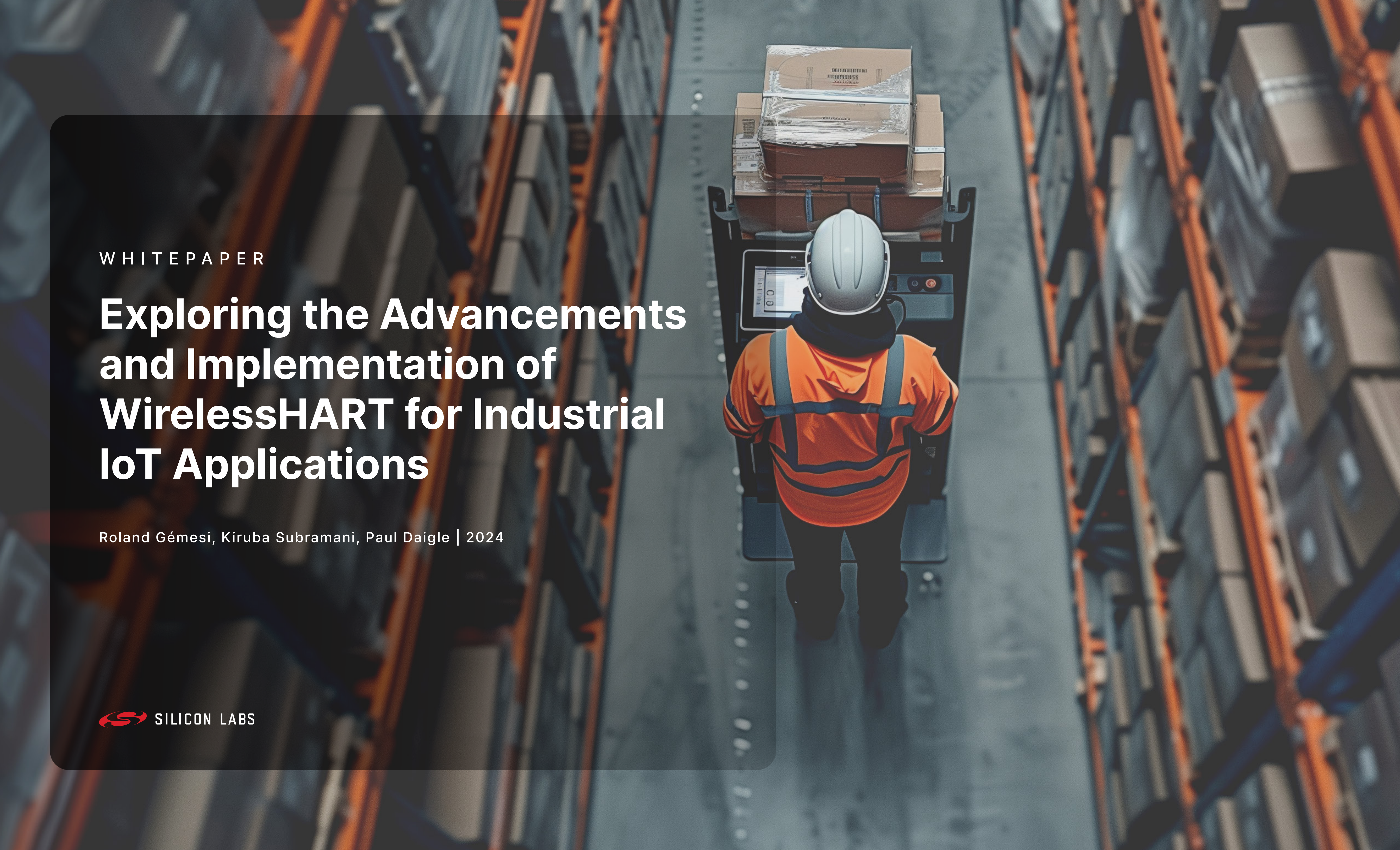


WHITEPAPER

Exploring the Advancements and Implementation of WirelessHART for Industrial IoT Applications

Roland Gémesi, Kiruba Subramani, Paul Daigle | 2024

SILICON LABS

Introduction

Highway Addressable Remote Transducer (HART) **[1]** is a wired communication protocol that is extensively used in process industries. With over 40 million devices deployed, HART is the global standard for digital communication over 4-20 mA analog current loops, connecting distributed control systems with field instruments, such as sensors and actuators.

