEE 802.15.4 based standards like WirelessHART (IEC 62591) and ISA 100.11a were developed by the HART communication foundation and the international society of automation (ISA), respectively. The PROFIBUS and PROFINET user organization (PNO) has adopted WirelessHART for the "Wireless Sensor Actuator Network for Process Automation" (WSAN-PA) standard. In 2011, another 802.15.4 based standard called WIA-PA (IEC 62601) emerged.

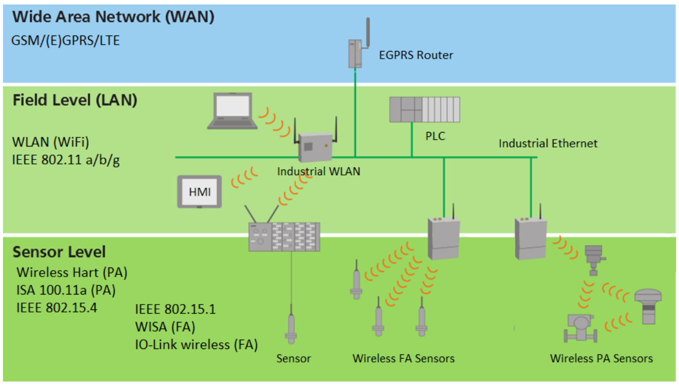

Fig. 1. Industrial Wireless Systems [1]

Factory automation (FA) applications have more demanding requirements regarding latency, synchronism and reliability, especially for closed-loop control applications. This has so far delayed the market penetration of wireless systems in the factory automation domain, especially on the sensor level. A recently emerged standard WIA-FA (IEC 62948) is based on IEEE 802.11 (WiFi), but raises questions about its suitability in coexistence scenarios with other wireless systems.

The emerging PNO standard "IO-link wireless" is based on several predecessor technologies, such as 802.15.1, WISA and WSAN-FA [4-7]. WISA was originally developed by ABB as a proprietary technology and a range of products were successfully deployed by ABB. In 2010 however, ABB made it available to the PNO for adoption to an open standard called WSAN-FA, where an important goal was to define a seamless integration into existing engineering tool chains, for which the engineering and management concept of IO-Link [8][9] has been chosen. In 2012, the WSAN-FA standard was released by the PNO, but not adopted by any vendor, because of significant specification gaps. This has led to further reworking activities, protocol improvements and a renaming to "IO-Link Wireless", which is currently in the final specification phase [8]. The basic system structure is depicted in Fig. 2.

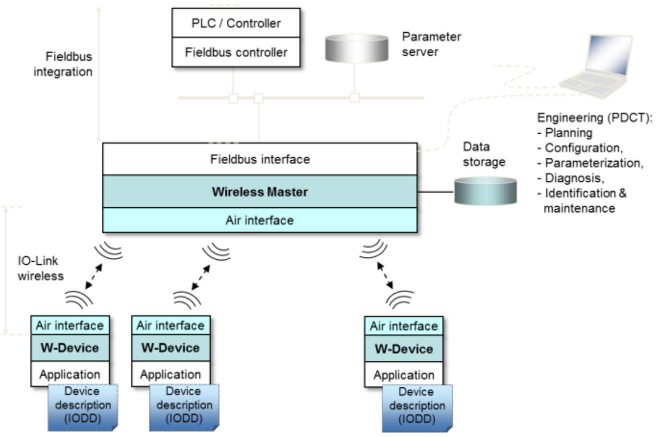

Fig. 2. Structure of an IO-Link wireless system

A typical application problem in FA is the connection of movable machine parts, which is traditionally realized by trailing cable systems, slip rings or sliding contacts. Since these connection technologies lack from high installation and maintenance costs, wear and lower reliability, a suitable wireless system for replacement is an attractive perspective. These specific applications require "cable-like" performance criteria, but usually not roaming capabilities in terms of *intercell* mobility, since they take place in the proximity of the same wireless basestation, thus are working *intracell*.

Therefore *intercell* mobility was not a primary requirement for the development of the "IO-Link wireless" standard, but it later became clear that it is a necessary feature for many applications in factory automation, such as tool changers, conveyor belts or RFID-like warehouse applications. This led to the definition of the *intercell* roaming concept for "IO-Link wireless", which this work will present.

In the following, an overview on basic roaming concepts for wireless communication systems is given and subsequently the new roaming approach for "IO-Link wireless" is presented.

II. WIRELESS ROAMING CONCEPTS

The term "roam" means "to wander around, to go from place to place without a certain direction or purpose."[10] The term "Roaming" is however used differently in different technical wireless contexts, which will be shortly outlined in the following.

