



IEEE Standard for A Smart Transducer Interface for Sensors and Actuators—Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats

IEEE Instrumentation and Measurement Society

Sponsored by the
TC9 Sensor Technology (IM/ST) Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

26 June 2010

IEEE Std 1451.7™-2010

IEEE Standard for Smart Transducer Interface for Sensors and Actuators— Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats

Sponsor

TC9 Sensor Technology (IM/ST) Committee

of the

IEEE Instrumentation and Measurement Society

Approved 25 March 2010

IEEE-SA Standards Board

Abstract: Data formats designed to facilitate communications between radio frequency identification (RFID) systems and smart RFID tags with integral transducers (sensors and actuators) are introduced in this standard. New transducer electronic data sheet (TEDS) formats for smart RFID tags, based on the IEEE 1451 family of standards, are defined. Also, a comprehensive command set for smart RFID tags is defined.

Keywords: network capable application processor (NCAP), radio frequency identification (RFID) tag, sensor command, sensor integration, sensor interface, sensor standard, smart RFID tags, transducer electronic data sheet (TEDS), transducer interface module (TIM)

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2010 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 26 June 2010. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-6245-4 STD96058
Print: ISBN 978-0-7381-6246-1 STDPD96058

IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS.**”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This introduction is not part of IEEE Std 1451.7-2010, IEEE Standard for Smart Transducer Interface for Sensors and Actuators—Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats.

This standard describes communication methods and data formats, and it provides a transducer electronic data sheet (TEDS) for sensors working in cooperation with radio frequency identification (RFID) systems. This document does not outline, recommend, or prescribe any specific air-interface protocol. This document is intended to be air-interface agnostic.

This standard is the seventh member of the IEEE 1451 family of standards. In the IEEE 1451 family, transducers (sensors or actuators) are connected to a transducer interface module (TIM), which is connected to a network capable application processor (NCAP) to allow network access of transducer data. IEEE Std 1451.0™-2007 [B1]^a defined a set of common functionality, commands, and TEDS for the family of IEEE 1451 smart transducer standards. IEEE Std 1451.1™-1999 [B2] defined a smart transducer object model and communication methods to facilitate the access of smart transducer in a network. IEEE Std 1451.2™-1997 [B3] defined serial interfaces for connecting transducer modules to a network processor. IEEE Std 1451.3 [B4] defined a transducer interface for distributed multidrop systems. IEEE Std 1451.4™-2004 [B5] defined a mixed-mode transducer interface that allows the transfer of digital transducer electronic data sheet and analog sensor signals on the same wires. IEEE Std 1451.5™-2007 [B6] defined a wireless communication interface for connecting transducers using various wireless communication protocols.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

^aThe numbers in brackets correspond to those of the bibliography in Annex F.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims 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. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was completed, the Sensor and RFID Integration (IM/ST/RFID) Working Group had the following membership:

Curtis L. Rozeboom, *Chair*
Kang Lee, *Vice Chair*

Paul Chartier
Farron Dacus
Randy Drago

Steve Fick
Craig K. Harmon
Bill Hoffman

Dan Kimball
Alfonso Rodriguez-Herrera
Darold Wobschall

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Royce Beacom
Martin J. Bishop
Keith Chow
Ryon Coleman
Thomas Dineen
Carlo Donati
Randy Drago
David Droste
Lee Eccles
Sergiu Goma
Randall Groves
Werner Hoelzl
Piotr Karocki

James Kemerling
Chad Kiger
Jeremy Landt
Kang Lee
G. Luri
Gary Michel
Jeffrey Moore
Jay Nemeth-Johannes
Michael S. Newman
Ulrich Pohl
Josef Preishuber-Pfluegl
Robert Robinson
Alfonso Rodriguez

Curtis L. Rozeboom
Bartien Sayogo
James E. Smith
Matthew Smith
Joseph Stanco
Rene Struik
Walter Struppler
Mark Sturza
David Tepen
Jonathan Tucker
Stephen Webb
Oren Yuen
Janusz Zalewski

When the IEEE-SA Standards Board approved this amendment on 25 March 2010, it had the following membership:

Robert M. Grow, *Chair*
Richard H. Hulett, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Karen Bartleson
Victor Berman
Ted Burse
Clint Chaplin
Andy Drozd
Alexander Gelman
Jim Hughes

Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Hung Ling
Oleg Logvinov
Ted Olsen

Ronald C. Petersen
Thomas Prevost
Jon Walter Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Kathryn Bennett
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	2
2. Normative references.....	2
3. Definitions, acronyms, and abbreviations	2
3.1 Definitions	2
3.2 Acronyms and abbreviations	3
3.3 Conformance	3
3.4 Word usage.....	3
4. Transducer and RFID system interface specification	4
5. Air interface applicability [RFID and real-time locating system (RTLS)]	5
6. Sensor security and data structures.....	6
6.1 Overview	6
6.2 Sensor security system basic operation.....	6
6.3 Sensor identifier.....	9
6.4 Sensor characteristics TEDS (Type 1).....	10
6.5 Sample and Configuration Record.....	23
6.6 Event Administration Record	31
6.7 Event records	34
7. Command overview.....	36
7.1 Read-Sensor-Identifier.....	39
7.2 Read-Primary-Characteristics—TEDS	40
7.3 Write-Sample-and-Configuration	41
7.4 Read-Sample-and-Configuration	43
7.5 Read-Alarm-Status	45
7.6 Read-Single-Memory-Record.....	46
7.7 Read-Event-Administration-Record	48
7.8 Read-Event-Record-Segments.....	51
7.9 Read-Partial-Event-Record-Segment.....	53
7.10 Write-Event-Administration-Field-7	54
7.11 Read-Any-Field	56
7.12 Erase-Event-Administration Record.....	57
7.13 Erase-Event-Records	58
7.14 Erase Sample-and-Configuration Record	60
7.15 Begin-End-Mission.....	61
7.16 Challenge	63
7.17 Reader-Authenticate	65
7.18 ReadWriteLock-Keys	68
7.19 Request-RN	70
7.20 Encryption-ON-OFF	71
7.21 Close-Secure-Session	73
8. RFID communications.....	75
8.1 Support for commands.....	75
8.2 Addressing and subaddressing of sensors.....	75

Annex A (normative) Sensor types	77
Annex B (normative) Extension codes	78
Annex C (informative) Physical interfaces.....	79
Annex D (informative) Integration of IEEE 1451.7 transducers with other IEEE 1451 devices	81
Annex E (informative) Sensor authentication and encryption.....	83
Annex F (informative) Bibliography	86

IEEE Standard for Smart Transducer Interface for Sensors and Actuators—Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This standard defines data formats to facilitate communications between radio frequency identification (RFID) systems and smart RFID tags with integral transducers (sensors and actuators). The standard defines new transducer electronic data sheet (TEDS) formats based on the IEEE 1451 family of standards. This standard also defines a command structure and specifies the communication methods with which the command structure is designed to be compatible.