WirelessHART **[2]** was introduced in 2007 as the first industrial mesh protocol that adds wireless capability to HART while maintaining backward compatibility with existing HART systems. WirelessHART uses a standard 802.15.4 radio transceiver that is restricted to the globally accessible 2.4 GHz frequency band. In the higher layers of the protocol stack, WirelessHART includes numerous adaptations and extensions over the 802.15.4 standard to meet the stringent needs of industrial applications, such as low latency, determinism, robustness, and security. The following sections provide an overview of WirelessHART.

[1] FieldComm Group, "HART Protocol"

[2] FieldComm Group, "WirelessHART"

WirelessHART: System Architecture and Operation

A WirelessHART system **[3]** is shown in Figure 1, and it includes the following components:

Gateway: Central device that enables communication between the WirelessHART network and the process automation backend, which executes the host application. The backend is a wired Fieldbus or Ethernet network and can include, for instance, a Process Automation Controller (PAC), Distributed Control System (DCS), Data Historian, or Asset Management Software.

Access point: Device that interfaces the gateway with the WirelessHART network.

Field Device: Individual wireless node, usually a sensor or actuator, which also acts as a wireless router in the mesh network.

Wireless Router: Optional wireless device without a sensor or actuator that is used purely for routing data packets within the network.

Wireless Adapter: Allows interfacing wired HART devices to the wireless network.

Wireless Handheld Device: End-user device to support the installation, configuration, control, monitoring, and maintenance of the system.

