Wireless Sensor Networks - from Recent Developments to Industrial Standards

Kupris, Gerald
Freescale Halbleiter GmbH
Schatzbogen 7, 81829 München, Germany

1 The IEEE 802.15.4 Standard

Already for quite some time efforts in the industry are ongoing to attain standardization for wireless communication in radio nets of small range (WPANs - wireless personal area networks). Target markets here are for example house automation, sensor networks or industrial data communication.
IEEE 802.15.4® is a standard for short range wireless communication and has been ratified by the “Institute of the Electrical and Electronics Engineers” of the USA in May 2003. In this standard the physical characteristics of a radio interface (frequency bands, data rates, modulation procedures, frequency spreading) are defined.
The next higher level sitting on top of the PHY is the MAC (Media Access Control) layer. It defines how the radio interface is to be accessed. The two layers MAC and PHY are defined by the IEEE 802.15.4 standard and are described in a work of more than 600 pages, which can be downloaded from the internet [1].
Based on the IEEE 802.15.4 standard several technologies for Wireless Sensor Networks have been defined. Examples for these technologies are ZigBee, ZigBeePro and 6LoWPAN. In the industrial space, technologies like WirelessHART and ISA100.11a are winning recognition.

2 ZigBee and ZigBee PRO

Based on the IEEE 802.15.4 standard a group of manufacturers and users has been formed, which under the name of “ZigBee” [2] would like to achieve a wide compatibility based on standardized application profiles. Devices of different manufacturers should understand each other and should be able to work together in a network.
In the IEEE 802.15.4 standard already the first beginnings of the description of a network layer (NWK) can be found, however the only architectures defined here are star and cluster tree. All other network architectures require a special network layer, which goes beyond the definitions of the IEEE standard. This network layer and the other layers up to the standardized application profiles are specified by the ZigBee Alliance. The user will have the possibility to take the fixed characteristics of the application profiles, in order to integrate these profiles into his application.
ZigBee Application profiles are a collection of messages, message formats, processing actions and related services designed to be interoperable. In the case of public application profiles, the ZigBee Alliance specifies these services to allow for interoperability between OEM vendors’ products. Every ZigBee node contains one or more application profiles. As a customer, the only decision to make is whether to use a public ZigBee Alliance profile or to create a private profile. Private profiles have the advantage of being simple to implement and flexible for the project. Public profiles have the advantage of being interoperable among vendors, but at the expense of extra code size and complexity.
The application profile defines as well, which ZigBee stack profile is used by the application. A stack profile is a collection of parameter values and configuration settings that determine the specific performance of a ZigBee stack variant and govern interoperability between stacks provided by different vendors. Within ZigBee 2006, there is one stack profile defined, the “ZigBee Stack Profile”. The profile ID of the “ZigBee Stack Profile” is 0x01. It supports both Home and Commercial applications. Another available stack profile is the “ZigBee PRO Stack Profile” which has been defined by the ZigBee Alliance in 2007.

*) Note: IEEE® is the trademark of the Institute of Electrical and Electronic Engineers, Inc. [1].
ZigBee™ is the trademark of the ZigBee Alliance [2].
WirelessHART™ is a registered trademark of the HART Communication Foundation [5].
Synkro™ is a trademark of Freescale Semiconductor [3].

