Wireless Industrial Control Networks

by

Victoria Pimentel and Bradford G. Nickerson

TR13-223 , February, 2013

Faculty of Computer Science
University of New Brunswick
Fredericton, N.B. E3B 5A3
Canada

Phone: (506) 453-4566
Fax: (506) 453-3566
E-mail: fcs@unb.ca
http://www.cs.unb.ca

Contents

Chapter 1

Industrial Communication Networks

Automation is the use of machines, control systems and technologies for industrial processes. Today, automation is considered a very wide area and is typically used to optimize productivity of process automation industries.

Åkerberg's work [2] state:

> "In the automation domain, many different communication protocols exist on various media such as fiber, copper cables, radio, or even power-line carrier communication."

In this area, communication can be used for interconnecting different devices, control loops and for monitoring and supervising, among others.

Figure 1.1 shows an example of an automation network divided into other different networks. Each network runs an specialized protocol that satisfies the requirements of that particular network. At the Server Network shown in Figure 1.1, one of the most popular protocols is Object Linking and Embedding for Process Control [2] that runs over TCP/IP. At the Control Network a very common protocol is the Manufacturing Message Specification [2] running over TCP/IP, as well. At the Field Network exists many protocol specifications and a very common approach is the idea of the fieldbus.

Åkerberg [2] states:

> "...the visions of autonomous systems, that can be followed, diagnosed and maintained from remote are not far from reality, but stress the need for security and safety solutions."

This can be illustrated as shown in Figure 1.1 where both wired and wireless networks are used in different levels of an automation network. However, the communication that is carried out through these networks is typically very critical, arising security and safety concerns. Initially, the automation networks where developed to be isolated, but requirements are now changing, networks are now integrated with other networks and are no longer closed. The challenge is to keep up with these new technologies and requirements without disregarding important properties of industrial communication listed on [2].

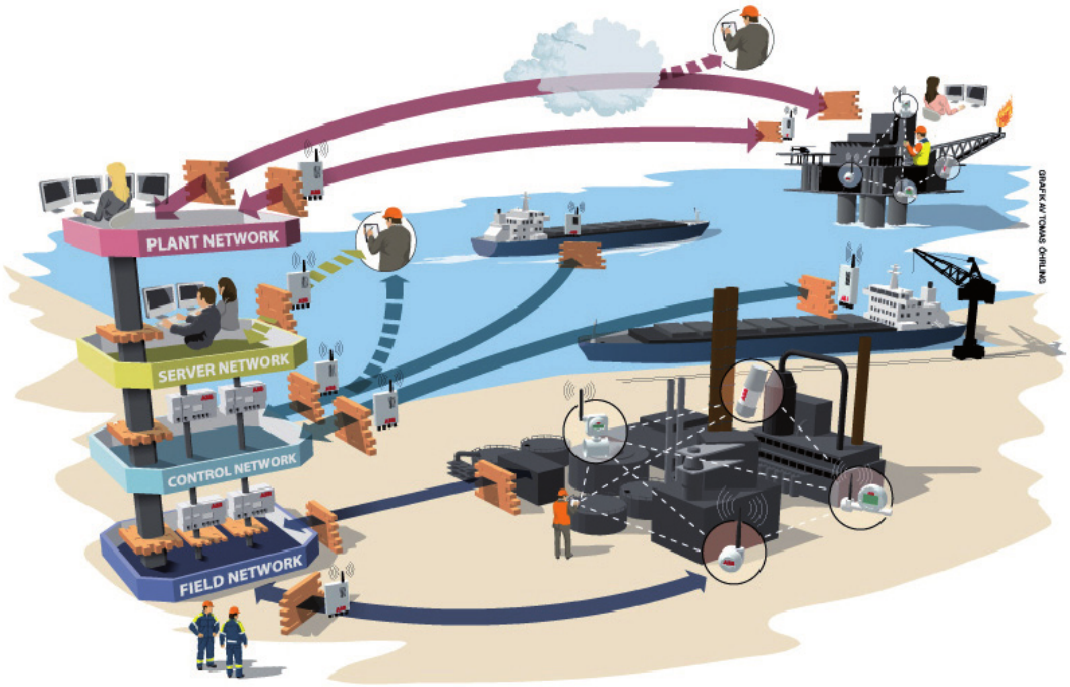


Figure 1.1: Automation networks are divided into different networks (from [2]).

1.1 Fieldbus Systems

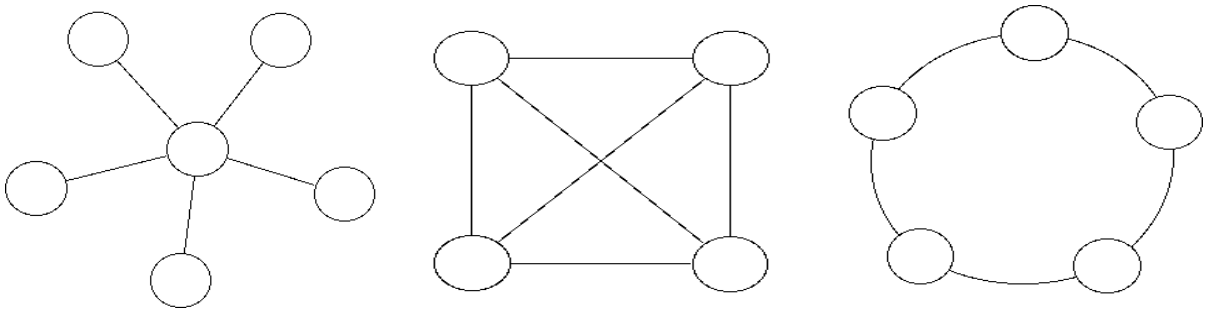
The fieldbus was first developed 20 years ago. However, "there exists no clear-cut definition for the term" [34]. Some of the definitions are based on the fieldbus applications and are considered to be restrictive because of the complexity that the fieldbus has gained today; more nodes are getting incorporated into the fieldbus network.

Originally, fieldbuses were conceived as an isolated network. Thus, security was not a big issue [34]. However, as illustrated in Figure 1.1, fieldbus devices are now been integrated into other networks in which security becomes an essential topic. This implies that security concepts must be implemented into the fieldbus systems, increasing computational effort.

"The most promising research field for technological evolution is the wireless domain. The benefits are obvious: no failure-prone and costly cabling and high flexibility, even mobility." [34] However, there arise several concerns as well, specially security related.

1.1.1 Definition of Fieldbus

The Fieldbus Foundation provides an elaborate explanation when defining the fieldbus. For the purposes of this report, the definition presented will be shortened to the following: "A Fieldbus is a digital, two-way, multi-drop communication link..." [13]. Then, the fieldbus is a **communication link** that enables **two-way** communication between **several devices** in a shared medium. Another way to restrictively define the fieldbus is as a network in which



(a) Star (b) Point-to-point (c) Ring

Figure 1.2: Network topologies.

devices are connected (hung) directly into a shared medium [26].

The fieldbus network was developed to avoid wiring problems that arise when working with some networks topologies, e.g. point-to-point and star-like.

The star-like network topology is shown in Figure 1.2 (a). All the nodes are to be connected to a central master device. Figure 1.2 (b) shows a point-to-point network topology. All devices can communicate directly to each other, which means each device is wired to the rest. These two topologies can become problematic when dealing with large amounts of devices, as required in industrial networks. For the point-to-point topology, there are $\sum_{i=0}^{n-1} n - i$ wired connections needed for n devices. Adding and removing devices from the network also become complicated tasks.

The bus could be seen as the ring topology shown in Figure 1.2 (c). Devices are connected into a shared medium and they can communicate between each other through the bus.

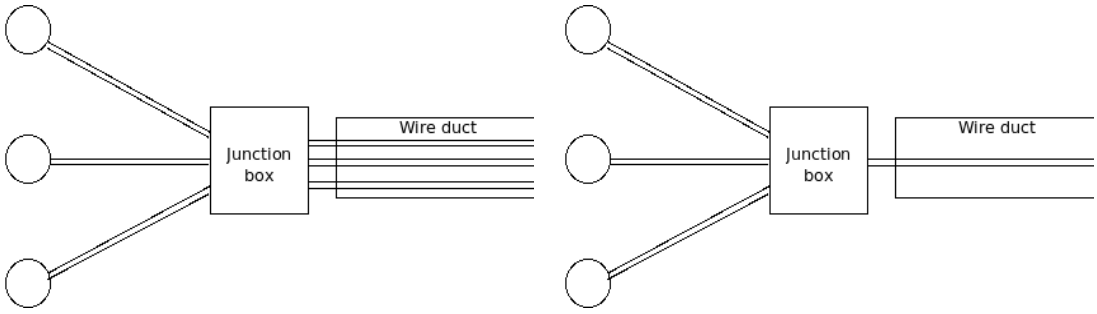
The fieldbus can also be compared to the 4-20 m.A. technology represented in the diagram shown in Figure 1.3 (a). Each device is connected to a junction box using a pair of wires. Then, each pair of wires travels through the wiring duct. For the diagram shown in Figure 1.3, there are a total of 6 wires needed to connect 3 devices.

On the other hand, Figure 1.3 (b) shows the diagram using fieldbus devices. If the fieldbus devices cannot be directly connected to the network, they are connected to a kind of junction box, as shown in Figure 1.3 (b). From the junction box through the wiring duct there is only one pair of wires over which digital data is transmitted from all three devices to a controller.

These three comparisons are used as an introduction of the fieldbus concept to the reader and to present the problems that fieldbus attempts to solve.

The fieldbus was developed to become a standard. This means that any fieldbus compatible device should operate with another, regardless of the manufacturer. This would be an important advantage for large industrial systems in which many kind of devices are needed to interact with others and provides interoperability. However, today there are many fieldbus specification protocols.

Still, "...there is much more to the idea of the fieldbus" [34]; flexibility and modularity, configureability, maintainability and distribution of information.



(a) 4-20 mA. (b) Fieldbus.

Figure 1.3: Diagrams that describe wiring using 4-20 m.A. and fieldbus technologies [26].

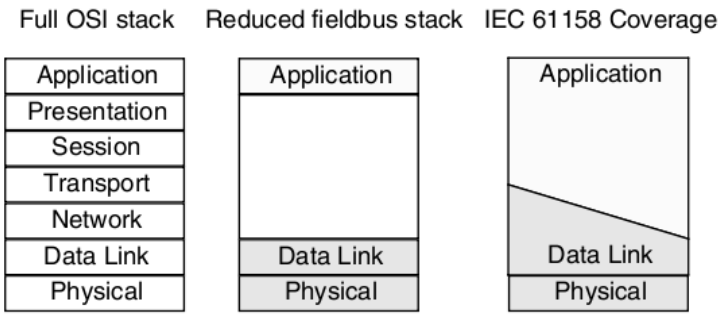


Figure 1.4: Layer structure of a typical fieldbus protocol stack as defined by IEC 61158 (from [34]).