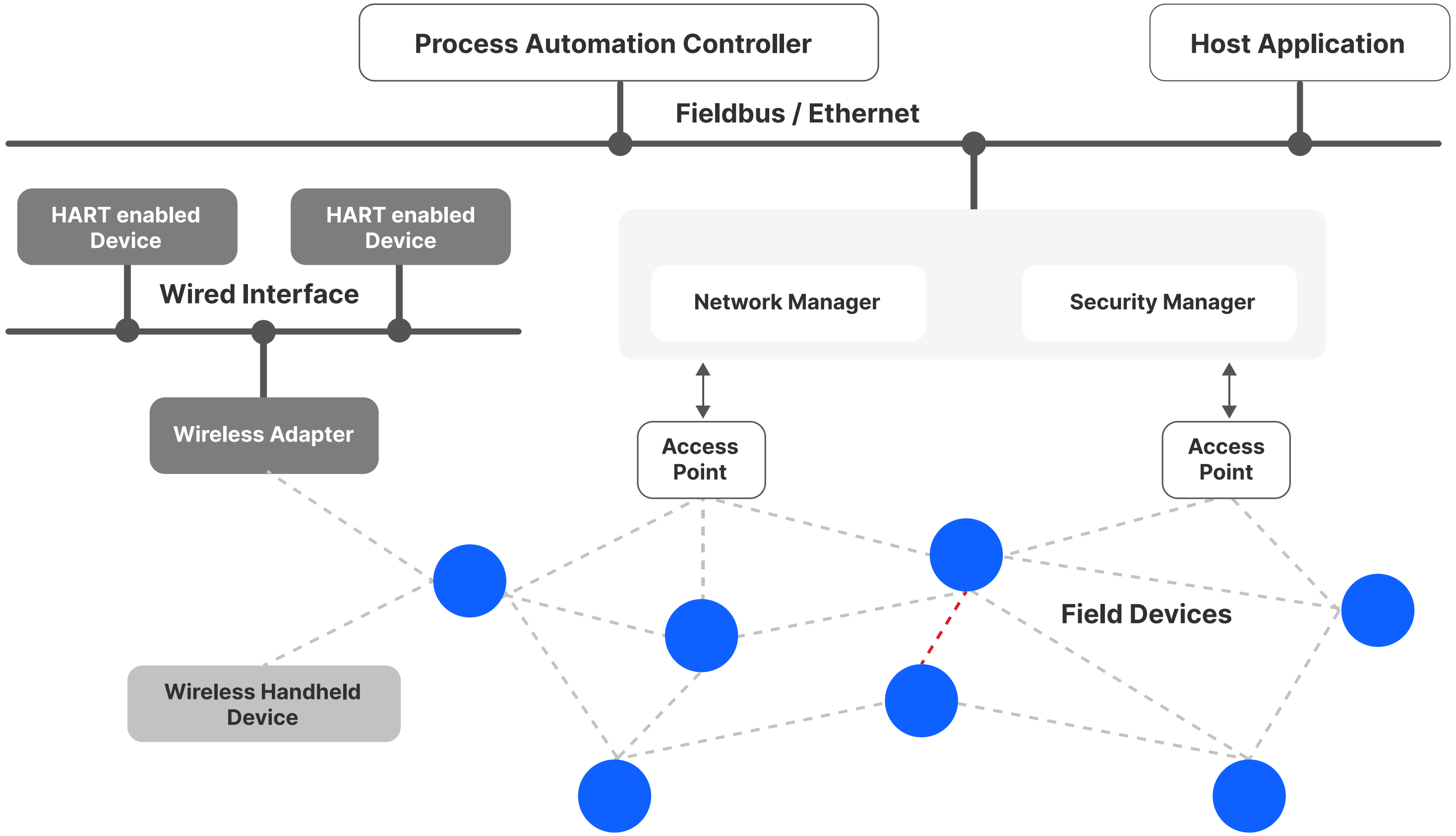


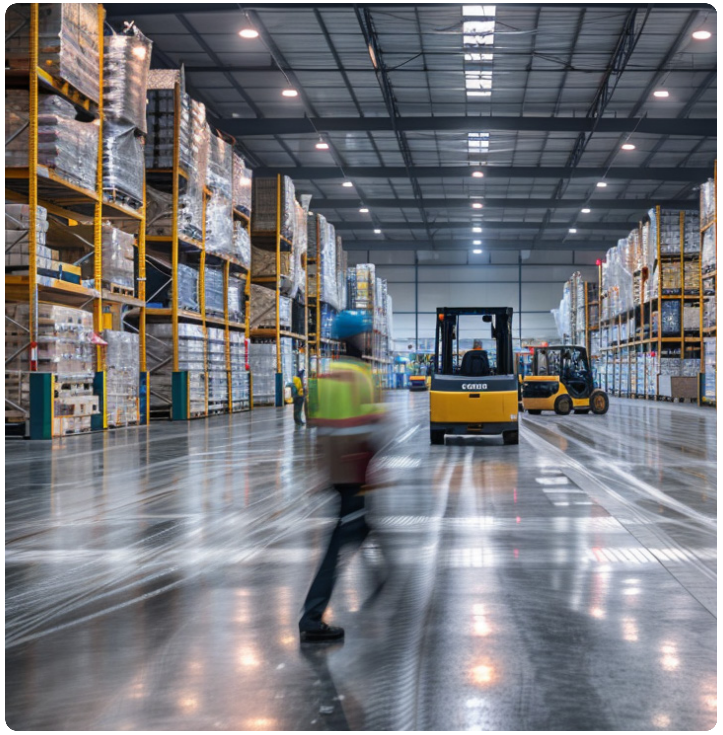
Figure 1. WirelessHART System Architecture

[3] Emerson, "System Engineering Guidelines IEC 62591 WirelessHART"

A WirelessHART network is formed around the gateway, which usually acts both as a security manager and a network manager. It initializes the wireless network and adds new field devices as they are commissioned. As a security manager, it is responsible for generating, storing, and managing security keys, as well as maintaining and controlling the network access list. As a network manager, it is responsible for centrally organizing the radio transmission time schedules, frequency hopping sequence, and communication routes along the whole wireless mesh network. It is also responsible for managing the topology, monitoring network health, and adapting routes between field devices.

The resulting wireless network is a redundant, self-organizing, self-healing, adaptive mesh network, which can be centrally managed by the network manager. The central configuration enables optimization for various needs, such as robustness, latency, determinism, or battery life. For instance, to increase robustness, WirelessHART offers the following techniques:

- **Time diversity:** The protocol uses time-scheduled communication and supports redundant data transmission over multiple time slots to mitigate transient communication issues.
- **Channel diversity:** The protocol uses channel hopping, where the redundant data transmissions occur on different frequencies, thereby protecting against channel selective fading and RF interference.
- **Route diversity:** The protocol supports defining redundant routes in the mesh network to improve network robustness against route failure.



