TECHNICAL REPORT

ISA-TR100.14.01-2011
Trustworthiness in
Wireless Industrial Automation:
Part I –
Information for End Users and Regulators

Approved Date – 26 May 2011

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR100.14.01-2011, Part I.

This document has been prepared as part of the service of ISA toward a goal of uniformity in the field of instrumentation. 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 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; 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. The Department is further aware of the benefits to 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, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, 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 concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. 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 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 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.

The following served as voting members on the ISA100 committee:

G. Mulligan	Consultant
A. Oliver	Worsley Alumina Pty Ltd.
L. Periera	FlexWorks Solutions International
T. Phinney	Consultant
R. Phung	Consultant
K. Pister	Dust Networks
I. Radomsky	ElTav Ltd.
S. Riendeau	Hydro-Quebec
T. Russ	StreetSmart Technology LLC
P. Sereiko	E-Senza
D. Sexton	GE Global Research
H. Storey	Herman Storey Consulting
J. Strecker	Frontier El Dorado Refinery
R. Struik	Consultant
W. Thoren	Endress+Hauser Process Solutions AG
K. Towers	Cooper Industries
Qin Wang	Univ. of Science and Technology, Beijing
Quan Wang	Chongqing Univ. of Posts and Telecommunications
J. Werb	Consultant
C. Whitehead	Rockwell Automation
L. Winkel	Siemens AG
G. Yon	EPS Corporation
M. Zielinski	Emerson Process Management

The following served as members of the Standards and Practices Board and approved the document on 26 May 2011:

NAME	COMPANY
D. Dunn, Vice President	Aramco Services Co.
R. Bartusiak	ExxonMobil Research & Engineering
P. Brett	Honeywell Inc.
J. Campbell	ConocoPhillips
M. Coppler	Ametek Inc.
E. Cosman	The Dow Chemical Company
B. Dumortier	Schneider Electric
J. Federlein	Federlein & Assoc. Inc.
J. Gilsinn	NIST/MEL
E. Icayan	ACES Inc.
J. Jamison	EnCana Corporation Ltd.
K. P. Lindner	Endress + Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
T. McAvinew	Instrumentation and Control Engineering, LLC
R. Reimer	Rockwell Automation
S. Russell	Valero Energy Corp.
N. Sands	DuPont
H. Sasajima	Yamatake Corp.
T. Schnaare	Rosemount Inc.
J. Tatera	Tatera & Associates Inc.
I. Verhappen	Industrial Automation Networks Inc.
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa IA Global Marketing (USMK)
D. Zetterberg	Chevron Energy Technology Co.

This page intentionally left blank.

Introduction

Wires. What's to like about them? They're unreliable, expensive, heavy, and vulnerable. Wouldn't it be great to do away with them as we largely have in our daily lives? What's stopping you?

You do not trust wireless.

Our purpose is to dispel misconceptions and myths about wireless sensor networks and provide you with the information you need to make sure that your introduction of wireless sensors is successful. The purpose of this document is to make wireless understandable and fun. We the authors think it is and hope that we can convey the excitement to you, along with the benefits.
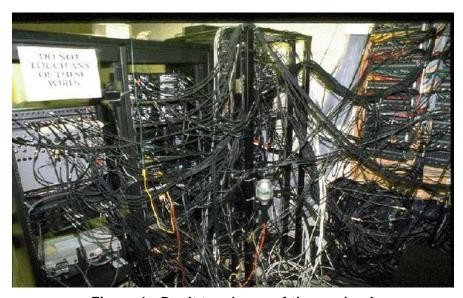

Figure 1 - Don't touch any of these wires!

Don't touch any of these wires. Why not? Make no mistake; we clearly understand why you don't trust wireless for your Industrial Automation and Control System (IACS). There have been too many false starts and false claims in the past. The proclamations of ubiquitous sensing haven't been realized. But there is a lot happening in the broader "M2M" world beyond industrial sensing that lays the groundwork. (See "When Everything Connects," *The Economist*, April 28-May 4, 2007.) And does the jungle of wires shown in Figure 1 really seem like the best solution? There is a lot you can do now that makes good business sense. So what is preventing you from trusting wireless sensors for your IACS?

1. **Reliability:** Will the data you need be available when and where you need it? Will the maintenance of the wireless system be higher than the wired alternative? Will the additional capability you get be worth the risk and capital expenditure? You need assurance against unintended consequences as you make the transition.
2. **Security:** Will your data stay where it belongs? Will your IT department allow wireless in the facility? Will an intruder be able to take control of your processes?
3. **Resiliency:** When the system is disrupted, how long will it take to restore? Will it restore itself? Will your technicians be able to fix it? Will the system scale to fit your full implementation?

