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*

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

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

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.

TABLE OF CONTENTS

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.

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

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:

- 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/.

4.1. CYBERSECURITY THREATS

The cybersecurity attack impacts (see Table 2) are taken from MITRE ATT&CK framework. These attacks could be initiated by malicious cyberactors, including cybercriminals, insiders, or nation-states/state-sponsored groups (i.e., advanced persistent threat actors). These cybersecurity attack impacts are the result of successful cyberattack tactics and techniques to gain initial access; develop, deliver, and execute an exploit; maintain persistence in the system/sensor; escalate privileges; evade detection; discover sensor operations; move laterally; collect information; command and control the sensor; inhibit response functions; and impair measurements.

TABLE 2 Cybersecurity attack impacts

Number	Threats to operations
1	Damage to sensor property
2	Denial of sensor control
3	Denial of sensor measurements
4	Loss of sensor availability (including Ransomware/Digital Extortion)
5	Loss of sensor control
6	Loss of productivity/revenue
7	Loss of sensor protection
8	Loss of sensor safety
9	Loss of sensor measurement
10	Manipulation of sensor control
11	Manipulation of sensor measurement
12	Theft of operational sensor information

4.2. CYBERSECURITY ISSUES

The common issues that result in poor cybersecurity defenses to mitigate the attack objectives are listed in Table 3 and came from various IEEE and independent market research surveys.

TABLE 3 Key cybersecurity issues

Number	Common cybersecurity issues
1	No consistent security mechanisms at the communication protocol levels
2	No end-to-end encryption (sensor-to-cloud or sensor-to-user)
3	No systemwide key management [public key infrastructure (PKI)]

Number	Common cybersecurity issues
4	No zero-trust policy implemented
5	No widespread usage of 128-bit or longer encryption
6	No consistent data protection independent of network security
7	Too many standards, frameworks, and proprietary solutions
8	No device authentication
9	No Common Weakness Enumeration (CWE) for sensors
10	Other

5. IEEE SENSOR STANDARDS

The importance of technology standards is a well-known necessity for mass-market adoption. Numerous publications exist that describe cybersecurity risks potentially associated with MEMS and other sensors. In addition, it is well known that there are no industry efforts or governmental regulations actively driving the industry to standardization. While the industry has learned to live with the status quo, there are expectations that this will be more harmful in the long run. The lack of standards also poses challenges to early solutions needed for after-the-life management of electronic hardware.

Industry needs standards that:

- Address fundamental framework issues for system-level integration and cybersecurity.
- Work with current and emerging technologies.
- Will serve as a base for conformity assessment programs.
- Have wide industry support.
- Enable mass-market adoption.
- Allow industry to prepare for future challenges posed by issues such as e-waste and potential implications because of policies such as right to repair and those related to climate change.

IEEE has a portfolio of standards that address some of the needs stated above, such as the following:

- IEEE Std 1451™, a family of sensor standards, includes a set of network-independent communication interfaces for connecting transducers to servers and specifications of transducer electronic data sheets (TEDS) for each transducer.[9, 10]

- ISO/IEC/IEEE 21451 defines a set of transducer signal treatment services based on signal treatment algorithms as application programming interface (API), which is used for applications to use or call these transducer signal treatment services.
- IEEE Std 2700™ includes a minimum set of performance parameters defined with required units, conditions, and distributions for each MEMS sensor.[11]
- IEEE P2888.1™ defines the vocabulary, requirements, metrics, data formats and APIs for acquiring information from sensors, enabling definition of interfaces between the cyber world and physical world.[12]

IEEE recognizes a need to modify existing standards and create new standards that would meet industry needs.

6. COMMON DEPLOYMENT MODELS FOR IOT SENSORS

The majority of sensors are deployed in one of the following two ways:

a) Sensors residing on the same hardware platform [see Figure 1a)]: Android APIs are used for sensors residing on the same hardware platform with the Android operating system. This solution is typical for Android-based consumer electronic devices such as smartphones. Android APIs are available as open-source and support MEMS and sensors.

b) Sensors residing on different hardware platforms interacting with each other to create and IoT System that interfaces with the remote IT-based core industrial control and support systems in the Operational Environment [see Figure 1b)].

