Interconnecting WirelessHART and Legacy HART Networks

Shahid Raza, Thiemo Voigt
Swedish Institute of Computer Science (SICS)
SE-16429 Kista Stockholm, Sweden
{shahid, thiemo}@sics.se

***Abstract*—WirelessHART is a novel standardized wireless sensor network protocol for industrial process automation. The WirelessHART protocol is designed with the aim to complement the HART protocol by providing wireless extension to it. However, due to the different physical and data-link layers the two protocols are not directly interoperable. WirelessHART is based on IEEE 802.15.4 mesh networks whereas HART is a 4-20mA analog wired protocol. Keeping in view the huge installations of HART networks throughout the world we feel the need to integrate HART and WirelessHART networks as the WirelessHART standard does not specify the means to securely connect the two networks.**

In this paper we provide different options to integrate WirelessHART and legacy HART networks. We start integrating the two networks using a gateway. However, gateway based integrations are sometimes not feasible and are insecure. The main contribution of this paper is that we provide a novel and comparatively secure solution to interconnect WirelessHART networks with HART networks. We specify and design a new WirelessHART Integrator that extends the capabilities of the WirelessHART adapter and provides integration at the network level rather than at the device level only. We also analyze and compare our solution with gateway and adapter based solutions.

I. Introduction

WirelessHART [1] [2] is the first IEC approved international standard for wireless sensor networks designed primarily for wireless communication in the industrial process automation. WirelessHART is not a completely new protocol; rather it is a wireless extension to the Highway Addressable Remote Transducer (HART) protocol [3]. Since 1990, the HART protocol is available as an open protocol for industrial process automation and control. The latest version is HART 7.2 that includes wireless process data transmission and acquisition capabilities and is formally named WirelessHART™.

HART is a widely used protocol in the automation industry. Currently there are thousands of HART networks and millions of HART devices operating throughout the world. To take advantage from legacy HART networks and to be a successful wireless industrial automation standard, WirelessHART networks should be able to interoperate with legacy HART networks. Unfortunately, due to the different physical and data-link layers [4], WirelessHART is not directly compatible with legacy HART despite that the protocols share many common features. The WirelessHART standard provides mechanisms to integrate HART *devices* with WirelessHART networks, but the integration of HART *networks* with WirelessHART *networks* is missing in the standard. In this paper we present different options to connect the WirelessHART network with the HART network. To the best of our knowledge our work is the first attempt towards integrating HART and WirelessHART networks. There have been solutions to connect the legacy other process automation wired network to the wireless networks [5]; however, these solutions are not applicable to the HART/WirelessHART network.

We start with an integration solution where the WirelessHART Gateway is used as a point of integration. Here, the Gateway can be used as a standalone device, can be added in the HART I/O subsystem, or it can be put in a PC card where the HART modem is plugged in. However, there is only one Gateway in the WirelessHART network hence it is not feasible to connect it securely and directly with the HART Masters.

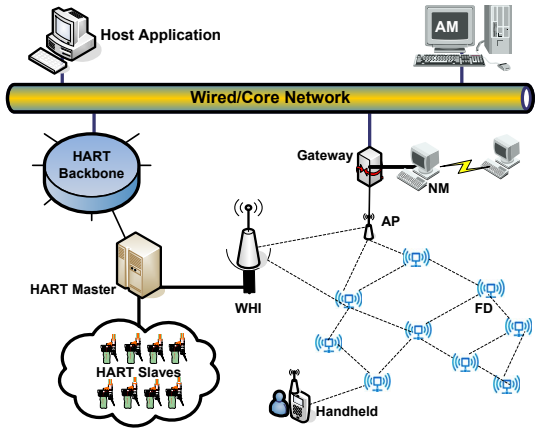

Fig. 1. A WHI securely integrates HART and WirelessHART networks

WirelessHART is a secure standard while the legacy HART[1] is an insecure protocol. We provide a novel, comparatively secure, flexible, and scalable solution to connect HART networks with WirelessHART networks. Our main contribution is the design of a WirelessHART Integrator (WHI) that securely

[1]In the remainder of the article HART refers to HART 6 and earlier and WirelessHART refers to HART 7 and above.

978-1-4244-8077-7/10/$26.00

connects HART networks with WirelessHART networks without the need to change or replace the existing HART or WirelessHART devices. Unlike the adapter that connects wired HART slave devices with WirelessHART networks, our WHI connects a HART *Master* with the WirelessHART network. A HART Master is a controller that controls the field instruments or HART slave devices connected together through a current loop (the HART network is named as current loop). Figure 1 shows this architecture which is explained in Section IV-A.

We analyze and evaluate this novel solution by comparing it with host level integration using either the WirelessHART Gateway or device level integration with adapters. Our comparison is based on parameters such as scalability, flexibility, security, etc. We conclude that our solution is more practicable, secure, reliable, and scalable.

