WHITEPAPER

Unlock Industrial Connectivity with ISA100 Wireless

Roland Gémesi, Kiruba Subramani, Paul Daigle | 2024

SILICON LABS

Introduction

ISA100 Wireless, also known as ISA100.11a and IEC 62734, is a wireless networking standard developed especially for industrial applications **[1]**. While it is built upon the 802.15.4 radio transceiver specifications and operates in the 2.4 GHz frequency band, it includes numerous extensions to meet the stringent requirements of process control applications, such as determinism, robustness, and security. ISA100 Wireless is suitable for a wide range of process control applications, such as monitoring and open and closed loop control, including both supervisory and regulatory use cases, where a latency in the order of 100 ms is required.

The standard offers secure end-to-end IP-based communication using 6LoWPAN, enabling seamless integration with other IP-based solutions and cloud services, making it appropriate for the Industrial Internet of Things (IIoT) **[2]**. Although the standard does not specify the application layer, it is capable of tunneling any application data over the wireless network. ISA100 Wireless is centrally configurable and designed to be a highly flexible standard, thereby requiring solution builders to ensure interoperability among devices from different vendors.

In the following sections, an overview of this wireless standard is provided.

[1] isa100.org, Wireless Systems for Automation

[2] Raptis et al., "A Survey on Industrial Internet with ISA100 Wireless", IEEE Access, 2020

ISA100 Wireless: System Architecture and Operation

The system architecture of an ISA100 Wireless network is shown in **Figure 1** and explained below: **[3]**

Input/Output (I/O): Sensor/actuator device that can transmit and receive its messages without participating as a relay in the mesh network.

Router: Dedicated routing-only devices, excluding I/O functionality, that can relay messages within the ISA100 Wireless network. While I/O devices with routing capability can serve this purpose, this feature is not mandated by the standard.

Gateway: Device that translates messages between the IPv6 backbone and the plant's wired fieldbus network, such as Modbus, OPC, or PROFINET. In practice, the gateway can integrate the roles of the system manager, security manager, and even the backbone router.

System Manager: Often a part of the gateway implementation, the system manager plays a central role in the network, where it is responsible for resource management, such as address allocation, communication scheduling, and setting up routes between wireless devices. The system manager is also responsible for configuring features defined in the ISA100 Wireless standard.

Security Manager: Often a part of the gateway implementation, the security manager plays a central role in enabling, configuring, and supervising the secure operation of all network devices that are based on the adopted security policy.

System Time Source: Role for maintaining a common time source to enable network-wide time synchronization.

Provisioning device: Handheld end-user device for provisioning, commissioning, and configuration of new devices.

