EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Efficient integration of secure and safety critical industrial wireless sensor networks

Johan Åkerberg[1*], Mikael Gidlund [1], Tomas Lennvall[1], Jonas Neander[1] and Mats Björkman[2]

Abstract

Wireless communication has gained more interest in industrial automation due to flexibility, mobility, and cost reduction. Wireless systems, in general, require additional and different engineering and maintenance tasks, for example cryptographic key management. This is an important aspect that needs to be addressed before wireless systems can be deployed and maintained efficiently in the industry.

In this paper, we take an holistic approach that addresses safety and security regardless of the underlying media. In our proposed framework we introduce security modules which can be retrofitted to provide end-to-end integrity and authentication measures by utilizing the black channel concept. With the proposed approach, we can extend and provide end-to-end security as well as functional safety using existing automation equipment and standards, such as Profisafe, Profinet IO, and WirelessHART. Furthermore, we improve the WirelessHART standard with periodic and deterministic downlink transmissions to enable efficient usage of wireless actuators, as well as improving the performance of functional safety protocols.

1. Introduction

Recently the automation industry has shown a strong interest in migrating substantial parts of the traditionally wired industrial infrastructure to wireless technologies to improve flexibility, scalability, and efficiency, with a significant cost reduction. The main concerns about reliability, security, integration, along with the lack of device interoperability, have hampered the deployment rate. To address these concerns, WirelessHART [1], the first open and interoperable wireless communication standard especially designed for real-world industrial applications, was approved and released in 2007. ISA 100.11a is becoming a standard for process automation and factory automation [2]. Many automatic meter reading, automatic metering infrastructure systems are being installed with ZigBee [3] or various proprietary solutions [4,5].

Even though wireless communications offer many benefits, some wired fieldbuses will still remain within industrial communications. Therefore it is necessary to integrate these two technologies such that they interoperate seamlessly. The main problem to solve before wireless communication can be used and deployed efficiently is to develop an efficient and adequate solution for integrating wireless communication with existing fieldbuses and emerging field networks while supporting functional safety and security. This would enable an expansion of the communication effectively into areas where wired communication has challenges with respect to cost, mobility, or mechanical wear.

Most of the research work done in the field of wireless extension to traditional fieldbus communication lack in giving a complete solution to efficient integration. This article proposes a complete framework for providing secure and safe communication in wireless/wired networks. On top of that, we present a solution: periodic and deterministic transmissions from gateway to actuators in a WirelessHART network, which has never been shown before.

Related work: Industrial communication has progressed enormously in the last decade with the replacement of the traditional one-to-one connections between sensors/actuators and controllers by networked connections. In wired fieldbus communication, functional safety, security, and integration have been addressed with respect to Profibus and Profinet [[6], and the references therein]. In [7], Dzung et al. present a detailed survey about the security situation in the automation domain. In [8], Jasperneite and Feld describe Profinet and the usage in automation, which serves as a good introduction to the area. In addition, they

* Correspondence: johan.akerberg@se.abb.com
[1]ABB AB, Corporate Research, Forskargränd 7, 721 78 Västerås, Sweden
Full list of author information is available at the end of the article

propose two different approaches for tight integration of Profibus and Interbus using Profinet IO.

Wireless extensions of automation networks and fieldbuses have been researched in different forms. Willig et al. discuss many issues and solutions related to wireless fieldbus systems [9]. In [10], Gungor and Hancke present the state-of-the-art of industrial wireless sensor networks and open research issues. In [11], Vitturi et al. present results from an experimental evaluation using experimental industrial application layer protocol on wireless systems. In [12], Ishii presents results on multiple backbone routers to enhance reliability on wireless systems for industrial automation. In [13], Miorandi and Vitturi analyzed the possibilities of implementing Profibus DP on hybrid wired/wireless networks, based on Ethernet and Bluetooth, respectively. In [14], Sousa and Ferreira discussed and described the role of simulation tools in order to validate wireless extensions of the Profibus protocol. Other related research work on wireless extensions for traditional Profibus can be found in [15-22].

Recently, WirelessHART has received a lot of attention in both academia and industrial automation. In [23], Lennvall et al. presented a performance comparison between the WirelessHART and ZigBee standards. Their conclusion was that ZigBee is not suitable for wireless industrial applications due to poor performance, and security is optional while in the WirelessHART standard it is mandatory. Security in industrial wireless sensor networks have been heavily discussed and in [24], Raza et al. presented a security analysis of the WirelessHART protocol against well known threats in the wireless media. WirelessHART has also been considered for control applications in process automation [25]. In [26], Nixon et al. presented an approach to meet the control performance requirements using a wireless mesh network (e.g., WirelessHART). Their main conclusion was that device and network operation must be synchronized.

Functional safety and communication in open transmission systems have been laid down in IEC 62280-2 [27], and Deuter et al. address this in their work with Virtual Automation Networks (VAN) [28]. In [29], Trikaliotis and Gnad evaluate different mapping solutions for WirelessHART integration. However, their work has not considered how to deal with WirelessHART specific functionality, engineering efficiency, or secure and safety-critical communication. There are ongoing standardization activities for integrating WirelessHART devices into Profibus/Profinet networks within Profibus International and wireless cooperation team. However, the main difference is that we take a holistic approach including safety and security that is not considered for standardization so far.

Contributions: Our detailed contributions in this paper can be summarized as follows:

- We propose and demonstrate a framework for wired and wireless communication addressing both functional safety and security. The framework is based on the black channel [30] concept and provides end-to-end security using security modules and existing functional safety protocols.
- We demonstrate the proposed framework with a proof-of-concept implementation using Profisafe, Profinet IO, and WirelessHART using an industrial control system. The integration method allows security and safety-related configuration to be engineered and downloaded to the WirelessHART network. This approach is novel as previous work has not considered security nor safety.
- We propose a new service called *periodic downlink transmission* for WirelessHART, that enables periodic and deterministic transmissions from gateway to WirelessHART actuators. This service enables the use of wireless actuators to be part of a control loop, or actuators with timing constraints. In addition, the service improves the safety function response time with a factor of 8, when using Profisafe on WirelessHART.

Outline: The reminder of the paper is organized as follows. In Section 2 the basics of the most important technologies used in this paper are introduced. In Section 3 we present a framework for safe and secure communication. In Section 4 we use the proposed framework, to realize and evaluate safe and secure communication using Profinet IO, WirelessHART, and Profisafe. Then, in Section 6 we propose an improvement for WirelessHART to enable periodic and deterministic data transfer to actuators, which is of importance for wireless control. Finally, in Section 7 we conclude the paper.

2. Preliminaries

In this section we will present the basics of the technologies used in this paper. We start with the industrial Ethernet protocol Profinet IO, then we present the WirelessHART technology. Finally we introduce the safety protocol Profisafe.

A. Profinet IO

Profinet IO is one of the Ethernet-based fieldbus protocols from the IEC 61784 standard and is the successor of Profibus. Profinet IO uses switched 100 *Mbit/s* networks to transmit both real-time and non real-time data. For non real-time communication, Remote Procedure Calls (RPC) are used on top of UDP/IP. For real-time data, a dedicated layer is defined on top of Ethernet. The application layer can either communicate via RPCs or directly on the real-time channel [31-33].