1.1.2 ISO/OSI Communication Stack

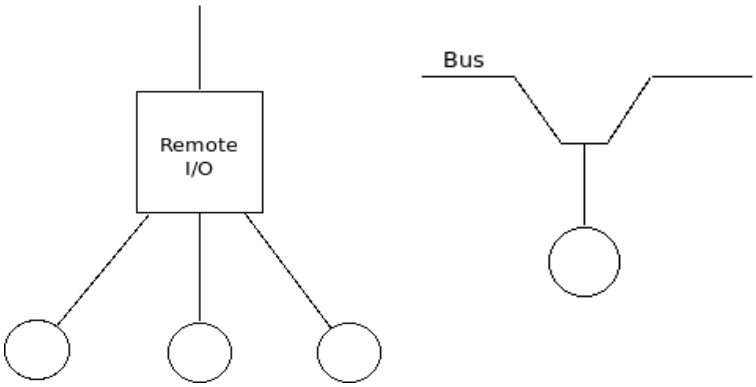
Fieldbus protocols are modeled according to the OSI model. However, there are some differences regarding the protocol stack.

Fieldbuses are typically single-segment networks that are widely used in industrial networks. The network load and the communication processes that the network undergoes are well known and not in constant change. Thus, the network and transport layers from the OSI model implemented in the fieldbus standard are very rudimentary and nearly removed.

The session and presentation layers from the OSI model handle virtual sessions between computers for the application layer. In industrial networks, these features are not necessary. Thus, these two layers are also removed from the fieldbus standard.

If a functionality from any of these layers is needed, e.g. in building automation with a possibly high number of nodes, they are implemented on layers 2 or 7 as defined by the IEC 61158 fieldbus standard as shown in Figure 1.4.

Regarding the physical layer, devices can be connected to a fieldbus following a tree structure as shown in Figure 1.5 (a). This structure is used to connect devices that cannot be connected to the network directly. These devices are connected point-to-point to a remote I/O device that provides access to the network. The remote I/O device acts as the communication link between the fieldbus network and devices that are not capable of transmitting



(a) Tree structure. (b) Bus.

Figure 1.5: Tree and bus structure for fieldbus [26].

network packets. The remote I/O device receives data from the connected devices, assembles the packets with the device information and sends the packets to the fieldbus network.

Intelligent devices that enable direct communication can be connected to the bus network directly as shown in Figure 1.5 (b).

These two structures are connected to a bus segment which is the shared medium between all the devices connected to the bus network. The fieldbus topology can work with more than one bus segment using a repeater device. A repeater is a node on the bus segment that extends to another bus segment, giving way to what is known as a multi-bus segment topology as shown in Figure 1.6. Nodes 1 to 7 connected to the fieldbus segments in Figure 1.6 can be intelligent fieldbus devices or tree structures.

The information transmitted from one device in a network segment will become available to all other devices connected to the same bus segment and to other bus segments through a repeater. The repeater device provides communication between bus segments, which are the layers on the fieldbus topology. Node 4 from Figure 1.6 can communicate with node 7 and the packet will become available to the rest of the nodes as well. This implies that there should be some control over which device uses the media and when, in order to avoid collisions. This function is carried by the fieldbus mastership.

The application layer is divided into the Fieldbus Message Sublayer (FMS) and the Fieldbus Access Sublayer (FAS). The FMS builds messages following the fieldbus standard and the FAS manages addressing on the virtual communication channel. The data link layer carries out the communication protocol set by FAS.

There was proposed to add a user layer on top of the application layer to handle configureability aspects. This last layer is meant to be a tool for programmers and network administrators.

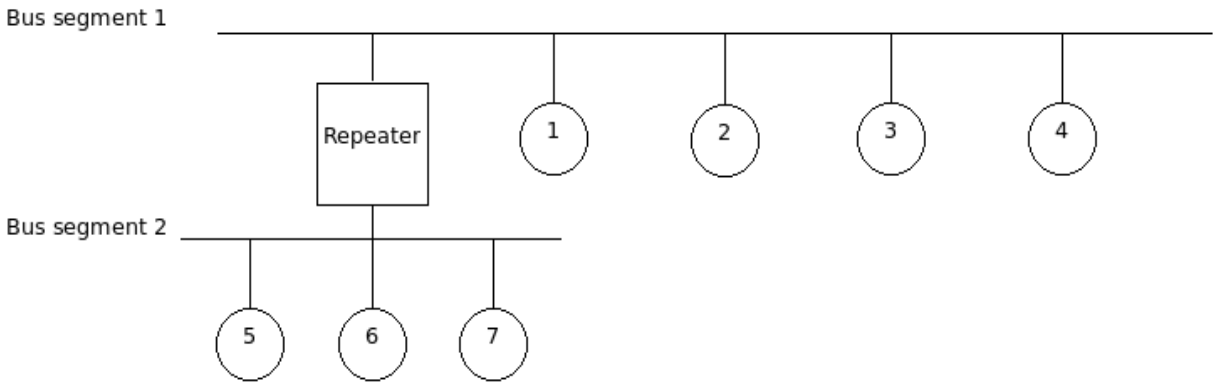


Figure 1.6: Fieldbus topology [26].

1.1.3 Fieldbus on Industrial Control Systems

Figure 1.7 (a) shows a network topology using the fieldbus in an automation system. Figure 1.7 (b) shows the topology for the fieldbus solutions offered by the ABB group [16].

1.1.4 Fieldbus Standardization

The International Electrotechnical Commission (IEC) is an organization that has played an important role on the fieldbus standardization. However, because of the many and different application fields of the fieldbus systems, inside the IEC there are two committees working on standardization activities [34]:

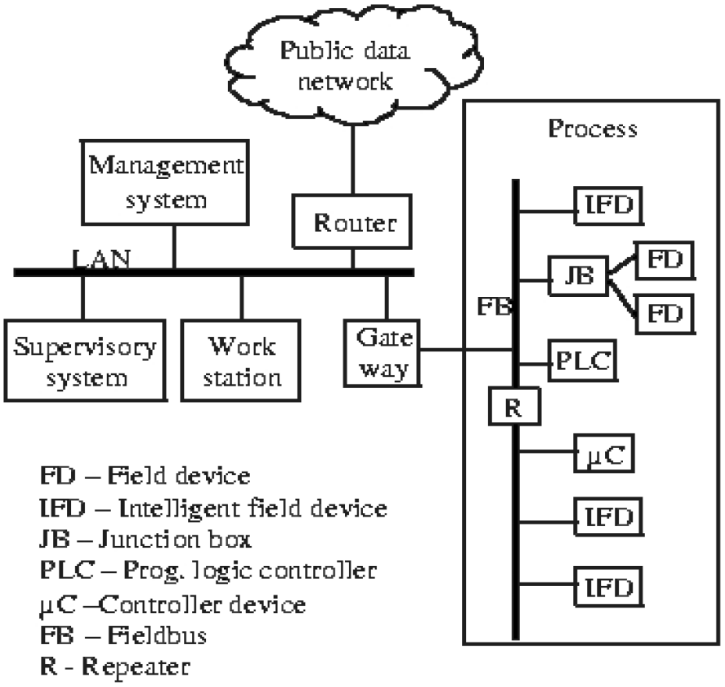
- Industrial-Process Measurement and Control/Digital Communications.
- Switchgear and Controlgear/Low-Voltage Switchgear and Controlgear.

Inside the International Organization for Standardization (ISO) there are another 3 committees working [34];

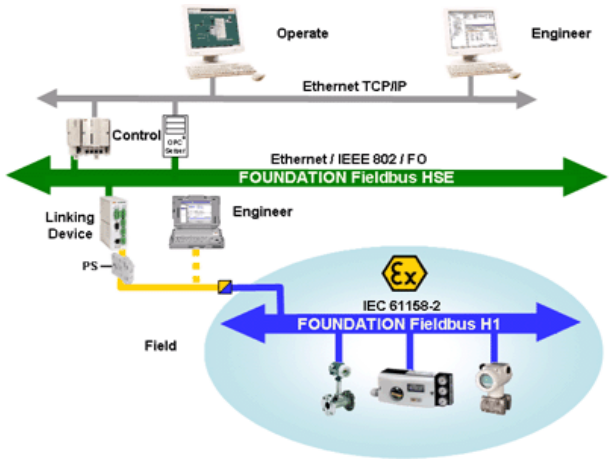
- Road Vehicles/Electrical and Electronic Equipment.
- Industrial Automation Systems and Integration/Architecture, Communications and Integration Frameworks.
- Building Environment Design/Building Control Systems Design.

On the other hand and working in parallel, there are the European Committee for Electrotechnical Standardization (CENELEC) and European Committee for Standardization (CEN). CENELEC also divides the work into committees [34];

- Fieldbus, Low-Voltage Switchgear and Controlgear Including Dimensional Standardization.



(a) Fieldbus architecture found in industrial automation systems (from [18]).



(b) Foundation Fieldbus solutions from ABB (from [16]).

Figure 1.7: Fieldbus applications on industrial control systems.

Table 1.1: Industrial Ethernet profiles defined in IEC 61784.

IEC 61158 Protocol	IEC 61784 Profile	Ethernet-based Brand Name
Foundation Fieldbus	CPF-1	Foundation Fieldbus
ControlNet	CPF-2	EtherNet/IP
PROFIBUS	CPF-3	PROFInet
Interbus	CPF-6	Interbus
-	CPF-10	VNET/IP
-	CPF-11	TCnet
-	CPF-12	EtherCAT
-	CPF-13	EPL (Ethernet Powerlink)
-	CPF-14	EPA
-	CPF-15	Modbus

- Home and Building Electronic Systems.

And within the CEN, there is the Building Automation, Controls and Building Management committee [34].

The IEC 61158 defined 8 main types of protocols that have defined the international fieldbus today. In fact, these protocols are related to CENELEC standards as well [34] and they are:

1. Foundation Fieldbus H1 and HSE (high speed Ethernet).
2. ControlNet.
3. PROFIBUS.
4. P-net.
5. WorldFIP.
6. Interbus.
7. Swiftnet.