A. *Cell phone networks*

In the context of mobile cell phone networks, "Roaming" ensures that a traveling wireless device (i.e. a mobile cell phone) is always kept connected to a provider network. Thus when a mobile phone is used outside of the range of its home network it is able to automatically connect to another available cell network to which it is compatible. The exchange procedure that takes place between the networks is called "Handover" or "Handoff", which is usually initiated autonomously by the system when the signal strength (RSSI) of the new cell is stronger than that of the previous one.

Above this technical level, "Roaming" is generally referring in in wireless telecommunications to the ability for a cellular customer to automatically access voice calls, data and other services when travelling outside the geographical coverage area of the home network by using a visited network of another phone company, using the own subscriber identity in the visited network. This is technically supported by mobility management, authentication, authorization and accounting billing procedures.

B. *Wireless local area networks*

In WLANs, "roaming" and "handover" are often used synonymously to describe the handover procedure of a wireless mobile device between two wireless access points in the same LAN. The movement of a roaming mobile device is considered unpredictable, i.e. in office environments where people walk around with laptops. The goal is the same as in mobile cell phone networks, keeping the communication uninterrupted as best as possible. Handover initiation is usually also performed based on RSSI. The mobile devices are usually equipped with just a single radio that has to release communication with the old cell before communication with the new cell can be established ("break before make"). When the handover on the wireless level has been completed, the traffic to and from the mobile device must be reorganized in the backbone network, which usually creates an interrupt in communication that adds up to the wireless handover procedure and can become critical for real-time applications.

Approaches for a true seamless handover utilize two radios in the mobile device which allow simultaneous communication with the old and new cell during the handover procedure, yielding an uninterrupted communication during handover when the backbone network also supports a seamless re-routing of the communication traffic destined for the wireless devices. Unfortunately there are no standardized solutions defined yet.

C. *Wireless Process Automation (PA) networks*

In PA, where wireless standards are often based on IEEE 802.15.4, the capability of self-organizing mesh networks by relaying the data packets allows mobility that is entirely different from the previously described cell-based roaming approaches. Traffic is "routed" or "relayed" from one wireless hop to the next until the final destination is reached. Thus a chain of wireless stations must be present between sender and receiver when they cannot "see" each other directly. In case a wireless hop in that chain fails, the packet can be routed through an alternative wireless path. It can even be stored in a hop until a next hop or respective the destination is available again. This yields a reliable, but slow and nondeterministic data delivery, which is suitable for most of the applications in process automation that are representatives of the class of soft real-time, such as monitoring, open-loop control applications (with human intervention) or slow closed-loop applications.

D. *Wireless Factory Automation (FA) networks*

In factory automation, fast closed-loop control applications belong to the class of hard real-time, where given temporal deadlines have to be strictly met [1].

No established wireless standard that can currently fulfill both these hard real-time requirements and *intercell* roaming. It must be noted that true seamless *intercell* roaming is technically only achievable with mobile devices that are equipped with at least two radios to communicate with two cells at the same time during the handover procedure. Additionally the backbone network must support mechanisms for redundant traffic routing to several cell base stations and seamless switchover of the traffic between the cells involved in the handover procedure. Since multiple radios in mobile industrial devices are usually economically and technically not feasible (i.e. for small sensor sizes), the idea of true seamless handover was skipped for the “IO-link wireless” roaming concept.

III. Roaming in the Context of Control Systems

Control systems in factory automation consist mostly of a single PLC with a precisely defined topology of I/O-devices, being conceptually a master-slave system. The communication relationships between PLC and I/O-points resemble a star topology, sometimes a tree topology when data preprocessing takes place in the hierarchical layers below the PLC. The process data exchange between PLC and I/O-points is organized in a cyclic isochronous fashion to achieve a deterministic and synchronized timing behavior, avoiding jitter. New approaches are emerging that are event based and support the interaction of multiple PLCs with synchronization based on timestamps and precise clock synchronization mechanisms like IEEE 1588. However, in all cases, unpredictable control behavior is by definition not allowed in all of these systems. If it happens anyway, it must be dealt with by a kind of “exception handling” that usually leads to a failsafe state, thus halting the system.

From this perspective, FA control systems are in most cases programmed to handle a clearly defined process flow. That process can incorporate implicit alternatives, but these must be known beforehand. This assumption is the basis for the new roaming concept in “IO-Link wireless".