The Profinet IO device model assumes one or several Application Processes (AP) within the device. Figure 1 shows the internal structure of an AP for a modular field device. The AP is subdivided into as many slots and subslots as needed to represent the physical I/Os of the device. The structure of an IO-Device is described in a General Station Description (GSD) file [34]. By importing the GSD file into the control system, knowledge is gained regarding the device, for example modules, submodules, parameters, and data types. With this information the engineering tools of the control system can generate the configuration necessary for communication with the device.

Profinet IO uses virtual local area network (VLAN) [35] on top of the Ethernet layer to be able to prioritize real-time frames over non-real-time frames in the switches. The Profinet IO real-time protocol resides on top of the VLAN layer. The Profinet IO Payload Data Unit can carry at most 1412 bytes I/O data including IO Producer Status (IOPS) and IO Consumer Status (IOCS) [32]. The upper restriction in I/O length is due to the fact that a Profinet IO real-time frame must fit into one Ethernet frame to avoid fragmentation of messages.

B. WirelessHART

WirelessHART is a reliable and secure mesh networking technology designed for process measurement, control, and asset management applications. It operates in the 2.4 *GHz* ISM band, utilizing IEEE 802.15.4 compatible direct sequence spread spectrum (DSSS) radios, channel hopping, and time division multiple access (TDMA). All devices are time synchronized and communicate in prescheduled fixed length time-slots. Time slots are grouped together into superframes which are repeated according to a specified rate.

WirelessHART is a robust network technology which provides 99.9% end-to-end reliability in industrial process environments [1]. This is achieved through the use of channel hopping and self-healing capabilities of the mesh network. When paths deteriorate or become obstructed the self-healing property of the network ensures it will repair itself and find alternate paths around obstructions.

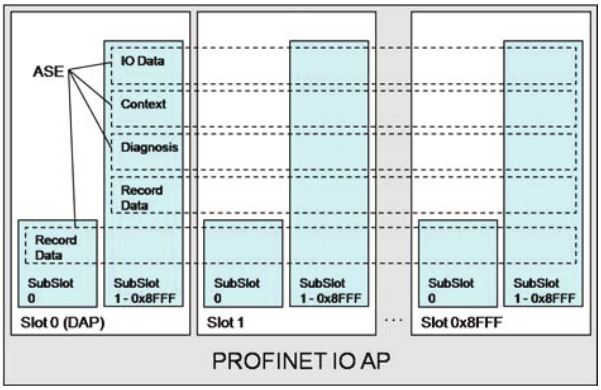

Figure 1 Profinet IO device model.

Every WirelessHART network consists of five types of devices:

(1) A *gateway*: It connects the control system to the wireless network.
(2) An *access point*: Is usually part of the gateway and acts as the radio interface, and multiple AP's are making it possible to communicate on different channels in parallel.
(3) A *network manager*: Is normally part of the gateway and is responsible for managing the wireless network.
(4) A *security manager*: Manages and distributes security encryption keys, and also holds the list of devices authorized to join the network.
(5) *Field devices*: These are devices directly connected to the process (measurement and control), or equipment (asset monitoring) or adapters which connects wired HART devices to the wireless network (retrofit).

WirelessHART is a secure and reliable protocol, which uses the advanced encryption standard (AES) with 128 bit block ciphers. A counter with Cipher block chaining message authentication code mode (CCM) is used to encrypt messages and calculate the message integrity code (MIC). The standard supports end-to-end, per-hop, and peer-to-peer security. End-to-end security is provided on the network layer, while the data link layer provides per-hop security between the two neighboring devices. Peer-to-peer security is provided for secure one-to-one sessions between field devices and handhelds during configuration. WirelessHART devices need a join key to join the network securely. The join key can be individual, or the same for the complete network. When a device joins the network for the first time, the join key needs to be programmed via a local port.

C. Black channel and Profisafe

Most industrial safety protocols for fieldbus communication are based on the principle of the *black channel* [36], using the experience from the railway signaling domain [27,37]. Safe applications and non-safe applications share the same standard communication system, the black channel, at the same time. The safe transmission function, e.g., the safety layer, comprises all measures to deterministically discover all possible faults and hazards that could be infiltrated by the black channel, or to keep the residual error probability under a certain limit

without relying on services provided by the network. Therefore, the black channel principle limits the certification effort to the safe transmission functions, i.e., the safety nodes and their safety layers, as they do not rely on the standard transmission system which includes switches, routers, gateways, transmission protocols, etc. The principle of the black channel is visualized in Figure 2. In comparison, a *White Channel* approach requires all components, including network components, involved in the safety function to be subject to safety certification, and is therefore a less attractive alternative with respect to cost and life cycle management.

Profisafe [38] is one of four safety protocols described in the IEC 61784-3 standard [36]. Profisafe, or functional safety communication profile 3/1 (FSCP 3/1) as it is referred to in the IEC 61784 standard [38], can be used with both Profibus and Profinet. Profisafe's way of safety communication is based on the principle of the black channel. Figure 3 illustrates the Profisafe protocol layer, and Profisafe comprises all measures to deterministically discover all possible faults and hazards that could be infiltrated by the black channel, or to keep the residual error probability under a certain limit [38]. Profisafe is approved for application on black channels with a bit error probability up to 10^{-2} [38]. As illustrated in the figure, the safety layer is maximum 5 bytes long (Control Byte, and Cyclic Redundancy Check 2 [CRC2]), where the CRC2 protects the integrity of process data, as well as the safety-related configuration (F_Parameters). In addition, a control/status byte is used to control and supervise the safety function. A toggle-bit resides within the control byte, and is used to synchronize the safety layer, and indirectly to trigger timeouts in the safety layer. The virtual consecutive number (VCN) is used to deal with unintended repetition, incorrect sequence, loss, and insertion of messages, as well as memory failures within switches. The VCN is incremented on each edge of the toggle-bit, and the CRC2 includes the CRC1 and VCN to reduce the safety layer overhead. For a more thorough description of Profisafe, see [38-40].

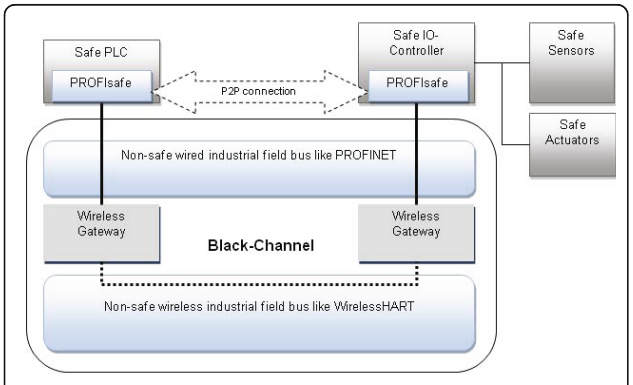

Figure 2 The black channel principle, where safety-related and non safety-related communication co-exist on the same standard transmission system (Profinet and WirelessHART). The black channel is excluded from functional safety certification as the safe transmission function (Profisafe) comprises all of the measures to deterministically discover all possible faults and hazards that could be infiltrated by the black channel.

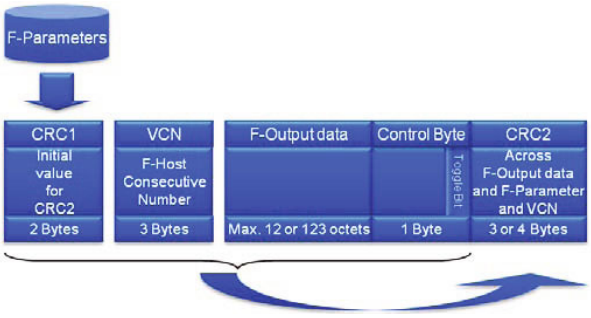

Figure 3 Illustration of the Profisafe protocol layer.

