International Journal of Embedded and Wireless Communication Systems
Volume1, Issue 3 2025

Wireless Interfaces for Embedded System with Intelligent Sensors and Actuators

Peng Ran[1], Jun Wu[2]

Chongqing University of Posts and Telecommunications, Chongqing 400065, China Chongqing Kaize Technology Co. Ltd., Chongqing 400042, China

Research Article

Date of Submission: 10-04-2025 **Date of Acceptance: 17-07-2025** **Date of Publication: 23-08-2025**

ABSTRACT: The new embedded system makes extensive use of the wireless interfaces. The characteristics required for such services are analyzed by a research of the parameters. To link intelligence-based actuators and sensors, these interfaces are significantly altered. They enable the number of wires, object control, and distance monitoring.

Keywords: Wireless Interfaces, Embedded Systems

Introduction

For a long time, embedded microprocessor systems have been utilized in nearly every facet of our lives, including public events, businesses, residences, workplaces, vehicles, and more. Because of this, its characteristics—like reliability, flexibility, security, adaptability, cost, size, etc.—are constantly and swiftly enhanced.

Alongside the control devices, microcontrollers, which have a wide variety of building blocks and improved functionalities, the peripherals (sensors, actuators, etc.) quickly evolve and become more "intelligent." It is therefore necessary to improve communication methods between humans and embedded systems, as well as between embedded system components (Figure 1) and within a network of embedded systems. This is in addition to the fact that embedded systems are occasionally used in harsh environmental conditions like electromagnetic interference, temperature fluctuations, humidity, dust, vibration, etc. As an example, think about how embedded systems' user interfaces have changed over time, beginning with buttons, keyboards, seven-segment indicators, and LCDs and concluding with the practical and comfortable use of modern touchscreen devices, like the popular smartphones, tablets, and other personal mobile devices.

The increasing number of programmable devices in embedded systems demands the rapid development of wireless interfaces in order to do away with cable connections. There are several of them, depending on the application areas of embedded systems [1], [2]. These days, their main applications include remote industrial monitoring and control, access control, smart sensor networks, machine-to-machine and man-machine interaction, and smart home applications.In relation to study cases in Microprocessor Circuits and Embedded Systems for the Bachelor of Electronics degree students at the Technical University of Gabrovo, this paper looks at some of the most popular contemporary wireless interfaces in the fields of home automation and the Internet of Things (IoT).

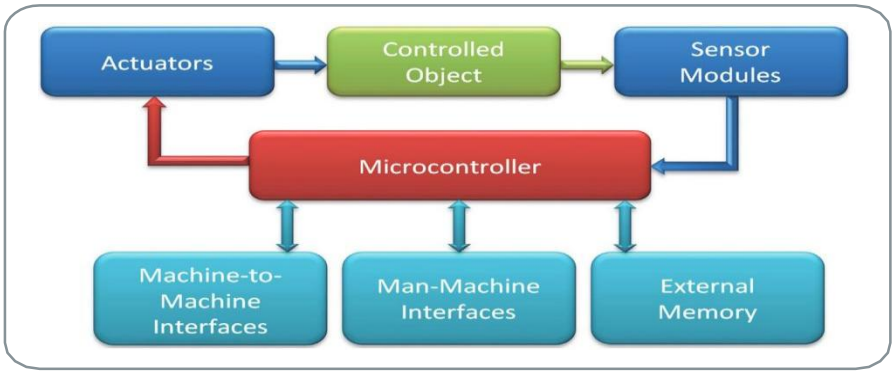


Figure 1. Hypothetic block diagram of an embedded system

1. A Short Survey On Wireless Interfaces For Embedded Systems Applications

1.1 Infrared Data Association (IrDA)

IrDA is an optical open channel interface that enables peer-to-peer communication across short distances. The baud rate is 2.4 kbps. One Gbps is achievable at a distance of one meter, according to several standards that specify six ranges with different data coding and application zones [3]. The light emitter and detector have angles ranging from 15°% to 30°% and up to 15°%, respectively. As a result, the two communication gadgets have to face the same way. The amount of power utilized is quite low.
This technique does not conflict with radio frequency technologies, is reasonably unregulated, and is reasonably priced. The optical channel offers a relatively high level of data transfer security, but it also has the drawback of needing the devices to be in line of sight.

IrDA evolves into a potential optical wireless communication technology that provides data rates of 5 and 10 gigabits per second at larger angles and three-meter distances.

The IrDA interface may be used in small autonomous embedded systems, mobile control devices (such smartphones and tablets), industrial and medical equipment, etc. due to the short-range connection.

Several microcontrollers, including several Microchip 16-bit and 32-bit microcontrollers, include built-in IrDA standard compatibility via their UART modules and an additional IR Encoder/Decoder and IR Transceiver [4].

1.2 Bluetooth

Originally designed specifically to replace wire cords in computer peripherals, Bluetooth (IEEE Standard 802.15.1) is currently one of the technologies utilized for wireless communication in embedded systems. It makes use of the 2.4 GHz unlicensed industrial, scientific, and medical (ISM) radio spectrum [5].