IV. Roaming with IO-Link wireless

Similar to the concept of "piconets" in Bluetooth [11], an “IO-Link wireless” network consists of one master and a number of devices directly connected to it, forming a "star-topology" (Figure 2). To enable roaming between "piconets", one approach discussed in [12] is based on packet relaying, inserting an extra layer in the protocol stack to handle logical connections on top of the physical connections. However, when the data communication is not thought of as a constant communication channel between two entities, these rather complex relaying techniques for data forwarding are not needed in the protocol stack.

Based on this, when the device loses the connection to its current master, the new master can take over the device without having to relay all the received data from or to the initial master. This alternative approach significantly reduces complexity for the roaming technique and is thus applied for IO-Link wireless.

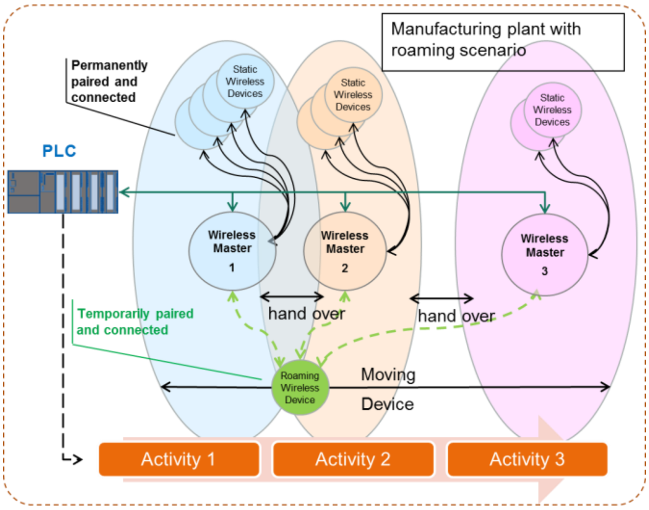

Fig. 3. Scenario with fixed and roaming devices

The wireless masters are specified as fixed network nodes (access points), which also embody the LAN and fieldbus protocol stacks to be able to communicate via the local network with the control application (PLC). Figure 3 indicates that every master has a wireless coverage area that can, but must not overlap with neighboring masters. Spatial overlapping is not a problem for “IO-Link wireless”, because a coordinated frequency hopping is utilized. Non-roaming static devices are permanently paired to just one dedicated master and can only move *intercell*. For *intracell* roaming, the pairing information of moving devices must be initially configured to all the masters that are in the predefined roaming path, but the device is temporarily connected to only one master when it is in the respective coverage area. During the connected phase, the roaming device has full process data communication availability like one of the static devices. During handover, process data communication is not feasible. But this is not critical for the application when the "handover connect" and "handover disconnect" procedure is synchronized with the PLC program, which controls the activity flow anyway.

Similar to Bluetooth, “IO-Link wireless” incorporates mechanisms for "Discovery" and "Pairing", to detect and authenticate devices before connection establishment between a master and wireless devices.

The "Discovery" procedure enables a master to discover which unpaired devices are in its range and what their unique addresses (UniqueID's) are. Masters regularly issue "Scan Request" messages. An unpaired device that receives such a "Scan Request", answers with a "Scan Response" message that contains the UniqueID of the device.

The "Pairing" procedure establishes an actual connection between master and device if the UniqueID received in the “Discovery” procedure is listed in the master's pre-engineered configuration of allowed devices. The master then issues a "Pairing Request" message that gets responded by a "Pairing Response" message from the device (Figure 4). When this procedure is successfully completed, the master notifies its application (PLC) that the device is present and ready to be operated by the application.

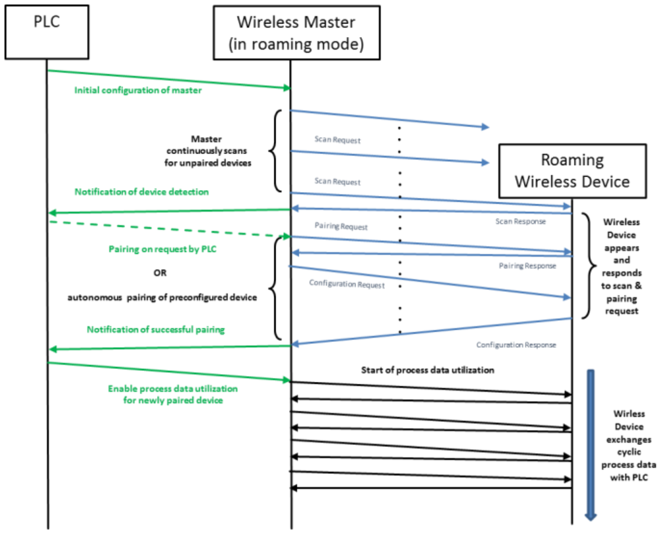

Fig. 4. “Handover connect” of a roaming device

These standard discovery and pairing mechanisms can also be used for roaming in the context of control system applications. This is simply achieved within the system by notifying the PLC about the connection states of the roaming devices and designing the PLC program accordingly. When a roaming device appears in the coverage area of a master, the PLC gets notified and can decide to exchange process data with the device. When the processing activity with the device is finished or the device is moving out of the range of its current master and the link quality drops below a certain threshold value, an “Unpairing” procedure will be initiated and the control program can execute the next process step or wait in its current execution state for the next allowed roaming device to appear.