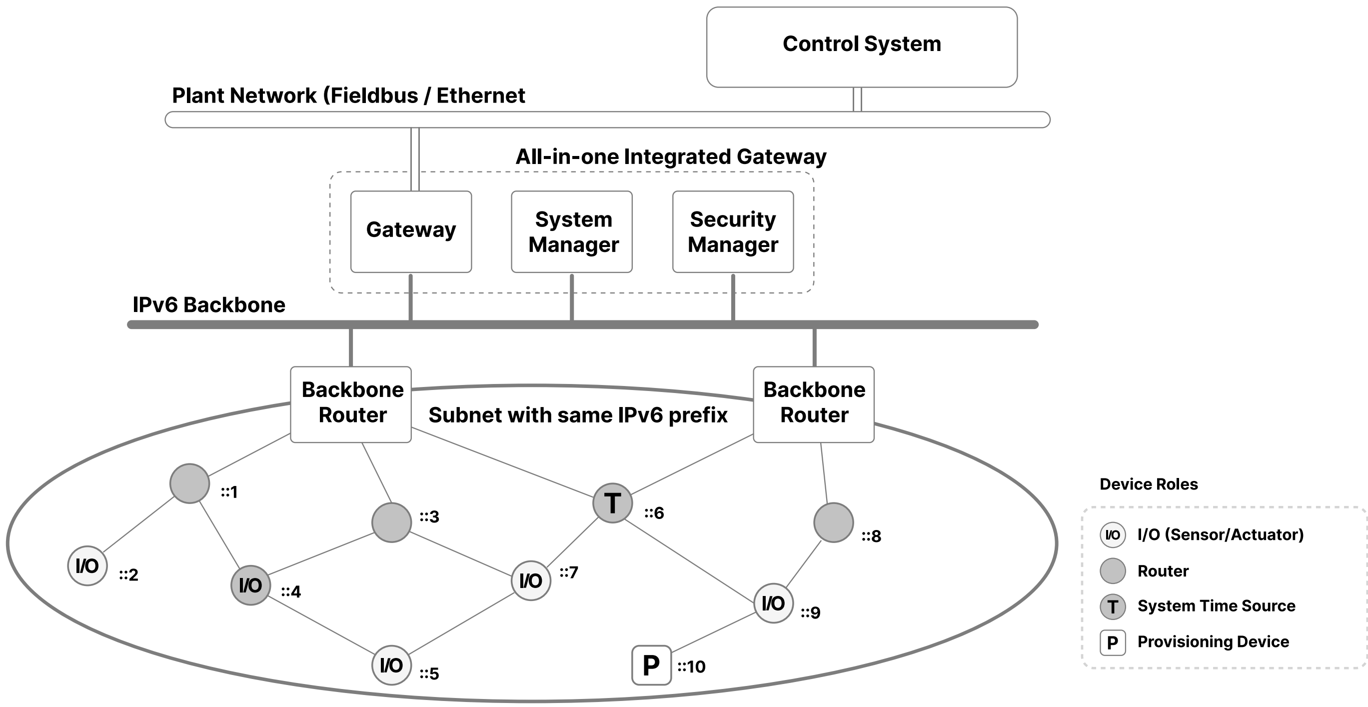

Figure 1. ISA100 Wireless System Architecture

[3] ISA100 WCI, The Technology Behind the ISA100.11a Standard – An Exploration

ISA100 Wireless is based on 6LoWPAN **[4]**, standardized in IETF RFC4944, enabling efficient IPv6 networking over a low-rate, low-power wireless network. As shown in **Figure 1**, the wireless network acts as a stub in the IPv6 network. The role of the backbone router includes translating addresses between 6LoWPAN and IPv6 formats, packet compression and expansion, fragmentation and reassembly, and IP routing in the IPv6 backbone network. Hence, message forwarding within the wireless network happens using short addresses and compressed messages, and the backbone router makes it seamless for the rest of the network.

ISA100 Wireless offers several techniques to achieve robust communication within the wireless network, such as:

- **Time diversity:** The protocol uses time scheduling to achieve deterministic communication. Time slots are pre-allocated centrally by the system manager, and they can be optimized to improve robustness and latency.
- **Frequency diversity:** The protocol specifies different channel hopping schemes, where each device changes the communication frequency between successive timeslots. This increases the probability of successful transmissions, making the protocol resilient against channel selective fading and RF interference.
- **Spectrum management:** The system manager adaptively changes the channel allocation based on performance metrics received from the wireless devices. Channels known to be impacted by an RF interferer can manually be added to an exclusion list for a configurable period of time.
- **Path diversity:** The protocol supports redundant routes in the network to improve robustness against a route failure. Different routes are supported based on the type of traffic, such as periodic updates, event notifications, or bulk data transfer. Routes are managed centrally and adapted based on diagnostics and statistics received from the devices.

The resulting wireless network is adaptive, self-organizing, and self-healing, which can be centrally managed by the system manager. With 6LoWPAN and IPv6, ISA100 Wireless achieves end-to-end IP addressability for each node, thereby enabling easy integration into IoT solutions. It provides a robust networking foundation for industrial needs and enables tunneling for any application layer protocol.