II. Background

The WirelessHART protocol is developed to complement the legacy HART protocol. Both protocols are used for industrial process automation and share some common features. All messages in HART and WirelessHART flow in the form of commands that are predefined in the standard.

A. HART Network

Both HART and WirelessHART protocols are based on OSI 7 layers architecture. The HART protocol only defines physical, data-link, and application layers whereas the WirelessHART standard defines five layers (no separate session and presentation layers). The HART network can be formed by both point-to-point or multi-drop current loops. In point-to-point network only one device is connected to the current loop; whereas, in multi-drop network multiple devices can be connected to the current loop. Figure 2 shows a complete HART system consisting of both point-to-point and multi-drop HART networks where slave devices are connected to a HART Master through a current loop, a Distributed Control System (DCS), and Plant Automation Hosts (PAHs).

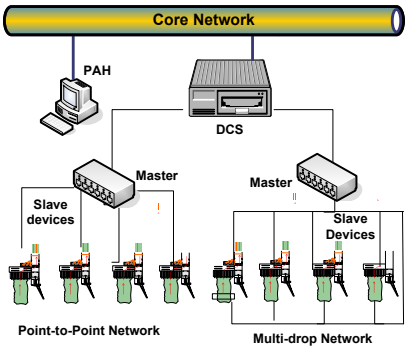

Fig. 2. Two HART networks with point-to-point and multi-drop topologies and a HART backbone

Security: HART is an insecure protocol since no cryptographic security mechanisms are used to protect the messages among the different HART network components. HART features communication error detection using single parity check coding schemes [6]. This scheme adds an overhead of 1 bit after each 8 bits; details can be found in [7].

B. WirelessHART Network

The WirelessHART network is a collection of wireless devices: field devices, adapters, routers, access points, and handheld devices [8]; and wired entities: Network Manager, Gateway, security manager, and Plant Automation Hosts (PAH). The Network Manager provides overall management, network scheduling and monitoring, network initialization functions, and resource management. The Network Manager collaborates with the Security Manager for the management and distribution of security keys. The protocol stack is based on a seven layer OSI stack with additional security and MAC sub layers. WirelessHART is a self healing and self organizing wireless protocol, in that the devices are able to find neighbors and establish paths with them, and detect network outrages and reroute. The wireless devices are connected using a mesh network where each device acts as a router. The WirelessHART standard uses Frequency-Hopping Spread Spectrum (FHSS) [9] and uniquely assigned time slots using Time Division Multiple Access (TDMA). Figure 3 shows a WirelessHART network having a Network Manager (NM), a Security Manager (SM), a gateway for interoperability between the wireless and wired parts, PAHs, and other wireless devices such as Field Devices (FD), Access Points (AP), handheld devices, routers, and adapters.

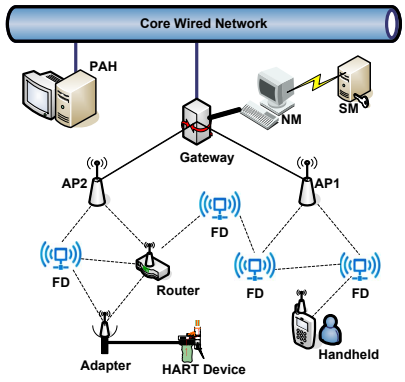

Fig. 3. Complete WirelessHART network with wireless and wired parts

Security: WirelessHART is a secure and reliable protocol. Advanced Encryption Standard (AES-128) block cipher in Counter with CBC-MAC Mode (CCM) [10] is used for encryption of messages and calculation of a Message Integrity Code (MIC). The WirelessHART standard provides end-to-end, per-hop, and peer-to-peer security. End-to-end security is enforced to secure the communication between the source and destination devices from malevolent insiders The network layer provides end-to-end security. The data-link layer provides per-hop security between two neighboring wireless devices. Per-hop security is a defense against outsiders, i.e. devices that are not part of WirelessHART network. All traffic in the WirelessHART network flows through the gateway;

however, a handheld device can create a secure and direct peer-to-peer session with the field devices. We have earlier analyzed security in WirelessHART [11].

Attributes	*HART*	*WirelessHART*
Physical Layer	4-20mA wiring	IEEE 802.15.4-2006
Data-link Layer	Token Passing	TDMA & FHSS
Network layer	Undefined	Defined
Application Layer	Legacy HART	Legacy HART
Security	No	Mandatory

TABLE I
COMPARISON BETWEEN HART AND WIRELESSHART NETWORKS

Table I shows comparison between the HART and WirelessHART protocols that needs to be kept in mind when interconnecting the two networks.