3. Proposed framework for safe and secure communication

In wired fieldbus communication, most fieldbus protocols provide a safety protocol that can be used to fulfill functional safety requirements. Wireless technologies mostly come with a security solution due to the nature of the open media. However, the security measures and capabilities are technology dependent, ranging from optional security (ZigBee) to an extensive and mandatory part of the technology (WirelessHART). Using both wired and wireless fieldbus technologies to complement each other cause many new challenges, especially with respect to integration and maintenance, but also with safety and security considerations as illustrated in Figure 4. In addition, the figure illustrates the gap between safety and security with respect to the media, i.e., no security measures in the wired segments and no safety measures in the wireless segments. It is of vital importance to achieve "seamless integration" of wired and wireless communication, to increase design, engineering, and maintenance efficiency. In industrial settings, different technologies will most probably be deployed even in the future, as it is extremely difficult to solve all industrial requirements with one standard/protocol. Therefore, we present a framework to deal with safety and security in heterogeneous networks, that hides the technical underlying differences, and provides a unified approach for safety and security.

In order to address the issues with respect to safety and security, regardless of the type of media, i.e., wired or wireless, we propose a framework based on the principle of the black channel. The proposed framework uses the principle of the black channel, where each layer comprises all measures necessary to fulfill the safety or security requirements,

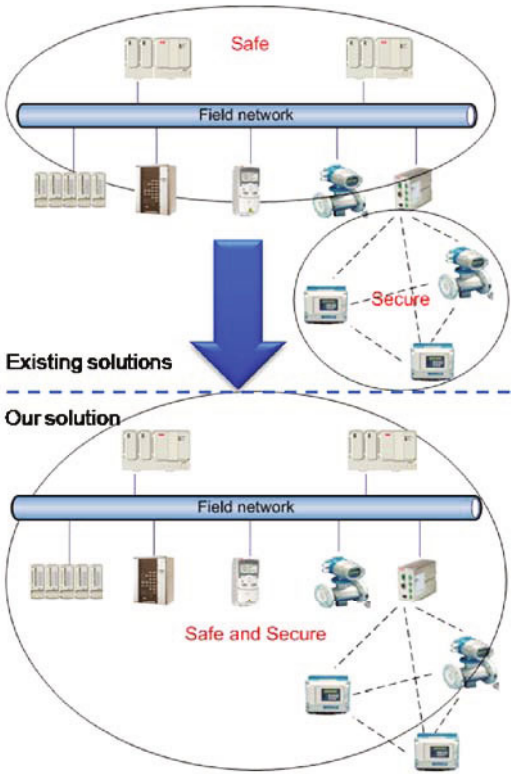

Figure 4 The *upper part* of the figure illustrates the current situation, where security is generally only considered in wireless communication and safety is considered in wired communication. The *lower part* illustrates the desired situation provided by the proposed framework, where safety and security are considered regardless of communication media.

Figure 5 The figure illustrates the proposed framework for safe and secure communication, where the Security Layer treats the Fieldbus Layer as a black channel, and Safety Layer treats the Security and Fieldbus Layer as a black channel. Security and/or Safety can be added depending on the actual requirements and needs.

without relying on services provided by other layers, thus reusing existing automation equipment and transmission protocols. The framework concerns equipment found within the context of an automation system on the field network level, i.e., Programmable Logic Controller (PLC), Distributed Control System (DCS), actuator, sensor, wired fieldbus, and in addition wireless networks. Figure 5 illustrates the proposed method, where a security layer is added between the communication layer and the application layer, using the communication layer as the black channel. The security layer is not added within the scope of the Open Systems Interconnection model (OSI model), but rather between the OSI model and the application to avoid conflicts with standards and to allow end-to-end security. In the same manner the safety layer is used between the communication layer, or security layer depending of the usage of the security layer. For safety certification reasons, the security layer is part of the safety layer's black channel. Within the proposed framework, safety and security layers can be utilized independent of each other and are deployed based on the current requirements. This approach enables end-to-end security as well as safety, without adding any safety or security requirements on the transmission media. Furthermore, our approach suits both modular field devices such as distributed I/O's and compact devices such as field instrumentation. Within a modular device, the safety/security layers are deployed, using the device access point and backplane buses as a black channel. In the case of a modular I/O, both safe, secure, and traditional I/O modules can co-exist independent of the safety/security layers. Our approach enables a broad range of applications where safety/security enabled devices can co-exist with already existing field devices. With our approach, the safety layer and security layer can be used independently and be deployed according to the specific requirements. Furthermore, the safety and/or security layer can be deployed on node-to-node basis, and co-exist on the same hybrid transmission system for full flexibility.

As in the case of safety protocols, our approach adds more or less redundancy in certain layers depending on the functionality provided by the black channel. The advantage of our proposed framework is that the underlying technologies and standards belonging to the black channel do not have to provide specific functionality, as the upper layers do not rely on them. To exemplify, if a security layer is added, there will in some cases be a redundancy in the wireless segment, but the wired segment will be protected. The trade-off for end-to-end security could be partially overlapping security measures. However, end-to-end security is achieved even if there is partial security in a subsystem. Nevertheless, a certain degree of redundancy with respect to security is desired. For example, security measures in the wireless segments need a secure mechanism for joining the network for authorized access. Secondly, a common term in the context of security is *defense-in-depth*, i.e., several layers of security mechanisms are deployed to make it more difficult to bypass the security measures. Therefore, redundancy with respect to security, or in other words, defense-in-depth, has advantages. In summary, our proposed

framework is based on the black channel and provides a general solution for end-to-end security and safety in wired/wireless networks and is transparent to the underlying transmission media.

4. Seamless integration of safe and secure wired/wireless communication

In this section we demonstrate our proposed framework using existing automation equipment and standards, addressing safety and security, using Profinet IO, Profisafe, and WirelessHART. In order to retrofit security in Profinet IO we introduce a concept called *security modules* [41]. In this work, we have chosen the aforementioned technologies, but other technologies can also be used, since our proposed framework is technology independent. Different technologies (ISA100.11a, IEEE 802.15.4) will most likely achieve a different level of integration, engineering efficiency, and run-time performance, but still achieve safe and secure end-to-end communication.

It is not sufficient today in the industry only to provide gateway (GW) functionality, since that introduces a set of challenges for the end-users during the complete life-cycle. When new technologies are introduced, either as replacement or as a complement to existing technologies, it is expected that the new technologies and solutions are equivalent to or better than existing technologies and solutions. Therefore we start by presenting an integration method, which allows seamless integration of WirelessHART in automation systems using Profinet IO.

A. Communication model

From the Profinet IO device model, illustrated in Figure 1, it can be seen that a subslot (instance of a submodule) allows for example both IO Data and Record Data, where the former is used to transport process values from and to the devices, and the latter to transport device configuration data. It is also possible for subslots to transfer diagnostic data, such as process or device alarms. Hence, the concept of subslots (submodules) is central in modeling Profinet IO devices. The concept of a slot (instance of a module), will be treated as a container grouping subslots into physical or logical units.