Each Bluetooth device has a unique address that allows other devices to recognize it. Without the user's input, the devices establish the connection on their own.

In a Bluetooth system, every device is referred to as a "piconet." In a piconet, a master device can communicate with up to seven slave devices, and the slaves can only connect with each other via the master. A gadget could be a

Only one of the four piconets is a master at the same time. The piconets are connected by the master. The piconet's members synchronize their frequencies so that they are in contact with one another after starting data transfer.

The benefits of Bluetooth technology include compact equipment size, ease of use, data security, strong support, and standard development. The inability to set up intricate network setups and rather high power consumption are two disadvantages.

1.3 ZigBee

ZigBee (IEEE Standard 802.15.4) is intended for shorter distance range, lower cost, lower power consumption, lower data

transfer rates, more compact, and simpler variant of wireless personal area networks (WPANs) in comparison to Bluetooth. It uses the same frequency range of 2,4 GHz [6]. ZigBee realizes various network topologies - star, tree and mesh.

The devices (nodes) in the ZigBee network can be:

• ZigBee Coordinator, (one in a piconet) which can communicate with other networks and to save data about its own;

• ZigBee Router, which can pass data on from other devices and serves as an intermediate router;

• ZigBee End Device – the simplest kind of device, which can communicate only with the above two.

The minimal power consumption is a result of the fact that the slaves are in sleep mode most of the time. They activate for short time intervals only to confirm their presence in the network.

There are four main application areas for ZigBee technology: smart homes, connected lighting, utility industry, zigbee smart energy. The last one is a standard for interoperable products that monitor, control, inform, and automate the delivery and use of energy and water.

1.4 Radio-Frequency Identification (RFID)

RFID uses electromagnetic fields to automatically identify and track tags attached to objects.

The typical components of a RFID system are a tag, a reader and an antenna. Various types of tags and readers are used. They can work in several frequency ranges, providing data exchange in different distances: low frequencies (LF) - 125 kHz - 134 kHz, in a distance up to 10 cm; high frequencies (HF) - 13,56 MHz in a distance up to 30 cm; ultra-high frequencies (UHF) 433 MHz and 856 MHz - 960 MHz in a distance up to 100 m; 2450-5800 MHz (microwave) - 1 - 2 m and 3.1–10 GHz ultra-wideband (UWB) - 200 m.

The various frequency ranges of RFID are specified in the ISO/IEC 18000 standard, except the last, which is not standardized. ISO/IEC 14443 and ISO/IEC 15693 define smart card and proximity card interfaces operating in the HF range [7].

The tags are three types: passive, semi-passive and active. Passive tags have no their own power supply. They are supplied by the electromagnetic energy received from the reader. That is why the distance allowed is shorter than at the active - typically to 10 m. Active tags (with own power supply - battery) transmit signal to send information stored in the chip at distances up to 100 m. Typically, active tags are used to identify large objects, wagons, containers, etc., which should be monitored over long distances, electronic labels in warehousing, etc. [8].

Active tags themselves are of two types: transponders, which are awakened by the reader, switch on their power and response, and beacons, which periodically wake, switch on and transmit a signal to the reader.

The semi-passive tags use own power source only to switch on the tag. Unlike active transponders, they have a transmitter. They are used for larger distances and transmit in the frequency range of 850 to 950 MHz.

The common application of RFID technology in the field of embedded systems is in the first two frequency ranges - such as access control, pet identification, tracking of goods, etc. Various forms of tags exist: bracelets, badges, stickers, labels, chips, cards, pins tags for clothing, ampoules for pets chipping, etc.

Although RF technologies in their origin are not appropriate for Internet access, their further development makes it possible [9].

The technology is comparatively easy to implement using microcontrollers with RF transmitters, like Microchip’s PIC12/16.

1.5 Near Field Communication (NFC)

NFC (ISO/IEC 14443 and ISO/IEC 18000-3) is a modern variety of RFID in the 13,56 MHz frequency range, allowing very short distance communication – up to 10 cm [10]. It is applicable for assets identification, access control, contactless payment,

etc.

There are three NFC communication modes:

• NFC peer-to-peer - for data exchange between two paired mobile devices;

• NFC reader/writer - in which one of the devices is active - it sends signals and receives the data sent form the passive device;

• NFC card emulation - NFC-enabled devices like smartphones could be used as credit cards for contactless payment or ticketing.

Initially the technology is designed for access control (identification) and digital tickets in public transportation. Later it is introduced in payment cards (as integrated chips) and smartphones for contactless payment.

NFC is very suitable for configuring of embedded systems using the results of other applications available for smart devices like graphics processing, complex calculations, GPS positioning, Internet communications. Similarly, NFC applies when the smart device wishes to obtain information from an embedded system.

Other useful applications of NFC include passive tags, embedded in advertisement posters and information boards, thereby sending useful information to the users, like scanning QR code.

Smartphones can operate as a reader and as a tag, which makes possible peer-to-peer communication. By holding the smartphone to the NFC-enabled device, the user is able to connect via Bluetooth much faster than pairing devices manually.

The main implementation problems are the proper infrastructure and the data safety.