Since the introduction of WirelessHART, process industries have developed several guidelines and best practices for deploying and using the WirelessHART protocol **[3]**. For instance, when it comes to transmission range, single-hop communications can achieve a 30 m range in the presence of obstructions, but a much longer range is feasible without obstructions or in a multi-hop communication setup. Likewise, network latency of less than 100 ms can be achieved in the case of a star topology, but the achieved latency generally depends on the network size and topology. Finally, the network size can scale to 80 devices without experiencing performance impacts but can grow even further to 250 devices with performance tradeoffs, for instance, in latency, throughput, or battery life.

[3] Emerson, "System Engineering Guidelines IEC 62591 WirelessHART"

WirelessHART Protocol Stack

The OSI communication stack of WirelessHART is shown in **Figure 2 [4-5].**

Wireless Networking Stack (WPAN)	
Application/ Application Support	Command oriented HART Protocol, Request/Response mode, Publish mode, Notifications, Block Transfer
Transport Layer	Connection-oriented Transport, Connection-less Transport
Network Layer	Centrally managed multipath graph routing, Source routing, Proxy routing, Security
Data Link Layer	802.15.4 MAC customized, with modifications F/TDMA, Centrally managed TDMA, Synchronized Channel hopping, Shared slots (CSMA-CA), Security
Physical Layer	• 802.15.4 (2006) PHY • 2.4 GHz, OQPSK, DSSS, 250 kbps, max. 10 dBm

Figure 2. WirelessHART Protocol Stack

The physical layer of WirelessHART uses the 802.15.4 (2006) standard with the restriction to use only 15 worldwide supported channels, as shown in Figure 3. This greatly simplifies the design, certification process, and deployment of WirelessHART devices in different countries without requiring country-specific configuration changes. WirelessHART uses 2 MHz wide RF channels that are spaced 5 MHz apart, with a maximum transmit power of 10 dBm. It uses Offset Quadrature Phase Shift Keying (OQPSK) modulation and a data rate of 250 kbps. Finally, the use of Direct Sequence Spread Spectrum (DSSS) allows the wireless standard to be resilient against RF interference and channel fading.

To achieve robust industrial-grade communication in the congested 2.4 GHz frequency band, WirelessHART uses the following techniques: The MAC layer of WirelessHART uses Time Division Multiple Access (TDMA) to achieve collision-free and deterministic communication. The protocol leverages Frequency Hopping Spread Spectrum (FHSS) to communicate on a different wireless channel after each time slot, and finally, the protocol supports excluding wireless channels that are heavily congested and suffer from poor performance.

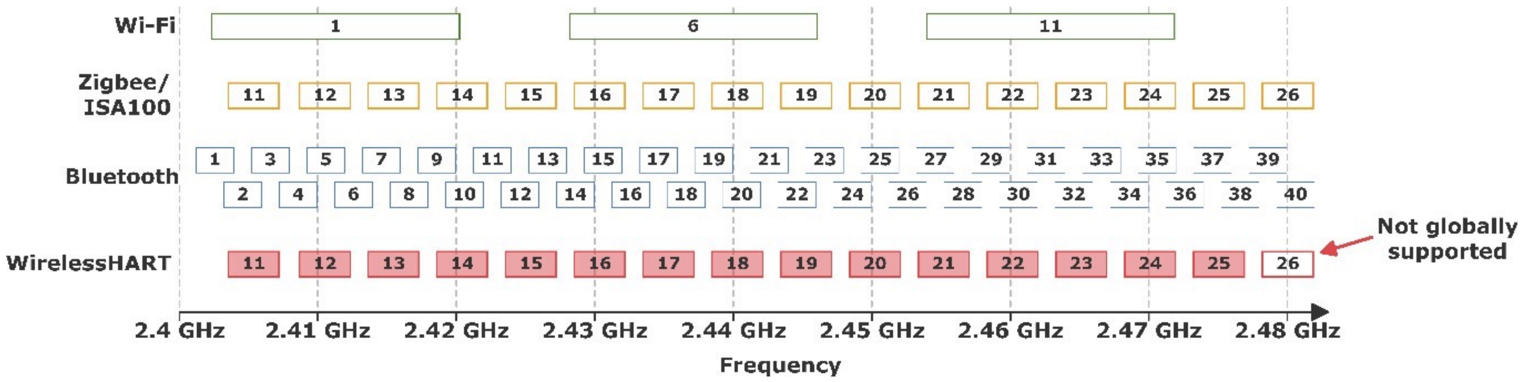


Figure 3. Frequency Channels of WirelessHART

[4] Devan et al, "A Survey on the Application of WirelessHART for Industrial Process Monitoring and Control", Sensors 2021, no. 15