Table 1.1 shows that Foundation Fieldbus, ControlNet, PROFIBUS and Interbus were redefined as profiles in the IEC 61784 where Ethernet-based protocols were introduced. Table 1.1 shows many other new Ethernet-based fieldbus systems that become part of IEC 61784 [34].

The four IEC 61158 protocols and the Ethernet-based industrial protocols presented in Table 1.1 are very popular today. The Foundation Fieldbus is considered to dominate the worldwide process control market for interconnecting smart field devices, as Profibus is considered to dominate the manufacturing automation market [25].

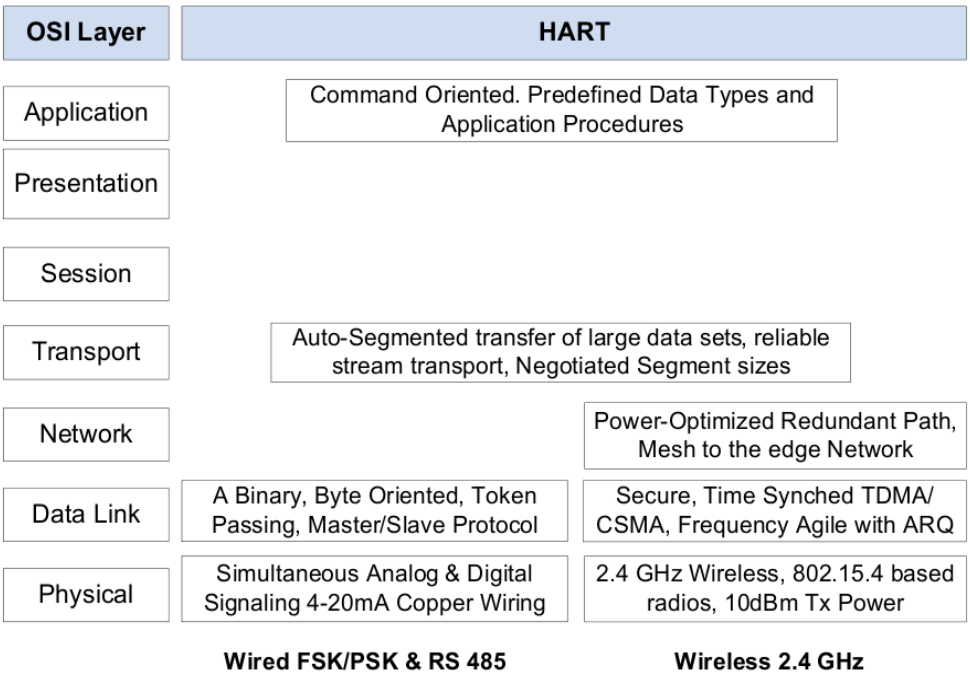


Figure 1.8: HART communication protocol stack (from [36]).

1.2 Wireless Automation Networks

Radmand et al. [33] present a comparison of the current industrial Wireless Sensor Network standards. They introduce, describe and compare Zigbee, WirelessHART and ISA 100.11a. They conclude that WirelessHART and ISA 100.11a address many of Zigbee weaknesses and that the Zigbee application context is commercial and less suitable for industrial applications than WirelessHART and ISA 100.11a. WirelessHART and ISA 100.11a share some common characteristics, such as the use of IEEE 802.15.4 at the physical and MAC layers.

WirelessHART is considered by Åkerberg as an "...international and industrial standard for Wireless Sensor Networks..."[2]. However, an interesting feature of ISA 100.11a, absent in WirelessHART, is that the network layer uses headers compatible with IETF 6LoWPAN standard, which potentially suggests the use of 6LoWPAN as the backbone network [33].

1.2.1 WirelessHART

WirelessHART (Wireless Highway Addressable Remote Transducer Protocol) was developed by the HART Communication Foundation.

WirelessHART physical layer and part of the data link layer are based on IEEE 802.15.4 However, one of the attractive features of WirelessHART is the use of the Time Division Multiple Access (TDMA) at the data link layer, as shown in Figure 1.8. Super frames of time slots are defined to coordinate communication between devices on the network [33].

On a WirelessHART network there are many different devices communicating. Radmand

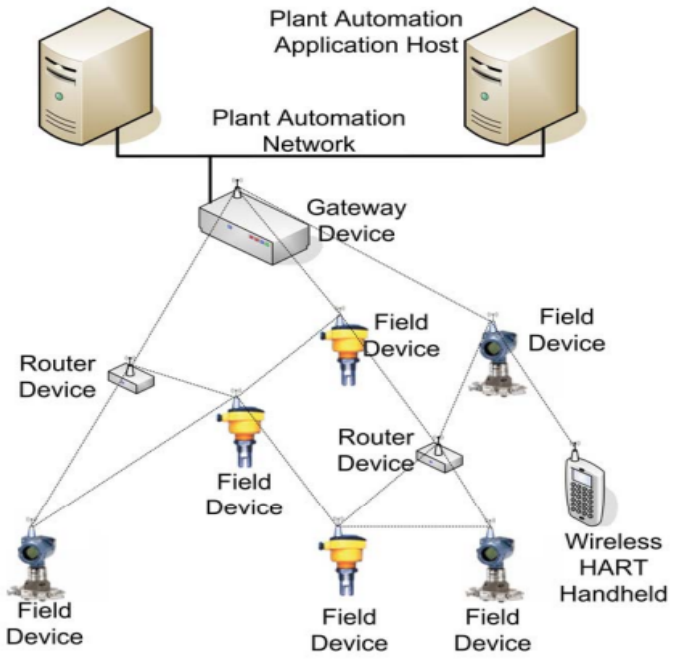


Figure 1.9: Example of a WirelessHART network (from [36]).

et al. explain [36]:

> "... the basic elements of a typical WirelessHART network include: (1) Field Devices that are attached to the plant process, (2) Handheld which is a portable WirelessHART-enabled computer used to configure devices, run diagnostics, and perform calibrations, (3) A gateway that connects host applications with field devices, and (4) A network manager that is responsible for configuring the network, scheduling and managing communication between WirelessHART devices."

"Thus WirelessHART is essentially a centralized wireless network"[36].

All these devices are required to forward packets on behalf of other devices. To achieve this, WirelessHART implements its own network and transport layers. WirelessHART defines two routing protocols: Graph Routing, that uses the structure of a graph to represent the network; and Source Routing, that uses a sequence of device identifiers to indicate the path that the packet must travel for network diagnosis.

At the application layer, WirelessHART defines several commands, responses, data types and status reporting. Communication between the devices and gateway is achieved using these predefined commands and generating the corresponding response.

An example of a WirelessHART network is shown in Figure 1.9.

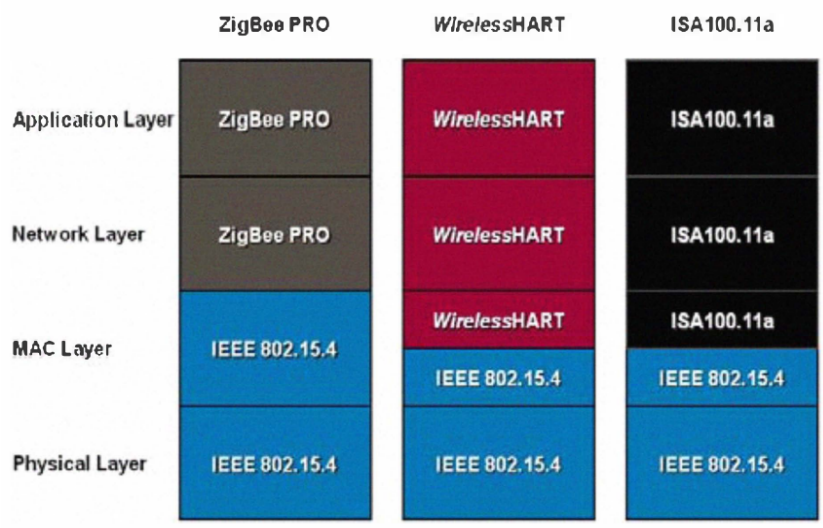


Figure 1.10: Protocol stack for the Zigbee, WirelessHART and ISA 100.11a wireless communication standards (from [33]).

1.2.2 ISA 100.11a

ISA 100.11a is an industrial wireless automation standard developed by the International Society of Automation (ISA). The corresponding IEC emerging standard is based on ISA-100 and is called IEC 62734. ISA 100.11a was developed with a "comprehensive coexistence strategy" [33], which means that the standard was designed to be able to work with other networks using different standards.

As shown in Figure 1.10, ISA 100.11a shares the IEEE 802.15.4 standard on the physical and data link layers with WirelessHART. Thus, both ISA 100.11a and WirelessHART work on the 2.4 GHz frequency, they support mesh and star topologies and they incorporate strategies to optimize coexistence with other users of the 2.4 GHz frequency [33]. ISA 100.11a and WirelessHART also support channel hopping.

WirelessHART defines its own network and transport layers. However, on ISA 100.11a these layers are based on TCP or UDP (IPv6). ISA 100.11a is said to be designed to support native and tunneled application layers [39].

The application layer on ISA 100.11a communicates services to users and management processes. Native ISA 100.11a objects can be passed and manufacturers can define their own [39].

An example of an ISA 100.11a network is shown in Figure 1.11.

