IEEE SA
STANDARDS ASSOCIATION

IEEE SA ICAP WHITE PAPER

IEEE CONFORMITY ASSESSMENT PROGRAM (ICAP)
IEEE INDUSTRY ROUNDTABLE MEETING

INTEROPERABILITY AND CYBERSECURITY FOR IOT-ENABLED SENSOR DEVICES

Authored by

Raymond K. Boncek, *Lockheed Martin*

Sri Chandrasekaran, *IEEE*

Julian K. Chang, *Boeing*

Ravinder Dahiya, *Northeastern University*

Bruce Hecht, *Massachusetts Institute of Technology*

Sridhar Kowdley, *US Department of Homeland Security*

Brent Lunceford, *Memstronics*

Ted Osinski, *IEEE*

Kyoko Roberts, *Hitachi High-Tech*

Ravi Subramaniam, *IEEE*

IEEE

Documents
Document Sharing Hub

Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

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

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 30 November 2022. Printed in the United States of America.

PDF: STDVA25782 978-1-5044-9187-7

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

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.

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

Copyright © 2022 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE CONFORMITY ASSESSMENT PROGRAM (ICAP) DOCUMENTS

This IEEE Conformity Assessment Program (ICAP) publication ("Document") is not a consensus standard. Specifically, this Document is NOT AN IEEE STANDARD. IEEE expressly disclaims all warranties (express, implied, and statutory) related to this Document, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, or currency. In addition, IEEE disclaims any and all conditions relating to results. This ICAP document is supplied "AS IS" and "WITH ALL FAULTS."

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

TABLE OF CONTENTS

ABSTRACT 6

1. INTRODUCTION 6

2. CRITICAL SUCCESS FACTORS FOR IEEE SENSORS PROGRAM 7

3. KEY INTEROPERABILITY ISSUES 8

4. KEY CYBERSECURITY ISSUES AND VULNERABILITIES 8

4.1. Cybersecurity Threats 10
4.2. Cybersecurity Issues 10

5. IEEE SENSOR STANDARDS 11

6. COMMON DEPLOYMENT MODELS FOR IOT SENSORS 12

7. REFERENCE SENSOR ARCHITECTURE FRAMEWORK 14

8. REFERENCE ARCHITECTURE COMPONENTS 15

8.1. Sensor Device Firmware 15
8.2. Sensor Data 15
8.3. Communication Protocols 16
8.4. Payload message formats 16
8.4.1. JavaScript Object Notation (JSON) 16
8.4.2. Data Visibility: Queries and Searches 16

9. INTEROPERABILITY REQUIREMENTS 17

9.1. Sensor Data Interoperability Requirements 17
9.1.1. Standard-based vocabulary for sensor parameters 17
9.1.2. Global identifiers 17
9.1.3. Device Provisioning 18
9.1.4. Standard taxonomy for sensor categories 18
9.1.5. Sensor event data sent to upstream devices 18
9.1.6. Application programming interfaces (APIs) 19
9.2. Communication Protocols Requirements 19
9.3. Data Transfer Protocol Requirements 19
9.4. Data Visibility: Queries and Search Requirements 19
9.5 Standard Interoperability Data Sheet 20

10. CYBERSECURITY REQUIREMENTS 20

11. SUPPLEMENTAL IEEE SERVICES 21

11.1. Educational 21
11.2. Certification 21

Documents
Document Sharing Hub

Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

11.3. IEEE Sensors Registry 21
11.4. Sustainable Technology 22

12. PLANS TO MITIGATE INTEROPERABILITY AND CYBERSECURITY ISSUES 22

12.1 Mitigation plan for interoperability issues 22
12.2 Mitigation plan for cybersecurity issues 23

13. RECOMMENDATIONS 24

13.1. Foundational data 24
13.2. Cybersecurity protection profiles 25
13.3. Application programming interfaces 25
13.4. Implementation Guidelines 26
13.5. Standards 26
13.6. List of Proposed Recommendations 26

14. SUMMARY AND CALL TO ACTION 28

Documents
Document Sharing Hub
Copyright © 2022 IEEE. All rights reserved.
Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

INTEROPERABILITY AND CYBERSECURITY FOR IOT-ENABLED SENSOR DEVICES

ABSTRACT

This white paper examines the biggest interoperability and cybersecurity issues facing the IoT-enabled sensors and makes recommendations to remedy them. In addition, it proposes a plan to enable the sensor market to take advantage of IoT capabilities. A draft version of this white paper served as supporting material for the IEEE Sensors Roundtable meeting of industry leaders that was held in Austin, Texas, on September 14-15, 2022. This final version has been updated with the recommendations from the Roundtable meeting.

1. INTRODUCTION

Internet of things (IoT) concept in sensors and actuators has experienced exponential growth during the last decade and are poised for continued mass-scale adoption in smart cities, manufacturing, energy, Industrial IoT, healthcare, environment monitoring, digital agriculture, and automotive industries, including the forthcoming autonomous vehicles markets. This explosive growth has exposed issues that are beginning to plague the adoption of IoT across industries. This white paper will mostly refer to IoT sensors to simplify the message with the understanding that these IoT sensors are smart sensors and that IoT actuators are also included in this message.

Network interoperability and cybersecurity are the two most important issues consistently identified in smart microelectromechanical systems (MEMS) and sensors industry surveys and market reports and they are the biggest impediments to market growth. These issues manifest themselves in increased implementation costs, added complexity to systemwide cybersecurity solutions, and result in closed-loop/proprietary system solutions that reduce free-market competition. Another major concern is that devices with IoT sensors are not positioned to take full advantage of the IoT features and capabilities. In response to requests to address these challenges, IEEE, the world's largest standards organization and a trusted neutral party, will work with the sensors industry to develop comprehensive solutions.