This paper focuses on the model represented in Figure 1b).

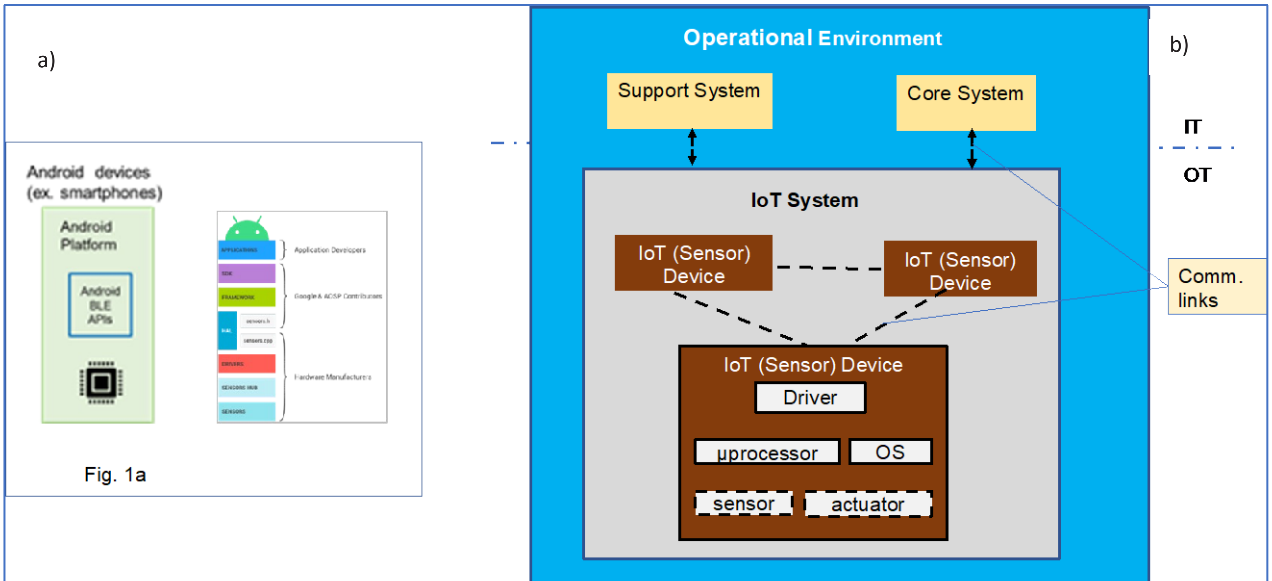
[9] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

[10] The IEEE 1451 series of standards are inactive but can still be accessed. Please see the IEEE SA website for details on the series, which contains IEEE Std 1451.0™, IEEE Std 1451.1™, IEEE Std 1451.2™, IEEE Std 1451.3™, IEEE Std 1451.4™, IEEE Std 1451.5™.

[11] IEEE Std 2700™, IEEE Standard for Sensor Performance Parameter Definitions.

[12] At the time of this publication, IEEE P2888.1, Draft Standard for Specification of Sensor Interface for Cyber and Physical World, is still in the drafting process and has not been officially approved.

FIGURE 1 **a) Sensors on Same Hardware Platform**
b) Networks of Sensors on Different Hardware Platforms



Support System= Control, configuration, maintenance of IoT
System (includes Gateway/Server IT)
Core System= Operational Applications, Processed Sensor
Data, etc… (includes Cloud OT)

