



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.08-2017

Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers

Approved 24 April 2017

NOTICE OF COPYRIGHT

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.



Documents
Document Sharing Hub

ISA-TR84.00.08-2017, Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers

ISBN: 978-1-945541-56-8

Copyright © 2017 by the International Society of Automation. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the publisher.

ISA
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709
E-mail: standards@isa.org



Documents
Document Sharing Hub

Preface

This preface, as well as all footnotes, is included for information purposes only and is not part of ISA-TR84.00.08-2017.

This technical report has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of automation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA, 67 T.W. Alexander Drive; P.O. Box 12277; Research Triangle Park, NC 277099; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards, recommended practices, and technical reports. The Department is further aware of the benefits of USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, the Department will endeavor to introduce SI and acceptable metric units in all new and revised standards to the greatest extent possible. The Metric Practice Guide, which has been published by the Institute of Electrical and Electronics Engineers (IEEE) as ANSI/IEEE Std. 268-1992, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all interested individuals in the development of ISA standards. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS 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 DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT 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 DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

ISA (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

This technical report is a work product of the ISA84 standards development committee. The following served as leaders of ISA84 during the technical report's development and publication:

NAME/AFFILIATION	LEADERSHIP POSITION
Rahul Bhojani, BP	Co-Chair
Paul Gruhn, aeSolutions	Co-Chair
Richard Dunn, DuPont	Vice Chair
Nicholas Sands, DuPont	Co-Managing Director
Dennis Zetterberg, Chevron	Co-Managing Director

This technical report was developed by ISA84 Working Group 8 under the shared leadership of Kevin Klein and Greg LaFramboise of Chevron, and Ted Schnaare of Emerson.

The following served as members of the ISA Standards and Practices Board and approved the document on 24 April 2017:

NAME	AFFILIATION
M. Wilkins, Vice President	Yokogawa
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc.
E. Cosman	OIT Concepts, LLC
D. Dunn	Consultant
J. Federlein	Federlein & Assoc. LLC
B. Fitzpatrick	Wood Group Mustang
J. Gilsinn	Kenexis Consulting
J.-P. Hauet	KB Intelligence
D. Lee	Avid Solutions
G. Lehmann	AECOM
K. Lindner	Endress+Hauser Process Solutions AG
T. McAviney	Consultant
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
G. Nasby	City of Guelph Water Services
M. Nixon	Emerson Process Management

D. Reed
N. Sands
H. Sasajima
H. Storey
K. Unger
I. Verhappen
D. Visnich
W. Weidman
J. Weiss
D. Zetterberg

Rockwell Automation
DuPont
Fieldcomm Group Inc. Asia-Pacific
Herman Storey Consulting
Consultant
Industrial Automation Networks
Burns & McDonnell
Consultant
Applied Control Solutions LLC
Chevron Energy



This page intentionally left blank.

CONTENTS

Introduction	9
1 Scope	11
2 References	11
3 Definitions of terms and acronyms	11
3.1 Definitions	11
3.2 acronyms.....	13
4 Wireless sensor network design	14
4.1 Introduction	14
4.2 IPL Criteria.....	14
4.3 Design and layout of the wireless sensor network	14
4.4 Availability.....	17
4.5 Security.....	22
4.6 Purchasing and factory acceptance testing.....	25
4.7 Commissioning and validation testing	25
5 Operations and maintenance phase	26
5.1 Spectrum management.....	27
5.2 KPIs for monitoring the network performance	28
5.3 Diagnostics and testing	31
5.4 Power management.....	32
5.5 Battery maintenance.....	32
5.6 Security.....	32
5.7 Auditing.....	32
5.8 Operation and maintenance performance assessment	32
6 Management of Change (MOC)	32
6.1 Application program / Configuration management	33
6.2 Embedded software management.....	33
6.3 Utility software management.....	33
Bibliography	34
Annex A – Implementation checklists.....	37

Figures

Figure 1 – Example connection architectures for process control networks 16

Figure 2 – Publication latency timeline 20

Figure 3 – Request-response latency timeline 20

Tables

Table 1 – Acronyms..... 13

Table 2 – Considerations for wireless network design and layout 15

Table 3 – Security threats and countermeasures 23

Table 4 – Operation and maintenance clauses 27

Table 5 – KPIs for monitoring network performance 29

Introduction

The use of wireless technology for communication, devices and systems is prevalent in most industry sectors. The process sector has begun using wireless communication and devices in monitoring applications. The movement to utilize the benefits of wireless technology is being reviewed for applications in safety controls, alarms and interlocks (SCAI). While the use of wireless technology has benefits, there are also considerations to ensure safe and reliable operation.