1.2.3 Market Penetration

WirelessHART is been used by widely known automation device suppliers such as ABB, Emerson, Siemens, Phoenix Contact, among others. Some of the companies using WirelessHART for their automation processes are Bayer, BP, ConocoPhillips, Shell, Statoil, PE-

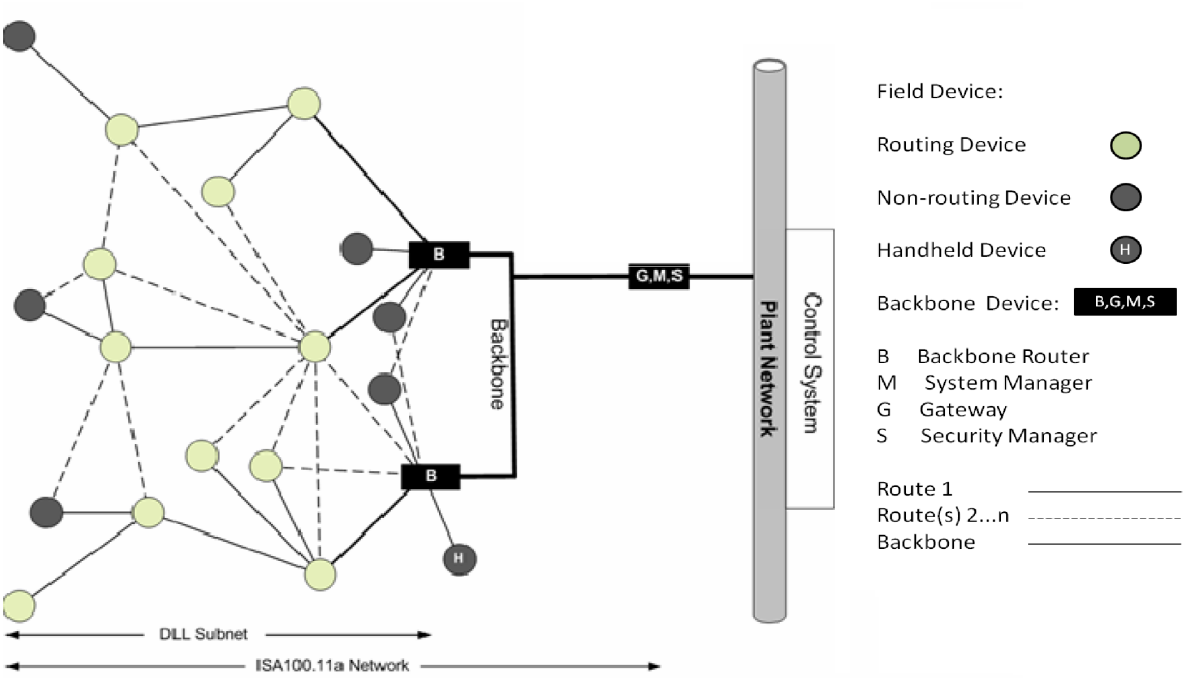


Figure 1.11: Example of an ISA 100.11a network (adapted from [22]).

MEX, among others, as stated on a recent press release [14]. According to this press release, WirelessHART worldwide installed networks exceed 8,000.

ISA, on the other hand, lists as corporate partners companies that are also widely known such as CE Controls, Honeywell, Cooper Bussman, among others. An important automation supplier developing using ISA 100.11a is Yokogawa [9].

Based on the results of a recent study made by ON World Inc., Purvis states in her article [32] that "WirelessHART is used by 39% of the surveyed end users up from 13% in ON World's previous survey completed in Q1 2010". This means that in less than 3 years the use of WirelessHART has tripled. Purvis goes on to say that [32]:

> "Preferences for wireless mesh standards continue to diverge with end users equally preferring either WirelessHART or a hybrid strategy that includes both WirelessHART and ISA100.11a"

This implies that ISA 100.11a remains as an attractive option.

Chapter 2

6LoWPAN

IPv6 over Low-power Wireless Personal Area Networks (6LowPAN) is a protocol designed to incorporate wireless networking on small (low power and processing limited) devices using the latest version of the IP protocol, IPv6. 6LowPAN is meant to play an important role in the emerging *Internet of Things*.

The idea behind the *Internet of Things* is that more and more embedded devices will become IP enabled and part of the Internet. Examples of systems using IP are home automation and industrial automation, and a very popular example of embedded devices are mobile phones. As stated by Shelby and Bormann [35]:

> "The scale of the Internet of Things is already estimated to be immense, with the potential of trillions of devices becoming IP-enabled. The impact of the Internet of Things will be significant, with the promise of better environmental monitoring, energy savings, smart grids, more efficient factories, better logistics, better healthcare and smart homes."

2.1 Definition and Architecture

Today, there are many protocols and solutions for wireless embedded devices. The reason is the wide range of applications with different requirements. Shelby and Bormann [35] list the characteristics of the ideal use for 6LoWPAN in applications where:

- "embedded devices need to communicate with Internet-based services,
- low-power heterogeneous networks need to be tied together,
- the network need to be open, reusable and evolvable for new users and services, and
- scalability is needed across large networks infrastructures with mobility."

6LoWPAN is a working draft of the Internet Engineering Task Force (IETF) [19] and is presented by Shelby and Bormann [35] as a standard that enables the efficient use of IPv6 on small devices.

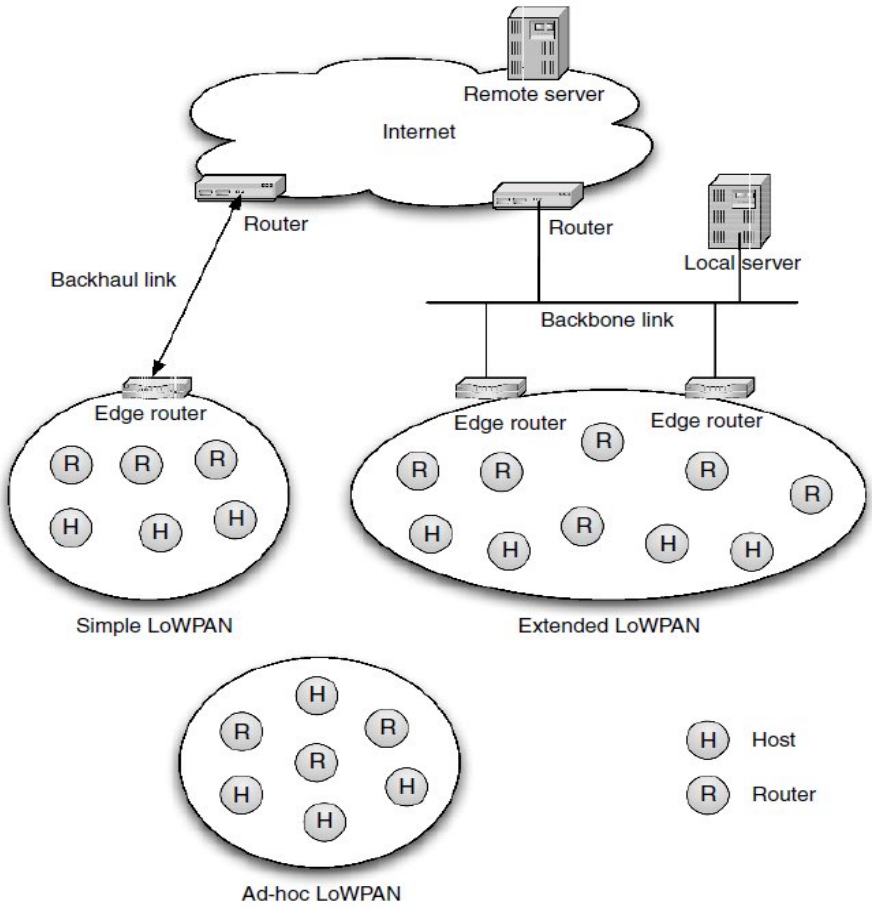


Figure 2.1: The 6LoWPAN architecture (from [35]).

Shelby and Bormann [35] define a *stub network* as an island of wireless embedded devices that does not serve as transit for other networks. These *stub networks* are connected between each other and form the Wireless Embedded Internet.The 6LoWPAN architecture is made up of a set of LoWPAN's (Low-Power Personal Area Networks) which are IPv6 *stub networks* that can be connected to other networks and to the Internet.

Figure 2.1 shows three different kinds of LoWPAN's; Simple LoWPAN, Extended LoWPAN and Ad-hoc LoWPAN [35].

- A Simple LoWPAN is a set of host and router nodes connected to another IP network through one LoWPAN edge router. The edge router can be connected to the router of another IP network through a shared or a point-to-point link.

- An Extended LoWPAN is made up of LoWPAN's of more than one edge router that share a backbone link and the IPv6 *prefix* (the first 64 bits). This means that IPv6 addresses are stable through the Extended LoWPAN and the movement of a node between two edge routers is simple.

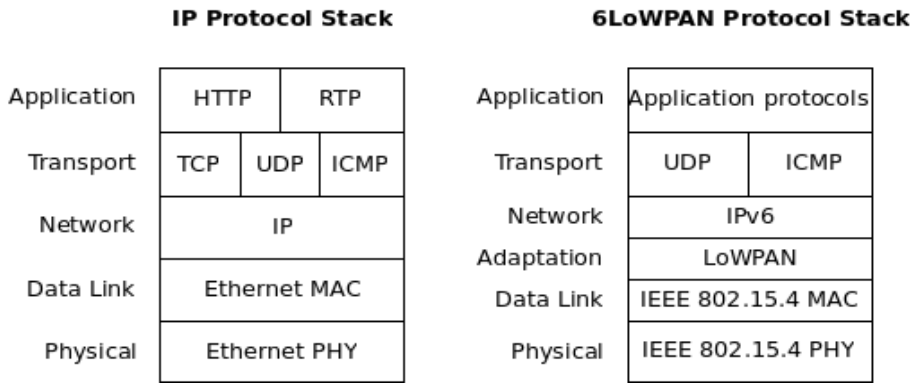


Figure 2.2: IP and 6LoWPAN protocol stacks (adapted from [35]).

- An Ad-hoc LoWPAN operates without a defined structure and is not connected to the Internet.

Each of the LoWPAN networks contains a set of host and router nodes that share an IPv6 *prefix* which is distributed by the edge router and routers through the LoWPAN network.

An important mechanism of IPv6 is the Neighbor Discovery [35]. This protocol is responsible for the configuration and interaction of router and host nodes in the same link. Topology changes, e.g. adding or removing a node, are supported through the LoWPAN and a node may participate in more than one LoWPAN at a time, this is handled by the edge routers.

2.2 Protocol Stack

As shown in Figure 2.2, the IPv6 protocol stack with 6LoWPAN is very similar to the IP protocol stack. Differences lie in that 6LoWPAN only supports IPv6, for what an adaptation layer has been defined [35]. Physical and data link layers share the IEEE 802.15.4 standard. The LoWPAN Adaption Layer is defined on top of the IEEE 802.15.4 MAC layer and serves to optimize IPv6 over IEEE 802.15.4. The network layer only supports IPv6 and the transport layer uses ICMPv6 and UDP.

Shelby and Bormann [35] state:

> "The easiest way to enable a wireless embedded device with 6LoWPAN is by integrating an existing protocol stack, either with a network processor, a stack included with an operating system or by integrating a stack into an embedded software project."

Shelby and Bormann define seven basic components that a protocol stack for 6LoWPAN would typically include, they are: radio drivers, medium access control, IPv6, UDP, ICMPv6, Neighbor Discovery and socket-like or other API to the stack.