Due to the unique properties of a subslot, we model physical WirelessHART devices as modules, and WirelessHART functionality as submodules. The main advantage with this approach is that we can separate functionality from a device. Thus we can model the WirelessHART functionality as submodules, such as HART commands, independent of a specific device. Then the devices are modeled as modules, independent of their capabilities, and we assign the capabilities (submodules) that are supported by that device (module). Secondly, our approach allows parametrization, diagnostics, and process data for each WirelessHART function which is illustrated in Figure 6.

Furthermore, we model the network manager as one module with two different submodules. The *Network ID* submodule only contains Record Data (configuration data) to allow the DCS to download the Network ID to a specific network manager. The second submodule holds the configuration data of the *Join Key* to be used by the network manager in the joining phase of WirelessHART devices. Additional functionality that needs to be remotely configured by the DCS can be modeled and extended in the same manner. In this way, we can engineer and distribute configuration data to the network managers from a central location, using existing engineering tools. The second module in Figure 6, *Field Device*, contains three different submodules. The first submodule has only configuration data containing the *Tag Name* of the WirelessHART device which is used by the gateway to automatically map a specific Profinet IO slot/subslot to the corresponding WirelessHART device. As illustrated in Figure 7, the gateway resolves the addresses of the WirelessHART devices by querying the devices for their *Tag Name* and maps them into slots using the actual *Tag Name* stored in the subslots.

The last submodules represent different *HART Commands* that have IO Data and Record Data, i.e. *burst rate, burst mode, burst message, and safety related configuration*, that the DCS will download to the WirelessHART device. In this way, all WirelessHART devices

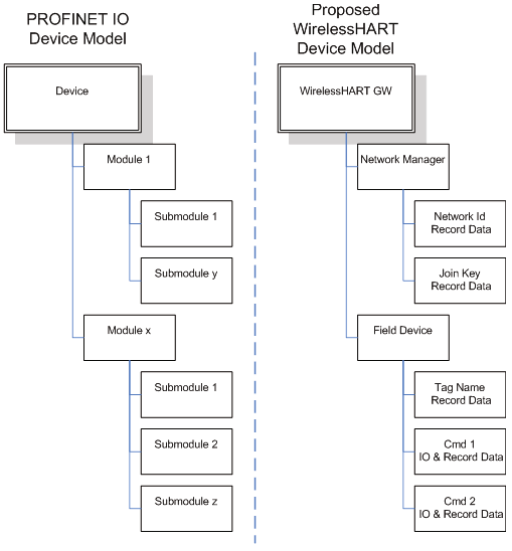

Figure 6 WirelessHART physical or logical devices are modeled as modules, and the module indicates the communication status of the device. WirelessHART functionality is modeled as submodules, which can communicate configuration data (Record Data Items) and/or process values (IO Data). The submodules can also indicate their status for additional status information.

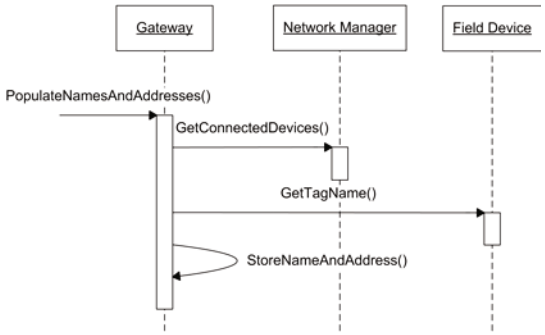

Figure 7 The WirelessHART gateway queries the network manager for a list of active WirelessHART devices. Using the list of active devices from the network manager, the gateway queries the active devices for their tag names. Now the gateway can map the device network address to a Profinet IO slot.

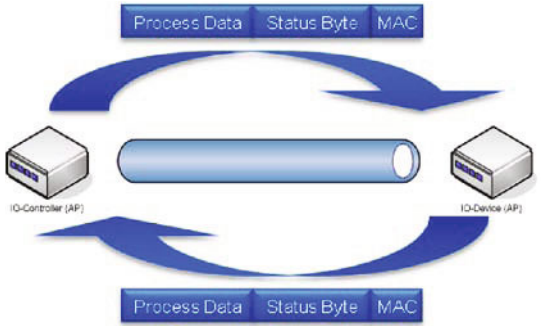

Figure 8 An example where security modules protect the integrity and authentication of the process data transmitted on Profinet IO.

and HART Commands can be modeled, and most important be configured and maintained in a central engineering system.

The main advantage of our proposed integration method is that the already existing engineering tools in the DCS can be used to engineer and maintain the WirelessHART networks at a central location, in the same way as existing field devices. In addition, engineering and maintenance of the WirelessHART devices is simplified, as the configuration will be automatically downloaded after replacement of faulty components, thus reducing the down time. Moreover, the separation of HART commands, physical and logical units in the model simplifies both the design of the gateway and most important the usage of the gateway when considering safety and security. Other existing integration work or methods can be used as well, but will most probably not be beneficial to use with respect to safety, end-to-end security, as well as engineering and maintenance efforts of the latter.

B. On-demand configuration data

$$WDTime_i = \begin{cases} OFDT & \text{if } i = s \text{ (sensor } F\_Device) \\ F\_WD\_Time_{sensor} + WCDT_{F\_Host} + T_{cyF\_Host} & \text{if } i = sb \text{ (sensor bus)} \\ OFDT + WCDT_{F\_Host} & \text{if } i = h \text{ (} F\_Host) \\ F\_WD\_Time_{actuator} + WCDT_{F\_Device} + DAT & \text{if } i = ab \text{ (actuator bus)} \\ OFDT & \text{if } i = a \text{ (actuator } F\_Device) \end{cases} \quad (1)$$

To reduce the possibility that cryptographic keys are compromised, they should ideally be distributed once. In addition, the cryptographic keys should be updated on a regular basis to avoid that the keys are identified from the ciphertext (Figure 8).

Our solution transmits the keys on-demand in plain text from the engineering station to the WirelessHART gateway, by using the Discovery and Configuration Protocol (DCP) provided by Profinet IO. The keys are programmed in non-volatile memory in the WirelessHART gateway by using write-only Manufacturer Specific Parameters, and are distributed by the WirelessHART gateway in ciphertext to the WirelessHART devices. Doing it in this way, the cryptographic keys are assigned in the same way, using the same engineering tool, as IP-addresses for Profinet IO field devices without any changes in the Profinet IO standard. security modules use the same concept [41], and this enables a simple key distribution mechanism for Profinet IO and WirelessHART. Distribution of security-relevant data should in general be transmitted with additional protection compared to for example IP-addresses. However, this additional protection, e.g., encryption, needs major changes in the Profinet IO standard and has therefore neither been further investigated nor implemented. This approach supports the process of automatic key updates, by replacing the manual process with an automatic service that updates the keys on a regular basis. The join key and the Network ID of the WirelessHART Device must initially be configured via some local port for security reasons; otherwise the WirelessHART Device cannot join the network and create a secure channel for key updates. Key distribution is mostly the weakest link, even in this case, and is a general and known problem within the area of automation. Our proposed solution is to be treated as an intermediate solution for key distribution until a proper standard suiting the needs of automation is developed. Nevertheless, our proposed solution bridges an important gap towards security for automation equipment at field level.

