ISA-100.11a-2009

An ISA Standard

Wireless systems for industrial automation: Process control and related applications

5

INTRODUCTION

0.1 General

The ISA100 Committee was established by ISA to address wireless manufacturing and control systems in areas including:

- The environment in which the wireless technology is deployed;
- Technology and life cycle for wireless equipment and systems; and
- The application of wireless technology.

The Committee's focus is to improve the confidence in, integrity of, and availability of components or systems used for manufacturing or control, and to provide criteria for procuring and implementing wireless technology in the control system environment. Compliance with the Committee's guidance will improve manufacturing and control system deployment and will help identify vulnerabilities and address them, thereby reducing the risk of compromising or causing manufacturing control systems degradation or failure.

This standard is intended to provide reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. This standard defines the protocol suite, system management, gateway, and security specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices supporting very limited power consumption requirements. The application focus is to address the performance needs of applications such as monitoring and process control where latencies on the order of 100 ms can be tolerated, with optional behavior for shorter latency.

To meet the needs of industrial wireless users and operators, this standard provides robustness in the presence of interference found in harsh industrial environments and with legacy non-ISA100 compliant wireless systems. As described in Clause 4, this standard addresses coexistence with other wireless devices anticipated in the industrial workspace, such as cell phones and devices based on IEEE 802.11x, IEEE 802.15x, IEEE 802.16x, and other relevant standards. Furthermore, this standard allows for interoperability of ISA100 devices, as described in Clause 5.

This standard does not define or specify plant infrastructure or its security or performance characteristics. However, it is important that the security of the plant infrastructure be assured by the end user.

0.2 Document structure

This standard is organized into clauses focused on unique network functions and protocol suite layers. The clauses describe system, system management, security management, physical layer, data link layer, network layer, transport layer, application layer, gateway, and provisioning. Each clause describes a functionality or protocol layer and dictates the behavior required for proper operation. When a clause describes behaviors related to another function or layer, a reference to the appropriate clause will be supplied for further information.

The following terms are used in this document to describe device behavior:

- Mandatory: behavior or a protocol that is required for a device to state compliance with the standard (e.g., symmetrical keys).
- Optional: behavior or protocol defined in the standard that is not required for compliance to the standard but, if implemented, shall be compliant with the standard (e.g., asymmetrical keys).
- Configuration: setting of a parameter that will alter behavior and can be set by the system manager (e.g., network layer hop limit). Configurations where defaults are appropriate will state those defaults (e.g., network layer hop limit = 64).

- Capability: ability of device to perform to a specified level (e.g., number of children a router can support). Profiles will specify a minimum capability.
- Feature: notable characteristic of a device (e.g., battery powered).

Mandatory behavior (also referred to as normative behavior) is denoted by the use of the term shall. Non-mandatory behavior (also referred to as informative behavior) is denoted by the use of the terms may or recommended.

The mandatory and optional communication protocols defined by this standard are referred to as native protocols, while those protocols used by other networks such as legacy fieldbus or HART communication protocols are referred to as foreign protocols.

0.3 Disclaimers

ISA does not take any position with respect to the existence or validity of any patent rights asserted in connection with this document, and ISA disclaims liability for the infringement of any patent resulting from the use of this document. Users are advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Pursuant to ISA's Patent Policy, one or more patent holders or patent applicants may have disclosed patents that could be infringed by use of this document and executed a Letter of Assurance committing to the granting of a license on a worldwide, non-discriminatory basis, with a fair and reasonable royalty rate and fair and reasonable terms and conditions. For more information on such disclosures and Letters of Assurance, contact ISA or visit www.isa.org/StandardsPatents.

Other patents or patent claims may exist for which a disclosure or Letter of Assurance has not been received. ISA is not responsible for identifying patents or patent applications for which a license may be required, for conducting inquiries into the legal validity or scope of patents, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory.

ISA requests that anyone reviewing this Document who is aware of any patents that may impact implementation of the Document notify the ISA Standards and Practices Department of the patent and its owner.

Additionally, the use of this standard may involve hazardous materials, operations or equipment. The standard cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions. The user of this standard must exercise sound professional judgment concerning its use and applicability under the user's particular circumstances. The user must also consider the applicability of any governmental regulatory limitations and established safety and health practices before implementing this standard.

NOTE The ISA100 standards development committee, which developed this ISA standard, is seeking feedback on its content and usefulness. If you have comments on the value of this document or suggestions for improvements or additional topics, please send those comments by email, fax, post, or phone to:

ISA100

ISA Standards

67 Alexander Drive

Research Triangle Park, NC 27709 USA

Email: standards@isa.org

Tel: +1 919 990 9200 Fax: +1 919 549 8288

ISBN: 978-1-936007-26-4

An ISA Standard

ISA100.11a-2009

Wireless systems for industrial automation: Process control and related applications

1 Scope

This project will define the OSI layer specifications (e.g., PhL, DL, etc.), security specifications, and management (including network and device configuration) specifications for wireless devices serving application classes 1 through 5 and optionally class 0 for fixed, portable, and moving devices.

NOTE Usage classes are described in Annex C.

The project's application focus will address performance needs for periodic monitoring and process control where latencies on the order of 100 ms can be tolerated, with optional behavior for shorter latency.

This project will address:

- Low energy consumption devices, and also those applications that have latency and latency variability constraints, with the ability to scale to address large installations;
- Wireless infrastructure, interfaces to legacy infrastructure and applications, security, and network management requirements in a functionally scalable manner;
- Robustness in the presence of interference found in harsh industrial environments and with legacy systems;
- Coexistence with other wireless devices anticipated in the industrial work space, such as IEEE 802.11x, IEEE 802.16x, cell phones, and other relevant standards; and
- Interoperability of ISA100 devices.

2 Normative references

The following standards and specifications contain provisions which, through references in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision and may be changed without notice, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE See the bibliography for non-normative references.

ANSI X9.63-2001, *Public key cryptography for the financial services industry - Key agreement and key transport using elliptic curve cryptography*. American Bankers Association, November 20, 2001

FIPS 197, *Advanced encryption standard (AES)*, Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November 26, 2001