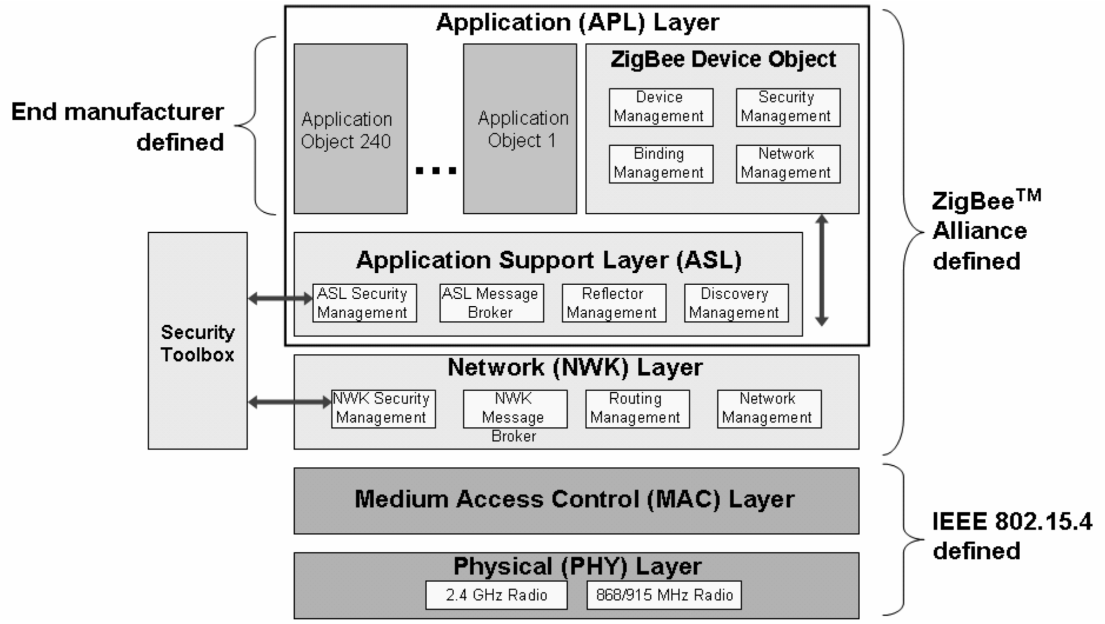

Figure 1: Protocol stack for IEEE 802.15.4 / ZigBee [2]

The application profile defines as well, which ZigBee stack profile is used by the application. A stack profile is a collection of parameter values and configuration settings that determine the specific performance of a ZigBee stack variant and govern interoperability between stacks provided by different vendors. Within ZigBee 2006, there is one stack profile defined, the “ZigBee Stack Profile”. The profile ID of the “ZigBee Stack Profile” is 0x01. It supports both Home and Commercial applications. Another available stack profile is the “ZigBee PRO Stack Profile” which has been defined by the ZigBee Alliance in 2007.
Existing ZigBee Application Profiles are for example: the Smart Energy (SE) profile, the Home Automation (HA) profile, the Commercial Building Automation (CBA) profile, the Wireless Sensor Application (WSA) profile.
An important part of the ZigBee concept is frequency agility: during the formation of the WPAN the coordinator decides on which of the 16 available 804.15.4 channels the network should be build. In the ZigBee 2006, this channels stays fixed for the time of the existence of the network; whereas the ZigBee 2007 specification allows changing the channel if interference occurs.

3 WirelessHART

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Field bus, a digital industrial automation protocol. The protocol was developed by Rosemount Inc. for their smart field instruments. Soon it evolved into HART. In 1986, it was made an open protocol. Since then, the capabilities of the protocol have been enhanced by successive revisions to the specification. The September 2007 publication of the WirelessHART standard as part of the HART 7.0 specification marks an important milestone in the rapid acceptance of wireless technology for process operations.
WirelessHART is a wireless mesh network communications protocol for process automation applications. It adds wireless capabilities to the HART Protocol while maintaining compatibility with existing HART devices, commands, and tools.
Each WirelessHART network includes three main elements (Figure 3 [5]):

- Wireless field devices connected to process or plant equipment.
- Gateways that enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
- A Network Manager responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.