C. Communication with security modules

Security for industrial field networks is also important when deploying a defense-in-depth strategy. *security modules* [41] is a concept that makes it possible to retrofit a security layer on top of Profinet IO, without changing the underlying transmission system or standards. By using security modules on top of Profinet IO, end-to-end network security can be achieved and ensure

authentication, integrity and confidentiality for real-time communication. security modules are modeled in the GSD file in addition to the already existing modules. In this way, depending on the actual security risk assessment, security modules or standard modules can be instantiated and coexist. The security modules extend the I/O data with a security layer, mainly to protect the integrity and authentication of the I/O data in Profinet IO. The cryptographic keys to be used with security modules are distributed using the same method as described in Section 4-B. Thus, the concept of security modules fits nicely together with the WirelessHART integration using Profinet IO. By combining security modules with the proposed WirelessHART integration, we consider security both for wired and wireless fieldbus communication, using the principle of the black channel.

D. Safety function response time

One of the most important metrics for safety-critical applications is the time between a detected error and the transition to a safe state. In Profisafe, the Safety Function Response Time (*SFRT*) specifies the worst-case time before a safe state is achieved in the presence of errors or failures in the safety function [38]. Depending on the application, the requirements of *SFRT* range from milliseconds to seconds. The *SFRT* for our approach can be described and derived, using the same notation as in IEC 61784-3-3, as follows.

The total safety function delay consists of delays from several entities, i.e., sensor (*F_Device*), actuator (*F_Device*), bus, and DCS (*F_Host*), which adds up to the total delay. The delay from each entity i varies between a best case and a worst case delay time, denoted as $WCDT_i$. For safety reasons every entity has a watchdog timer $WDTime_i$ which takes necessary actions to activate the safe state whenever a failure or error occurs within the entity [38]. The particular equations for the entities i of $WDTime_i$ are shown in (1), where OFDT is defined as the One Fault Delay Time and Tcy_{F_Host} is the period time of the DCS. The Device Acknowledgment Time (*DAT*), is the time required to process a new safety PDU based on current process values when a new VCN is recognized. Finally, the failsafe watchdog timeout *F_WD_Time* for Profisafe is defined as [38]

$$F\_WD\_Time = 2Tcy + DAT + HAT, \quad (2)$$

where *Tcy* is the period time for bus transmissions, and the host acknowledgment time (*HAT*) is the time required to create a new safety PDU with the following VCN when an acknowledgment from the device is detected. The *F_WD_Time* for Profisafe is given in (2) but since our approach includes WirelessHART we need to extend (2) as follows

$$F\_WD\_Time = 2Tcy_{PNIO} + 2Tcy_{WH} + DAT + HAT + WCDT_{GW}, \quad (3)$$

where Tcy_{PNIO} is the period time of Profinet IO, and Tcy_{WH} is the period time of WirelessHART, and finally $WCDT_{GW}$ is the worst case delay time of the Profinet IO/WirelessHART gateway.

Given n entities, the SFRT for our proposed approach can be calculated as follows [38]

$$SFRT = \sum_{i=1}^{n} WCDT_i + \max_{i=1,2,\ldots,n}(WDTime_i - WCDT_i), \quad (4)$$

where $\sum_{i=1}^{n} WCDT_i$ defines the total worst case delay time and $\max_{i=1,2,\ldots,n}(WDTime_i - WCDT_i)$ adds the maximum difference between an entity's watchdog time-out and worst case delay time. Thus, the *SFRT* is the sum of all worst case delays and the largest watchdog margin to avoid spurious failsafe trips.

5. Implementation and performance evaluation

The proof-of-concept implementation consists of the automation system 800xA communicating to a WirelessHART gateway using Profinet IO. One WirelessHART device is connected to the WirelessHART network. The reason for the minimalistic test setup is to measure the safety function performance in an controlled environment, e.g., easier to identify bottlenecks and limiting parameters. The performance evaluation scenario can easily be extended to more realistic setups whenever needed. Several measurements have been performed on the proof-of-concept implementation with different settings of the burst rate Tcy_{WH} of the WirelessHART device given in (5), i.e., the period time of updates sent from the WirelessHART device, in order to measure the total achieved safety function response time. The security layer is part of the black channel, and is therefore not explicitly mentioned in the performance evaluation. The security evaluation is rather dependent on the cryptographic algorithms used and is not covered in this paper. However, in addition to the safety-critical data an additional MIC is transmitted in order to provide end-to-end authentication and integrity of the packet, which do not have a significant contribution to the overall run-time performance.

$$Tcy_{WH} = \{500,\ 1000,\ 2000,\ 3000,\ 4000,\ 5000\}\,[ms] \quad (5)$$

The frequency distribution of the period times are shown in Figure 9. In the upper part of the picture, the frequency distribution of the time between two consecutive WirelessHART telegrams Δt_{WiHART} sent from the

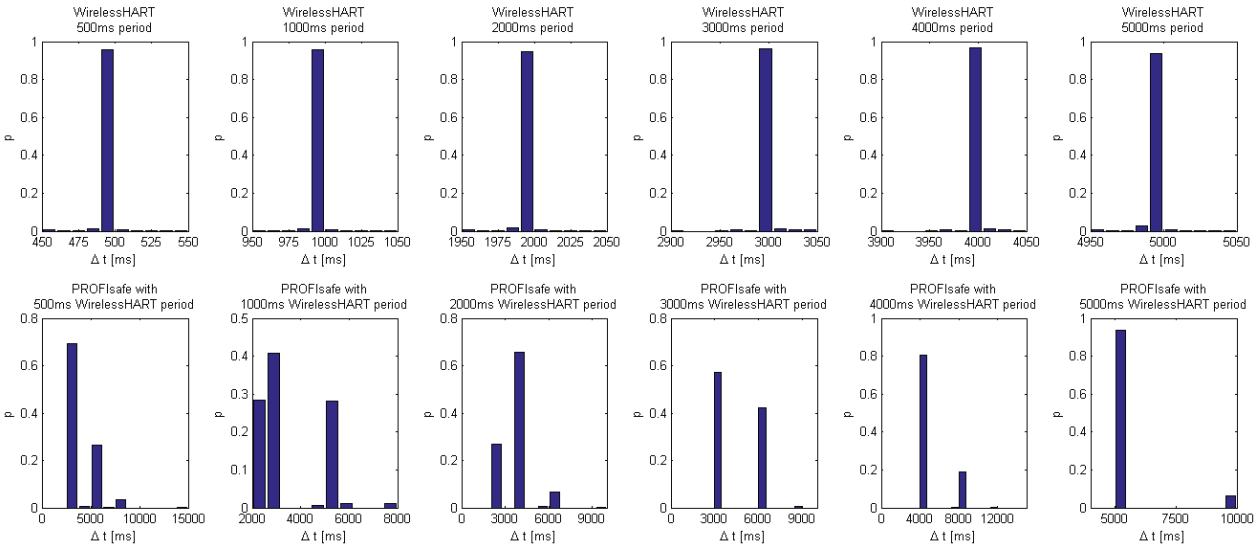

Figure 9 The *upper graphs* show the frequency distribution of the time between consecutive WirelessHART telegrams, $\Delta t_{W\ i\ H\ A\ RT}$, at different WirelessHART period times, $Tcy_{W\ H}$. The *lower graphs* show the frequency distribution of the time between transitions on the Profisafe toggle-bit, $\Delta t_{Profisafe}$, at the same WirelessHART period times, $Tcy_{W\ H}$, as in the upper graphs. The population size for $\Delta t_{Profisafe}$ is ≥ 1200 for all $Tcy_{W\ H}$.