1.2 Purpose

The purpose of this standard is to provide methods for interfacing transducers and RFID tags, and for reporting transducer data within the RFID infrastructure. This standard will reduce the cost and time required to integrate transducer and RFID systems, as well as provide a means for device and equipment interoperability.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO/IEC 19762-1-5:2008, Information Technology—Automatic Identification and Data Capture (AIDC) Techniques—Harmonized Vocabulary (all parts).¹

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* and the ISO/IEC 19762-1-5:2008 series should be referenced for terms not defined in this clause.² This clause provides definitions that are either not found in other standards, or have been modified for use with this standard. Also included in this clause are definitions of data types, string language codes, compact physical units, and a unique identification system.

3.1.1 1451.7 sensor: A device that responds to biological, chemical, or physical stimulus (such as heat, light, sound, pressure, magnetism, motion, and gas detection) and provides a measured response of the observed stimulus.

3.1.2 event sensor: A sensor that detects a change of state in the physical world. The fact that a change of state has occurred, and/or instant in time of the change of state and not the state value, is the “measurement.”

3.1.3 message: Information that is to be passed between devices as a single logical entity. A message may occupy one or more packets.

3.1.4 sensor: A device that responds to biological, chemical, or physical stimuli (such as heat, light, sound, pressure, magnetism, motion, and gas detection) and transmits the resulting signal or data for providing a measurement, operating a control, or both.

¹ ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/ Suisse (<http://www.iso.ch/>). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>). IEC publications are available from the Sales Department of the International Electrotechnical Commission, Case Postale 131, 3 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse (<http://www.iec.ch/>). IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA.

² *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.

3.1.5 smart transducer: A smart transducer is a transducer that provides functions beyond those necessary for generating a correct representation of a sensed or controlled quantity. This functionality typically simplifies the integration of the transducer into applications in a networked environment.

3.1.6 time tick: The number of sample intervals that have occurred.

3.1.7 transducer electronic data sheet: A data sheet stored in some form of electrically readable memory, which describes a Transducer Channel.

3.2 Acronyms and abbreviations

ADC	analog-to-digital converter
AES	advanced encryption standard
AI	air interface
EUI	extended unique identifier
FIFO	first-in–first-out
LI	local index
LSB	least significant bit
LST	last sample taken
MSB	most significant bit
OUI	organizational unique identifier (allocated by IEEE)
RC	rollover count
RFU	reserved for future use
RN	random number
RFID	radio frequency identification
RFU	reserved for future use
RTLS	real-time locating system
SCap	sample capacity
SCOEOET	sample count of events outside either threshold
SF	scale factor
SFE	scale factor exponent
SFS	scale factor significand
SI	International System of Units, reference the International System of Units (SI)
SO	scale offset
SPI	serial peripheral interface
TEDS	transducer electronic data sheet
TI	total index
TIM	Transducer Interface Module
UTC	Coordinated Universal Time
VLSI	very large-scale integration
XOR	exclusive OR

3.3 Conformance

Conformance to the specifications within this standard requires that all nonoptional sections be implemented in the vendor device.

3.4 Word usage

Several keywords are used to differentiate among various levels of requirements and options, as follows:

Shall

The key word “shall” indicates a mandatory requirement. Designers are required to implement all such mandatory requirements to ensure interoperability with other products that conform to the specifications in this standard.

Recommended

Recommended is a key word indicating flexibility of choice with a strong preference alternative. The word “should” has the same meaning.

Should

Should is a key word indicating flexibility of choice with a strong preference alternative. The phrase “it is recommended” has the same meaning.

May

May is a key word that indicates flexibility of choice with no implied preference.

4. Transducer and RFID system interface specification

This standard specifies a set of features that allow a smart transducer to communicate with the outside world using the techniques employed by RFID systems. The list below shows the four design elements that must be embodied in all smart transducers, which conform to this standard:

Essential elements of a conformant smart transducer:

- Communications protocol
- Command structure
- Transducer electronic data sheet (TEDS)
- Transducer data

The communications protocol provides the direct link between the outside world and the smart transducer. At the time of publication of this IEEE standard, Clause 5 identifies a number of the ISO/IEC Air Interface specifications that are candidates for supporting this standard; other air interfaces may also support this standard. Each air interface protocol that supports IEEE 1451.7 shall refer to it as a normative reference and implement the requirements specified in this document. The command structure is the language, specified in Clause 7, with which the actions of the smart transducer are controlled. The TEDS contains the capability and configuration information, as specified in Clause 6, for each particular smart transducer. The transducer data, also described in Clause 6, constitute the results of sensor measurements.

Figure 1 provides an example of the minimum components required in a system interfaced with an IEEE 1451.7-compliant transducer. The elements common to all IEEE 1451.7-compliant systems are shaded.

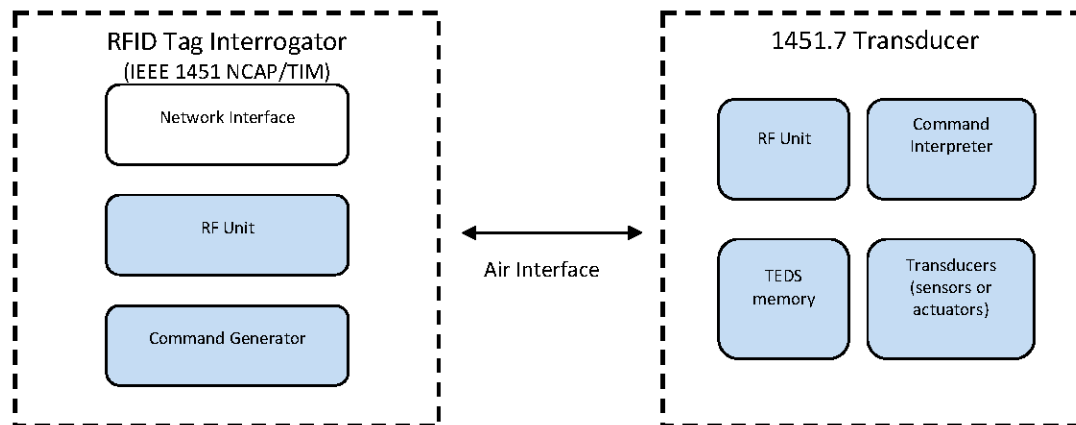


Figure 1 —RFID system interface with smart transducer

For clarity, Figure 1 does not show the numerous other hardware elements common to generic RFID tag interrogators and IEEE 1451.7 transducers.