[5] "When HART goes wireless: Understanding and implementing the WirelessHART standard", 2008 IEEE International Conference on Emerging Technologies and Factory Automation,

To achieve robust industrial-grade communication in the congested 2.4 GHz frequency band, WirelessHART uses the following techniques: The MAC layer of WirelessHART uses Time Division Multiple Access (TDMA) to achieve collision-free and deterministic communication. The protocol leverages Frequency Hopping Spread Spectrum (FHSS) to communicate on a different wireless channel after each time slot, and finally, the protocol supports excluding wireless channels that are heavily congested and suffer from poor performance.

Communication between WirelessHART devices occurs in 10 ms long time slots. During each time slot, the transmitting device sends a data packet and waits for an acknowledgment from the receiver. The protocol forms a superframe by allocating a configurable number of such time slots, which periodically repeats, as shown in Figure 4. The superframe is centrally controlled by the network manager, which allocates every timeslot to a transmitting and receiving device, as well as the wireless channel over which the communication takes place. The resulting timeslot and channel allocation are distributed to the field devices for individual radio scheduling. In addition, the standard also supports features such as message broadcasting and sharing timeslots among multiple transmitters on a contention basis using Carrier Sense Multiple Access (CSMA).

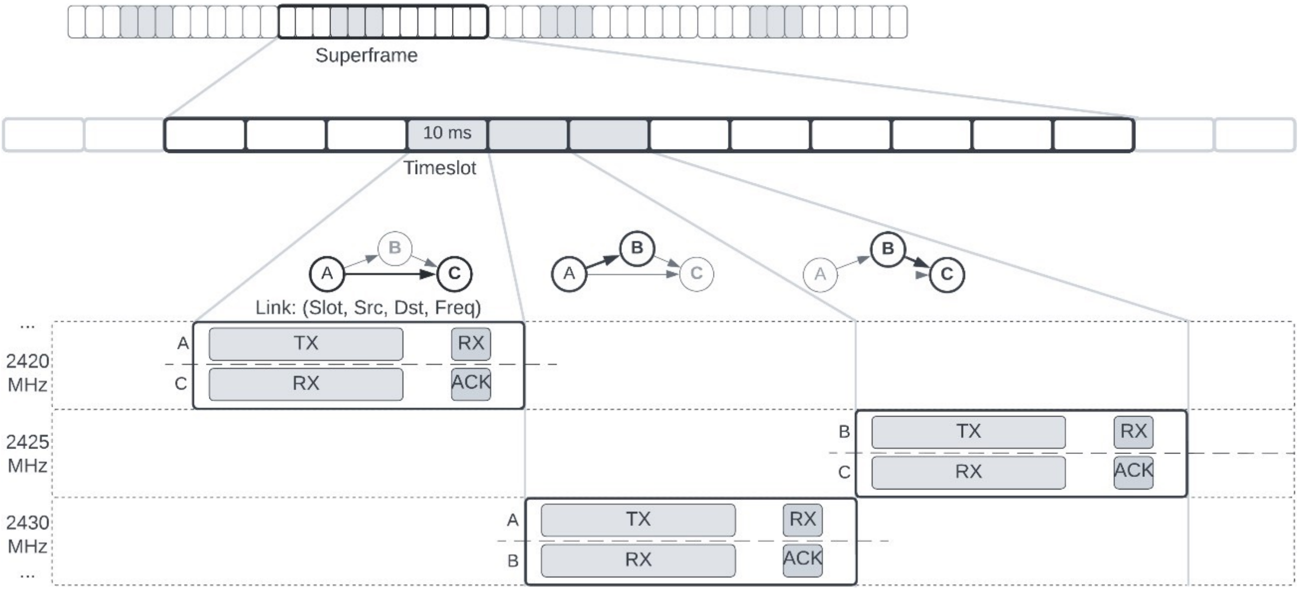


Figure 4. MAC layer of WirelessHART

The network layer of WirelessHART supports multiple routing mechanisms to establish a robust mesh network. Two of the mechanisms are listed below:

- **Graph routing** is the main routing scheme of WirelessHART, where the network routes are determined centrally by the network manager and distributed to the individual field devices of the mesh network. This routing scheme offers flexibility, such as configuring different routes for uplink, downlink, and broadcast communication. Moreover, redundant paths can also be defined to support path diversity.
- **Source routing** is a supplemental routing mechanism for network diagnostics and configuration purposes. In this scheme, the source device determines the route of the packet and writes the ordered list of intermediate hops within the packet's routing header. Intermediate nodes relay the packet based on this information without requiring any a priori configuration.

The network layer of WirelessHART makes it a highly configurable protocol because the network manager has full control over both the network-wide F/TDMA schedule and the graph routing. For instance, the network manager can optimize both the routing scheme and the MAC layer to achieve low latency and improve overall robustness. When optimizing for latency, the network manager can limit the network to a star topology or prioritize routes of interest in the routing graph based on the F/TDMA schedule. Similarly, when improving robustness, the network manager can allow a device to use multiple timeslots or add route diversity for the same transmission.

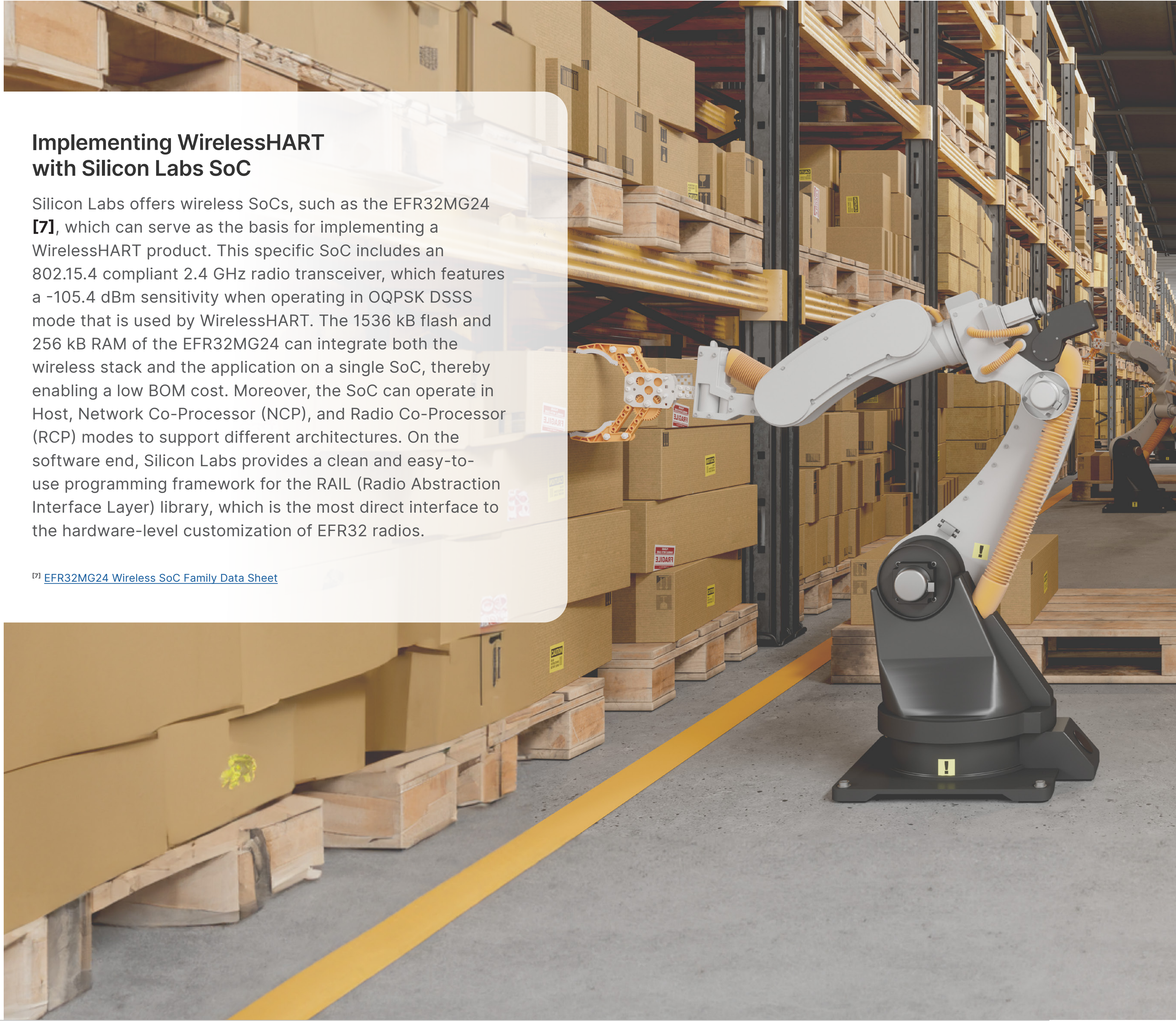
The transport layer of WirelessHART provides connection-oriented communication between the host application and field devices with the help of end-to-end acknowledgments and automatic repeat requests (ARQ). In addition, WirelessHART also supports connection-less transport without acknowledgment, which is suitable for cases where reduced overhead is preferred.