C. Motivation for Integration

The main motivation for HART-WirelessHART integration is to provide legacy support to the widely deployed HART networks. Hundreds of the HART based networks are installed world-wide. The contemporary WirelessHART standard is based on legacy *commands based* HART protocol and both are used for industrial process automation. To take full advantage of installed HART networks, WirelessHART should be able to communicate with HART networks and vice versa, i.e. there is a need for network-to-network integration. Probably WirelessHART is a future choice for the wireless communication in process automation system and due to its novel features the new manufacturing plants will prefer WirelessHART over HART networks.

The HART network and the HART backbone are connected through wires that may break; adding wireless can provide fault tolerance. If we have HART devices and the HART information is *trapped*, i.e. the installation and system only handles the 4-20mA, which is quite common, we can use WirelessHART and our new integrator to get this information. WirelessHART is a secure and reliable protocol and by integrating it with wired HART we can add security in the legacy HART protocol.

D. WirelessHART Adapter

The WirelessHART standard provides a reliable and secure way to connect HART *devices* with WirelessHART networks using adapters [8]. Adapters connect one (HART networks with a point-to-point topology) or more (HART networks with a multi-drop topology) HART enabled field devices with a WirelessHART network. In point-to-point HART networks we need an adapter for each HART device that needs to be connected with the WirelessHART network. Hence the adapter based solution is not practicable to connect complete HART networks with WirelessHART networks. In an automation plant there are usually more than one HART networks; however, an adapter can be used to access only a single HART device in point-to-point network and a single multi-drop network. The WirelessHART adapter provides direct integration but from device to network.

III. GATEWAY BASED INTEGRATION

The WirelessHART standard does not provide any precise network-to-network integration rather it highlights some network topologies that can be used to connect HART and WirelessHART networks. In this section we extend these architectures and elaborate the placement and connection of the Gateway with the HART network. These connections vary with the legacy HART network (point-to-point or multi-drop) and HART backbone architecture. The objective to connect HART and WirelessHART also affects the design; if the purpose is to read data from the device then only basic read commands will be implemented in the gateway, otherwise any number of commands can be implemented and any interface can be provided. The WirelessHART Gateway can be used as a PC card in the same PC board where HART modem is plugged in, can be used as a standalone device, or it can be used as a built-in component in the HART I/O system.

A. Gateway in PC Card

This solution is rather simple and easy. HART modems [12] can be used to provide HART-to-Ethernet messaging. A HART-to-WirelessHART Gateway can be used as a PC card in the same PC board where HART modem is plugged in. This will be a feasible application-level solution as both HART and WirelessHART share application layer specifications. This solution is feasible where the legacy HART network is already using a HART modem for integrating HART and Ethernet (or Wi-Fi, etc). Also, this approach simplifies the WirelessHART network architecture if we use the Network Manager and Security Manager as applications in the same PC where the Gateway is plugged-in. Also HART host applications can be placed in the same PC. Figure 4 shows this architecture.

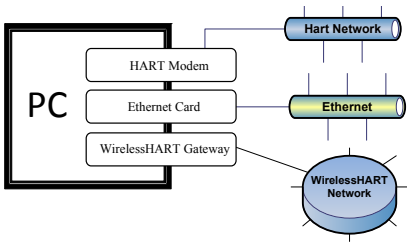

Fig. 4. Integrating HART and WirelessHART using Gateway as PC card

B. Gateway as Part of I/O Sub-system

If the HART network is not using a HART modem or if it is not feasible to use a modem based architecture in an automation plant then depending upon the available HART type (point-to-point and/or multi-drop) and the network architecture, the WirelessHART Gateway can be used as a built-in component in the I/O system. For the HART network, the I/O system is just another device and each I/O system must have one or more cards and each card must have one or more channels. Each channel supports one or more sub-devices (the HART devices). To integrate HART and WirelessHART

networks the Gateway can be plugged in as a *card* in the I/O system. Figure 5 shows this architecture.

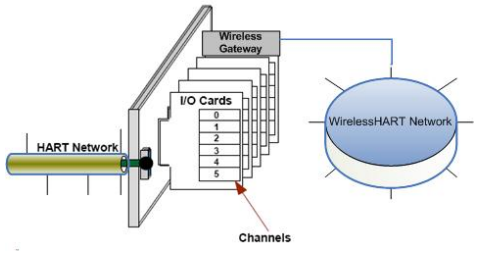

Fig. 5. Integrating HART and WirelessHART using Gateway as part of I/O subsystem

C. Standalone Gateway

A standalone gateway can be use to integrate the WirelessHART with HART networks. The gateway can be directly connected with any of the HART's I/O system or Field Transmission Assembly (FTA). The connecting cable can be any Recommended Standard (RS) specification but the WirelessHART recommends the use of RS485 cable to establish a connection between the FTA and the gateway. RS485 supports multi-drop and half duplex communication. Further, it has software flow control. The complete architecture for HART and WirelessHART network level integration is shown in Figure 6. The figure also shows the point of integration and the other components needed to put the system in action.