Input from the RFID Tag Interrogator or its network interface is processed by the Command Generator, and then transmitted by its RF Unit. Within the IEEE 1451.7 Transducer, the Command Interpreter processes radio signals sent to it from the RF Unit, into low-level control signals. These signals are required for the various functions of which the particular smart transducer is capable. As a minimum requirement, every 1451.7-compliant Transducer shall be able to retrieve data from the TEDS memory, and all data records.

5. Air interface applicability [RFID and real-time locating system (RTLS)]

The IEEE 1451.7 command structure supports the air interface communications protocols described in the following ISO/IEC standards; additional air interface protocols may be added by declaring compliance with this standard:

- ISO/IEC 18000-2:2009 [B9],³ Information Technology—Radio Frequency Identification for Item Management—Part 2: Parameters for Air Interface Communications below 135 kHz.
- ISO/IEC 18000-3:2009 [B10], Information Technology—Radio Frequency Identification for Item Management—Part 3: Parameters for Air Interface Communications at 13.56 MHz.
- ISO/IEC 18000-4:2008 [B11], Information Technology—Radio Frequency Identification for Item Management—Part 4: Parameters for Air Interface Communications at 2.45 GHz.
- ISO/IEC 18000-6:2006 [B12], Information Technology—Radio Frequency Identification for Item Management—Part 6: Parameters for Air Interface Communications at 860 MHz to 960 MHz.
- ISO/IEC 18000-7:2009 [B13], Information Technology—Radio Frequency Identification for Item Management—Part 7: Parameters for Active Air Interface Communications at 433 MHz.
- ISO/IEC 24730-2:2006 [B14], Information Technology—Real-Time Locating Systems (RTLS)—Part 2: 2.4 GHz Air Interface Protocol.
- ISO/IEC 24730-5:2000 [B15], Information Technology Automatic Identification and Data Capture Techniques—Real Time Locating Systems (RTLS)—Part 5: Chirp Spread Spectrum (CSS) at 2.4 GHz.

³ The numbers in brackets correspond to those of the bibliography in Annex F.

6. Sensor security and data structures

IEEE 1451.7 sensors are designed on a hierarchical structure with the following two levels:

- a) The sensor type (e.g., temperature or relative humidity) determined by its physical design
- b) The data type defined by the measured or derived data extracted from the sensor (e.g., present sampled value, or a count of occurrences of out-of-limit samples, or a detailed data log)

Effectively, the hierarchy separates the functions of which an IEEE 1451.7 sensor is capable from the type of data that are extracted.

6.1 Overview

This standard specifies sensor types and scaling for RFID sensor data acquisition, files that control data acquisition and hold desired sensor data, and commands for accessing data files. The data available for extraction from each sensor shall consist of the following:

- The sensor identifier (6.3)
- The sensor characteristics record (6.4)
- The sample and configuration record (6.5)
- The event administration record (6.6)
- The event record (6.7)

6.2 Sensor security system basic operation

This standard specifies optional security in two forms, which are *air interface security* and *direct sensor security*. Either or both of these may be used, and there are options within the two forms.

Air Interface Security provides methods for the sensor to take advantage of the security built into a particular RFID air interface. It operates by the tag passing a security status code to the sensor informing the sensor of the security state of the tag. The sensor then appropriately limits its command execution according to a security function code programmed by the user. If the sensor is deeply embedded within the tag electronics, then this method of sensor security is as secure as the air interface security. However, air interface security has limitations in that it is not available for all air interfaces, is commonly not fully secure in a cryptographic sense, is sometimes “one way” with only the reader authenticating to the tag, and it may be physically defeated for modular sensors.

To overcome these problems, direct sensor security is also specified. This standard provides for sensor security ranging from a simple password system for reader-only authentication, to encrypted two-way authentication of reader and sensor, to authentication of reader and sensor on each command/response exchange, to encryption of data flow in the link. There is a high degree of flexibility provided, such as a choice of encryption algorithms and the opportunity to specify different algorithms and different keys for authentication and data encryption (different keys must be supported if different algorithms are allowed for authentication and data encryption because the key length can differ). Other flexibility includes reader-commanded random number (RN)/security token lengths that may be different for each link and that may change from initial authentication to continuing authentication of an established session. Authentication and encryption may also be independently commanded as applying to either or both links. Under this system, optional encryption capability is required to authenticate the tag to the reader. The reader may, if desired, authenticate itself to the tag without encryption using only a password.

The type of security supported by the sensor is reported in the TEDS. Because this standard allows both Air Interface Security and Direct Sensor Security to be implemented simultaneously, separate fields for security capability description are provided for each. If the two security function codes are programmed to different levels, the sensor will default to the security level of the more secure (it will limit command set execution for both to that specified by the most limiting). The two passwords/keys may be different, and if different, both will be required to access the sensor.

6.2.1 Air interface security system support

The air interface security may be supported through a security status reporting system (using the “Tag Security Status Code”) where the tag reports to the sensor the security state it is in, and the sensor responds appropriately. Typically, the Tag Security Status Code reports to the sensor whether the tag has “authenticated” that the reader is authorized for some degree of sensor access via a password method (improved air interface security using encryption-based authorization is under development). A 3-bit Tag Security Status Code is provided for this function, as defined in Table 12. The code from this table is preappended to the payload of the air interface “transport command” that moves sensor commands as payload to the sensor controller. The sensor controller interprets how to respond to the Tag Security Status Code of the tag as defined in the Air Interface Security Function Code of Table 14. The Air Interface Security Function Code is basically a user-programmed choice of the air interface security capabilities as defined in the Air Interface Security Capabilities Code field of TEDS Table 2. It operates by specifying the classes of command that the sensor may execute, for example allowing read operations but not write operations without having passed air interface security. See 6.5.7 for specific information on the command classes.