Copyright © 2022 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

This white paper is a compendium of issues, concerns, and recommendations communicated to IEEE primarily through the webinars and the Roundtable meeting of industry technical experts and business executives.

The intent of this white paper is twofold: Firstly, to allow IEEE to come up with the organizational structure and a roadmap to implement the issues defined in this paper. Secondly, to establish a starting point for industry to begin working on the solutions.

2. CRITICAL SUCCESS FACTORS FOR IEEE SENSORS PROGRAM

With agreement from the industry, the critical success factors (CSFs) outlined next, will guide the IEEE approach to solve the interoperability and cybersecurity problems associated with IoT sensors. The CSFs are as follows:

- Open, unified, and cybersecure guidance developed for connecting IoT smart sensors and devices to applications
- Platform independence and accommodation for leading access methods
- Standards architecture built on widely adopted and open standards
- Targeting of specific market segments
- Extensibility for different sensor types
- Sensors and electronic hardware designed for seamless reuse across different platforms as well as for easy repairability
- Fast initial development and incremental releases of standards, recommended practices/ guidelines, and test specifications
- Independent certification program that supports the standards
- Industry commitment to implement recommendations

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

3. KEY INTEROPERABILITY ISSUES

The following issues consistently arise in IEEE and industry surveys and independent market research reports.

TABLE 3 IoT sensor interoperability issues

Number	Issue
1	**Limited hardware choice** Many sensor and gateway manufacturers collaborate to ensure that their products are interoperable and cybersecure; however, they won't work with other devices. This approach limits choices available to prospective buyers as well as limits the alignment of hardware with solutions needed for emerging global challenges such as sustainability and electronic waste.
2	**Limited connectivity** There are a number of communication protocols implemented by sensors and gateway manufacturers, and the implementations vary. Only sensors that have been tested and approved by a gateway vendor can be assured of connectivity.
3	**Varied data quality** Data quality and differences in returned parameters are a significant issue in the sensors industry. Most sensor manufacturers do not comply with standards, and standards have not adequately addressed data quality. As a result, sensor parameters have different formats and return different values for the same sensor type from different manufacturers. Buyers are in the dark, as they do not know the sampling methods, the algorithms for calculating parameters, and the time intervals for capturing data.
4	**Non-standard accessing methods [application programming interfaces (APIs)]** Applications must rely on proprietary access methods from sensors or network gateways/server manufacturers.
5	**Misleading product data sheets** Despite liability, product data sheets are often misleading. Integrators often must procure sensors and do their own testing to determine sensor functionality, data quality, and sensor performance.

4. KEY CYBERSECURITY ISSUES AND VULNERABILITIES

The cybersecurity issues and requirements listed in this paper are intended to be a guideline for the development of a comprehensive mitigation plan. The industry must reach consensus as to the requirements that should be implemented and the timeframe for implementation. IEEE encourages adoption of industry best practices, guidance, standards, and frameworks. A short list of them is as follows:

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...

- NIST Cybersecurity Framework: US National Institution of Standards and Technology (NIST)[1]
- Zero Trust Maturity Model: Cybersecurity and Infrastructure Security Agency (CISA)[2]
- Payment Card Industry Data Security Standard (PCI DSS): PCI Security Standards Council (PCI SSC)[3]
- HIPAA Security Rule: The Health Insurance Portability and Accountability Act of 1996 (enforced by US Department of Health and Human Services)[4]
- ISO/IEC 27001: A jointly developed standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) on how to manage information security[5, 6]
- Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408): A jointly developed standard by ISO and IEC that defines general concepts and principles of information technology (IT) security evaluation[7]

IEEE's intention is to focus on specific data- and technology-related cybersecurity issues.

The following two tables—adapted from the MITRE ATT&CK framework filtered for Industrial Control Systems (ICS)[8]—outline common cybersecurity attack impacts or cyberthreats to operations. These cybersecurity attack impacts are the likely objectives of an attacker and are not ranked by severity or importance. These cyberthreats to operations will increase in scale and frequency with emerging technologies such as the next generation of wireless (5G and 6G) because they promise to bring a standard communication link with greater bandwidth and more ubiquitous access to IoT sensors. To mitigate these threats to operations, an end-to-end cybersecurity resiliency approach must be implemented that anticipates, withstands, recovers from, and adapts to cybersecurity attacks.

[1] US National Institution of Standards and Technology, "Cybersecurity framework," https://www.nist.gov/cyberframework.
[2] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," https://www.cisa.gov/zero-trust-maturity-model.
[3] PCI Security Standards Council, "At a Glance: PCI DSS 4.0," https://docs-prv.pcisecuritystandards.org/PCI%20DSS/General%20Guidance/PCI-DSS-v4-0-At-A-Glance.pdf.
[4] Health Insurance Portability and Accountability Act of 1996, HR 3103, 104th Cong., Public Law No. 104-191, https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf.
[5] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/standard/54534.html.
[6] ISO/IEC 27001:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary, https://www.iso.org/standard/73906.html.
[7] ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, https://www.iso.org/standard/50341.html.
[8] MITRE ATT&CK, "ICS Matrix," https://attack.mitre.org/matrices/ics/.

Copyright © 2022 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE Conformity Assessment Program (ICAP)—IEEE Industry Roundtable Meeting—Interoperability And Cybersecurity for IoT-Enabled...