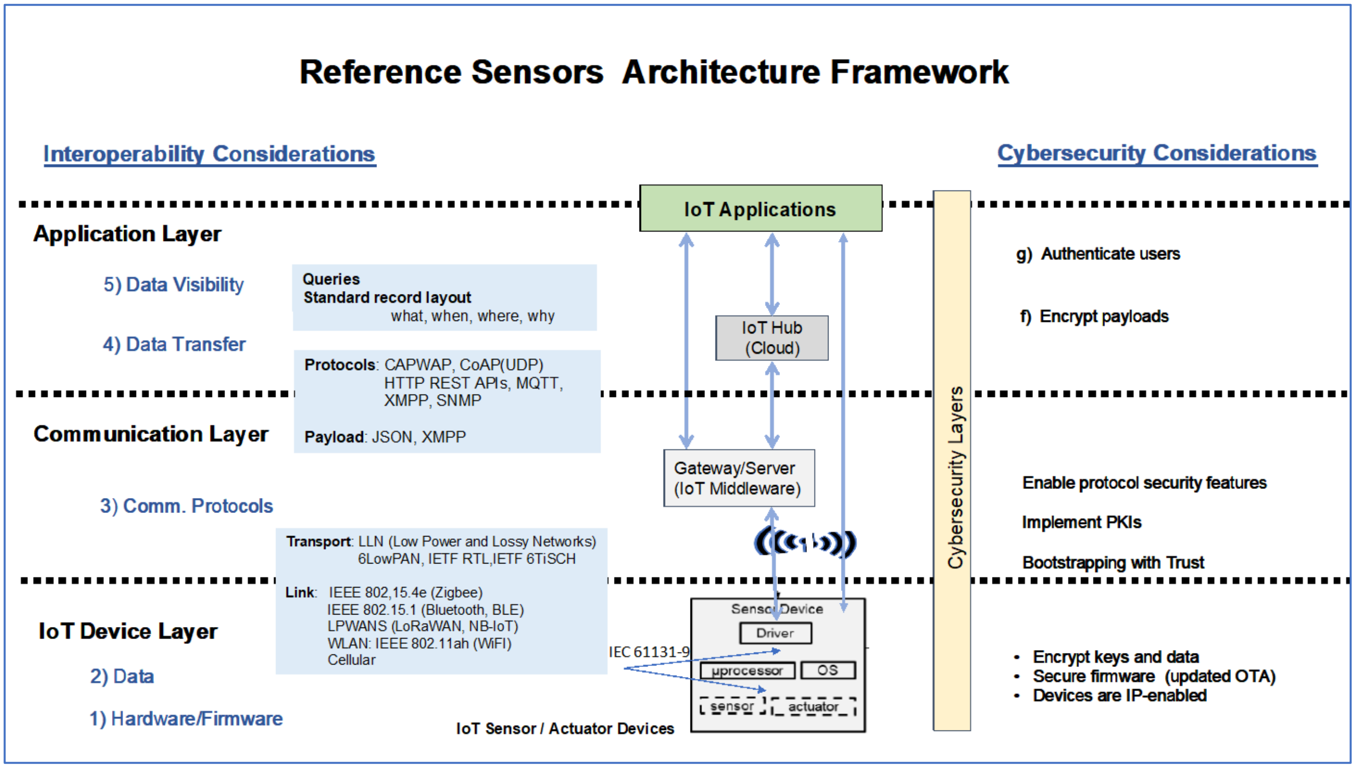
Adapted from NIST SP 800-213

Fig. 1b

7. REFERENCE SENSOR ARCHITECTURE FRAMEWORK

The Reference Architecture Framework (see Figure 2) is conceptual, and its purpose is to facilitate understanding and discussion of common interoperability, cybersecurity, and IoT issues.

FIGURE 2 Reference Sensors Architecture Framework



The reference architecture is open and flexible. It allows sensor devices to operate in a push-pull mode (for push-mode, sensors initiate communication with an application; for pull mode, applications request sensors to send data) or for sensor devices to communicate directly with a cloud server.

It collects the physical object status and transmits it to the IoT application through the layers. The IoT application will analyze the data and will communicate the negative outcome to the relevant layer and to the affected devices. Each layer is vulnerable and prone to cyberattacks that can cause malfunctioning of the individual sensor or even the entire sensor network. Thus, cybersecurity overlaps all layers and must deal with trust management, confidentiality, integrity, availability, and authentication to protect sensors from attacks.

8. REFERENCE ARCHITECTURE COMPONENTS

The purpose of the sensor's reference architecture layers and components presented in Figure 2 is to show areas of sensor or actuator deployment that would benefit from interoperability and cybersecurity standardization.

8.1. SENSOR DEVICE FIRMWARE

Sensor device firmware in the *sensing layer* of the reference architecture encompasses the embedded, but potentially reprogrammable, executable driver code that controls the bootup/initialization and operating processes for the sensors or actuators and the integrated circuit (IC) board to which they are attached.