6.2.2 Direct sensor security system support

The sensor manufacturer and the user through programming options may extend or replace the air interface security with direct or embedded sensor security. Such security may share a password or key(s) with the air interface or may be different. The “password” used for one-way authentication is replaced by a “key” or keys when encrypted two-way, two-way authentication is used. If both security methods are supported, then the sensor will assume the higher security level of the two Security Function Codes (Field 6 and Field 7) programmed in the Sample and Configuration Record of Table 11. The Sensor Security Function Code (Field 7) of Table 11 is a user-selected choice from the options available under the detailed descriptions of Table 6.

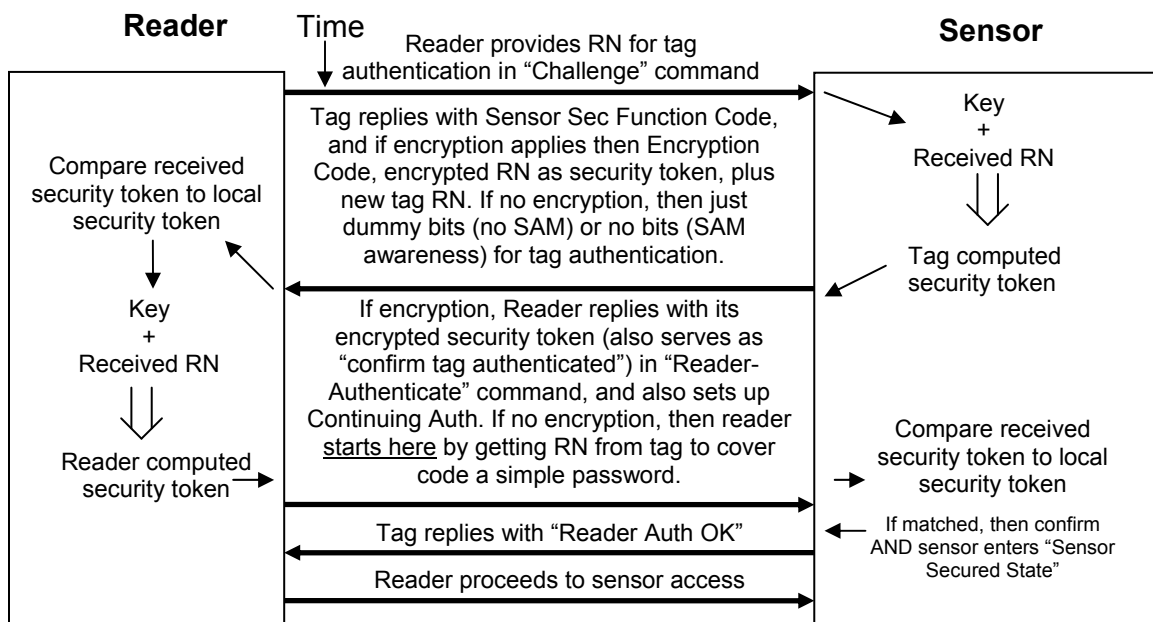
The direct sensor security can be as simple as the reader authenticating itself to the sensor via a simple password. This standard provides a structure and a command set that can allow for “Two-Way Authentication,” meaning that both Reader and Sensor can privately authenticate that the other has a secret key. Passwords may currently be 16, 32, 64, or 128 bits long. Keys may also be any of these lengths, and also they may be any number if a specific key length is specified as always associated with a particular encryption algorithm. An algorithm in this standard may also be left open with respect to length, and then the particular length specified in the TEDS of Table 2.

The two-way authentication is implemented with a private key encryption system. This requires not only selection of particular encryption or hashing algorithms but also random number generation on both reader and sensor. For each authentication, random numbers are generated by each side (reader or tag) to be used in combination with the secret key to generate constantly changing “security tokens” (an encryption function output that is a function of both the key and the new random number) that prove the authenticity of the side receiving the random number and generating the security token. Because the secret and untransmitted key is essential to generating the security tokens, the random numbers are transmitted in plaintext (unless the full communication is encrypted). For example, for the sensor to authenticate the reader, the sensor provides the reader with a random number. The reader encrypts or hashes that random number with the key (both are inputs to the encryption function) and sends the encrypted result (reader security token) back to the sensor. The sensor has also run the same random number and key through the

encryption algorithm and obtained an internal result that it can compare to the result provided by the reader. If they match, this proves to the sensor that the reader has the key. This result was achieved without ever having to transmit the key where it could be intercepted by an eavesdropper. This process may be extended to encryption of regular message traffic, and not just authentication.

The flow of events to perform two-way authentication is shown in Figure 2. If encryption is not available or not selected for use, then reader skips the tag authentication part of the process. In that case, the first step is for the reader to request a random number (Request RN command) from the sensor to use in “exclusive OR (XOR) cover coding” a transmission of the reader authenticating password to the sensor (via the Reader-Authenticate command). Because the random number used for cover coding was transmitted in the clear where it could be intercepted, and in this case, there is no encryption (the openly transmitted RN itself serves as a kind of key to “uncover” the password), this is a very modest degree of security. The only reason it provides modest security is that the tag transmission of the RN is usually a low-power transmission, such that an eavesdropper must be within a fairly limited range to perform the intercept. It is suitable to prevent casual access to the sensor by unauthorized readers, but it is not suitable to prevent determined access. This same situation applies to air interface security where the reader provides a cover coded password to the tag.

If a sensor supports two-way authentication, it may drop back to using this limited one-way reader-only authentication where the key serves as a password. If this operation is desired, it is commanded by the reader via the Encryption Usage flag in the Reader-Authenticate command. If “Continuing Authentication” whereby each command/response exchange is independently authenticated is supported, then that authentication may be two-way or one-way in either direction as chosen by the reader. If encryption of data flow is supported, then it may also be selected as two-way or one-way in either direction. More specific information is provided in the data structures and commands, and in particular in the description of the Reader-Authenticate command.



NOTE—SAM stands for security accounts manager.