WirelessHART device are plotted with the values of $Tcy_{W\ H}$ given in (5). In the same way, the frequency distribution of the measurements of the time between two transitions of the Profisafe toggle bit $\Delta t_{Profisafe}$ is plotted in the lower graphs, with Tcy_{WH} as given in (5). The toggle bit is used to synchronize the Profisafe state-machines, and is therefore also indirectly used for detection of protocol timeouts [38], thus it serves as a performance indicator. By comparing $\Delta t_{W\ I\ H\ A\ RT}$ and $\Delta t_{Profisafe}$ in Figure 9, it is obvious that downstream data to the device is transmitted on a best-effort basis, while the upstream data is transmitted on a periodic basis. Analyzing the frequency distribution of $\Delta t_{Profisafe}$, when $Tcy_{W\ H} \geq 3000\ ms$, it can easily be seen that the probabilities are distributed as multiples of $Tcy_{W\ H}$ (Figure 10).

Figure 11 shows the average time between transitions of the Profisafe toggle bit given $Tcy_{W\ H}$, $\overline{\Delta t_{Profisafe}}$, derived from the measurements. The most obvious observation is that $\overline{\Delta t_{Profisafe}}$ does ot correspond to $Tcy_{W\ H}$. The main reason for this is that WirelessHART does not provide periodic services from the gateway to the device. In addition to this, delays due to execution time in network components, devices, and unsynchronized tasks in the nodes add further delays. However, those delays are not visible in the graph until $Tcy_{WH} \geq 5\ s$, as the downlink transmissions are sent on best-effort basis. Sending commands from the DCS to the WirelessHART device and back takes approximately $3.4 \pm 1.4\ s$, derived from the measurements of the toggle bit when $Tcy_{W\ H} = 500\ ms$, and is order of magnitudes larger than the delays caused by network components. In comparison, sending periodic telegrams from the device to the

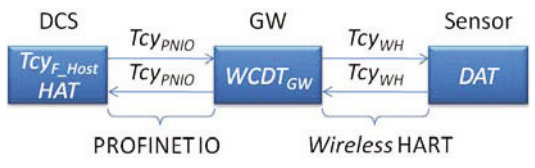

Figure 10 Test setup used for the performance evaluation using the settings from Table 1 and values of $Tcy_{W\ H}$ as given in (5).

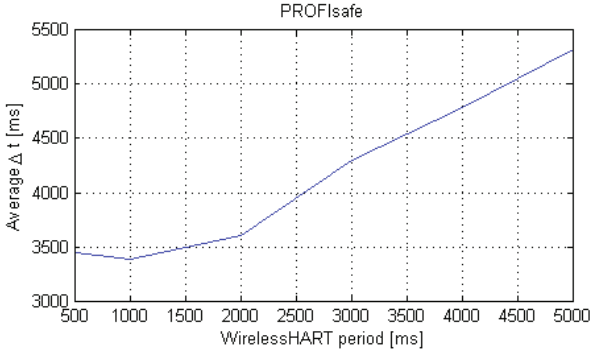

Figure 11 The graph shows the average time between transitions on the Profisafe toggle-bit given $Tcy_{W\ H}$, $\overline{\Delta t_{Profisafe}}$.

network manager takes 500 ± 5.6 *ms* derived from the measurements given that $Tcy_{W\ H}$ = 500 *ms*.

Based on the measurements, the *SFRT* can be calculated to 14.5 *s* using (1), (3), and (4), given the values in Table 1. A minimum SFRT of 14.5 *s* is a long time in automation (with SFRT typically in the range of milliseconds to seconds depending on the safety application requirements), and more nodes in the wireless network will significantly increase the SFRT to an extent where few application would benefit of wireless safety functions using current standard, e.g. the SFRT is derived from the application requirements. It should be noticed that the safety integrity level is achieved with the proposed approach. Instead of more detailed performance measurements, conducted in a minimalistic setup, we will analyze how to improve and achieve a deterministic $Tcy_{W\ H}$ without interfering with the self-healing attributes of WirelessHART. By improving $Tcy_{W\ H}$ we can shorten the minimum SFRT, thus enabling further applications without weakening the safety integrity, due to the principle of the black channel.

6. Periodic downlink transmission in WirelessHART

Based on the observations from the proof-of-concept implementation, we extend WirelessHART services in this section to support deterministic and periodic downlink transmissions to allow actuators and safety protocols more efficiently.

The WirelessHART standard targets industrial control system applications, thus we need to include actuators as a part of WirelessHART, to enable it to be used in representative industrial applications. Typically actuators require deterministic communication, thus best-effort communication is not sufficient in most cases.

A. Distributed control systems and WirelessHART

Traditionally, DCS periodically acquire data from sensors, execute a control application, and finally set the output values for the actuators. Typical period times for DCS's in process automation range from 250*ms* to 1*s*; however both faster (10 *ms*) and slower (5 *s*) period times exist. In the case where the period time is in the range of 10 *ms* WirelessHART is not the technology to be used. In that case, WISA can be used that is designed for update rates down to 10 *ms* [22].

Table 1 Values used for the calculations of the safety function response time (*SFRT*)[1].

Variable	Value	Description
OFDT	6 *ms*	One fault delay time
DAT	6 *ms*	Device acknowledgment time
HAT	6 *ms*	Host acknowledgment time
Tcy_{F_Host}	50 *ms*	Period time of DCS
Tcy_{PNIO}	128 *ms*	Period time of Profinet IO
Tcy_{WH}	3400 *ms*	Period time of WirelessHART
$WCDT_{F\_Host}$	100 *ms*	Worse case delay time of DCS
$WCDT_{GW}$	50 *ms*	Worse case delay time of GW

[1]See IEC 61784-3-3 for the definitions of the variables

The WirelessHART standard defines a method to set up efficient and periodic data transfer (≥ 250 *ms*) from a sensor to the gateway called *burst mode*. However, there is no definition for how to initiate efficient and periodic data transfer in the opposite direction (gateway to actuator), i.e. the standard lacks HART commands to initiate periodic data transfer to actuators. WirelessHART allows the use of proprietary methods to add functionality and therefore it is possible to provide efficient data transfer from the gateway to actuator. Unfortunately, current gateway/network manager vendors have focused on efficient data transfer from sensors to the gateway and therefore there is no support for the needed data transfer solution in the opposite direction. In fact, initial experiments point to vendors providing a solution which is shown in Figure 12. The figure shows a superframe which is scheduled with links (time slots), S_1, S_2, ..., S_n, for acquiring data from the sensors to the control application, and links, A_1, A_2, ..., A_n, for sending data from the control application to the actuators. As can be seen in the figure, all sensor data can be acquired within one superframe cycle, but it takes *n* superframe cycles to send data to all the actuators. In the schedule, we can see that the actuators are forced to share the same outgoing link. Furthermore, the time for the actuator to receive the data from the gateway triples when the actuator is one-hop away from the gateway. Our conclusion is that the network manager schedules far too few slots per cycle for outgoing traffic, so-called best-effort communication.

Using best-effort communication for distributing set-points for actuators in industrial control systems is far from optimal. To achieve good results from a control perspective, jitter and delays should be reduced as far as possible. All the set-points for the actuators need to be distributed back to the devices within the same cycle.

B. Proposed downlink transmission

We propose a novel solution where the WirelessHART Network Manager can schedule several outgoing slots (downlink transmission) from the gateway to the devices within the same cycle.