The bi-directional communication between the sensor or actuator and a driver should be based using IEC 611131-9:2022, which specifies a single-drop digital communication interface technology for small sensors and actuators SDCI (commonly known as IO-Link™). The operating systems (OS) and other protocols used to communicate between the sensors and any microprocessors are not considered here. What is important for cybersecurity considerations is the protection of firmware from malicious attacks.

Cybersecurity considerations: Access to the firmware is typically password protected, which is not sufficient protection. Hackers can gain access to firmware through other methods, for example, a malicious worm attack that does not require authenticated access to the firmware. Therefore, a strong authentication mechanism, integrity mechanism and/or built-in test mechanism to establish a root-of-trust state is warranted.

8.2. SENSOR DATA

Sensor data is often sent as a stream of message bits to an application on a dedicated port on a dedicated channel.

The formats and contents of the sensor messages are unstructured and not standardized even though there are IEEE standards that define sensor parameters, sampling methods, and calculation algorithms. This causes problems downstream: each edge device must be programmed to parse sensor data differently for each sensor manufacturer.

Cybersecurity considerations: Data protection offerings, such as encryption or integrity mechanisms, vary with sensor devices. Many of them do not offer any protection. Some implement lightweight or partial encryption.

8.3. COMMUNICATION PROTOCOLS

Most communication protocols implemented by sensor devices are based on IEEE standards. A list of the most common protocols for the link, transport and communication layers are provided on the Reference Architecture schematic.

8.4. PAYLOAD MESSAGE FORMATS

8.4.1. JAVASCRIPT OBJECT NOTATION (JSON)

JSON—JavaScript Object Notation—is a widely adopted text format for storing and efficiently transporting data. JSON is self-describing and easy to understand. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client and vice versa). It has become a preferred choice (unseating XML) for sensor applications.

Cybersecurity considerations: Cybersecurity should be provided by other components of the system. However, inspection of the code or DevSecOps pipeline used to build the code that creates the JSON message before releasing it into production would be warranted to ensure no flaws in message creation are introduced.

8.4.2. DATA VISIBILITY: QUERIES AND SEARCHES

The current IoT sensor devices and systems lack standardized query and search functionalities. Such features will become useful once IoT-based sensor systems are widely deployed and the issues around interoperability and cybersecurity are mitigated. The search and query functionalities already have been implemented in radio frequency identification–based (RFID-based) sensor systems. They are based on the ISO/IEC 19987:2017 standard—a GS1 Standard that defines EPC Information Services (EPCIS).[13] EPCIS's aim is to enable different applications to create and share visibility event data, within enterprises and across them as well. EPCIS enables partners to share and exchange sensor event data efficiently, providing a standard interface. The result is reduced time spent on integration because all involved parties can use the same interface regardless of the different database types used for storing that data.

[13] ISO/IEC 19987: 2015, Information technology — EPC Information services — Specification, https://www.iso.org/standard/66796.html.

9. INTEROPERABILITY REQUIREMENTS

The requirements listed in this section are intended to be a guideline for the development of a comprehensive plan and a solution to interoperability problems. The industry needs to reach consensus on which ones should be implemented and the time frame for implementation.

9.1. SENSOR DATA INTEROPERABILITY REQUIREMENTS

Sensor data interoperability requirements are outlined in 9.1.1–9.1.6.

9.1.1. STANDARD-BASED VOCABULARY FOR SENSOR PARAMETERS

A good source of information is IEEE Std 2700.[14] IEEE Std 2700 can be harmonized with Google APIs by adding two to four parameters for each sensor class. This would make independent certification based on an IEEE standard possible for consumer electronic devices. Examples of accelerometer parameters that can be added to IEEE Std 2700 are: *event value*, *timestamp,* and *jitter*. A gap analysis of all IEEE 2700 MEMS sensors and Google APIs is listed in the Appendix, and detailed analysis is available from IEEE upon request.

9.1.2. GLOBAL IDENTIFIERS

A universally unique identifier (UUID) of 10 bytes, should be a unique serialized number that is assigned to each sensor and should be locked.

It could consist of IEEE issued number for a sensor implementer (manufacturer, integrator, user), with sensor type added and a serial number appended to make it unique.