Since ISA100 Wireless was standardized in 2012, several guidelines and best practices have been adopted. For instance, a transmission range of 30 m can be expected in the presence of obstructions, but a range of 100 m is possible in a clear line-of-sight communication or when deployed in a multi-hop communication setup. The latency of ISA100 wireless communication is in the order of 100 ms. This latency is well below the data update period of practical process control devices, which is generally greater than 0.5 s. ISA100 Wireless networks usually scale up to 50 devices per backbone router and around 500 devices per system manager **[5]**. Moreover, ISA100 Wireless provides a lot of flexibility with various configuration options, as detailed in the following section.

[4] Emerson, A Comparison of WirelessHART™ and ISA100.11

[5] Yokogawa, Yokogawa Field Wireless Solution

ISA 100.11: Protocol Stack

The OSI protocol stack of ISA100 Wireless is shown in **Figure 2**.

Wireless Networking Stack (WPAN)	
Application/ Application Support	• ISA100 Native Protocol • Object Oriented • Protocol tunneling • Open for Implementation
Transport Layer	• Connection-less (UDP RFC768) Transport • Transport Layer Security (optional) • Standard IPv6 Networking
Network Layer	• 6LoWPAN (IETF RFC4944)
Data Link Layer	Mesh-under multipath graph routing, Source routing, Centrally managed
	802.15.4 MAC customized, Centrally managed F/TDMA, Channel hopping, CSMA-CA, Security (optional)
Physical Layer	• 802.15.4 PHY • 2.4 GHz, OQPSK, DSSS, 250 kbps, max. 10 dBm

Figure 2. ISA100 Wireless Protocol Stack

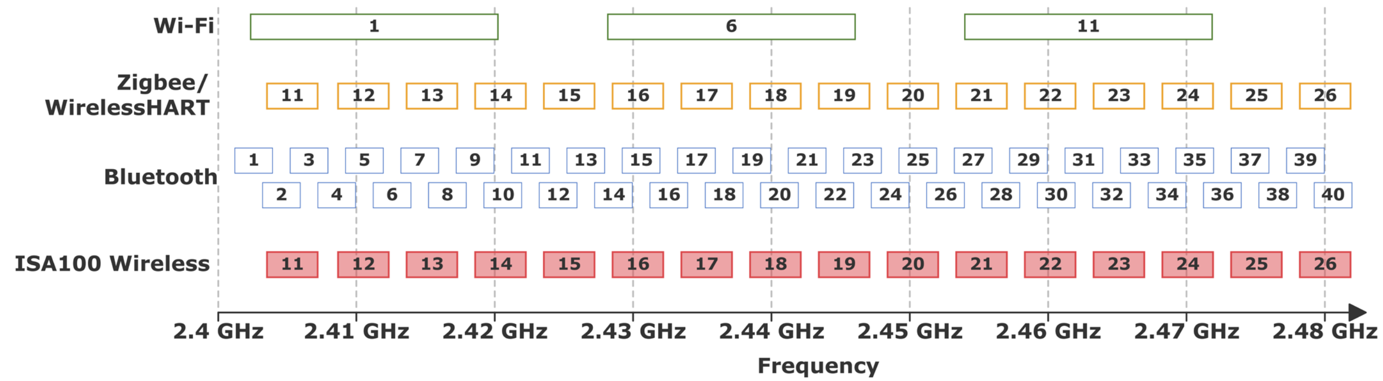

Figure 3. Frequency channels of ISA100 Wireless

The physical layer of ISA100 Wireless is based on the 802.15.4 standard, with the restriction to use only the channels in the 2.4 GHz ISM band. It allows the use of all the 16 specified RF channels, each 2 MHz wide and spaced 5 MHz apart, with center frequencies ranging from 2.405 to 2.480 GHz, as shown in Figure 3. The last channel, which is not worldwide supported, can optionally be disabled to meet global conformity. The transmission power of devices is adjustable up to 10 dBm, enabling a tradeoff between transmission range and battery life. ISA100 Wireless uses Offset Quadrature Phase Shift Keying (OQPSK) modulation with a data rate of 250 kbps. The protocol also employs Direct Sequence Spread Spectrum (DSSS) to achieve resilience against RF interference and channel fading.