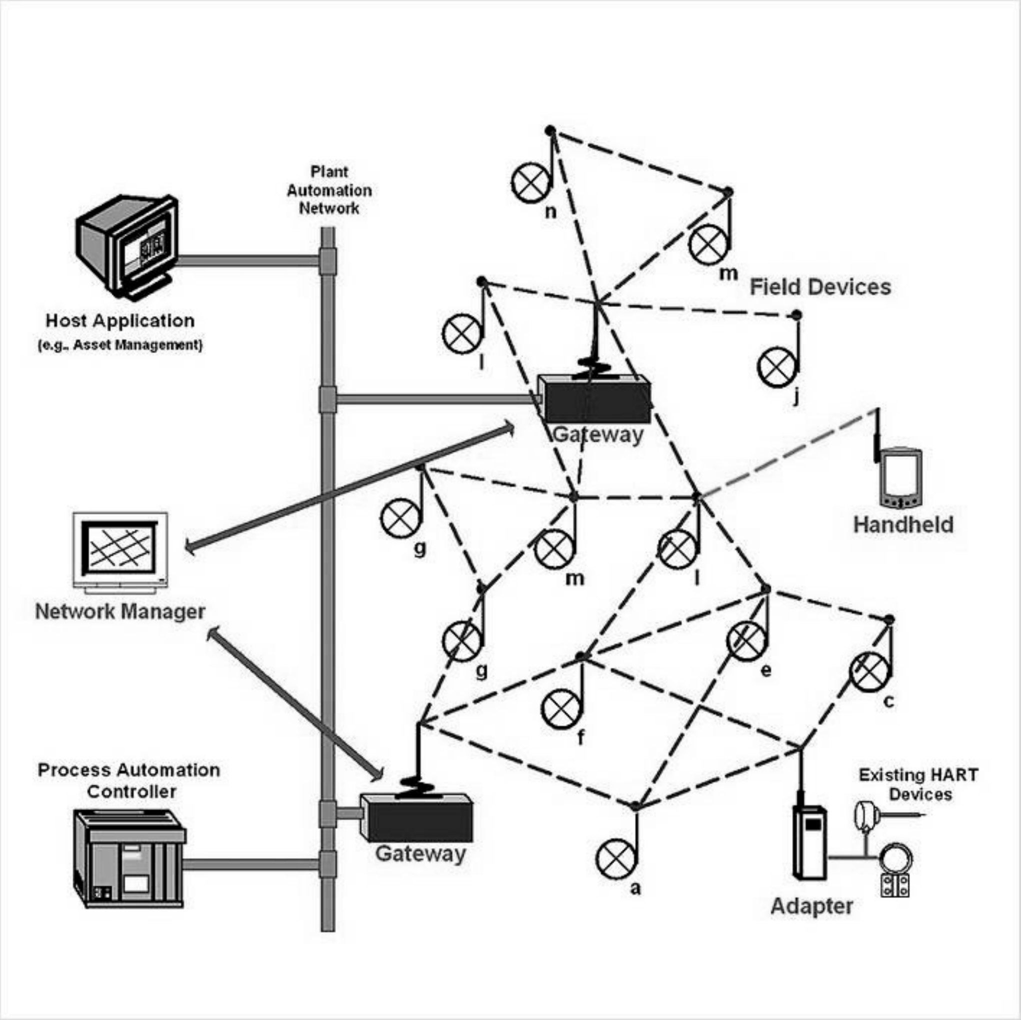

Figure 3: Elements of a WirelessHART implementation [4]

The wireless network uses IEEE 802.15.4 compatible radios operating in the 2.4 GHz Industrial, Scientific, and Medical radio band. The radios employ direct-sequence spread spectrum technology and channel hopping for communication security and reliability, as well as TDMA synchronized, latency-controlled communications between devices on the network. This technology has been proven in field trials and real plant installations across a broad range of process control industries.

Each device in the mesh network can serve as a router for messages from other devices. In other words, a device doesn't have to communicate directly to a gateway, but just forward its message to the next closest device. This extends the range of the network and provides redundant communication routes to increase reliability. The Network Manager determines the redundant routes based on latency, efficiency and reliability. To ensure the redundant routes remain open and unobstructed, messages continuously alternate between the redundant paths. Consequently, like the Internet, if a message is unable to reach its destination by one path, it is automatically re-routed to follow a known-good, redundant path with no loss of data. The mesh design also makes adding or moving devices easy. As long as a device is within range of others in the network, it can communicate.

4 ISA100.11a

Founded in 1945, ISA (The Instrumentation, Systems, and Automation Society) is a leading, global, nonprofit organization that is setting standards for automation. The ISA100 Committee addresses wireless manufacturing and control systems.