Alternatively, it can be based on GS1 Electronic Product Code (EPC) with 96, 128 or 256 bits or more.[15] The EPC is built on the GS1 Global Trade Item Number (GTIN) with added serial number plus other useful data. It is partially encrypted. The number could also contain context data such as sensor category or owner. There are many benefits to adding context data: conducting online searches, identifying counterfeit sensor devices, and coupling with certificates.

[14] IEEE Std 2700™, IEEE Standard for Sensor Performance Parameter Definitions.

[15] GS1, EPC Tag Data Standard (TDS), https://www.gs1.org/standards/rfid/tds.

9.1.3. DEVICE PROVISIONING

The concept of Transducer Electronic Data Sheets (TEDS),[16] has been adopted by many sensor manufacturers, but they did not necessarily follow any standard. TEDS are often used in the calibration and provisioning of sensors. It is proposed that a new lightweight and simplified standard for TEDS is developed that will be used for device provisioning only.

9.1.4. STANDARD TAXONOMY FOR SENSOR CATEGORIES

Industry uses different names for sensor categories and types. They also assign different numerical values to represent them. There are many benefits associated with standardized sensor categories. Standardization will allow meaningful comparison of same categories of sensors and will facilitate future searches or queries. The standard taxonomy should be promoted to the industry. This is a low hanging fruit.

9.1.5. SENSOR EVENT DATA SENT TO UPSTREAM DEVICES

The stream of bits coming from a sensor should be converted to meaningful sensor event data that can be stored, accessed, queried, and passed down the stream. A similar approach has been developed for RFID-based sensors and is a GS1/ISO standard. This will allow future queries to determine the following information about the sensors:

- What (sensor device)?
  Sensor ID (including owner number, sensor type, and serial number)

- When (time of the event)?
  Standard format date and time.

- Where (sensor location)?
  Standardize format for location.

- Why (business reason)?
  Was data sent part of regular transmission, ad-hoc, or error condition, etc.

[16] IEEE Std 1451.4™, IEEE Standard for A Smart Transducer Interface for Sensors and Actuators--Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats.

9.1.6. APPLICATION PROGRAMMING INTERFACES (APIs)

Standard RESTful APIs will allow simple and problem-free access to the sensor's data. The complexities of the system will be hidden from application developers. For APIs to be effective, the other recommendations listed previously should be implemented so that the system is interoperable and cybersecure. The RESTful APIS will ideally be available as open source to enable contributors to add more functionalities and features.

9.2. COMMUNICATION PROTOCOLS REQUIREMENTS

It is recommended to write implementation profiles for the most common communication protocols such as Bluetooth Low Energy (BLE). This would ease efforts to set up a communication link and exchange data between sensors and edge devices or clients. This is a common practice, for example, with BLE implementation profiles for medical devices. It is worth noticing that IEEE does not recommend supporting only one communication protocol.

9.3. DATA TRANSFER PROTOCOL REQUIREMENTS

Each protocol should have clearly documented messages/commands used for sensor data transfers. Data packets used in the commands should be based on standard vocabulary data. Showing message choreography might help. Data transfer protocol should be part of implementation profiles also.

9.4. DATA VISIBILITY: QUERIES AND SEARCH REQUIREMENTS

The data visibility requirements are as follows:

- The sensor data should be visible and shared within and across the enterprises. Users should be able to find out information about returned data, location of the sensor, calibration status, and other business data.
- The sensor event data should be accessible to authorized and secure searches and queries. This data may reside on an edge, web, or cloud server. Standard queries would facilitate web searches. ISO/IEC 19987:2017 can be leveraged or used as an example to accomplish this goal.[17]

[17] ISO/IEC 19987:2017, Information technology — EPC Information Services (EPCIS) Standard, https://www.iso.org/standard/72926.html.

9.5 STANDARD INTEROPERABILITY DATA SHEET

Industry needs a scaled down and focused Interoperability Data Sheet. It will compliment existing Product Data Sheets, which are often verbose, inaccurate, have different formats, and are not easily available.

10. CYBERSECURITY REQUIREMENTS

Cybersecurity requirements listed in this section are based on the issues discussed in the previous sections. They are intended to be a guideline for development of a comprehensive plan to mitigate cybersecurity problems. IEEE's intention is to focus on specific data and technology-related cybersecurity issues. Industry needs to decide which—if not all—of the following recommendations should be in the scope of the IEEE sensors program.