ISA100 Wireless defines its own data link layer to achieve industrial-grade robust communication in the congested 2.4 GHz frequency band. It is based on the 802.15.4 MAC layer with additional custom features and support for link layer packet routing.

The protocol uses Time Division Multiple Access (TDMA) as its main channel access mechanism. Communication occurs in distinct timeslots that have a configurable length. Timeslots are centrally configured and allocated to transmitter and receiver devices by the system manager. As shown in Figure 4, during a dedicated timeslot, the scheduled transmitter sends a data packet and waits for an acknowledgment from the receiver within the same timeslot. The protocol also supports Duocast, a mechanism that enables acknowledgment by multiple receivers within the same timeslot. The system manager also allocates sequences of timeslots to form superframes, which can be repeated periodically.

ISA 100.11: Protocol Stack

Besides the above-described TDMA scheme, ISA100 Wireless also applies two different frequency hopping modes to make the protocol more robust in the presence of interference. In slotted hopping mode, as shown in Figure 4, the used RF communication channel is changed for each time slot. In slow hopping mode, on the other hand, several timeslots are merged to create a longer timeslot, and the devices continue using the same RF channel for the entire duration of the timeslot. In this channel hopping scheme, multiple transmitters are allowed to share the same timeslot on a contention basis via Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). Moreover, slotted and slow hopping methods can be combined to improve latency because transmitters don't have to wait until the next allocated timeslot to communicate.

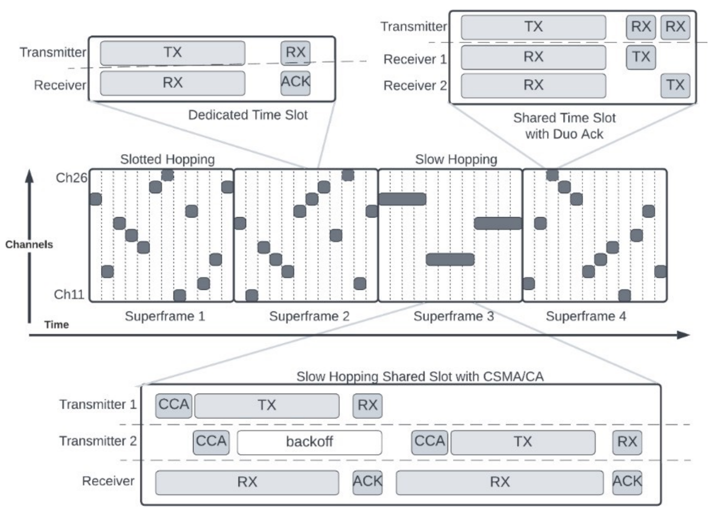

Figure 4. Frequency hopping of ISA100 Wireless

The data link layer also integrates link layer forwarding, also called mesh-under or L2 routing, to relay messages within the wireless data link (DL) subnet. As the DL subnet shares the same IPv6 prefix, the applied routing can take place with the use of short addresses. ISA100 Wireless supports two routing mechanisms:

- Graph routing is the main routing scheme in ISA100 Wireless, where network routes are determined centrally by the system manager and distributed to the individual devices. The system manager receives periodic network health reports from devices, and it adapts the routes if necessary. The standard supports using different graphs based on the type of transmitted data, such as event notifications, bulk transfers, or periodic updates. Moreover, the network supports redundant routes to ensure path diversity.

- Source routing is a supplemental routing mechanism where the source device determines the route of the packet and writes the ordered list of intermediate hops into the packet header. Intermediate nodes relay the packet based on this information without requiring additional topology information.