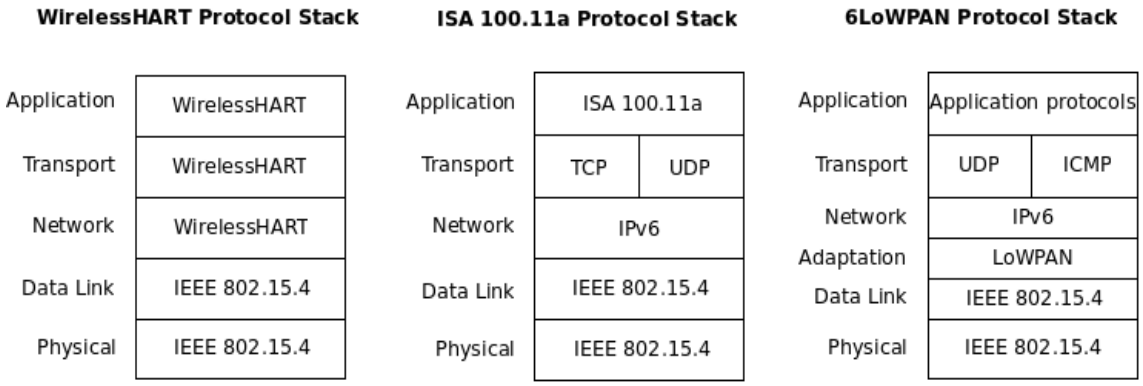


Figure 2.3: WirelessHART, ISA 100.11a and 6LoWPAN protocol stacks.

Figure 2.3 shows a comparison between the WirelessHART, ISA 100.11a and 6LoWPAN protocol stacks. All tree protocols have their physical and data link layers based on IEEE 802.15.4.

An important difference is that WirelessHART defines its own network and transport layer and they are not compatible with IPv6. This means that WirelessHART would meet only some of the components mentioned by Shelby and Bormann [35], e.g. radio drivers and the medium access control (IEEE 802.15.4).

On the other hand, ISA 100.11a does comply with these stack components. As mentioned on the previous chapter, the network and transport layers on ISA 100.11a are based on TCP or, most commonly, UDP over IPv6.

Examples for WirelessHART, ISA 100.11a and 6LoWPAN networks are shown in Figures 1.9, 1.11 and 2.1 respectively. The idea that rules these network designs is somehow similar; a set of field or host devices connected to one or more router or gateway device that handle configuration and addressing.

Chapter 3

Comparison

Based on the article by Petersen and Carlsen [30] on WirelessHART and ISA 100.11a, on the 6LoWPAN book by Shelby and Bormann [35], and on the ISA 100.11a standard [22], this chapter reveals some technical details on the WirelessHART, ISA 100.11a and 6LoWPAN standard specifications. The descriptions presented for each of the OSI protocol layers specify some of the important differences between the three standards.

3.1 Physical Layer

The physical layer is the interface to the physical medium and handles functions related to the radio frequency transceiver.

6LoWPAN, WirelessHART and ISA 100.11a physical layers are based in the IEEE 802.15.4 PHY standard with minor modifications. Operation is defined on the 2.4 GHz using channels 11-25. Channel 26 is not included in WirelessHART, while in and 6LoWPAN and ISA 100.11a is defined as optional. Each channel uses a bandwidth of 2 MHz and channels are spaced 5 MHz apart. WirelessHART and ISA 100.11a use a combination of Direct Sequence Spread Spectrum (DSSS), employed in IEEE 802.15.4, and Frequency Hoping Sequence Spread (FHSS) as modulation technique. A combination with Offset Quadrature Phase Shift Keying (O-QPSK) allows a raw bit rate of 250 Kbs. The maximum transmitted power is limited to 10 mW, which gives devices a range up to 100 m in outdoor conditions with direct line of sight.

3.2 Data Link Layer

The data link layer is responsible for providing a reliable communication link between two data link entities, providing access and synchronization of the radio channel. In both WirelessHART and ISA 100.11a, channel access is provided by the Time Division Multiple Access (TDMA) combined with frequency hoping.

For **WirelessHART**, the data link layer is defined as follows:

- Layer is divided into logical link control layer and a MAC sub layer.
- Data link layer is responsible for handling one-hop communication.
- Time slots for the transmission of data from a source device are defined of 10 ms and there is no frequency hoping pattern explicitly defined on the standard. Communication links and channel hop patterns are handled by the network manager.

For **ISA 100.11a**, the data link layer is defined as follows:

- Layer is divided into a MAC sub layer, MAC extension and an upper data link layer.
- The MAC sub layer is a subset of the IEEE 802.15.4 standard and is responsible of sending and receiving individual data frames.
- The MAC extension includes additional features not included in IEEE 802.15.4. These features are mainly concerning the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism.
- The upper layer is responsible of handling routing within a data link sub net. This sub net includes one or more sets of devices and stops at the backbone router. This means that, contrary to the OSI definition of the Data Link layer, mesh routing is handled by the ISA 100.11a data link layer.
- Each device is assigned a 16 bits data link sub net address and the standard supports graph and source routing.
- Time slots for the transmission of data from a source device are configurable and the standard defines 5 frequency hopping patterns.

For **6LoWPAN**, the data link layer is defined as follows:

- Routing and forwarding are performed based on 64-bit IEEE EUI (extended unique identifier, a globally unique bit combination) or 16 bit short addresses.
- Mesh forwarding between two data link layers is achieved using the 6LoWPAN adaptation layer.
- 6LoWPAN defines the mesh header for link-layer forwarding. The mesh header stores the address of the next hop and the current node doing the forwarding. This is done to avoid overwriting the originator and final destination addresses.

3.3 Adaptation Layer

The specification on how to transmit IP packets over other subnetworks is referred to as *IP-over-X*. The Internet is composed of many subnetworks, and packets might have to traverse these subnetworks in order to reach its final destination.

The adaptation layer on 6LoWPAN defines the specification for transmitting IPv6 packets over IEEE 802.15.4. The adaptation layer was defined to address certain problems that arise when working with IPv6 over IEEE 802.15.4 and the layer defines the specification on how to deal with these problems.

WirelessHART does not define an adaptation layer because the standard does not work with IPv6. On the other hand, ISA 100.11a does work with IPv6 but the standard does not define such adaptation layer. The functions that 6LoWPAN implement in the adaptation layer are carried out on ISA 100.11a network layer.

6LoWPAN defines the adaptation layer as follows:

- Once the corresponding IP address next hop destination for a packet is fixed, the adaptation layer is responsible for determining the data link address the packet needs to be addressed to.
- Layer might need to set up connections in subnetwork to figure out next data link address hop and provide information about further direction. These is done using the mesh header.
- Because IEEE 802.15.4 does not specify how to identify different types of packet encapsulations, this identification is carried out by the adaptation layer.
- IP packets must fit data units that the data link layer can transport. For this, the adaptation layer defines fragmentation and reassembly.
- Existing IETF standard for header compression and too heavyweight for 6LoWPAN. Thus, the adaptation layer defines header compression for 6LoWPAN.

3.4 Network Layer

The network layer is responsible for routing packets in the network.

For **WirelessHART**, the network layer is defined as follows:

- Layer is responsible of routing packet from source to final destination. The standard defines graph and source routing. All devices maintain a series of routing tables that are handled by the network manager.

For **ISA 100.11a**, the network layer is defined as follows:

- Layer is responsible for routing beyond the backbone router. The standard does not provide details on backbone and plant networks routing because these are out of the standard scope. The standard specifies interfaces for data exchange between the backbone and the network layer of this standard.

- Network layer is responsible of determining correct addresses, whether the address is a 16 bits data link sub net address or a 128 bits address for application endpoints and backbone networks. The layer also handles translation between these two types of address.

- The network layer of the point of ingress into a data link subnet performs fragmentation and the network layer of the point of egress from the data link subnet performs reassembly.

For **6LoWPAN**, the network layer is defined as follows:

- The layer is based on IPv6, which makes use of the Neighbor Discovery protocol for interactions between neighbors.

- The routing protocol fills a Routing Information Base (RIB) that contains all the information needed for the protocol. The RIB can usually be simplified to a Forwarding Information Base (FIB).

- Routing over network layers does not require support from the 6LoWPAN adaptation layer. Before the network layer sees the packet, the adaptation layer has decapsulated the packet.

- Two kinds of routing can be performed with 6LoWPAN; intra-LoWPAN routing and border routing.

- Intra-LoWPAN routing happens between two LoWPAN routers.

- Border routing happens at the edge of the LoWPAN network by a LoWPAN Edge Router or an IPv6 router on the backbone.

3.5 Transport Layer

The transport layer is responsible for end-to-end communication and operates in the communication end point.

For **WirelessHART**, the transport layer is defined as follows:

- Layer handles acknowledged and unacknowledged transactions.

For **ISA 100.11a**, the transport layer is defined as follows:

- Layer defines Transport Management Entity (TME), Transport Security sub layer and Transport Data Entity (TDE).
- TME configures and monitors the actions of the transport layer.
- TSS configures and monitors transport layer security functions and is responsible for maintaining security tables.
- TDE uses TSS to perform security operations on protocol data units that pass through the layer.
- Transport layer uses TDE service access point (TDSAP) to transmit and receive protocol data units with the application sub layer.
- Layer supports TCP and UDP protocols.
- Layer provides connectionless services, which extends UDP over IPv6. The extension provides better data integrity and an addition in authentication and encryption mechanisms.

For **6LoWPAN**, the transport layer is defined as follows:

- Layer supports UDP and ICMP protocols.

3.6 Application Layer

The application layer provides services to user-defined applications and defines communication services to enable object-to-object communication between applications.

For **WirelessHART**, the application layer is defined as follows:

- Layer defines commands, responses, data types and status reporting supported by the wired HART standard. Supported commands are divided into four groups; Universal Commands, Common Practice Commands, Device Families Commands and Device-Specific Commands.
- Universal Commands are defined in the IEC 61158-5-20 and IEC 61158-6-20.
- Common Practice Commands are a set of standardized, device independent commands that enhance interoperability.
- Device Families Commands are used by field devices and they are based on the type of process connection they support.
- Device-Specific Commands are developed by manufacturers outside HART. These commands are out of the standard scope.

For **ISA 100.11a**, the application layer is defined as follows:

- Layer is divided into upper application layer and an application sub layer.
- The upper application layer contains the application processes for the device and may be used to support protocol tunneling, among other functions.
- The application sub layer provides services for the upper application layer, such as object-oriented communication and routing objects within user application process.