The proposed solution includes a new WirelessHART command that the control application can use to request periodic transmissions to be set up to the actuators (outgoing slots). A new WirelessHART command is necessary, as existing commands to initiate periodic transmissions assume that the network manager is the

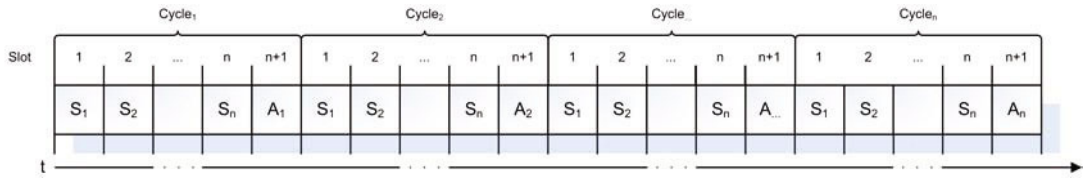

Figure 12 An example of WirelessHART cycles.

data sink. Since the typical period WirelessHART period is 250 *ms* - 1 *s* and a WirelessHART slot is 10 *ms* one can easily deduce that the maximum number of successive slots for an access point ranges from 25 to 100 slots if all nodes have a direct link to the network manager, and use only one channel at a time given the radio constraints. If a DCS serves as many sensors as actuators, there will only fit 12 incoming slots for sensor data, and 12 slots for actuator data, given a period time of 250 *ms*. This is because we only have 25 slots available in 250 *ms*, if all nodes have a direct link to the network manager. The WirelessHART standard communicate on 15 channels, hence, theoretically, adding 14 access points could increase the number of available slots 15 times, if the access points are scheduled to communicate simultaneously on different channels in parallel. Adding several access points make it possible to scale up the number of available slots from 375 to 1500, depending on the assumed period time of 250 *ms* to 1 *s*.

The packet in the WirelessHART standard can only travel one hop per slot. This introduces delays for devices which are several hops away from the gateway. Another issue is that a device usually either only can listen for a packet, or send a packet simultaneously. Relaying other devices' data will decrease the number of available slots, and could even increase the minimum allowed DCS period. Clustering the network is a solution which could reduce delays by creating simple one-hop clusters around several gateways, or Access Points if several are used. However, in order to create good network clustering proper planning of the architecture is important.

Assuming that only the period time of WirelessHART is changed, then ΔSFRT can be calculated using (1), (3), and (4) as follows:

$$\begin{aligned}\Delta SFRT &= SFRT - SFRT' \\ &= \sum_{i=1}^{n} WCDT_i + \max_{i=1,2,\ldots n}(WDTime_i - WCDT_i) - \\ &\left(\sum_{i=1}^{n} WCDT_i + \max_{i=1,2,\ldots n}(WDTime_i - WCDT_i)\right)'\end{aligned} \quad (6)$$

where *SFRT'* is the improved safety function response time. Under the assumptions

$$\begin{cases} Tcy_{WH} > Tcy_{PNIO} \\ WCDT_{F\_Host} > WCDT_{F\_Device} \\ Tcy_{F\_Host} > DAT \end{cases}$$

that are practically sound as the inequalities differ by order of magnitudes in most real installations, we get that

$$\max_{i=1,2,\ldots,n}(WDTime_i - WCDT_i) = WDTime_{sb} - WCDT_{sb},$$

where $WDTime_{sb}$ and $WCDT_{sb}$ are defined as watchdog timer and the worst case delay time between the sensor and DCS, respectively. Therefore (6) can be expressed of as in (7) using the same notation of indexes as in (1).

$$\begin{aligned}\Delta SFRT &= \left(\sum_{i=1}^{n} WCDT_i + WDTime_{sb} - WCDT_{sb}\right) - \left(\sum_{i=1}^{n} WCDT_i + WDTime_{sb} - WCDT_{sb}\right)' \\ &= WCDT_s + WCDT_{sb} + WCDT_h + WCDT_{ab} + WCDT_a + 2Tcy_{PNIO} + 2Tcy_{WH} + DAT + HAT \\ &\quad + WCDT_{GW} + HAT + WCDT_{GW} - 2Tcy_{PNIO} - 2Tcy_{WH} - (WCDT_s + WCDT'_{sb} + WCDT_h \\ &\quad + WCDT'_{ab} + WCDT_a + 2Tcy_{PNIO} + 2Tcy'_{WH} + DAT + HAT + WCDT_{GW} - 2Tcy'_{PNIO} - 2Tcy'_{WH}) \\ &= WCDT_{sb} + WCDT_{ab} - WCDT'_{sb} - WCDT'_{ab} \\ &= 2(2Tcy_{PNIO} + 2Tcy_{WH}) - 2(2Tcy_{PNIO} + 2Tcy'_{WH}) \\ &= 4(Tcy_{WH} - Tcy'_{WH})\end{aligned}$$

Thus we can significantly improve the SFRT by 4(3400 - 250) = 12600 *ms* and reach a *SFRT* of 1.9 *s*, by implementing the improved WirelessHART functionality, as proposed in this paper. The proposed method improves the SFRT by almost a factor 8. In practice the improvement will be much better, since the problem is the downstream data from the WirelessHART GW to the WirelessHART device, which takes approximately 3.4 *s*, which is used for Tcy_{WH} in Table 1. This figure is an average, as the data is transmitted in a best effort manner and the jitter is very high. Thus the proposed improvement will not only contribute to the SFRT, but also minimize nuisance trips, as the jitter will be dramatically improved. The improvement in jitter is expected to be in the same range as shown in the upper graphs of Figure 9 as downlink slots are allocated in advance.

7. Conclusions

Today the wired fieldbuses are complemented with wireless devices and are moving towards the use of wireless infrastructures. Using wireless infrastructures within automation demands solutions with the same properties, such as safety and security, which exist today in the wired case. Today there exists no solution that

considers functional safety for wireless sensor networks and the wired fieldbuses lack security extensions within the context of industrial automation. The lack of these features will become a severe problem since scalable and modular solutions cannot be provided when integrating new wired/wireless devices into existing automation systems.

In this paper we have taken an holistic approach to wireless sensor networks in automation, and propose an integration framework of wireless sensor networks. Our proposal is based upon the principle of the black channel and security modules where safety and security measures can be deployed and co-exist depending of current requirements. security modules is a concept where a security layer, providing measures for end-to-end integrity and authentication that can be retrofitted on existing automation systems. We demonstrate that the proposed framework can be applied on a industrial automation system using Profisafe, Profinet IO, and WirelessHART.

Our performance measurements clearly indicate that periodic and deterministic downlink transmissions from the WirelessHART gateway to the WirelessHART devices are needed. Therefore, we extend WirelessHART with periodic and deterministic downlink transmissions, to deal with this problem. In addition, we also solve the general problem of using WirelessHART for control applications, enabling the usage of WirelessHART actuators that require periodic and deterministic transfer of set-points for successful operation.

8. Competing interests

The authors declare that they have no competing interests.