The network layer in ISA100 Wireless utilizes 6LoWPAN as defined in RFC4944. The backbone router has many functionalities; one of them is the critical role of routing between the DL subnet and the IPv6 backbone. 6LoWPAN in the network layer of the backbone router is responsible for translating device addresses from the 16-bit short format on the DL subnet side to the 128-bit long address format on the IPv6 side and vice versa. Besides, 6LoWPAN inherently supports the fragmentation and reassembly of large IPv6 packets on the backbone router. To decrease the network traffic caused by IPv6 overhead, 6LoWPAN also performs compression of the IPv6 and UDP headers. While routing in the IPv6 backbone is also the responsibility of the network layer, it is beyond the scope of ISA100 Wireless specification.

In the transport layer, ISA100 Wireless provides a connection-less transport service based on UDP, which can simultaneously accommodate multiple application layer protocols. Therefore, the standard does not enforce a specific application layer but enables tunneling of any non-native application traffic through the ISA100 Wireless network. Moreover, ISA100 wireless offers an object-oriented application model, which can be tailored to be easily integrated into new designs.

The tunneling feature of ISA100 wireless makes it an application layer agonistic communication basis for a wide range of use cases. For instance, PROFIsafe is an application sublayer that takes care of the functional safety of communication. By adding PROFIsafe on top of ISA100 Wireless, the system can achieve functional Safety Integrity Level 2 (SIL 2) according to the IEC 61508 standard, which is required by safety and alarm applications, for instance **[6]**.

[6] ISA100 WCI, Safety and alarming applications using ISA100 Wireless

Security in ISA100 Wireless

The ISA100 Wireless standard offers state-of-the-art security mechanisms at multiple levels of the OSI stack. In the transport layer, every message can be end-to-end protected to ensure message confidentiality, data integrity, and source authentication, while the protocol supports hop-to-hop protection in the link layer.

The standard supports several security mechanisms, such as symmetric and asymmetric key cryptography, that are used for encryption and commissioning, respectively; however, the applied security mechanisms are configurable and optional. The security manager is responsible for controlling the overall security policy and for generating, distributing, and managing the required keys.

Implementing ISA100 Wireless with Silicon Labs SoC

Silicon Labs offers wireless SoCs, such as the EFR32MG24 **[7]**, which can serve as the basis for implementing an ISA100 wireless product. This specific SoC includes an 802.15.4 compliant 2.4 GHz radio transceiver, which offers -105.4 dBm sensitivity when operating in OQPSK DSSS mode used by ISA100. With 1536 kB flash and 256 kB RAM offered by the EFR32MG24, both the wireless stack and the application can be implemented on a single SoC, thereby enabling low BOM cost. Silicon Labs also has expertise in implementing 802.15.4-based communication stacks and offering building blocks, such as 6LoWPAN, that can be adapted for ISA100 Wireless. Moreover, the SoC can operate in Host, Network Co-Processor (NCP), and Radio Co-Processor (RCP) modes to support different architectures.

On the software offerings, 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. Silicon Labs also offers SoCs for other wireless technologies, such as Bluetooth Low Energy (BLE), that can be used to extend the current features of ISA100 Wireless.

[7] EFR32MG24 Wireless SoC Family Data Sheet

Summary

ISA100 Wireless is an industrial standard that is commonly used in the process automation industry for monitoring and open and closed-loop control applications. While the standard is based on the 802.15.4 radio specifications, the extensions of ISA100 Wireless add a lot of flexibility to meet stringent requirements, such as determinism, robustness, and security. Scalability and seamless operation are other core features of ISA100 Wireless that are enabled by using 6LoWPAN in the wireless nodes and in the IPv6 backbone. Silicon Labs offers several 2.4 GHz wireless SoCs, such as EFR32MG24, that have the required hardware and software features to implement an ISA100 Wireless device.