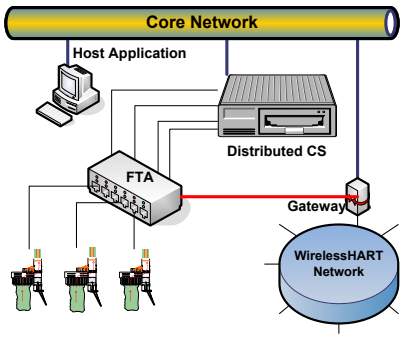

Fig. 6. Integrating HART and WirelessHART using standalone Gateway

Limitations: There is only one gateway in the WirelessHART network. The use of a gateway as an integrator may be a suitable choice in some scenarios but the proximity and placement of the gateway in the automation plant may not allow wired connections with multiple HART networks. In many deployments, the wiring of the HART network is already a mess. Moreover, the gateway based integration is not secure as the messages in the HART network travel all the way to the gateway without security. We present a novel, *comparatively* secure, and scalable solution to connect HART and WirelessHART network. In Section V we will analyze the gateway based integration and our solution. In the next section we present our solution.

IV. WHI: A Novel Integrator

We propose a new integration device that we call the WirelessHART Integrator (WHI). Unlike tradition WirelessHART adapter that connects the WirelessHART network with the HART slave device (field instrument) our WHI connects the WirelessHART network with the HART *Master*. A HART Master is a controller that controls one or more HART slave devices. The connection between the Master and slave devices is defined in the HART protocol and is through 4-20mA copper wires. The WHI converts WirelessHART messages to HART messages and sends them to the connected HART Master(s) that will transfer them to the connected slaves.

A. Network Architecture

On one end the WHI will be connected with any of WirelessHART wireless device and on the other side it will be connected with the HART Master. The connection between the WirelessHART devices and the WHI is through IEEE 802.15.4 as WirelessHART physical layer uses IEEE 802.15.4 wireless interface, whereas the connection between the WHI and HART Master can be any Recommended Standard (RS) discussed in IV-E. The HART Master is directly connected with slave devices that actually read process information. The HART Master can be any of the I/O system, DCS, Field controller, etc. From the WirelessHART point of view the WHI is yet another wireless device and from the HART viewpoint the WHI is a HART remote *I/O system*. Figure 1 shows a network architecture where the WHI is used as a network integrator to connect a HART and a WirelessHART network.

Our architecture integrates both HART and WirelessHART that helps in operating and administrating both the HART and the WirelessHART networks using a single administrative interface such as the Asset Manager [13]. Figure 1 also shows the placement of the Network Manager (NM), the Security Manager (SM) [14], and the gateway in the WirelessHART network. We have earlier discussed the placement of WirelessHART devices and their interaction [14].

B. WHI as Protocol converter

Unlike tradition WirelessHART adapter that can act as both HART Master or HART slave the WHI act a as remote I/O. The WHI has no direct connection with the HART slave devices. It interacts with the slave device through the HART Master. However the WHI needs to implement *Send Command to Sub-Device* (Command 77) and act as a bridging device and sets Protocol_Bridge_Device in the Flags byte of Identity command. This is necessary to tunnel/route gateway and host application messages to the HART slave devices. When a WHI receives a message from a WirelessHART device that need to be forwarded to a HART Salve it first extracts the actual WirelessHART data i.e. the aggregated Transport layer commands, and the destination slave device address. The WHI also knows the address of the connected HART Master. Later, the WHI constitutes a HART slave device Protocol Data Unit (PDU) by embedding the Slave message inside the Master message, as shown in Figure 8.

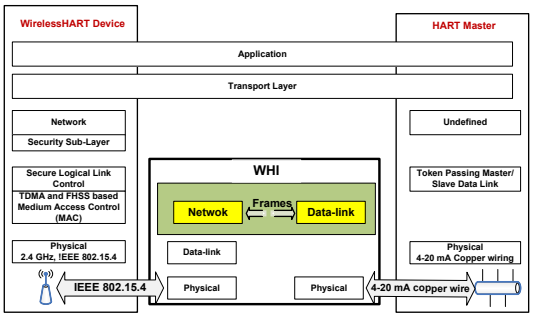

Fig. 7. WHI design and message flow between HART and WirelessHART networks

The WHI acts as a protocol converter that converts between HART and WirelessHART protocols. The protocol conversion occurs at the data-link layer. Figure 7 shows a schematic representation of the WHI's connections with WirelessHART device and HART Master. The WHI converts the WirelessHART Network Layer PDUs to the HART data-link layer PDUs and vice versa. Both HART and WirelessHART use the same addressing schemes and only the tag length in WirelessHART is increased to 32 character; the WHI adds this tag accordingly.