For **6LoWPAN**, the application layer is defined as follows:

- A set of basic paradigms for application protocols are applied to 6LoWPAN. These paradigms are; end-to-end, streaming, publish/subscribe and web services.
- For the end-to-end paradigm, only end-points participate in the protocol. For 6LoWPAN the paradigm provides one approach for protocol compression. Compression can be achieved by supporting the compressed format natively on the IP application endpoint.
- Many applications work with real time data. Typically, these applications employ UDP. Internet protocols provide a good framework for handling real time data which can be employed by 6LoWPAN, such as; Real time Transport Protocol (RTP), RT Control Protocol (RTCP), and Session Initiation Protocol (SIP).
- Publish/subscribe is a messaging paradigm in which the sender transmits data without knowing who the receiver is. Receivers subscribe to data based on the content. This paradigm plays an important role on the Internet of Things, where receiving data is more important than the sender information.
- Web services can be integrated into 6LoWPAN using different technologies. Two fundamental ways are using a gateway approach (web service implemented at the edge of the LoWPAN network) and a compression approach (web service is compressed for use over 6LoWPAN).

Chapter 4

High Quality, Secure and Safe Wireless Communication

As Åkerberg [2] explains, automation networks initially were placed in a central physical location. Devices were connected in a marshaling room and communication was based on proprietary wired solutions. Åkerberg states that "security was based on *security-by-obscurity* and *physical security*".

This situation has changed over time. One reason mentioned by Åkerberg [2] for this change is that the demand for information from the field devices has grown. More information is required for control algorithms and to improve the quality and quantity of final products. Networks are no longer closed and an automation network might be integrated in or connected to some other network. Along with this, concerns for more robust security arose.

On the other hand there is quality of service and safety. Safety refers to the reliability of the communication. Åkerberg [2] states that safe communication has always been taken to consideration and it is standardized and more mature. Still, there are many different proprietary safety protocols.

Achieving high quality, secure and safe communication is important for automation standards and protocols because these aspects need to be considered when designing a standard. Still, the standard should somehow provide flexibility, because each application has its own particular requirements. There are different types of communications that an application might need to achieve. Table 4.1 presents 6 usage classes of intended use of inter-device industrial wireless communication. Nickerson and Taylor [28] state that, nowadays, wireless communication in industrial control is primarily used for classes 3 to 5.

4.1 Quality of Service (QoS)

Currently, there are many definitions for QoS. For example, Campanella et al. define [7]:

> "QoS (Quality of Service) is a generic term which takes into account several techniques and strategies that could assure application and users a predictable service

Type	Class	Description	Characteristic
Safety	0	Emergency action	Always critical
Control	1	Closed loop regulatory control	Often critical
	2	Closed loop supervisory control	Usually non-critical
	3	Open loop control	Human in the loop
Monitoring	4	Alerting	Short-term operational consequence
	5	Logging and downloading/uploading	No immediate operational consequence

Table 4.1: Usage classes (adapted from [22]).

from the network and other components involved, such as operating systems."

Christin et al. [8] compare different protocols based on some aspects they consider important when evaluating QoS. They evaluate real-time traffic support using medium access control (MAC) mechanisms (TDMA and CSMA/CA). They also consider the transmission of superframes and priority management, which is based on the assignment of priority to the packets. Finally, they evaluate reliability based on mechanisms such as space and frequency diversity, and the use of acknowledged transactions.

Lo Bello et al. [6] state:

> "Offering real-time support on networks means that a predictable time behavior of communications can be guaranteed, either in a deterministic or in a stochastic way."

They explain that in hard real-time systems (systems where a packet that misses a deadline can have catastrophic consequences) deadline miss should never happen. On the other hand, for soft real-time systems (systems in which a deadline miss only entails a performance degradation) occasional violations of deadlines can be tolerated.

Predictable time behavior does not necessarily mean constant time behavior. Thus, the important aspect is to have an upper bound for QoS indicators such as "end-to-end packet delivery time, packet channel access time, roundtrip time, etc" [6]. The upper bound value can be used to evaluate if a packet will meet the specified deadline in a deterministic way or by calculating the probability that the packet misses the deadline.

Lo Bello et al. [6] state that for hard real-time traffic a *guaranteed service* is required. This means that there is a guarantee on the system timing behavior for the selected indicator. For soft real-time traffic, a *best-effort service* is suitable in which the system is allowed to deliver a lower quality than expected. Still, is important to keep in mind that a system should always deliver the best QoS it can provide.

Lo Bello et al. define that "the primary performance metrics are related to the timeliness of data exchange over the network" [6]. Typical real-time systems handle monitoring and control applications that require a response withing bounded delay combined with low jitter values.

Usually, transmitting a packer over a network is composed of several stages in which packets of different classes and with different priorities travel. To provide a bounded delay,

the delay on each stage must also be bounded and queue management is very important. Lo Bello et al. [6] specify that "suitable flow control algorithms, selective discarding, and packet marking policies are needed to support QoS for real-time traffic."

Response-time analysis (RTA) and network calculus (NC) are two analytical methods to evaluate real-time network performance [6]. Lo Bello et al. [6] define RTA as:

> "...a method to verify the schedulability of a task set in a processor or of a message set in a communication network, which is based on the response time computation and comparison with the deadline for each task or message in the set."

On the other hand, NC performs deterministic analysis in network where incoming traffic is unknown. Lo Bello et al. [6] refer to different applications of NC in industrial automation and wireless sensor networks.

Christin et al. [8] present a study that includes a comparison between WISA, WirelessHART, ISA 100.11a and ZigBee in terms of the aspects the defined to evaluate QoS. Part of the presented conclusions is that "the selected specifications differ with respect to the supported QoS requirements for industrial applications, particularly concerning real-time support and reliability".

Summarizing the comparison for WirelessHART and ISA 100.11a presented by Christin et al. [8] regarding real-time support, dedicated timeslots are supported by both standards. On the other hand, tunning the timeslot length is supported by ISA 100.11a, but not by WirelessHART. Changing the predetermined timeslot length allows the support for application specific requirements. Both WirelessHART and ISA 100.11a support message-based priority and superframes.

Regarding reliability support, Christin et al. [8] state that both WirelessHART and ISA 100.11a support a mesh topology and this is considered a good protection against node failures. Both standards support other mechanisms such as channel blacklisting and frequency hopping. Also, WirelessHART and ISA 100.11a support acknowledged transactions at the data link and transport layers.

4.2 Security

Granzer and Treytl [15] state that "...security can be defined as measures that protect system resources against adversaries that intentionally try to gain unauthorized, malicious access".

Granzer and Treytl [15] refer to the book *Security in Computing* [31] and list the following four classes of network attacks:

- Interception attacks: The adversary tries to gain unauthorized access to confidential data exchange over the network.
- Modification attacks: The adversary tries to change the data while it is being transmitted over the network.

Table 4.2: Typical security objectives in industrial automation (from [2] [12]).

Objective	Description
Confidentiality	The confidentiality objective refers to preventing disclosure of information to unauthorized persons or systems
Integrity	The integrity objective refers to preventing undetected modification of information by unauthorized persons or systems
Availability	Availability refers to ensuring that unauthorized persons or systems can not deny access or use to authorized users
Authentication	Authentication is concerned with the determination of the true identity of a system user
Authorization	The authorization objective is concerned with preventing access to the system by persons or systems without permission
Auditability	Auditability is concerned with being able to reconstruct the complete history of the system behavior from historical records
Nonrepudiability	The nonrepudiability objective refers to being able to provide proof to a third party of who initiated a certain action in the system, even if the actor is not cooperating
Third-party protection	The third-party protection objective refers to adverting damage done to third parties via the system

- Fabrication attacks: The adversary tries to insert malicious data.
- Interruption attacks: The adversary tries to interrupt the communication between devices and thus makes data unavailable.

To deal with these attacks, security measures must be implemented. Table 4.2 was extracted from Åkerberg's work [2] and lists the typical security objectives in industrial automation as presented by Dzung et al. [12]. Åkerberg [2] states that, unlike safety risks, security risks change over time.

Granzer and Treytl [15] consider that the main concerns for wireless communication networks is:

> "...the robustness to electromagnetic interference and in general the security goal of availability that can only be solved by proper organizational measures (e.g., redundant transmission paths)".

Some of the objectives presented in Table 4.2 are consistent with the security criteria presented by Christin et al. [8]. This security criteria is based on confidentiality of information, integrity of information, authenticity of communication peers and availability of information.

Again, Christin et al. evaluate the set of standards based on this criteria. Part of the conclusions of their work is [8]:

> "The selected standards are resistant against most of the considered attacks except for continuous jamming at all frequencies, collision and flooding attacks as well as traffic analysis. However, solutions against such particular kind of jamming and collision attacks are particularly difficult to find because the data transmission is made impossible in both cases."

Still, Christin et al. [8] consider that frequency diversity is a good mechanism to protect the network against intermittent jamming. They state that confidentiality is not addressed at all layers, but information filtering to unauthorized persons is made very difficult with current mechanisms. Finally, they consider that the implemented mechanisms ensure information integrity.

4.3 Safety

Granzer and Treytl [15] explain that security protects the system against intentional actions that can damage the system and may have harmful consequences to people. On the other hand, safety protects the system against unintentional states that do cause harm to humans.

When a system reaches a state that can cause harm to humans, special communication is needed to respond to this situation or to alert about the emergency. Jiang et al. [23] present a design for vehicular safety communication. They propose a system that warns the driver or the vehicle system of potentially dangerous situations. They present an example of this kind of situation where a vehicle that is stopping or moving slowly broadcasts its presence to other vehicles. Another vehicle approaching fast can be aware of the presence of the first vehicle and carry out the proper action (e.g. perform a quick maneuver) while broadcasting the message to other vehicles. To achieve this and other similar situations, Jiang et al. [23] define safety messages and safety communication protocols on top of the Dedicated Short Range Communication (5.9 GHz DSRC) standard.

In industrial and control networks, there are many situations that can cause harm to humans, e.g. extremely high or abnormal temperature or pressure values. In these situations, safety critical messages need to be transmitted over the network to alert about or respond to this situation.

Åkerberg [1] states:

> "The term safety-related is used to describe systems that are required to perform a specific function or functions to ensure that the risks are kept at an accepted level. Such functions are, by definition, safety functions."