ISA100.11a is the first of a family of standards to be defined by the ISA100 wireless working group. ISA100.11a is intended to provide reliable and secure operation for non-critical monitoring, alerting,

supervisory control, open loop control, and closed loop control applications. ISA100.11a defines the OSI stack, system management, gateway, and security specifications for low data rate wireless connectivity with fixed, portable, and moving devices supporting very limited power consumption requirements. ISA100.11a's application focus addresses performance needs for monitoring and process control where latencies on the order of 100 ms can be tolerated, with optional behavior for shorter latency.
The ISA100.11a specification is based on the IEEE 802.15.4 standard in 2.4 GHz. The Data Link Layer, the Network Layer, the Transport Layer and the Application Sub-layer are build on top of the IEEE 802.15.4 PHY and MAC (Figure 4).

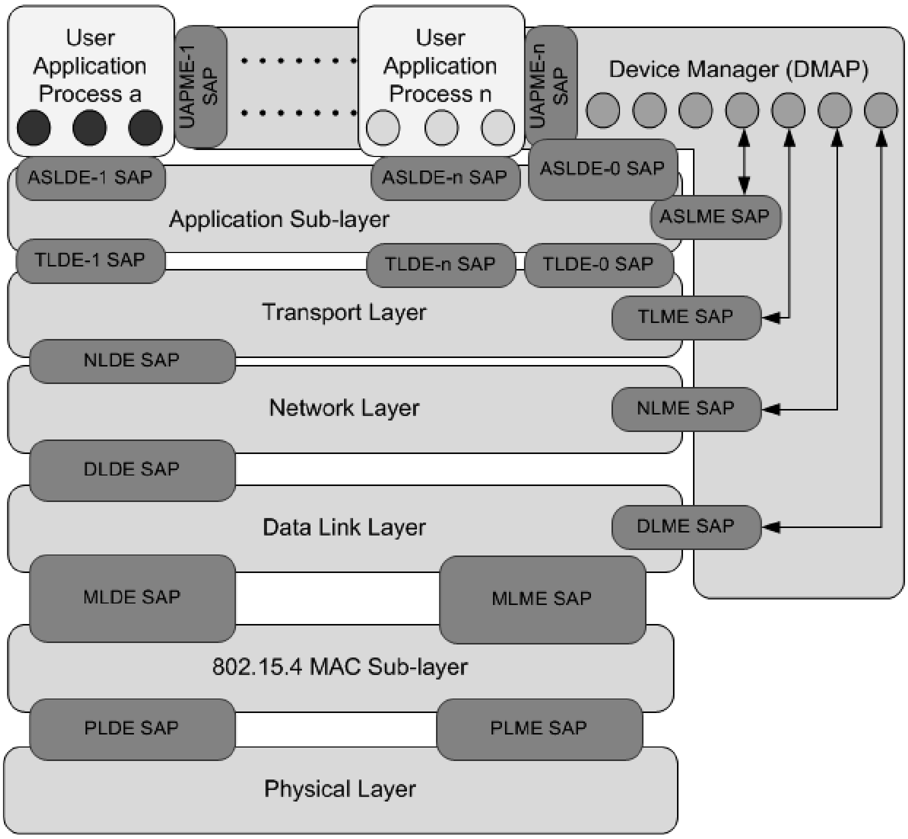

Figure 4: ISA100.11a reference model [6]

A typical ISA100.11a network includes all components required to route secure traffic, manage network resources and integrate with host systems. An ISA100.11a network consists of one or more ISA100.11a field networks that may be connected by a transit network to a plant network (figure 5).
An ISA100.11a field network consists of a collection of physical devices that communicate via IEEE 802.15.4-compatible wireless links using the ISA100.11a stack. Some field devices may have routing capabilities, enabling them to forward messages from other devices. But as opposed to WirelessHART, also non-routing devices are possible.
An ISA100.11a transit network consists of zero or more backbone routers or gateways, in addition to management devices such as system and security managers. The physical communication medium and network stack is unspecified and may include tunneling ISA100.11a packets over conventional transport or application layers.
An important concept of ISA100.11a is channel hopping. ISA100.11a utilizes radios compliant to IEEE 802.15.4-2006 operating in the 2.4GHz band, with channel hopping across 16 direct sequence spread spectrum (DSSS) channels. It uses intelligent channel hopping algorithms that provide interference rejection from other RF devices, as well as multipath rejection. In addition, ISA100.11a improves coexistence with other RF systems by not constantly utilizing the same spectrum. Intelligent channel hopping increases reliability by preventing the utilization of frequencies with consistently poor performance.