The WHI may provide two way accessibility i.e. the WirelessHART network can be accessed through the HART network and vice versa. However this may lead to serious security concerns when a device in an insecure HART will access the secure WirelessHART network. Section IV-E discusses these security concerns.

C. Message Formation

In order to send a message from a WHI to a HART slave device the HART message is wrapped inside an other HART message, Figure 8 shows this wrapping. In this figure, the

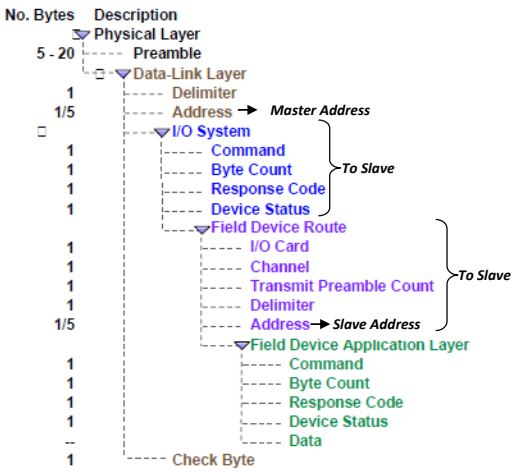

Fig. 8. Routing HART PDU from WHI to HART Slave through HART Master

address in the upper HART message is the Master address and the address in the embedded HART message is the actual slave address to whom the message is destined. The WHI uses HART *Send Command to Sub-Device* (Command 77) to tell the connected HART Master how to route the embedded message to the actual slave device.

D. Joining and Scheduling

The WHI is yet another WirelessHART wireless device and it has a Device ID and a Join Key which the WHI uses to join the WirelessHART network. After a successful join operation the WHI receives a nickname[2], the Network Key to securely send messages to the neighboring devices that are one hop apart, and Session Keys to create secure sessions with the gateway and Network Manager [11]. From the WirelessHART network all messages are securely sent to the WHI that forwards them to the actual slave devices; the security between the WHI and HART Master is discussed in Section IV-E.

WirelessHART devices use nicknames and unique IDs to send/receive messages to/from the Network Manager and gateway respectively. The WirelessHART Network Manager assigns a nickname and a unique ID only to the WHI and not to the connected Master and slave devices. This is because the HART Master and slaves are not WirelessHART devices and hence cannot create secure session with the gateway and the Network Manager. The *Send Command to Sub-Device* (Command 77) allows the WHI to pass embedded HART command to a destination sub-device i.e HART Master in this case. This significantly simplifies the Network Manager's scheduling job, i.e. slot assignment, channel hopping, routing, etc.. The Network Manager only needs to schedule the WHI in the WirelessHART network (see section 9.5 in [4]) and not the HART Master and slaves. This is also true if we use adapters to connect HART slave devices with the WirelessHART network; only adapters are scheduled and not the slave devices. However, the HART devices may incur overhead in the WirelessHART network; Section VI-A discusses this overhead.

The scheduling of HART devices in the WHI is not a major issue as only one HART Master is connected with the WHI. The HART Master is responsible for scheduling the connected slave devices which is well defined in the HART protocol. The WHI maintains a queue of requests for both HART side and WirelessHART side devices to allow systematic access to networks. WirelessHART uses TDMA to ensure contention free transmission. Each time-slot is 10ms long [1]. The WHI as a WirelessHART must meet this requirement. However, the response times on the wired HART networks is slower and it is not expected that the Command 77 will complete within a 10ms time slot. Hence the WHI as an I/O system must use the delayed response mechanisms, see section 7 in [8].

E. Connection between WHI and HART Master

The connection between the WHI and the HART Master varies with the type of Master. The HART Master can be any

[2]2-bytes Nicknames are used to uniquely identify the WirelessHART devices in the Network Manager

I/O system, Distributed Control System (DCS), field controller, or a Field Transmission Assembly (FTA). If the Master is a remote I/O, a DCS, or a field controller the connection between the WHI and Master can be Ethernet, RS485, or even Wi-Fi (if devices support it). However, if the Master is a FTA the connection will be RS485. In this case the WHI will handle commands 0-3, 11, and 13 [15].

The WHI can be placed just near to the HART Master and wiring will not be an issue as the WHI is wirelessly connected with the WirelessHART devices. However, security is a concern here as WirelessHART is a secure network and HART network is an insecure network. If the WHI and the HART Master are placed closed to each other in a secure physical environment, it will be hard to eavesdrop the wired communication link. Also, as there are no intermediate devices between WHI and HART Master it is hard to compromise the integrity of the message by a man-in-the-middle attack. However, the authentication of connected HART Master to the WHI and vice versa may be needed. Both WHI and HART Master are wired devices and resource scarcity is not really an issue. We propose the use of Public Key Infrastructure (PKI) based solution to secure this link. The WirelessHART Security Manager is a trusted entity in the WirelessHART network that can be used to build a PKI.