Can early indications of an impending disruption be detected in time to compensate, mitigate, or pursue an alternate control strategy?

These three concerns form the backbone of this document and the core of trustworthiness. We will describe how and why modern wireless IACS can be at least as trustworthy as the wired systems you are used to. We will also describe some of the ways wireless uniquely enables new capabilities that are not feasible with wires. If you think about wireless only as a one-for-one replacement for wires, you are missing the biggest reason to go wireless. Continue reading and learn how to address your concerns about using wireless sensors. We want your feedback, but most of all we want you to start using wireless sensors.

Our purpose is to give you the tools you need to make informed decisions about whether to consider wireless in your industrial automation and control systems (IACS). We will neither tell you which wireless technology to pursue, nor will we provide detailed trade-offs between alternative technologies. Rather, we will provide some background on the fundamental opportunities and challenges associated with wireless in the industrial environment and, we hope, enough knowledge to allow you to decide whether to push (or to support) your staff in evaluating wireless for particular applications in your organization. We are confident that wireless technology will become common in the IACS environment, but we believe prudence while we build and refine this technology is appropriate. We hope this document will contribute to your understanding.

FOREWORD

This document is the first of a pair of documents distinguished by the intended audiences. This document, Part I, is written primarily for the end user (owner) and regulator (includes all compliance authorities).

A companion document will be written primarily for manufacturers, vendors, designers, integrators, operators, and maintainers. That document, Part II, will contain more technical detail.
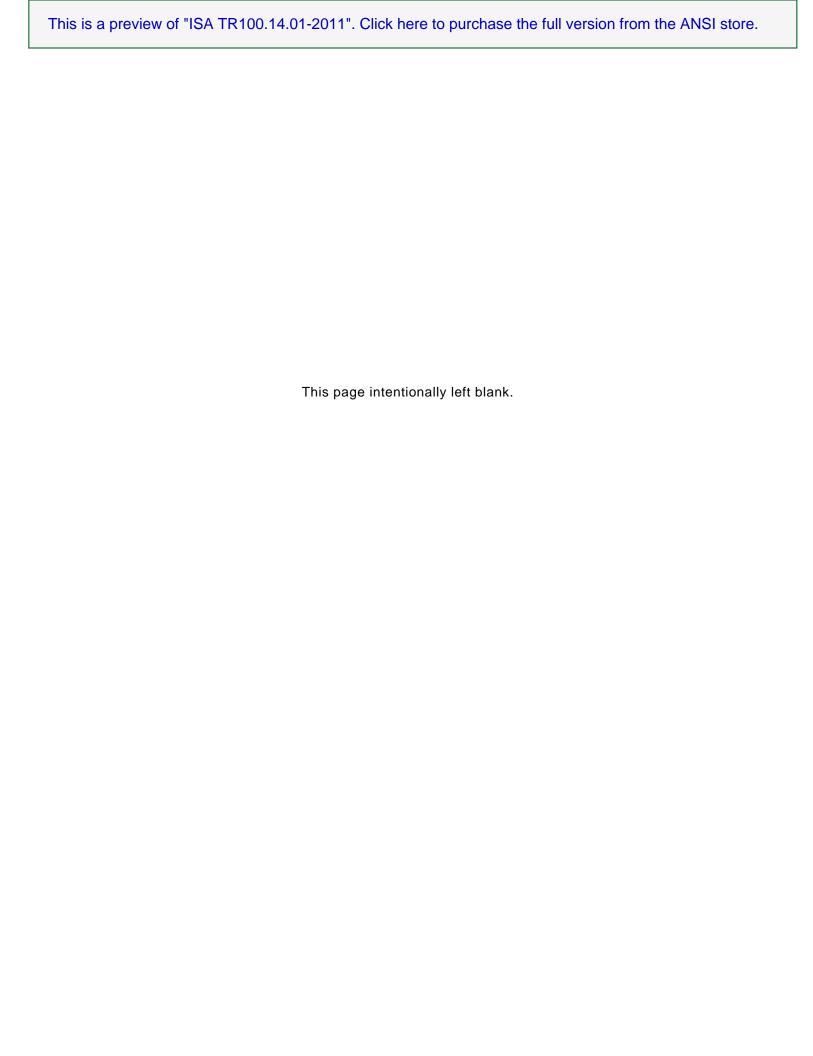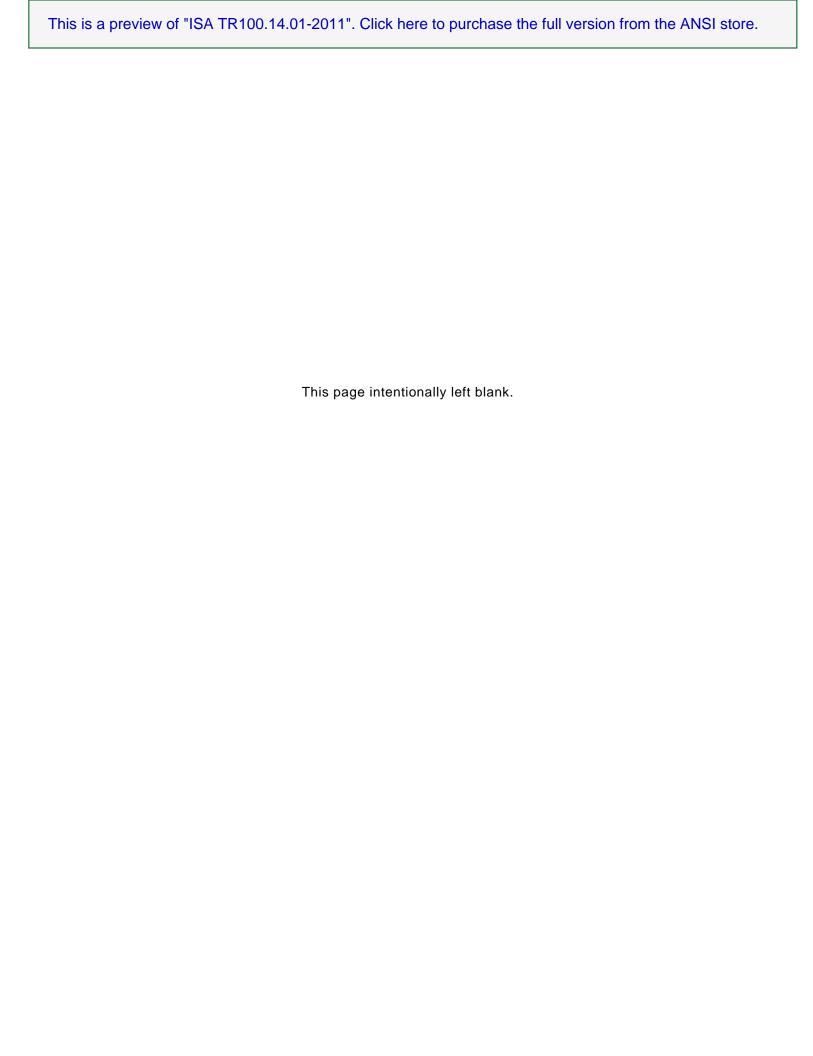
This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Trustworthiness in Wireless Industrial Automation:
Part I – Information for End Users and Regulators