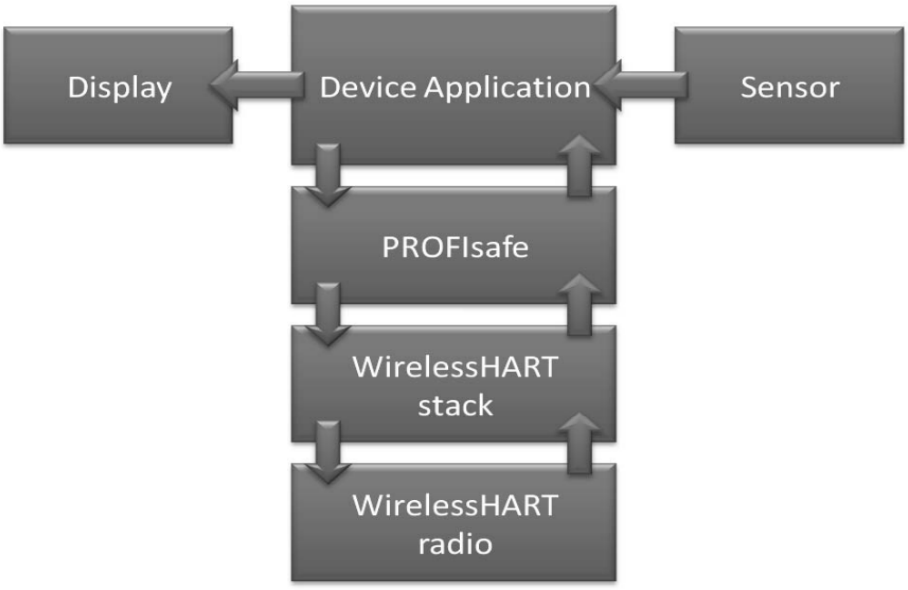


Figure 4.1: Architecture of the PROFIsafe enabled WirelessHART device using the principle of the black channel (from [5]).

Åkerberg et al. mention in their article [5] that the IEC 61508 [20] standard is meant to define a set of methods, measures and procedures that must be implemented in a device to claim a certain safety integrity. Åkerberg et al. explain that IEC 61508 is a risk based standard and it is based in the *black channel* principle. This principle is implemented to simplify the safety-related process by adding a safety layer on top of the standard transmission system (e.g. wired fieldbus). This allows that the transmission system does not perform any safety related task, but only serves as the transmission medium for data packets and safety frames. The black channel principle provides interoperability, because the safety layer can be implemented regardless of the transmission system and medium.

The IEC 61508 [20] standard is defined as a general set of rules that must be implemented by a protocol to claim certain safety integrity. On the other hand, the IEC 61784-3 standard [21] specifies rules and safety profiles for the fieldbus profiles presented in other IEC standards. "PROFIsafe is one out of four safety protocols described in the IEC 61784-3 standard" [5]. PROFIsafe can be used on top of PROFIBUS and PROFINET. PROFIsafe could also be implemented on top of other protocols, but this is not allowed according to the PROFIsafe policy [5].

The possible communication errors related to functional safety are presented in the IEC 61784-3 standard. They were extracted by Åkerberg [2] and are presented in Table 4.3. In the article from Åkerberg et al. [5], they present the communication errors from the IEC 61784-3 standard with a particular focus on measures that are important in wireless network. This wireless interpretation of communication errors impacting safety is presented in Table 4.3.

The safety protocols described in the IEC 61784-3 standard were designed for wired

fieldbus systems. How can safety be implemented on wireless networks?

Using the black channel principle, Åkerberg et al. [5] proposed and implemented a safety layer on top of a WirelessHART stack as an attempt to add safety capabilities into a "wireless industrial fieldbus" [5]. Their proposed design is presented in Figure 4.1 where the PROFIsafe safety layer was added on top of the WirelessHART stack.

The implementation and proof of concept performed by Åkerberg et al. show that it is possible to enable safety functionality combining WirelessHART and PROFIsafe. However, one of the observations presented in the study is that WirelessHART is not fast enough in some cases where "a short safety function response time is needed", because the WirelessHART standard limits the "shortest periodic transmission for one device ... to 250ms" [5]. Another observation made by the authors is that the proposed implementation of the black channel using WirelessHART did not implicate any major challenges. However, some mechanisms need to be improved to reach shorter round-trip time and shorter safety function response time.

A later work by Taylor et al. [37] present high-level requirements of communication and control systems for safe and secure wireless networked control. They present a framework for safe and secure communication. This framework adds a security layer on top of the wired or wireless fieldbus layer, and a safety layer on top of the security later. The security layer uses the communication system as a black channel, and for the safety layer both the communication system and the security layer are used as the black channel.

Taylor et al. [37] also present a framework for safe and secure control based on the implementation of a Wireless Networked Control System Coordination Agent (WNCSCA). The WNCSCA was designed to work along with the gateway to manage energy consumption, monitor processes and control performance. The WNCSCA interfaces between the Intelligent Control and Asset Management (ICAM) [38] system and the gateway of the wireless sensor-actuator network. The ICAM system manages low-level controllers, e.g. sending signals to controllers such as set points. WNCSCA was designed to coordinate between the communications and controls functionality [37].

For wireless control loops, the communication from the gateway to the actuator is considered critical [37]. However, WirelessHART does not define how to initiate efficient and periodic communication from the gateway to an actuator [37]. Åkerberg et al. [4] present an extension to WirelessHART to provide periodic downlink transmission from the WirelessHART gateway to a WirelessHART actuator. This downlink scheme has been showed to reduce the safety function response time (SFRT) significantly [4]. However, this solution is considered viable for slower industrial processes requiring sampling rates on the order of a few seconds.

Table 4.3: Possible communication errors (adapted from [2] and [5]).

Error	Description	Wireless Channel Implementation
Corruption	Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference	Data in a wireless channel are subject to interference and noise and bits can be corrupted easily. The bit error rate gives an indication of the quality of a channel
Unintended repetition	Due to an error, fault, or interference, old not updated messages are repeated at an incorrect point in time	Repetition can occur if messages were not sent over the wireless channel properly, but they will most likely be handled by the wireless protocol itself
Incorrect sequence	Due to an error, fault, or interference, the predefined sequence associated with messages from a particular source is incorrect	If the wireless protocol does not control the sequence of the messages, it can be problematic for the PROFIsafe protocol
Loss	Due to an error, fault, or interference, a message is not received or not acknowledged	This is one of the major problems in wireless communication, because it can happen due to multiple causes e.g. electromagnetic disturbance, interference with other wireless communication techniques, signal loss etc.
Unacceptable delay	Messages may be delayed beyond their permitted arrival time window, for example due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such manner that services are delayed or denied	If messages get lost and must be re-transmitted several times, if multi-hopping is used (sending the message from node to node over several hops) or if the wireless channel is occupied by another sender for a longer period, then delay is an effect that will affect the PROFIsafe protocol
Insertion	Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity	This is more unlikely in wireless networks, unless missing security measures allow access for attackers
Masquerade	Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a non-safety relevant message may be received by a safety relevant participant, which then treats it as safety relevant	This is also more a security issue as above
Addressing	Due to a fault or interference, a safety relevant message is sent to the wrong safety relevant participant, which then treats reception as correct	This might be a more unlikely scenario

Chapter 5

Summary, Conclusions and Future Work

Industrial communication networks is a very active field and a wireless approach can potentially lead to significant cost saving and improvement in the quality (i.e. efficiency, safety, and transparency [29]) of the control processes carried out. Wireless networks reduce costs of installation, wiring (e.g. $120 per meter [28]) and operation.

Although industrial networks are widely used and they have countless applications, e.g. industry, manufacturing, and home automation [10], there is a standardization process that is still going on. Devices from different manufacturers are not always compatible and this becomes an issue for large industrial systems where many kind of devices are needed.

Nivis [27] is a company that provides solutions for wireless sensing and control networks. They provide standards-based communication and software. Table 5.1 presents a comparison between the Nivis implementations of three of the main standards for wireless industrial networks; WirelessHART, ISA 100.11a and 6LoWPAN. These standards correspond to the three major standards studied in this report, but they are only a small subset of all the possibilities existing today for automation and industrial networks.

Standardization is not the only further work in wireless industrial and control networks. Granzer and Treytl [15] state that:

> "The lack of state-of-the-art security measures at the field level of many industrial communication systems almost solely allows implementing security measures on top of the automation networks".

They explain that this solution introduces overhead and threatens interoperability. Security at all levels must be considered and this security measure can be helpful for accidental errors or safety issues [15].

Dang and Sisinni [11] study three industrial communication standards; WirelessHART, ISA 100.11a and OCCARI. One of their conclusions is that security is ensured by means of cryptography, specifically for authentication (the identity of the sender of a packet) and message integrity.

Table 5.1: Nivis technologies comparison (adapted from [27]).

Feature	Nivis ISA 100.11a	Nivis WirelessHART	Nivis 6LoWPAN
Number of devices per Gateway	100	100	3000+
Network scalability (through one centralized manager)	600	400	3000+
Mesh layers support	6	6	25
Maximum packet size	1028 bytes	1028 bytes	2048 bytes
Latency	$<$ 1 second	$<$ 1 second	$<$ 30 seconds
Application layer	Object-based	Command-based	CoAP-based
Target application	Process automation	Process automation	Metropolitan Area Networks (MANs)
Supports distributed system management for redundancy	Yes	No	Yes
Supports remote firmware upgrades	Yes	Yes	Yes
Peer to peer communication supported	Yes	No	No
Battery powered devices capable of routing (true battery powered mesh)	Yes	Yes	No
Supports star topology networks with battery powered end nodes (ultra long life routing nodes)	Yes	No	Yes
Two-way communication	Yes	Yes	Yes
Supports IPV6 (6LoWPAN) and utilities	Yes	No	Yes
Multi-path redundancy	Yes	Yes	Yes
Utilizes frequency hopping for robust communications	Yes	Yes	Yes
Channel blacklisting mechanism for robust communications	Yes	No	Yes
RoLL (RPL) routing protocol	No	No	Yes
Web services to device	No	No	Yes
802.15.4-2006 compliant	Yes	Yes	Yes
802.15.4g compliant	No	No	Yes
802.15.4e compliant	No	No	Yes
802.15.4 compliant security - AES128 bit encryption	Yes	Yes	Yes
Supports end-to-end security	Yes	Yes	Yes
2.4GHz radio supported	Yes	Yes	Yes
900MHz radio supported	Yes	No	Yes

For Granzer and Treytl [15], security is not equated to network security or cryptography, but to more organizational measures to be taken in consideration in the complete system and not in a dedicated part. This is consistent to the issue addressed by Taylor et al. [37] and they propose the integration of secure and safety communication for the system as a whole; including wired and wireless communications.

Dang and Sisinni mention important aspects of industrial communication in terms of the characteristics of the traffic. These characteristics are "the presence of deadlines, high-reliability requirements, and the predominance of short packets" [11]. Dang and Sisinni also state that there are few plants that implement wireless industrial communication systems. Thus, they consider a lack of *demonstrations* of the viability of such solutions. Is there a real industrial plant using wireless communications for process control and monitoring? If so, which usage classes of wireless communication from Table 4.1 are carried out? How is the performance of this network measured and guaranteed? If the safety function response time (SFRT) [4] is used as a metric, can existing wireless industrial control protocols be adapted to provide an estimation of the minimum SFRT a network can achieve?