We have earlier designed and implemented a Security Manager for the WirelessHART networks [14]. Our Security Manager, besides providing security services to the WirelessHART wireless devices, is used to secure the communication between the WirelessHART wired entities such as between the gateway and the Network Manager, gateway and host application, and Network Manager and Security Manager. To secure WHI-HART Master links, our Security Manager is able to generate and provide private keys and signed X.509 certificates to both WHI and HART Master. Before the actual communication, the WHI and HART Master can authenticate each other using these security credential and PKI [16]. This solution can be used to provide Confidentiality and Integrity, if needed.

V. Comparison: WHI Vs. Gateway Vs. Adapter

We have presented different ways to connect HART and WirelessHART devices/networks. The choice of the specific approach depends on user needs and the underlying HART architecture, e.g. adapter is the most appropriate choice when we need to connect a single HART device with a WirelessHART network. In this section we compare WHI versus gateway and WHI versus adapter based solution to integrate HART and WirelessHART *networks*.

A. WHI versus Gateway-based solutions

Integrating HART and WirelessHART networks using a gateway may be a good option in a few scenarios but is not always a feasible choice. The gateway already has number of dedicated wired connections. As a WirelessHART device, the gateway has wired connections with the host application and plant automation controllers, with the Network Manager, and with one or more WirelessHART access points. Furthermore, the gateway may also connect a WirelessHART network with other automation networks such as the Fieldbus [17] or ISA 100.11a [18]. Due to the proximity of the gateway it is sometimes simply not feasible to connect the gateway with the HART network using physical wiring. In real deployments HART wiring is already a mess. However, if the HART network is connected with the Ethernet using a HART modem and it is feasible to connect the gateway with the same PC where the HART modem is plugged in the gateway may be a better alternative to connect the two networks. Unlike a gateway, the WHI is a wireless and portable device and the change of the physical location will not require additional wiring as the WHI has only one physical link i.e. with the HART Master.

In an automation plants there are usually more than one HART networks. We may use multiple WHIs to connect more than one HART network with the WirelessHART. Since there is only one gateway in a WirelessHART network [8] the gateway based solution may not be used to connect multiple HART networks with the WirelessHART network; this is a major limitation of the gateway based solution.

Security is a distinctive feature of WirelessHART. A gateway based integration is less secure as the messages in the HART backbone flow as plain text all the way to the WirelessHART networks, unless the gateway is directly connected to the HART Master which is usually not feasible. The physical position of the gateway affects security: the closer the gateway to the HART Master the sooner the unencrypted HART message is converted to an encrypted WirelessHART message. The security can be provided by securing the links between the HART backbone components; however this may require a lot of work and installation of new devices and modules. We prefer to add security in the HART backbone. In the WHI solution, we only need to secure the connection between the WHI and HART Master; we propose a solution for that in section IV-E.

B. WHI versus Adapter-based solutions

A single WirelessHART adapter connects only one HART device to the WirelessHART network if the underlaying HART network is point-to-point current looped. A single adapter can connect multiple devices with the WirelessHART network if the HART network is multi-drop current looped. In point-to-point HART network, connecting multiple HART devices is cumbersome and does not scale since we need an adapter for each device. Theoretically, up to to 275,000,000,000 slave devices can be connected to a current loop but normally not more than 15 devices are connected to a multi-drop current loop in order to keep noise in transmissions down [3]. Connecting the (point-to-point) HART network with 15 devices to a WirelessHART network requires 15 adapters. Hence an adapter is not a feasible solution to connect HART and WirelessHART *networks*. The key advantage of the WHI over adapter-based solutions is scalability in that the number of additional devices in the WirelessHART network is lower using the WHI-based solution.

VI. Evaluation and Discussion

The WirelessHART standard is in its inception stage and the architecture of WirelessHART Network Manager is still not clear in the standard. Also, we have no open gateway and Network Manager to test our solution. Therefore, we cannot conduct experiments with real WirelessHART networks. However, we theoretically evaluate our WHI, the gateway, and the adapters based solutions using network parameters such as bandwidth, computation, security, reliability, scalability, etc.

A. Network Overhead

Connecting HART network with the WirelessHART network through WHI apparently inserts large overhead in the WirelessHART network and may prone to the network congestion, collision, interference, etc. However, this is actually not the case as WirelessHART offers time slotting (using TDMA scheduling) and channel hopping (FHSS). Although the WHI may utilize more network resources (bandwidth, time slots, etc) there will probably be very low interference and collisions (as WirelessHART standard claims) as each message will be sent in specific time slot and on particular channel. WirelessHART uses the 2.4 GHz frequency band. It shared this band with ZigBee, Bluetooth, ISA 100.11a, etc which makes it prone to interference.