Figure 2—Two-way secure authentication with exit points

6.3 Sensor identifier

Each sensor shall have a 64-bit (an 8-octet array) sensor identifier (ID), which is compliant with the global identifier format defined in the IEEE 64-bit extended unique identifier (EUI-64) as shown in Table 1. The most significant 3 or 4 octets of a EUI-64 are the 24-bit or 36-bit Company_ID [organizational unique identifier (OUI)], which is obtained from the IEEE registration authority. The IEEE administers the assignment of OUI-24 or OUI-36 Company_ID. The least-significant 28-bit or 40-bit extension identifier is assigned by the manufacturer. The Sensor ID is permanently encoded by the sensor manufacturer. This is in addition to any unique identifier(s) that the RFID tag might contain.

Table 1 —Sensor ID

Company ID	Extension identifier
OUI-24 24 bits	40 bits
OUI-36 36 bits	28 bits

Guidelines for the 64-bit global identifier (EUI-64) registration authority can be found at <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.

For example, assume that a manufacturer's IEEE-assigned OUI-24 Company_ID value is ACDE48₁₆ and the manufacturer-selected extension identifier for a given component is 234567ABCD₁₆. The EUI-64 value generated from these two numbers is ACDE48234567ABCD₁₆, whose byte and bit representations are illustrated in Figure 3.

Company ID			Extension identifier					field
addr+0	addr+1	Addr+2	addr+3	addr+4	addr+5	addr+6	addr+7	order
AC	DE	48	23	45	67	AB	CD	hex
10101100	11011110	01001000	00100011	01000101	01100111	10101011	11001101	bits
most significant bit (MSB)			least significant bit (LSB)					

Figure 3—OUI-24 example

For example, assume that a manufacturer's IEEE-assigned OUI-36 Company_ID value is 8765432AB₁₆, and the manufacturer-selected extension identifier for a given component is 567ABCD₁₆. The EUI-64 value generated from these two numbers is 8765432AB567ABCD₁₆, whose byte and bit representations are illustrated in Figure 4.

Company ID					Extension identifier				Field
addr+0	addr+1	Addr+2	addr+3	addr+4	addr+4	addr+5	addr+6	addr+7	order
87	65	43	2A	B	5	67	AB	CD	hex
10000111	01100101	01000011	00101010	1011	0101	01100111	10101011	11001101	bits
MSB					LSB				

Figure 4 —OUI-36 example

6.4 Sensor characteristics TEDS (Type 1)

The TEDS is the primary means of identifying the sensor's functional capability. The structure of the primary sensor characteristics is defined in Table 2,⁴ with further detailed specifications in 6.4.1 through 6.4.18.

Table 2 —Primary Sensor Characteristics TEDS (Type 1)

Field	Name	Size	Reference	Example/note
1	TEDS type	3 bits	6.4.1	001 ₂ .
2	Sensor type	7 bits	6.4.2	0001110 ₂ = Relative humidity.
3	Units extension	5 bits	6.4.3	Subtype, e.g., for chemical sensors.
4	Sensor map	16 bits	6.4.4	
5	Data resolution	5 bits	6.4.5	Sensor capability.
6	Scale Factor Significand	11 bits	6.4.6	Sensor capability.
7	Scale Factor Exponent	6 bits	6.4.6	Sensor capability.
8	Scale Offset Significand	11 bits	6.4.6	Sensor capability.
9	Scale Offset Exponent	6 bits	6.4.6	Sensor capability.
10	Data uncertainty	3 bits	6.4.7	Sensor capability.
11	Sensor Reconfiguration Capability	1 bit	6.4.8	0 = NO, 1 = YES.
12	Memory Rollover Capability	1 bit	6.4.9	0 = NO, 1 = YES.
13	Air Interface Security Capability Code (see NOTE 1)	3 bits	6.4.10	See Table 5 for details.
14	Sensor Security Capability Code (see NOTE 1)	3 bits	6.4.11	000 ₂ = No Direct Sensor Security. If greater than zero, then at least one-way password security is supported. If greater than zero and at least one authentication encryption algorithm is supported, then two-way initial encrypted authentication is also supported. See the Continuing Authentication Capability Field of this table for directions supported when continuing to authenticate each command. See Table 6 for Sensor Security Capability Code assignments.
15	Sensor Authentication Encryption Capability Map	7 bits	6.4.12	Choices of encryption algorithms for authentication that the sensor supports. If all zeroes, then encrypted authentication is not supported.
16	Sensor Data Encryption Capability Map	7 bits	6.4.13	Choices of encryption algorithms for data that the sensor supports. If all bits are zero, then data encryption is not supported. If data encryption is supported, the directions supported are detailed in the Data Encryption Capability Field of this table.
17	Sensor Authentication Password/Key Size (see NOTE 2)	3 bits	6.4.16	000 ₂ = 16 bits, 001 ₂ = 32 bits, 010 ₂ = 64 bits, 011 ₂ = 128 bits, 100 ₂ ~ 111 ₂ = reserved for future use (RFU).

⁴ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

Field	Name	Size	Reference	Example/note
18	Sensor Data Encryption Key Size (see NOTE 3)	3 bits	6.4.17	000 ₂ = 16 bits, 001 ₂ = 32 bits, 010 ₂ = 64 bits, 011 ₂ = 128 bits, 100 ₂ ~ 111 ₂ = RFU.
19	Random Number Sizes Supported (see NOTE 4)	3 bits	6.4.14	000 ₂ = 16 bits, 001 ₂ = 16 & 32 bits, 010 ₂ = 16, 32 & 64 bits, 011 ₂ = 16, 32, 64, & 128 bits, 100 ₂ ~ 111 ₂ = RFU.
20	Continuing Authentication Capability Field (see NOTE 5)	2 bit	6.4.15	See Table 9 for details.
21	Data Encryption Capability Field	2 bit	6.4.18	Table 10 for details.
22	Clock Accuracy (see NOTE 6)	3 bits		00: >10% 001: 10% 010: 5% 011: 2% 100: 1%. 101: 300 ppm 110: 100 ppm 111: <100 ppm
23	RFU	17 bits		
TOTAL		128 bits		

NOTE 1—If the air interface and sensor security systems are both supported and if Security Function Codes based on the capability codes are programmed to different levels, then the more secure mode shall apply to how the sensor processes commands.