The relevant performance indicator for this roaming feature is the duration of the "handover connect" phase, thus the time between the roaming device becoming visible for the new master and actual start of process data communication. For “IO-Link wireless”, this can be guaranteed in worst case to be below one second. This assumption is based on the applied frequency hopping algorithm with a maximum of 78 data communication frequencies and 2 disjoint configuration frequencies to control the handover procedure. Since the dwelling time on each frequency hop is given with 1,6ms, one complete hopping cycle with maximum channel usage is always below 128ms. Even in worst case scenarios with a maximum allowed 3 retries, 500ms will not be exceeded on the wireless protocol level. Additional 500ms are assumed as processing time to and from the PLC. Measurements on actual test setups with interference scenarios will be provided in a later work.

V. Conclusion

In this work, some wireless roaming concepts were shortly presented:

1) Cellular radio systems with handover decisions based on RSSI measurements.

2) Meshed wireless networks that route traffic from hop to hop until the destination is reached.

3) “IO-Link wireless”, which is basically a cellular radio system within a local area control network, is coordinating control flow information in the PLC program with handover decisions. For this, the existing discovery and pairing mechanisms are used, whose activities are communicated to the PLC. This approach eliminates the need for complex technical solutions to achieve seamless handovers, but allows important application scenarios in the factory automation domain with very low engineering effort. This provides a key success factor for the acceptance of the emerging new standard “IO-Link wireless”.

References

[1] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, H. Klessig, „Requirements and current solutions of wireless communication in industrial automation”, IEEE International Conference on Communications Workshops, Australia, pp. 67-72, June 2014.

[2] Engineering and Operation of Wireless Sensor Networks, NAMUR Std. NA 137, July 2011.

[3] T. Sauter, S. Soucek, W. Kastner, and D. Dietrich, “The Evolution of Factory and Building Automation” IEEE Industrial Electronics Magazine, vol. 5, no. 3, pp. 35–48, 2011.

[4] G. Scheible, D. Dzung, J. Endresen, and J.-E. Frey, “Unplugged but connected – Design and Implementation of a Truly Wireless Real-Time Sensor/Actuator Interface,“ IEEE Industrial Electronics Magazine, vol. 1, issue 2, 2007, pp. 25-34.

[5] H.-J. Körber, H. Wattar, G. Scholl, “ Modular Wireless Real-Time Sensor/Actuator Network for Factory Automation Applications,” IEEE Transactions on Industrial Informatics, vol. 3, no. 2, May 2007.

[6] R. Heynicke, D. Krüger, H. Wattar, and G. Scholl, “Modular Wireless Fieldbus Gateway for Fast and Reliable Sensor/Actuator Communication,” IEEE International Conference on Emerging Technologies and Factory Automation, pp. 1173 – 1176, 2008.

[7] J. Kjellsson, A. E. Vallestad, R. Steigmann, and D. Dzung, “Integration of a Wireless I/O Interface for PROFIBUS and PROFINET for Factory Automation", IEEE Transactions on Industrial Informatics, vol. 56, no. 10, pp. 4279 - 4287, Oct. 2009

[8] IEC 61131-9: Programmable controllers – Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI)

[9] R. Heynicke, D. Krush, G. Scholl, B. Kärcher, J. Ritter, P. Gaggero, M. Rentschler, "IO-Link Wireless Enhanced Sensors and Actuators for Industry 4.0 Networks", Proceedings of 18th International AMA Conference on Sensors and Measurement Technology, Nuremberg, May 2017

[10] Webster's Dictionary, http://www.websters1913.com/words/Roam

[11] Specification of the Bluetooth System, Covered Core Package, Version: 4.0. The Bluetooth Special Interest Group; Kirkland, WA, USA: 2010.

[12] Pals, H., Dai, Z.R., Grabowski, J.H.N.: UML-based modeling of roaming with Bluetooth devices. In: Proceedings of the First Hangzhou-Lübeck Workshop on Software Engineering (HL-SE’03), Vol. 506. University of Hangzhou, China, Nov. 2003.