While the application layer of WirelessHART adopts a command-response type of communication, it also supports other types, such as one-way data publishing, spontaneous notifications, and block transfer of large data. In the command-oriented communication mode, the HART application layer ensures interoperability with legacy HART devices. The following types of commands are used in the communication:

- **Universal Commands** must be supported by all HART devices in the system, for instance, to read device status and process variables.
- **Common Practice Commands** are optional but strongly recommended, as they provide additional functionality for the communication and configuration of field devices.
- **Wireless Commands** are specific to WirelessHART to support network formation, maintenance, and security, as well as other background functions.
- **Device-specific commands** are used to support functions specific to a field device or to implement vendor-specific commands.

Security in WirelessHART

WirelessHART provides security at multiple levels in the OSI stack using 128-bit AES encryption **[6]**. In the network layer, every message is end-to-end protected to ensure message confidentiality, source authenticity, and data integrity. In addition, a common shared key is used by all the devices in the network to facilitate message broadcasting. Individual keys are assigned to each device during commissioning and are updated periodically to offer an even higher level of protection. Moreover, the commissioning process and communication with the wireless handheld devices are also secured. Besides network layer security, the MAC layer also provides data integrity between successive communication hops in the mesh network.



Implementing WirelessHART with Silicon Labs SoC

Silicon Labs offers wireless SoCs, such as the EFR32MG24 **[7]**, which can serve as the basis for implementing a WirelessHART product. This specific SoC includes an 802.15.4 compliant 2.4 GHz radio transceiver, which features a -105.4 dBm sensitivity when operating in OQPSK DSSS mode that is used by WirelessHART. The 1536 kB flash and 256 kB RAM of the EFR32MG24 can integrate both the wireless stack and the application on a single SoC, thereby enabling a low BOM cost. Moreover, the SoC can operate in Host, Network Co-Processor (NCP), and Radio Co-Processor (RCP) modes to support different architectures. On the software end, Silicon Labs provides a clean and easy-to-use programming framework for the RAIL (Radio Abstraction Interface Layer) library, which is the most direct interface to the hardware-level customization of EFR32 radios.

[6] WirelessHART Security

[7] EFR32MG24 Wireless SoC Family Data Sheet

Summary

WirelessHART is an industrial standard used in process automation, control, and monitoring systems. While it uses the 802.15.4 radio transceiver, numerous adaptations, such as direct sequence spread spectrum, frequency hopping, etc., have been added. This allows the protocol to mitigate the effects of RF interference and channel fading, thereby meeting the stringent needs of industrial applications. Moreover, by being a centrally managed mesh network, WirelessHART is able to support redundant routes between wireless nodes in the network, which allows it to achieve the robustness requirement. Finally, WirelessHART maintains backward compatibility with wired HART, which includes supporting existing devices, commands, and software tools. As an IoT solutions provider, Silicon Labs SoCs, such as EFR32MG24, have the required hardware and software features to implement a WirelessHART device.