NOTE 2—For sensor authentication, the term “password/key” is used instead of simply “key” because this field functions as a key if the sensor has authentication encryption but as a password if it does not. Although sensor authentication password/key sizes are 16 bits and greater, if Sensor Security Capability Code is 000, then there is no password or key and this overrides the password/key length field. It is possible via the Sensor Authentication Encryption Capability Map to select a standardized encryption algorithm with a key length that overrides the key length field. The key length field is to allow algorithms that support multiple key lengths to specify the particular length the tag uses. For example, the advanced encryption standard (AES) can have key lengths of 128, 192, and 256 bits (although only 128 is specified for this standard version).

NOTE 3—Although sensor data encryption key sizes are 16 bits and greater, if the Sensor Security Capability Code is 000, then there is no key and this overrides the key length field. It is possible via the Sensor Data Encryption Capability Map to select a standardized encryption algorithm with a key length that overrides the key length field.

NOTE 4—A random number generator is needed to support authentication, which it does by providing a continuously changing number to encrypt into a security token that proves the key is possessed. The supported random number sizes in this version are all or a subset of 16, 32, 64, and 128. Although the random number size is 16 bits and greater, if the Sensor Encryption Capability Code is 000, then there is no random number generator, and this overrides the Random Number Size field. The actual random number sizes to be used by each side of the link are provided by the Challenge command for the initial authentication, and by the Reader-Authenticate command for Continuing Authentication. See NOTE 5.

NOTE 5—Continuing Authentication is an optional ability to authenticate all commands and responses individually, as opposed to a single authentication where it is assumed that following authentication commands are not subject to hostile action.

NOTE 6—Clock accuracy applies to logged data and, if supported, then also to the Secure Session Timer of Table 16. The range of values shown is suitable for the two main classes of reference sources, which are free running relaxation (RC) oscillators (trimmed and untrimmed) and low-cost, low-power crystal timers (such as standard 32.768 kHz watch crystal-based Real Time Clocks).

The manufacturer shall permanently lock the Primary Sensor Characteristics TEDS.

6.4.1 TEDS type

This field identifies the TEDS format. For the purpose of this standard, the only relevant code is 001₂ for the Primary Sensor Characteristics TEDS.

NOTE—The total number of TEDS formats that may be specified in this standard is nominally limited to 8 (but that may be extended using the type 2 or 3 TEDS).

6.4.2 Sensor type

The Sensor Type field defines the International System of Units (SI) unit, or derived SI unit that the sensor is capable of monitoring. The 7-bit sensor type code value is all that is required for sensor data processing to identify the associated unit and to process the data.

Annex A lists the code values that are assigned and supported by this standard.

6.4.3 Units extension

The only units extension that has been defined in this standard is for chemical substances. These qualify the sensor type with a unit of measure of *amount of substance (Moles)*, or parts per million.

The code values are defined in Annex B.

6.4.4 Sensor map of supported measurement codes

The Sensor Map field indicates the capability of the sensor to provide data of the types defined in Table 3. Each sensor shall support at least one type of data. The code value represents the position in the field of a bit set to 1 to indicate that the sensor supports the particular type of measurement. As read from left to right, the first position is designated by code value 0.

Code values 0 through 9 denote measurement types for which only one measured value is returned in response to a request for data. Code values 10 through 13 denote measurement types for which multiple data values can be returned by the sensor.

The number of bits in each measured value size of data is determined by the code value for Field 5 of the Primary Sensor Characteristic TEDS (Table 2).

The bit sequence (for Table 3) is mapped from left to right and it indicates the presence (with a 1) or absence (with a 0) of a measurement capability. Examples are listed after Table 3.

Table 3 —Supported measurement type codes

Code value	Measurement type	Single/multiple	Field size in event record
0	Present (point-of-time) value	Single	Data = 1 to 32 bits (see 6.4.5)
1	Maximum (or peak) value	Single	Data = 1 to 32 bits (see 6.4.5)
2	Minimum (or lowest) value	Single	Data = 1 to 32 bits (see 6.4.5)
3	Average value	Single	Data = 1 to 32 bits (see 6.4.5)
4	Variance	Single	Data = 1 to 32 bits (see 6.4.5)
5	Standard deviation	Single	Data = 1 to 32 bits (see 6.4.5)
6	Observed value at a predetermined sample time	Single	Data = 1 to 32 bits (see 6.4.5) Also requires specific sample count value (see 6.6.7)
7	Sample count and data value upon sample time after alarm has tripped	Single	Data = 1 to 32 bits (see 6.4.5), and specific sample count value (see 6.6.8)
8	Count of readings over maximum threshold value	Single	Data = 1 byte with the value incremented by 1 for each event
9	Count of readings below minimum threshold value	Single	Data = 1 byte with the value incremented by 1 for each event
10	Data log of observed value recorded at each sample interval	Multiple, record for each event	Data = 1 to 32 bits (see 6.4.5)
11	Data log of observed value with time tick (8-bit code) reporting outside either threshold	Multiple, record for each event	Time tick = 1 byte Data = 1 to 32 bits (see 6.4.5)
12	Data log of observed value with time tick (16-bit code) reporting outside either threshold	Multiple, record for each event	Time tick = 2 bytes Data = 1 to 32 bits (see 6.4.5)
13	Data log of all observed values after an initial alarm value has triggered	Single record for time stamp and multiple record for each event	Sample data = 1 to 32 bits (see 6.4.5) Also requires specific sample count value (see 6.6.10)
14	Temperature Time Integration	TBD ^a	TBD
15	RFU		

^aTBD = to be determined.

EXAMPLE

Bit map 111000000010000 indicates that the sensor supports the following measurement types:

- Present (point-of-time) value
- Maximum (or peak) value
- Minimum (or lowest) value
- Observed value with time tick (8-bit code) reporting outside either threshold

6.4.5 Data resolution

The Memory Resolution field identifies the numeric data format that is used to convey sensor data for Measurement Codes 0 to 13. The data format shall be the number of bits, from 1 to 32, of output data defined by the manufacturer. In most cases, this will be equivalent to the bit output of the analog-to-digital converter (ADC), but may also be truncated.

The 5-bit code in Field 5 of the Primary Sensor Characteristics TEDS shall have the value 00000₂ for a 1-bit output and the value 11111₂ for a 32-bit output.