1.6 Z-Wave

Z-Wave is one of the newest wireless technologies in the RF range. It operates in the sub-GHz band, thereby avoiding interference with other wireless technologies in the 2.4 GHz range (Bluetooth, ZigBee, etc.) [11], [12].

It is designed especially for home automation and Internet of Things. A Z-Wave hub (network controller) manages the communication. It allows a distance control via remote web access.

Up to 232 devices could be connected in a mesh network topology in a line of sight up to 100 m. Repeaters (hops) are used in case of obstacles - maximum four hops in a network, increasing the distance up to 200 m.

The devices are interoperable - all they apply ITU-T G.9959 global radio standard and they are compatible, regardless the manufacturer or brand.

Presently over 1700 interoperable Z-Wave products for various home automation applications are available: lighting, lock, various sensors, power management, irrigation, thermostats, etc. Over 70 million products are sold worldwide [12].

1.7 WiFi

IEEE wireless network standard WLAN 802.11is initially intended to connect wirelessly mobile devices in a local network, beginning later to be used for Internet connection [13].

While the above wireless standards can be used quite successfully to connect a microcontroller with a periphery for rela- tively short distances, the WiFi is used in two directions:

• To connect the user with the system using the widely spread mobile devices - smartphones, tablets, laptops, in short distance.

The advantage is that a regular user without professional qualification could easily configure the connection with new de- vices, unlike ZigBee for instance.

• To connect embedded systems and their blocks with World Wide Web [14];

It is a rapidly growing technology with a great potential. On one hand it gives an opportunity for flexible and rapid monitoring and control of wirelessly connected embedded client devices, so called “Internet of Things” (or “Wireless Connectivity of Things”), ànd on the other it could be applied successfully together with perspective cloud computing.

Another advantage of WiFi is the high data rate. An amendment to the IEEE 802.11-2007 wireless-networking standard specifies significant increased data rates - from 54 Mbit/s to 600 Mbit/s, using multiple antennas in order to improve network throughput.

It is the most expensive technology in comparison to the above mentioned, but is getting cheaper through the years. In addition, it is significantly cheaper than using a dedicated touch panel for an embedded system.

WiFi is a suitable way to configure and control remotely embedded systems from long distances around the world and from a variety of devices.

Table. 1 presents a short summary of the main features of the above examined short range wireless technologies.

2. Conclusion

This article provides a brief overview of the characteristics, constraints, and potential applications of contemporary wireless technology in embedded systems, namely home automation and the Internet of Things.

These days, the most popular wireless technologies are WiFi and Bluetooth, which were first created for personal and professional connection. They are dependable, efficient, and constantly evolving under IEEE802 subgroups of standards, enabling the use of standard personal digital devices. Although it is the most costly method, WiFi is the most adaptable and expandable. For the implementation of a ubiquitous man-machine interface, both methods are ideal.

The radio frequency range interfaces have different properties and, therefore, different application areas. It is not necessary for LF devices to communicate in a line of sight. They are designed for low-data-transfer, short-distance communication. In contrast to HF, UHF, and microwaves, the connection is stable near metal objects, water, etc. Access control, object tracking, and positioning are some of their primary application areas.

Z-Wave, Wireless Sensor and Actuator Network protocol DASH7, networking protocol for Internet of Things (IoT) Thread, EnOcean and Insteon technologies for home automation, and other rapidly evolving fields like building and industrial automation, IoT, and sensor networks imply

Technology	Network topology	Data transfer rate	Wavelength/ Frequency range	Distance, m	Power consumption	Internet connectivity	Smart mobile devices access
IrDA	peer-to-peer	2,4 kbps-1 Gbps	850–900 nm	0,1-1	low	difficult	not very suitable
Bluetooth	peer-to-peer;star; piconets with up to 7 nodes	1 - 3 Mbps	ISM: 2,4 GHz	0,1 - 100	1 - 100 mW	yes	most suitable
ZigBee	peer-to-peer; star; mesh	250 kbps (20 kbps)	ISM: 2,4 GHz (868 MHz in Europe)	10-100	1 - 100 mW; typically 1 mW	yes	not suitable
RFID	peer-to-peer	LF: 4-8 kbps; HF: 6.7 kbps to 848 kbps	LF: 125–134 kHz HF: 13.56MHz	LF: up to 10 cm HF: up to 100 cm	very low	difficult	not suitable
NFC	peer-to-peer	106, 212 or 424 kbps	13.56MHz	< 20 cm; typical - 4 cm	Tag: none Reader: very low; typically 1 mW	difficult	most suitable
Wi Fi	star	11 (b), 54 (g), 600 (n) Mbps, (ac) 1,3 Gbps; (ad) 7 Gbps	(n) ISM: 2,4 GHz и/или 5 GHz; (ac) 5 GHz	30-100	highest	excellent	most suitable
Z-WAVE	peer-to-peer; mesh, up to 232 nodes	40 - 100 kbps	ISM: 868.42 MHz (Europe)	up to100 m; up to 200 m with 4 hops; typically up to 30m	very low; typically 1 mW	difficult	most suitable