The following requirements should be considered for implementation; however, this may not constitute a complete list:

- Cybersecurity vocabulary for sensors (creation or adoption)
- Integrity protections for sensor hardware and firmware/software, including a root of trust
- Secure communication channels between IoT Sensors and between IoT Sensors and the remote Core and Support systems.
- Best practice cryptography for critical stored data and for end-to-end (sensor-to-cloud) message encryption
- Privileged user authentication for updates or changes to silicon, sensor devices, or gateway servers
- Logging of sensor-related events and the ability to timestamp these events
- Message input/output validation checks for format quality and data ranges (where possible)
- Command verification

These requirements could be documented in a sensor cybersecurity profile recommended practice or guideline. Other industries, such as the medical device industry, have documents such as IEEE P2621.1™, Draft Standard for Wireless Diabetes Security Assurance Evaluation: Connected Electronic Product Security Evaluation Program and MDCG 2019-16, Guidance on Cybersecurity for medical devices (Medical Device Coordination Group, European Union).[18]

[18] MDCG 2019-16 (Rev.1, July 2020), Guidance on Cybersecurity for medical devices, https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf.

11. SUPPLEMENTAL IEEE SERVICES

IEEE recognizes that it needs to offer additional services that will help implement agreed-upon interoperability and cybersecurity requirements. These services will be defined with the help of the sensors industry. IEEE will work with the industry to create and promote these services.

11.1. EDUCATIONAL

The IEEE Sensors Council is a leading organization dedicated to sensor standards, promotion of the technology, and delivery of educational services for the sensors industry.[19] The Sensors Council will expand its role and will offer additional educational services recommended by the industry roundtable meeting.

11.2. CERTIFICATION

The IEEE Conformity Assessment Program (ICAP) will play a leading role in creating a conformity assessment program for the sensor program.[20]

ICAP has a history of creating conformity assessment programs (certification programs) for several technologies. ICAP workgroups define test specifications, certification criteria, and certification programs. Based on the ICAP-defined program, IEEE will accredit independent test laboratories to test submitted sensor devices. IEEE will issue a certificate upon reviewing test reports and recommendations by a test laboratory. ICAP will also be promoting certified devices by listing them on the IEEE Sensors Registry.

11.3. IEEE SENSORS REGISTRY

The IEEE Sensors Registry is a web-based service for sensor registration and is already operational.[21] The purpose of the IEEE Sensors Registry is to restore trust in sensor product data sheets. This listing of IEEE-verified sensor data sheets allows buyers to find the right sensors for their implementations based upon performance parameters and data sheets.

[19] IEEE Sensors Council, https://ieee-sensors.org/.
[20] IEEE Conformity Assessment Program, "Products and programs," https://standards.ieee.org/products-services/icap/index.html.
[21] IEEE Sensors Registry, https://sensorsregistry.ieee.org/.

11.4. SUSTAINABLE TECHNOLOGY

The sensors and electronics hardware are critical for rolling out IoT concept in several applications. This makes it important to have stable supply chain, and the use of sustainable materials and practices so that the adverse health and environment impact of such hardware (e.g., through e-waste) after their end-of-life can be contained. IEEE recognizes that it needs to offer sustainable technological solutions through initiatives such as climate action.

12. PLANS TO MITIGATE INTEROPERABILITY AND CYBERSECURITY ISSUES

12.1 MITIGATION PLAN FOR INTEROPERABILITY ISSUES

Mitigation plans for interoperability issues should include the following actions:

a) Standardize vocabularies (nomenclature) for sensor interoperability and cybersecurity

b) Develop a sensor standard/implementation guideline and test the specification based on IEEE Std 802.11bf™[22]

c) Develop/adopt standardized APIs

d) Develop sensor implementation profile documents for IoT sensors that include:

   1) Sensor data

   2) Communication protocols (BLE as the first protocol)

   3) RESTful APIs

e) Create an education program to showcase best practices

f) Establish a strong sensor certification program for devices

g) Establish a certification program for professionals (industry specific for verticals)

h) Reward conforming products by listing them on IEEE Sensors Registry

[22] IEEE Std 802.11bf is an amendment to IEEE Std 802.11™, Technology--Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks--Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. The amendment covers Enhancements for Wireless Local Area Network (WLAN) Sensing.