All messages in the WirelessHART network flow through gateway, i.e two devices must have sessions with the gateway to communicate with each other; Handheld device creates direct peer-to-peer sessions. In the WHI based solution HART messages traverse the WirelessHART twice i.e. from WHI to gateway and from gateway to the destination device. On the other hand, the gateway provides a more WirelessHART friendly solution as HART messages will only travel from the gateway to the destination devices. The bandwith requirements in the WirelessHART network will be high in adapters and WHI based solutions, whereas bandwith requirements in the HART backbone will be high in gateway based solution.

B. Bandwidth

WirelessHART operates at 250 kb/s, HART operates at 1200 bits/s, and the HART backbone is connected through Ethernet that provides bandwidth in MBs. The high bandwidth in the HART backbone allows messages to reach the gateway faster than through the WirelessHART network. However, the gateway is a central hub and is physically connected to many other devices (Network Manager, APs, Host applications, etc.) and may be with networks such as ISA100.11a [18], Fieldbus [17], etc. The gateway maintains a queue of requests for all these wireless and wired devices and networks. The gateway and the WHI may also need to maintain a queue of request for the HART network. Having multiple connections with other devices and networks the queuing time in the gateway based design increases and the overall latency in gateway based integration may become higher than the WHI based integration.

C. Security and Reliability

Security is the main advantage of using the WHI or adapters. WirelessHART is a secure network and the WHI is a WirelessHART device that supports full security features. The WHI is directly connected with the secure WirelessHART network and with the HART Master through a secure connection. Usually it is not feasible to connect the gateway directly to the HART Master and we may have multiple intermediate links. These intermediate connections are insecure and wired and provide room to intruders to break message security. We may secure the HART backbone but then we need to modify or replace the existing hardware and software in the installed base, which is not easy. It is more flexible and practicable to just add a WHI to securely interconnect the two networks. The adapter based solution is the most secure solution since the adapter is directly connected to a WirelessHART device. However, adapters only connect devices with the WirelessHART network but not the whole network.

WirelessHART is a reliable network as it provides time diversity (through TDMA), frequency diversity (through channel hopping), and path diversity by having links with the multiple neighbors (WirelessHART mandates links with at least two neighbors). On the other hand, HART is unreliable wired network as there is a single wired path between the HART devices. The WHI and the adapter provide reliable solutions as unreliable HART messages are routed through the reliable WirelessHART network. While wireless networks may suffer from interference which can cause packet loss, cable tear and damage is a huge problem which in many cases makes wireless solutions more reliable than wired ones [19].

D. Complexity and Scalability

If we add support for HART networks the complexity of the gateway increases while the overall network complexity remains same. For the WHI and adapter-based solutions, the size of the wireless network increases as more devices are added. The Network Manager has to manage and schedule network resources for these devices. Most scheduling problems have exponential complexity even for simple line networks [20]. Hence, when we halve the number of nodes the time to compute a suitable schedule is reduced from n to $\sqrt{n}$. Since the number of additional devices that participate in the WirelessHART network is much lower using the WHI-based approach, this solution has lower complexity and scales better than the adapter-based approach.

The WHI based solution offers full scalability; the new HART network can be easily integrated with the WirelessHART network using a WHI. In this case the WHI will just be a new WirelessHART device for the Network Manager and multiple devices can be connected with it later on. The adapter based design is less scalable as for each new HART device we need one adapter in the WirelessHART network. The gateway based network-to-network interconnection will be even less scalable as we have only one gateway and it not feasible to have wired links to the gateway from all the HART networks in the automation plant.

E. Cost

Adding support for HART networks in the gateway will increase the cost of the gateways; also, the wiring cost will drastically increase as it is not feasible to keep the gateway closer to the HART I/O subsystem. WHIs are wireless devices that can be kept very close to HART Master. They establish wireless connections with any of the WirelessHART wireless devices such as field devices, routers, access points, etc. adapters have a higher cost as multiple adapters are needed to connect more than one device to the WirelessHART network. In huge installations, device cost may be significant. Hebert also points out that wireless networks are cheaper to maintain [19].

F. Summary

WHIs connect HART network with WirelessHART networks whereas adapters connect HART devices with WirelessHART networks. In spite of having network wide integration solution WHI provide competitive performance and security compared to adapters. A WHI is not only a secure alternative to gateway integration functionalities but also a replacement of WirelessHART adapters in situations where multiple HART devices from a point-to-point HART network need to be connected with a WirelessHART network. Table II shows the comparison between the WHI, adapter, and the gateway based designs.