This technical report (TR) has been developed to describe the additional life cycle considerations that should be addressed when wireless technology is used in an Independent Protection Layer where the risk reduction claimed is less than or equal to 10. The implementation of safety instrumented functions has been specifically removed from consideration in the scope of this technical report, due to the additional uncertainties of measurement and communication timing inherent in the application of this technology; the current lack of standard methods for determining contribution of a mesh-style network to PFD/PFH (probability of failure on demand / probability of failure per hour) calculations and for evaluating the common cause contribution that would be introduced via a network shared between an initiating event and SCAI or between SCAI (common for wireless networks); and insufficient guidance addressing the systematic errors that can occur as a result of introducing obstructions or additional sources of interference in the wireless signal transmission path(s).

To simplify the discussion of wireless in this TR, it does not address wireless final elements and wireless systems where the logic for the function is located in a device of the network. The number of variables and complexity of implementing the logic in a device, similar to a fieldbus, would distract from the intent of this TR. In most cases, final elements for functions are not implemented with wireless devices due to the limitations of battery life.

This TR identifies additional considerations to be addressed during the design stage and the operating and maintenance phase of the safety life cycle when wireless technology is used in the implementation of a protection layer.

This page intentionally left blank.

1 Scope

- 1.1 This technical report (TR) addresses wireless technology-based sensors that are used in Independent Protection Layers (IPLs) providing a risk reduction factor of less than or equal to 10 (non-SIS IPL) by the authority having jurisdiction (typically the owner/operator or local regulatory authority), and establishes guidance and considerations for their utilization in the process sector. The use of wireless technology for higher risk reduction factors such as a Safety Instrumented Function has been specifically excluded from consideration in the scope of this technical report.
- 1.2 This TR does not address codes, regulations, and other requirements that apply only to the nuclear power industry.
- 1.3 This TR provides guidance in design and maintenance of wireless sensors used in a non-SIS IPL.
- 1.4 Recognizing that wireless sensor networks will have mixed data, not only risk reduction data but other process monitoring data as well, this TR applies to the wireless functions related only to risk reduction.
- 1.5 This TR provides guidance for fixed wireless sensor networks and portable and traveling wireless sensors that may periodically move from one part of a facility to another. The guidance provided is applicable for the periods of time when the sensors are connected to the network. An example of a sensor that periodically moves is a temperature monitoring point on a rail car.
- 1.6 Typical architectures for wireless sensor networks are shown in this TR; the guidance and considerations provided apply to both the sensor network as well as the associated wireless backhaul.
- 1.7 This TR does not cover notification classification (for example, alarms and alerts) or personnel actions associated with alarms. Refer to ANSI/ISA-18.2-2016 (see References immediately following) for alarm requirements.

2 References

The following documents are referenced in this document and are indispensable for its application. For each document, the latest edition (including any amendments) applies.

ANSI/ISA-84.91.01, *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks for the Process Industries*

ANSI/ISA-18.2, *Management of Alarm Systems for Process Industries*

(www.isa.org/standards)

3 Definitions of terms and acronyms

3.1 Definitions

Definitions and terminology used in this technical report are defined in ISA-84.00.01^[2] Part 1, Clause 3 (see bibliography). Additional definitions of terms used in this TR that are not previously defined are as follows:

3.1.1**backhaul**

a portion of a network that links smaller sub-networks to a main or core network

3.1.2**data packet**

a sequence of digital data representing a message or part of a message together with service digits including an address, organized to suit the transmission process and transmitted as a whole

[SOURCE: IEC 60050 ref. 721-09-02] ^[22]

3.1.3**fixed wireless**

wireless devices which do not move or move such a small distance that their network connections are not disturbed

3.1.4**gateway**

network device that is capable of caching wireless sensor network data and/or converting the wireless sensor network protocol to host protocols

3.1.5**latency**

the delay from input into a system to some desired output

3.1.6**Listen Before Talk (LBT)**

a technique used in radio communications whereby a radio transmitter first senses its radio environment before it starts a transmission

[SOURCE: IEEE 802.11] ^[16]

3.1.7**non-SIS IPL**

instrumented Independent Protection Layers which achieve a target risk reduction of less than or equal to 10.