Author details

[1]ABB AB, Corporate Research, Forskargränd 7, 721 78 Västerås, Sweden
[2]Mälardalen University, School of Innovation, Design, and Technology, Västerås, Sweden

Received: 12 January 2011 Accepted: 18 September 2011
Published: 18 September 2011

References

1. Hart 7 specification (2010), http://www.hartcomm.org/
2. Isa 100, wireless systems for automation (2010), http://www.isa.org/isa100
3. Zigbee alliance (2010), http://www.zigbee.org
4. L Hardy, M Gafen, A new highly-synchronized wireless mesh network model in use by the electric company to switch to automatic meter reading, Case study, in *5th International Conference on Networked Sensing Systems, 2008*. INSS 2008, 31–34 (June 2008)
5. T Zhong, Z Peng, Y Haibin, W Hong, Zigbee-based wireless extension of foundation fieldbus, in *6th IEEE International Conference on Industrial Informatics*, 661–666 (July 2008)
6. J Åkerberg, On security in safety-critical process control, Licentiate thesis, (November 2009). http://www.iss.mdh.se/index.php?choice=publications&id=2081
7. D Dzung, M Naedele, T Von Hoff, M Crevatin, Security for industrial communication systems. Proc IEEE. **93**(6), 1152–1177 (2005)
8. J Jasperneite, J Feld, Profinet: An integration platform for heterogeneous industrial communication systems, in *IEEE Conference on Emerging Technologies and Factory Automation*. **1**, 815–822 (September 2005)
9. A Willig, K Matheus, A Wolisz, Wireless technology in industrial networks. Proc IEEE. **93**(6), 1130–1151 (2005)
10. V Gungor, G Hancke, Industrial wireless sensor networks: Challenges, design principles, and technical approaches, IEEE Trans Ind Elec. **56**(10), 4258–4265 (2009)
11. S Vitturi, I Carreras, D Miorandi, L Schenato, A Sona, Experimental evaluation of an industrial application layer protocol over wireless systems. IEEE Trans Ind Inf. **3**(4), 275–288 (2007)
12. Y Ishii, Exploiting backbone routing redundancy in industrial wireless systems. IEEE Trans Ind Elec. **56**(10), 4288–4295 (2009)
13. D Miorandi, S Vitturi, A wireless extension of profibus dp based on the bluetooth system. Comput Commun. **27**(10), 946–960 (2004). doi:10.1016/j.comcom.2002.01.001
14. PB Sousa, LL Ferreira, Hybrid wired/wireless profibus architectures: Performance study based on simulation models. EURASIP J Wireless Commun Netw. **2010**(Article ID 845792), 25 pages (2010)
15. KC Lee, S Lee, Integrated network of profibus-dp and ieee 802.11 wireless lan with hard real-time requirement. in *IEEE International Symposium on Industrial Electronics*, **3**, 1484–1489 (2001)
16. L Rauchhaupt, System and device architecture of a radio based fieldbus-the rfieldbus system, in *4th IEEE International Workshop on Factory Communication Systems*, 185–192 (2002)
17. A Willig, Polling-based mac protocols for improving real-time performance in a wireless profibus. IEEE Trans Ind Elec. **50**(4), 806–817 (2003). doi:10.1109/TIE.2003.814992
18. C Koulamas, S Koubias, G Papadopoulos, Using cut-through forwarding to retain the real-time properties of profibus over hybrid wired/wireless architectures. IEEE Trans Ind Elec. **51**(6), 1208–1217 (2004). doi:10.1109/TIE.2004.839429
19. J-D Decotignie, Interconnection of Wireline and Wireless Fieldbusses, in *Industrial Electronics Series*, ed. by R Zurawski. The Industrial Information Technology Handbook (CRC Press, Boca Raton, FL, 2005)
20. M Alves, E Tovar, Engineering profibus networks with heterogeneous transmission media. Comput Commun. **30**(1), 17–32 (2006). doi:10.1016/j.comcom.2006.07.011
21. H-J Korber, H Wattar, G Scholl, Modular wireless real-time sensor/actuator network for factory automation applications. IEEE Trans Ind Inf. **3**(2), 111–119 (2007)
22. J Kjellsson, A Vallestad, R Steigmann, D Dzung, Integration of a wireless I/O interface for profibus and profinet for factory automation. IEEE Trans Ind Elec. **56**(10), 4279–4287 (2009)
23. T Lennvall, S Svensson, F Hekland, A comparison of wirelesshart and zigbee for industrial applications, in *IEEE International Workshop on Factory Communication Systems*, 85–88 (May 2008)
24. S Raza, A Slabbert, T Voigt, K Landernäs, Security considerations for the wirelesshart protocol, in *14th International IEEE Conference on Emerging Technologies and Factory Automation*, 1–8 (2009)
25. J Song, S Han, A Mok, D Chen, M Lucas, M Nixon, Wirelesshart: Applying wireless technology in real-time industrial process control, in *IEEE Real-Time and Embedded Technology and Applications Symposium*, 377–386 (April 2008)
26. M Nixon, D Chen, T Blevins, A Mok, Meeting control performance over a wireless mesh network, in *IEEE International Conference on Automation Science and Engineering (CASE)*, 540–547 (August 2008)
27. IEC 62280-2, Railway applications–Communication, signaling and processing systems–Part 2: Safety-related communication in open transmission systems. International Electrotechnical Commission (2002)
28. A Deuter, S Horn, M Wolframm, H Adamczyk, Safety-related data transfer in secure virtual automation networks, in *SICE Annual Conference*, 2208–2214 (August 2008)
29. S Trikaliotis, A Gnad, Mapping wirelesshart into profinet and profibus fieldbusses, in *14th International IEEE Conference on Emerging Technologies and Factory Automation*, 1–4 (2009)
30. J Åkerberg, F Reichenbach, M Björkman, Enabling safety-critical wireless communication using wirelesshart and profisafe, in *IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, 1–8 (September 2010)

31. IEC 61158-5-10, Industrial communication networks–Fieldbus specifications–Part 5-10: Application layer service definition–Type 10 elements. International Electrotechnical Commission (2007)
32. IEC 61158-6-10, Industrial communication networks–Fieldbus specifications–Part 6-10: Application layer protocol specification–Type 10 elements. International Electrotechnical Commission (2007)
33. H Kleines, S Detert, M Drochner, F Suxdorf, Performance aspects of profinet IO. IEEE Trans Nucl Sci. **55**(1), 290–294 (2008)
34. GSDML Specification for PROFINET IO. Version 2.20 (PROFIBUS Neutzerorganisation e.V., Germany, 2008)
35. D McPherson, B Dykes, VLAN Aggregation for Efficient IP Address Allocation. RFC 3069. (Amber Networks, Inc., Milpitas, CA, 2001)
36. IEC 61784-3, Industrial communication networks–Profiles–Part 3: Functional safety fieldbuses–General rules and profile definitions. International Electrotechnical Commission (2007)
37. IEC 62280-1, Railway applications–Communication, signaling and processing systems–Part 1: Safety-related communication in closed transmission systems. International Electrotechnical Commission (2002)
38. IEC 61784-3-3, Industrial communication networks–Profiles-Part 3-3: Functional safety fieldbuses–Additional specifications for CPF 3. International Electrotechnical Commission (2007)
39. J Åkerberg, M Björkman, Exploring network security in profisafe, in *Proceedings of the 28th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '09)* (Berlin, Heidelberg, Springer, September, 2009), pp. 67–80
40. M Miihlhause, C Diedrich, M Riedl, D Schmidt, Formalised specification of a test tool for safety related communication, in *IEEE Conference on Emerging Technologies and Factory Automation, 2007*, 38–44 (September 2007)
41. J Åkerberg, M Björkman, Introducing security modules in profinetio, in *14th International IEEE Conference on Emerging Technologies and Factory Automation*, 1–8 (September 2009)

doi:10.1186/1687-1499-2011-100
Cite this article as: Åkerberg *et al.*: **Efficient integration of secure and safety critical industrial wireless sensor networks.** *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:100.