6.4.6 Scale factors for transmitted data

The value of any particular sensor datum is a real number R , which is encoded for transmission as a binary integer N_b that is equivalent to the decimal integer N_d .

The real number R is calculated from N_d using the equation:

$R = N_d \times \text{SF} + \text{SO}$, where the scale factor SF is given by $\text{SF} = \text{SFS}_d \times 10^{\text{SFE}_d}$ and the scale offset SO is given by $\text{SO} = \text{SOS}_d \times 10^{\text{SOE}_d}$

The scale factor parameters SOS, SOE, SFS, and SFE are defined next.

The binary Scale Factor Significand (SFS_b) is a signed 11-bit binary number that represents the decimal Scale Factor Significand (SFS_d), which is defined to have 2048 possible values between −1.024 and +1.023, inclusive. The binary Scale Factor Significand is calculated by multiplying the decimal Scale Factor Significand by 100010, rounding to the nearest integer, and then converting to the signed 11-bit binary format in which −102410 = 100000000002, and +102310 = 01111111112. It is encoded in Field 6 of the TEDS.

NOTE 1—The 11-bit binary format representation is a two's-complement numeral system.

The binary Scale Factor Exponent (SFE_b) is a signed 6-bit binary number that represents the decimal Scale Factor Exponent (SFE_d) in the format in which −32₁₀ = 100000₂ and +31₁₀ = 011111₂. It is encoded in Field 7 of the TEDS.

The binary Scale Offset Significand (SOS_b) is a signed 11-bit binary number that represents the decimal Scale Offset Significand (SOS_d), which is defined to have 2048 possible values between −1.024 and +1.023, inclusive. The binary Scale Offset Significand is calculated by multiplying the decimal Scale Offset Significand by 100010, rounding to the nearest integer, and then converting to the signed 11-bit binary format in which −102410 = 100000000002, and +102310 = 01111111112. It is encoded in Field 8 of the TEDS.

The binary Scale Offset Exponent (SOE_b) is a signed 6-bit binary number that represents the decimal Scale Offset Exponent (SOE_d) in the format in which −32₁₀ = 100000₂ and +31₁₀ = 011111₂. It is encoded in Field 9 of the TEDS.

NOTE 2—This declaration holds the range of the error to 0.05% to 0.5%, with the average value of 0.13%.

EXAMPLE 1

Mains voltage monitor, range 216 V to 253 V, with 8-bit ADC

The real number 216 is represented by decimal 0 and therefore by binary 0, and the real number 253 is represented by decimal 255 (based on the capability of the 8-bit ADC) and therefore by binary 11111111. The consequent constraints on the scale factor SF and scale offset SO are:

$$\begin{aligned} 216 &= 0 \times \text{SF} + \text{SO} \\ 253 &= 255 \times \text{SF} + \text{SO} \end{aligned}$$

Therefore, $\text{SO} = 216 = 0.216 \times 10^3$, and $\text{SF} = (253 - 216)/255 = 0.145 = 0.145 \times 10^0$, and

$$\text{SOS}_d = 0.216_{10}, \text{ and } \text{SOS}_b = 00011011000_2$$

$$\begin{aligned} \text{SOE}_d &= 3_{10}, \text{ and } \text{SOE}_b = 000011_2 \\ \text{SFS}_d &= 0.145_{10}, \text{ and } \text{SFS}_b = 00010010001_2 \\ \text{SFE}_d &= 0_{10}, \text{ and } \text{SFE}_b = 000000_2 \end{aligned}$$

EXAMPLE 2

Temperature sensor, range $-10\text{ }^{\circ}\text{C}$ to $75\text{ }^{\circ}\text{C}$, with 12-bit ADC

The real number -10 will be represented by decimal 0 and therefore by binary 0, and the real number 75 will be represented by decimal 4095 (based on the capability of the 12-bit ADC) and therefore by binary 1111111111. The consequent constraints on the scale factor SF and scale offset SO are:

$$\begin{aligned} -10 &= 0 \times \text{SF} + \text{SO} \\ 75 &= 4095 \times \text{SF} + \text{SO} \end{aligned}$$

Therefore $\text{SO} = -10 = -1 \times 10^1$, and $\text{SF} = (75 + 10)/4095 = 0.0208 = 0.208 \times 10^{-1}$, and

$$\begin{aligned} \text{SOS}_d &= -1.000_{10}, \text{ and } \text{SOS}_b = 10000011000_2 \\ \text{SOE}_d &= 1_{10}, \text{ and } \text{SOE}_b = 000001_2 \\ \text{SFS}_d &= 0.208_{10}, \text{ and } \text{SFS}_b = 00011010000_2 \\ \text{SFE}_d &= -1_{10}, \text{ and } \text{SFE}_b = 111111_2 \end{aligned}$$

6.4.7 Data uncertainty

This field contains a code corresponding to a value that represents the accuracy of the transmitted data. The value is expressed as a percentage X of each transmitted value and means that the actual value is estimated, at the 95% level of statistical confidence, to differ from the transmitted value by an amount not exceeding $X\%$ of the transmitted value. Table 4 shows the codes and values.

Table 4 —Data uncertainty codes

Code	Value (%)
000	< 1
001	1
010	2
011	3
100	5
101	10
110	20
111	>20

EXAMPLE

Analysis conducted by the sensor manufacturer reveals that the expanded combined relative standard uncertainty due to the ADC performance characteristics (sensor manufacturing tolerances, and variations in environmental conditions within specified limits) is 7.89%. It is recommended that the manufacturer reports this value on its website and assigns the code 101.

6.4.8 Sensor reconfiguration

The sensor reconfiguration capability bit, (Field 11, Table 2) indicates whether or not the sensor supports the capability for the user to reconfigure the sensor. If this bit is set to 1, then reconfiguration is possible. If this bit is set to 0, then depending on the type of sensor and its use in an application, the sensor may be used as follows:

- To monitor only a single item.
- To monitor a different item until the end of service life of the sensor. This can be achieved by changing the unique item identifier on the RFID tag.

6.4.9 Memory rollover capability

Memory rollover applies only to Table 3—Measurement Codes Fields 10 to 13, which provide multiple data values. As successive sample data are recorded, the available memory may be filled. Without memory rollover, at the point where the memory becomes full the recording of data ceases, and a memory-full alarm is set. With memory rollover enabled, at the point where the memory becomes full the earliest record is overwritten on a first-in–first-out (FIFO) basis.