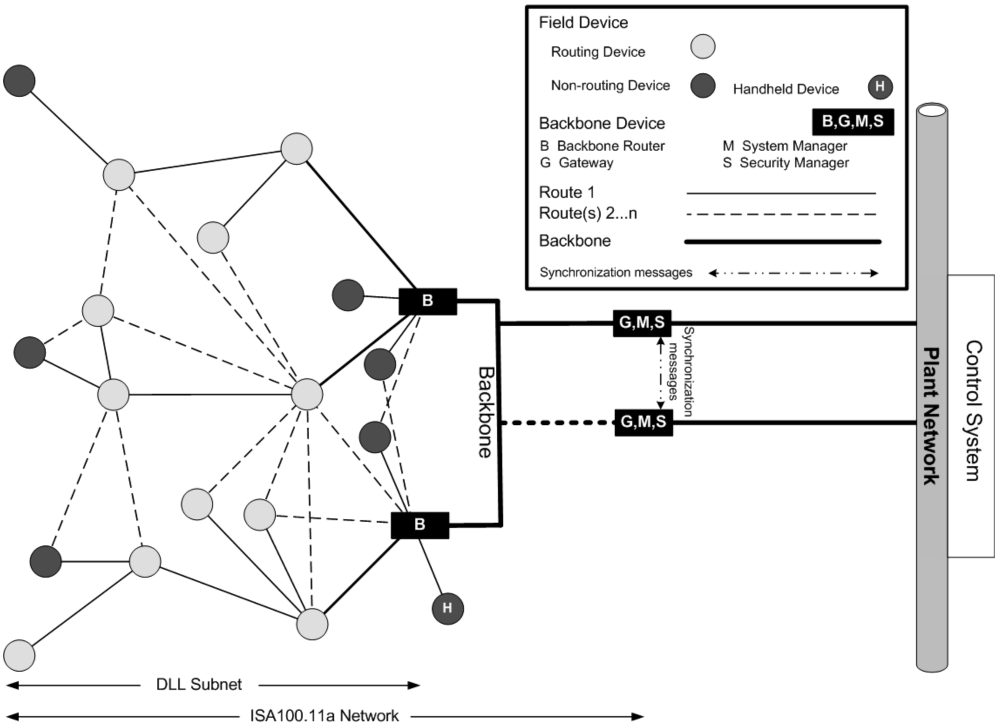

Figure 5: Typical ISA100.11a field network [6]

Time synchronized communication using configurable fixed timeslot duration, typically in the range of 10 ms – 15 ms, provides accurate time stamping and reliable low-power operation. ISA100.11a timeslot durations are configurable on a per-superframe (cyclic collection of timeslots) basis. The ability to configure timeslot duration supports ISA100.11a device interchangeability. In addition, configurable timeslots enable: longer timeslots to accommodate extended packet wait times, shorter timeslots to take full advantage of optimized implementations, longer timeslots to accommodate serial acknowledgement from multiple devices, longer timeslots to accommodate CSMA at the start of a timeslot (e.g. for prioritized access to shared timeslots), longer timeslots to accommodate slow hopping periods of extended length.
ISA100.11a supports both dedicated time slots for predictable, regular traffic and shared time slots for alarms and bursty traffic.

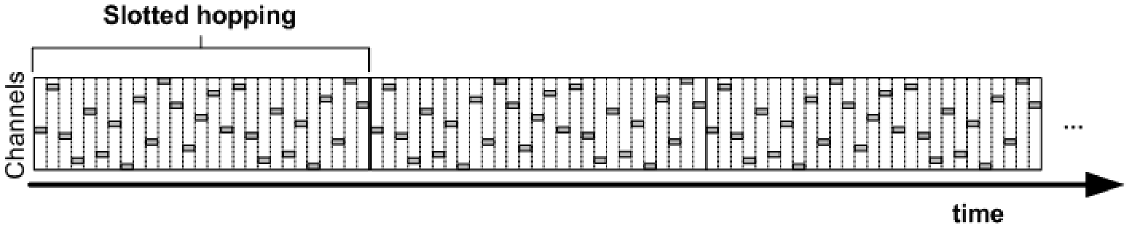

Figure 6a: ISA100.11a Slotted channel hopping [6]