1   Scope

This Part 1 Technical Report, in combination with the forthcoming Part 2, discusses trustworthiness associated with the use of wireless technology in industrial automation systems. Specifically excluded are those attributes that may be in common with wired systems and are therefore covered elsewhere, or attributes that are specific to other application domains such as healthcare applications. Also excluded are those attributes associated with ancillary issues such as health effects of RF or component materials (such as batteries). For this document, trustworthiness encompasses attributes associated with reliability, security and resiliency.

2   Purpose

Trustworthiness in Wireless Industrial Automation is divided into two distinct parts. Part 1 (this document) provides introductory information for the end users and regulators; Part 2 will provide more thorough technical details associated with trustworthy wireless systems.

Part 1 provides end users and regulators with information needed to understand the risks and advantages associated with use of wireless systems. The result should be confident decisions about when and where to use them in order to realize the benefits they offer. It is also intended to provide those in a regulator role with sufficient background information to understand the implications and consequences of rules and regulations that apply to use of wireless technology in industrial automation applications.

The document contains introductory material and information intended to demonstrate to the reader that wireless is a viable solution today. The reader will find embedded in Part 1 a few technical bits of guidance as an incentive to read Part 2. Part 1 introduces and uses technical terms to describe concepts that are common to many areas of computer technology and applications. The existence of multiple disciplines and communities which have developed their own approaches to deal with technical issues has produced a literature containing many different technical terms with considerable overlap in use and meaning. A set of terms has been adopted for Part 1 for purposes of presenting a consistent point of view. Detailed discussion of the choices of technical language and terminology is being deferred to Part 2.