Attributes	*Gateway*	*WHI*	*Adapter*
Reliability	Low	High	Higher
Security	No	High	Higher
Scalability	Difficult	Easy	Very Difficult
Bandwidth	High	Low	Low
practicability	Low	High	Very Low
Cost	High	Low	High
Latency	High	Low	Lower
Complexity	Depends	Depends	Depends

TABLE II
COMPARISON OF GATEWAY-BASED, WHI-BASED, AND ADAPTER-BASED SOLUTIONS TO INTEGRATE HART AND WIRELESSHART NETWORKS

VII. CONCLUSION AND FUTURE WORK

Gateway, adapters, or WHIs can be used to interconnect HART and WirelessHART networks. However the best choice depends to a large extent on user needs and the properties of the deployed HART network. Adapters are appropriate to connect multi-drop HART network devices with WirelessHART networks. When there is only one point-to-point HART network in the automation plant and it is feasible to securely and directly connect the gateway with the HART Master then the gateway based interconnection is the appropriate choice. Usually there are multiple HART networks in an automation plant and because of having only one gateway it is not feasible to directly connect the gateway with all the HART Masters since wiring will be cumbersome. Therefore we proposed a secure and reliable WirelessHART Integrator (WHI) based solution to connect the multiple HART networks with WirelessHART networks. We have shown that the WHI is a flexible and scalable solution. Our analysis and comparison shows that the WHI is feasible and preferable solution in term of security, reliability, scalability, practicability, etc. As future work we intend to develop a WHI and evaluate it on real WirelessHART networks.

ACKNOWLEDGMENT

This work has been performed within the SICS Center for Networked Systems funded by VINNOVA, SSF, KKS, ABB, Ericsson, Saab Systems, TeliaSonera, T2Data, Vendolocus and Peerialism. This work has been partially supported by CONET, the Cooperating Objects Network of Excellence.

REFERENCES

[1] Jianping Song, Song Han, Aloysius K. Mok, Deji Chen, Mike Lucas, and Mark Nixon. Wirelesshart: Applying wireless technology in real-time industrial process control. *Real-Time and Embedded Technology and Applications Symposium, 2008(RTAS-08)*, April 2008.

[2] Anna N. Kim, Fredrik Hekland, Stig Petersen, and Paula Doyle. When hart goes wireless: Understanding and implementing the wirelesshart standard. *IEEE International Conference on Emerging Technologies and Factory Automation*, pages 899–907, September 2008.

[3] Analog Services. About hart, 1999.

[4] *Network Management Specification,HCF_SPEC-085, Revision 1.1*. HART Communication Foundation, May 2008.

[5] Ivan Marc Author. Integration of mobile vehicles for automated material handling using profibus and ieee802.11 networks. *IEEE Transactions on Industrial Electronics*, 49(3), 2002.

[6] Cyril Leung. Evaluation of the undetected error probability of single parity-check product codes. *IEEE Transactions on Communications*, 31(2):250–253, 1983.

[7] *Token-Passing Data Link Layer Specifications, HCF_SPEC-81, Revision 1.1, Section 5.4*. HART Communication Foundation, May 2008.

[8] *WirelessHART Device Specification,HCF_SPEC-290, Revision 1.1*. HART Communication Foundation, May 2008.

[9] William Stallings. *Data and Computer Communications*, pages 277–282. Prentice Hall, eighth edition, 2006.

[10] D. Whiting, R. Housley, and N. Ferguson. *Counter with CBC-MAC (CCM), RFC 3610*. IETF, Network Working Group, Fremont, California 94538 USA, September 2003.

[11] Shahid Raza, Adriaan Slabbert, Thiemo Voigt, and Krister Landernas. Security considerations for the wirelesshart protocol. In *Proc. ETFA 2009*, 2009.

[12] SAMSON AG. *Technical Information, HART Communications, Part 4*. SAMSON AG, D-60314 Frankfurt, Dec 1999.

[13] $Industrial^{IT}$ *- Integrated Automation Solutions for Process Automation based on Aspect Object Technology*. ABB Automation Technology Products AB, system guide for system baseline 2, 3bse027508r201 edition, Dec 2002.

[14] Shahid Raza, Thiemo Voigt, Adriaan Slabbert, and Krister Landernas. Design and implementation of security manager for the wirelesshart network. In *Proc. WSNS 2009*, October 2009.

[15] *Common Practice Command Specification, HCF_SPEC-151, Revision 9.1*. HART Communication Foundation, May 2008.

[16] Carlisle Adams and Steve Lloyd. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[17] *Fieldbus Foundation*. http://www.fieldbus.org/.

[18] *The ISA100 Standards: Overview & Status*. http://www.isa.org/source/ISA100.11a_Release1_Status.ppt.

[19] Dan Hebert. Industrial networks adopt wireless, 2009.

[20] M. Adler, A.L. Rosenberg, R.K. Sitaraman, and W. Unger. Scheduling time-constrained communication in linear networks. *Theory of Computing Systems*, 35(6):599–623, 2002.