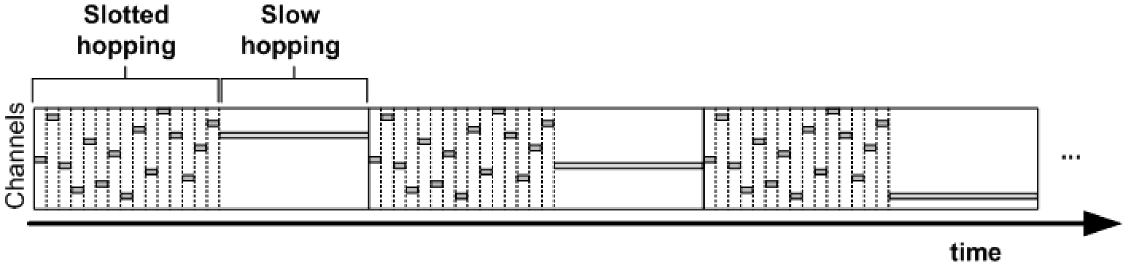

Figure 6b: ISA100.11a Hybrid operation [6]

5 The WiTECK Consortium

To provide a reliable, cost-effective, high-quality, portfolio of core enabling system software for industrial wireless sensing applications several leading enterprises in the industrial instrumentation, wireless components, and software development industries have formed the Wireless Industrial Technology Konsortium (WiTECK) [7].

WiTECK is in business to develop, promote and distribute on a non-profit basis one or more software communication stacks and supporting products and to encourage the use of these stacks on a standardized basis within the process control and factory automation markets worldwide.

WiTECK provides a corporate framework where companies can share the development risk and financial expense of writing complicated industry-standard based software stacks. The Intellectual Property policies are pre-defined and acknowledged as a condition of membership.

The first WiTECK development project is a stack based on the WirelessHART portion of the HART 7 specification. WiTECK chose this project for a number of reasons. First, WirelessHART is currently the only published and standardized specification for operating industrial wireless sensor networks for the process industry. Second, all WiTECK founding members are HART Communication Foundation members and supporters. WiTECK members are developing products or technologies around the specification. Currently there is only one source of software for the standard. WiTECK founders believe that a second source is required for the long term success of WirelessHART. Given the level of investment required to build a market around WirelessHART, the founders felt it economically prudent to develop a second source in a consortium.

Within the context of developing core software for approved standards, there are many extensions to the initial WirelessHART effort that could be undertaken, as well as development efforts for other new standards. All new projects will be selected by the membership and approved by the board of directors.

6 Hardware Requirements

To build an industrial wireless system suitable for WirelessHART and/or ISA100.11a, one can use a standard IEEE 802.15.4 chip set which is available from Freescale Semiconductor and other vendors. However, considerations have to be taken regarding two specialties of these standards:

- IEEE 802.15.4 recommends an RF output power of 0 dBm. However, WirelessHART defines an output power of +10 dBm. This means that one has to add an additional power amplifier to the standard IEEE 802.15.4 transceiver to meet the requirements in RF output power.
- Both WirelessHART and ISA100.11a use a time-slotted technology. So usually one has to add a temperature compensated clock source to the system in order to meet the time slots with high precision.

Therefore, the typical WirelessHART / ISA100.11a node is slightly more complex than a standard IEEE 802.15.4 / ZigBee node.

7 Conclusion

Based on the IEEE 802.15.4 several wireless technologies have been established. Each of these technologies addresses the unique requirements of a specific market. Therefore, it is believed that these different technologies will exist in parallel to each other. Freescale Semiconductor is providing hardware for IEEE 802.15.4 wireless communication and works on software and system solutions to support all of the introduced technologies.

8 References

[1] http://www.ieee802.org/15/pub/TG4.html
[2] http://www.zigbee.org
[3] http://www.freescale.com
[4] http://www.hartcomm2.org/index.html
[5] http://www.isa.org
[6] ISA100.11a Principles of operation
[7] http://www.witeck.org