Gungor and Hancke [17] go through the open issues of industrial wireless sensor networks (IWSN). They mention that there are technical problems to be solved "in analytic IWSN models in terms of communication latency and reliability, and energy efficiency" [17]. They propose the idea of incorporating a cognitive radio paradigm to a low-power industrial sensor node and controlling channel hand-off. They state that this idea can be a good mechanism to deal with radio frequency interference.

Åkerberg has been working in the wireless industrial communication area for more than three years. He is the author of several publications. In his work [1], he states that the challenge for functional safety is "to design the system in a way that prevents dangerous failures or to control them when they arise". In a later work, Åkerberg et al. [5] propose a first approach into integrating safety-critical functions into a wireless control network. One of their conclusions is that the integration using WirelessHART is easy, but further analysis is needed to ensure that the process loop time is satisfied. There is also a restriction from the WirelessHART standard because it limits the shortest periodic transmission of devices to 250 ms, while update frequencies for some industrial wireless sensors can be down to 10 ms, as presented in Table 1 of [3]. The Wireless Interface for Sensors and Actuators (WISA) [24] was designed to provide update rates down to 10 ms [37]. Thus, WISA seems to be a possible implementation in wireless networks that need a faster update rate than WirelessHART's 250 ms. Which usage classes from Table 4.1 can be implemented using WISA? How does WISA compares to ISA 100.11a and 6LoWPAN?

Åkerberg et al. [3] list important challenges yet to be achieved by industrial wireless sensor networks. They explain that, in order for these networks to be competitive and cost efficient, the industrial wireless sensor networks need to meet all the requirements that are accomplished by wired systems.

One of the challenges is related to the support of safety-critical operations and that industrial wireless networks cope with safety communication requirements. Industrial wireless systems provide confidentiality, authentication and integrity. However, optimization can be

made with respect to security to improve certain aspects such as energy consumption, latency and security overhead [3].

Regarding security, the most problematic situation is denial-of-service attacks [3]. The system should transition into a safe state under such an attack. On the other hand, security mechanisms need to be integrated into the overall automation system [3].

Current assumptions made by standards are that the protocol can handle mesh topologies with thousands of nodes and that devices are battery operated [3]. Åkerberg et al. state that these assumptions are not appropriate for industrial control. Thousands of nodes in an automation system do not belong to the same network and, if devices are assumed to be battery operated, the protocol should be energy optimized. Energy optimization could bring negative consequences on the latency and real-time performance of the network [3].

The most important open problems appear to be meeting strict latency requirements of regulatory control, addressing the safety usage class of wireless communication and the wide diversity of current approaches for deploying wireless communication in industrial control settings.

Considering the existing protocols studied in this report, 6LoWPAN and ISA 100.11a seem capable of providing a good solution for classes 1 to 3 from Table 4.1, because both standards are based on UDP for fast communication. Can 6LoWPAN be used in a wireless industrial control setting? If so, what are its limits compared to ISA 100.11a and WirelessHART?

For classes 4 and 5, an implementation of ISA 100.11a using TCP might be a good solution, as TCP supports useful acknowledgments for sent alerting and logging messages. On the other hand, WirelessHART provides an advantage over other protocols because is a proprietary solution that is not based on widely known protocols. As a consequence, WirelessHART can have more resistance to attacks, as the source code and operational details are not widely available.

Regarding the usage class 0 (emergency action), real-time control experiments need to be done to provide proof of the latency and update frequency capabilities of different protocols. Latency and other measures taken using real devices communicating a series of messages can evaluate the performance of protocols. This evaluation can estimate if a particular protocol is suitable for any of the usage classes.

Bibliography

[1] J. Åkerberg. On security in safety-critical process control, 2009. Licentiate thesis.

[2] J. Åkerberg. *On Safe and Secure Communication in Process Automation*. PhD thesis, Mälardalen University, School of Innovation, Design and Engineering, 2011.

[3] J. Åkerberg, M. Gidlund, and M. Björkman. Future research challenges in wireless sensor and actuator networks targeting industrial automation. *The 9th IEEE International Conference on Industrial Informatics (INDIN)*, pages 410–415, July 26-29 2011. Caparica, Lisbon, Portugal.

[4] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Björkman. Efficient integration of secure and safety critical industrial wireless sensor networks. *EURASIP J. Wireless Comm. and Networking*, 2011:100, 2011.

[5] J. Åkerberg, F. Reichenbach, and M. Björkman. Enabling safety-critical wireless communication using wirelesshart and profisafe. In *IEEE Conf. on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, 2010.

[6] L. L. Bello, J. A. Fonseca, and W. Elmenreich. *Real-Time Systems*, chapter 17 of The Industrial Electronics Handbook: Industrial Communication Systems. CRC Press, 2nd edition, 2011. Edited by Bogdan M. Wilamowski and J. David Irwin.

[7] M. Campanella, P. Chivalier, A. Sevasti, and N. Simar. Quality of service definition. Technical report, 2001. DANTE. Report: SEQ-01-030 D2.1. Project: SeQuin IST-1999-20841.

[8] D. Christin, P. S. Mogre, and M. Hollick. Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. *Future Internet*, 2010.

[9] Y. E. Corporation. Field wireless, yokogawa electric corporation, 2012. `http://www.field-wireless.com/en/`.

[10] T. Dang. *Wireless Communication Standards*, chapter 54 of The Industrial Electronics Handbook: Industrial Communication Systems. CRC Press, 2nd edition, 2011. Edited by Bogdan M. Wilamowski and J. David Irwin.

[11] T. Dang and E. Sisinni. *WirelessHART, ISA 100.11a, and OCCARI*, chapter 53 of The Industrial Electronics Handbook: Industrial Communication Systems. CRC Press, 2nd edition, 2011. Edited by Bogdan M. Wilamowski and J. David Irwin.

[12] D. Dzung, M. Naedele, T. P. V. Hoff, and M. Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93, No. 6, June 2005.

[13] F. Foundation. Glossary, 2006. `http://www.fieldbus.org`.

[14] H. C. Foundation. Wirelesshart installed networks exceed 8,000 at major manufacturing sites worldwide. *HART Communication Foundation Press Releases*, 2012. Austin, Texas. `http://www.hartcomm.org/hcf/news/pr2012/WirelessHART_installed.html`.

[15] W. Granzer and A. Treytl. *Security in Industrial Communication Systems*, chapter 22 of The Industrial Electronics Handbook: Industrial Communication Systems. CRC Press, 2nd edition, 2011. Edited by Bogdan M. Wilamowski and J. David Irwin.

[16] T. A. Group. Foundation fielbus solutions from abb, March 2011. `http://www.abb.com/cawp/gad02181/c1256d71001e0037c1256b5a003158ce.aspx`.

[17] V. C. Gungor and G. P. Hancke. *Industrial Wireless Sensor Networks*, chapter 6 of The Industrial Electronics Handbook: Industrial Communication Systems. CRC Press, 2nd edition, 2011. Edited by Bogdan M. Wilamowski and J. David Irwin.

[18] M. N. M. Hanna. Real-time analysis of fip-based systems. Master's thesis, Faculty of Engineering, Cairo University, October 2004.

[19] IETF. *6lowpan Status Pages*. `http://tools.ietf.org/wg/6lowpan`.

[20] International Electrotechnical Commission (IEC). *IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2005.

[21] International Electrotechnical Commission (IEC). *IEC 61784-3. Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions*, 2007.

[22] International Society of Automation (ISA). *ISA-100.11a-2011 Wireless Systems for Industrial Automation: Process Control and Related Applications*, May 2011.

[23] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich. Design of 5.9 ghz dsrc-based vehicular safety communication. *IEEE Wireless Communications*, October 2006.

[24] 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 Trans. on Industrial Electronics*, 56:4279–4287, 2009.

[25] B. G. Lipták and H. Eren. *Instrument Engineers' Handbook: Process Software and Digital Networks*, volume 3, page 353. CRC Press, 4th edition, 2012.

[26] S. Mukhopadhyay. The fieldbus network - i. Department of Electrical Engineering, Indian Institute of Technology, Kharagpur, 2008. `http://www.fieldbus.org`.

[27] N. W. S. Networks. Nivis technology comparison, 2012. `http://www.nivis.com/technology/comparison.php`.

[28] B. G. Nickerson and J. H. Taylor. Cognitive wireless networked control systems (cwincs), April 2011. Project proposal draft.

[29] P. Palensky. *Trends and Challenges for Industrial Communication Systems*, chapter 67 of The Industrial Electronics Handbook: Industrial Communication Systems. CRC Press, 2nd edition, 2011. Edited by Bogdan M. Wilamowski and J. David Irwin.

[30] S. Petersen and S. Carlsen. Wirelesshart versus isa100.11a. *IEEE Industrial Electronics Magazine*, December 2011.

[31] C. P. Pfleeger and S. L. Pfleeger. *Security in Computing*. Prentice Hall, 4th edition, 2006.

[32] M. Purvis. Wirelesshart adoption tripled since 2010. *PRWEB*, 2012. San Diego, California. `http://www.prweb.com/releases/2012/6/prweb9640930.htm`.

[33] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen. Comparison of industrial wsn standards. *4th IEEE International Conference on Digital Ecosystems and Technologies*, April 12-15 2010. Dubai, Unites Arab Emirates.

[34] T. Sauter. *Fieldbus Systems: History and Evolution*, chapter 13 of Integration Technologies for Industrial Automated Systems. CRC Press, 2006. Edited by Richard Zurawski.

[35] Z. Shelby and C. Bormann. *6LoWPAN: The Wireless Embedded Internet*. Wiley, 2009.

[36] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt. Wirelesshart: Applying wireless technology in real-time industrial process control. *IEEE Real-Time and Embedded Technology and Applications Symposium*, 2008. St. Louis, USA.

[37] J. H. Taylor, J. Åkerberg, H. M. S. Ibrahim, and M. Gidlund. Safe and secure wireless networked control systems. *IEEE Multiconference on Systems and Control*, October 3-5 2012. Dubrovnik, Croatia.

[38] J. H. Taylor and A. Sayda. Prototype design of a multi-agent system for integrated control and asset management of petroleum production facilities. *Proceedings American Control Conference*, June 2008.

[39] T. Whittaker. What do we expect from wireless in the factory? In *ETSI Workshop on Wireless Factory*, December 2008. Sophia Antipolis, France. Cambridge Consultants.