3.1.8**portable wireless**

wireless devices which can move but remain fixed while performing their functions and do not maintain communications when being moved

3.1.9**stale data**

data which is no longer up to date

3.1.10**throughput**

the rate of successful message delivery over a communications channel

NOTE Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

3.1.11**traveling wireless**

wireless devices that work when moving slowly within a restricted area and maintain communications

3.1.12

Wireless Sensor Network Access Point (WSN AP)

a wireless sensor network node that also has a wired connection and serves as an entry/exit point for wireless sensor data

3.2 acronyms

A complete list of acronyms can be found in ISA-84.00.01^[2] Part 1, Clause 3. The abbreviated terms and acronyms used in this document include:

Table 1 – Acronyms

Abbreviation	Full expression
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BPCS	Basic Process Control System
CRC	Cyclic Redundancy Check
dBm	Decibel-milliwatts
DoS	Denial of Service
IEC	International Electrotechnical Commission
I/O	Input / Output
IPL	Independent Protection Layer
IRT	IPL Response Time
ISA	International Society of Automation
ISM	Unlicensed radio bands intended for Industrial, Scientific, and Medical uses
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LQI	Link Quality Indicator
MIC	Message Integrity Check
MOC	Management of Change
NIST	US National Institute of Standards and Technology
NTP	Network Time Protocol
PER	Packet Error Rate
RFI	Radio Frequency Interference
RSL	Receive Signal Level
SAT	Site Acceptance Testing
SCAI	Safety Controls, Alarms, and Interlocks
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SSL	Secure Sockets Layer
Wi-Fi AP	Wi-Fi Access Point
WSN AP	Wireless Sensor Network Access Point
WSN	Wireless Sensor Network

4 Wireless sensor network design

4.1 Introduction

Wireless sensors and sensor networks addressed in this technical report are typically characterized by the following:

- Wireless sensors will have a shape and size similar to wired sensors. The sensing element, radio, and battery will be contained within the instrument body.
- Wireless sensors are typically battery powered although some devices may be powered from other sources such as environmental energy harvesters. Wireless sensors achieve long battery life through duty cycled operation resulting in typical battery life in the range of 5 to 10 years.
- Radios contained within wireless sensors generally operate in industrial, scientific and medical (ISM) radio bands, notably in the 2.4 and 5 GHz bands. Wireless sensors typically have user-configurable update periods. Data transmission may have variable latency (jitter) due to path diversity. The update period and jitter should be taken into account when assessing response time.
- Wireless networks used in industrial environments have built-in security features to protect over the air data transmission.

4.2 IPL Criteria

An independent protection layer (IPL) should meet all of the following criteria:

- Specificity – An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (for example, a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event; therefore, multiple event scenarios may initiate action of one IPL.
- Independence – An IPL is independent of the other protection layers and the initiating event associated with the identified danger. It is not recommended that two layers of protection for the same hazard share common elements of the same wireless network.
- Dependability – It can be counted on to do what it was designed to do. Both random and systematic failure modes are addressed in the design. Dependability includes both the integrity and the reliability of the function.
- Auditability – It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary. This includes access security and management of change.

If all of the above criteria are satisfied for a given IPL, it is assumed that the IPL in question is capable of reducing risk by one order of magnitude. For the purposes of this TR, it is assumed that the risk analysis team has already determined that the protection layer, including the wireless sensor, network, and communications, meet the specificity and independence criteria. Thus, no further guidance on these IPL criteria is provided in this TR. Instead, the TR focuses on providing information on how to establish a design that satisfies the dependability and auditability criteria for SCAI using wireless sensors with a risk reduction factor (RRF) of less than 10. For additional information on IPLs, see Annex F of ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod)^[4].

4.3 Design and layout of the wireless sensor network

4.3.1 General

In order to avoid nuisance trips due to poor network performance, it is critical to closely adhere to manufacturers' best practices when designing and laying out a wireless sensor network. Specific