The Memory Rollover Capability Field of the Primary Sensor Characteristics TEDS (Table 2, Field 12) is a single bit that indicates whether or not the sensor supports the capability to apply memory rollover on the sensor. If this bit is set to 1, then memory rollover is supported. The Sample and Configuration Record (Table 11, Field 5) has a bit that declares whether the application administrator for the current mission has enabled memory rollover.

6.4.9.1 Memory rollover capability for measurement code 10

Each sample in memory is referred to by an index that is one less than the sample number of the particular sample. For example, S_0 taken at relative time zero [the (Coordinated Universal Time (UTC) time stamp taken upon successfully starting a mission time plus the monitor delay value that gives the time monitoring actually begins] is the first sample, and S_1 taken one sample interval later is the second sample. If sample capacity $SCap$ is full, then the $SCap$ th sample has index $SCap - 1$. If memory rollover has occurred one time such that the very first sample (index zero) has been rewritten, then that once rewritten sample may be referred to as having “total index” = $SCap$, and “local index” = 0 (it is the 0 index element within this “pass”). At this point, the number of samples taken equals $SCap + 1$. If memory rollover is supported and enabled, then the correct time stamp of each sample can be easily calculated as follows:

Table 17, Field 1, gives the total number of segments (see 6.6) that can be stored, referred to as $C10SC$ (Code 10 sample capacity). The total number of samples that can be stored ($SCap$) is given by $32 \times C10SC$.

Letting SC be the current total sample count (tracked via Field 5 of Table 17), the number of times memory rollover has occurred is:

$$\text{Rollover Count} = RC = \text{Int} \left[\frac{SC - 1}{SCap} \right]$$

where $\text{Int}[x]$ is defined as the largest integer less or equal to x .

Next, define the variable local index (LI) as the index from 0 to $SCap - 1$ that describes a sample position.

Let us now define the last sample taken (LST) in the most recent memory rollover period as having local index Max (LI_{max}).

LI_{max} is given by:

$$LI_{max} = (SC - 1) - (SCap \times RC)$$

The total index TI (the index relative to the 0th index first sample taken) for samples in the most recent memory rollover period (those with local index $\leq LI_{\max}$) is given by:

$$TI = (SCap \times RC) + LI \quad (\text{for local index} \leq LI_{\max})$$

The TI for samples taken in the previous (next to last) roll over period (those with indexes from $LI_{\max} + 1$ to $SCap - 1$) is given by:

$$TI = [SCap \times (RC - 1)] + LI \quad (\text{for local index} > LI_{\max} \text{ and } RC > 0)$$

The time stamp in seconds of the LIth indexed sample ($t(LI \text{ indexed sample})_s$) in memory, so long as TI is properly calculated as per the above based on the position of LI relative to $LI_{\max}$, is always given by:

$$t(LI \text{ indexed sample})_s = UTC + MD_s + (TI \times SaIn_s)$$

where UTC is given in Field 1 of Table 11, MD_s is the monitor delay in Field 3 of Table 11 expressed in seconds, and $SaIn_s$ is the Sample Interval in Field 2 of Table 11 expressed in seconds. Then, $t(LI \text{ indexed sample})_s$ can be converted to any desired time stamp format.

These equations may also be used to find the data of interest (find the proper local indexes) that corresponds to a certain time period. The pertinent manipulations of the previous equations are presented next.

First,

$$TI = \text{Round} \left[\frac{[t(\text{desired})_s] - UTC - MD_s}{SaIn_s} \right]$$

where $\text{Round}[x]$ returns the nearest even integer to x .

And then

$$LI = TI - RC \times SCap \quad (\text{if } TI \geq SCap \times RC)$$

or

$$LI = TI - (RC - 1) \times SCap \quad (\text{if } TI < SCap \times RC)$$

6.4.9.2 Memory rollover capability for measurement code 11

If memory rollover is supported and enabled, then the correct time stamp of each sample is given by the time tick associated with it. Notice that when the sample count is beyond the encoding capacity, the sensor shall stop writing records to the memory assigned for this measurement code. Table 17, Field 2 (Code 11, sample capacity), gives the total number of segments that can be stored. The total number of samples that can be stored (SCap) is given by $32 \times C10SC$.

The number of times memory rollover has occurred is:

$$\text{Rollover Count} = \text{Int} \left[\frac{\text{SCOEOET} - 1}{\text{SCap}} \right]$$

where SCOEOET (sample count of events outside either threshold) is given in Field 9 of Table 17.

The time of the particular LI sample can be calculated as follows:

$$t(\text{LI indexed sample})_s = \text{UTC} + \text{MD}_s + [\text{Sample Tick}(\text{LI indexed sample}) \times \text{SaIn}_s]$$

$t(\text{LI indexed sample})_s$, MD_s , and SaIn_s are as defined in 6.4.9.1.

6.4.9.3 Memory rollover capability for measurement code 12

If memory rollover is supported and enabled, then the correct time stamp of each sample is given by the time tick associated with it. Notice that when the sample count is beyond the encoding capacity, the sensor shall stop writing more records in the memory assigned for this measurement code. Table 17, Field 3 (Code 12 sample capacity), gives the total number of segments that can be stored. The total number of samples that can be stored (SCap) is given by $32 \times \text{C10SC}$. The number of times memory rollover has occurred is:

$$\text{Rollover Count} = \text{Int} \left[\frac{\text{SCOEOET} - 1}{\text{SCap}} \right]$$

where SCOEOET is given in Field 9 of Table 17.

The time of the particular LI sample can be calculated as follows:

$$t(\text{LI indexed sample})_s = \text{UTC} + \text{MD}_s + (\text{Sample Tick}(\text{LI indexed sample}) \times \text{SaIn}_s)$$

$t(\text{LI indexed sample})_s$, MD_s , and SaIn_s are as defined in 6.4.9.1.

6.4.9.4 Memory rollover capability for measurement code 13

These calculations are only valid if the alarms are triggered. Field 6 of Table 17 reveals the alarm status.

If memory rollover is supported and enabled, then the correct time stamp of each sample can be easily calculated as follows:

The number of times memory rollover has occurred is:

$$\text{Rollover Count} = \text{RC} = \text{Int} \left[\frac{\text{SC} - \text{SC@1TE}}{\text{SCap}} \right]$$