12.2 MITIGATION PLAN FOR CYBERSECURITY ISSUES

IEEE strongly recommends that companies adhere to existing cybersecurity frameworks (such as the NIST Cybersecurity Framework and NIST SP800-213 IoT Device Cybersecurity Guidance[23]) and the device frameworks discussed in the previous sections of this publication. IEEE mitigation strategy will work within these frameworks.

Based on the input and analysis of the cybersecurity threats and issues, the implementation of the following protection mechanisms is recommended:

- Support for unique/immutable sensor device identification (logical is ideal, but physical at a minimum)
- Protection mechanisms for configuration of the sensor device
- Protection mechanisms for storing, accessing, and transporting data (from sensor to cloud)
  - Defining criticality of data levels based on the operational use of the sensor
  - Developing key management standards for cryptography used
- Protection mechanisms for:
  - Sensor devices
  - Edge device/servers
- Protection mechanisms for secure communication channels
- Protection mechanisms for application software in development and for monitoring during operation
- Establishment of cybersecurity certification for professionals
- Creation of protection profiles for silicon and gateway
- Support for the generation of sensor log event information
- Secure time distribution and usage for sensor devices

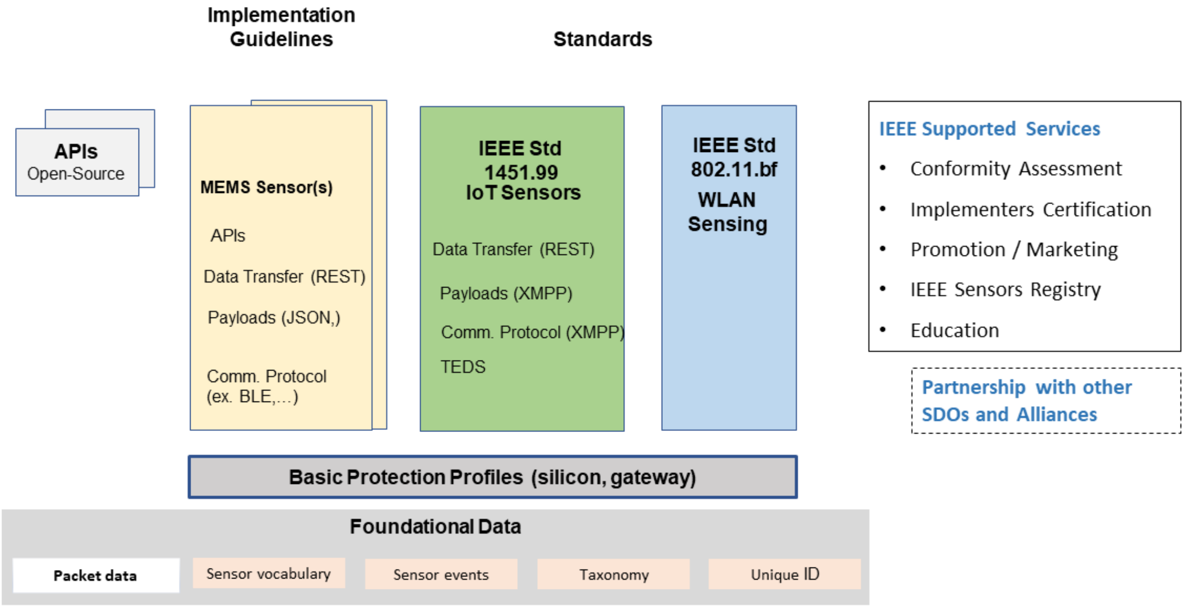
These recommendations might take the form of sensor cybersecurity guidelines or best practice documents that will complement the sensor implementation profiles. Furthermore, establishment of a strong education program for sensor cybersecurity is highly recommended.

[23] NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.

13. RECOMMENDATIONS

The recommendations outlined in this report (as depicted in the Figure 3) may involve the development of a new standard, an update to or extension of existing standards, implementation of a guideline or profile creation, and adoption and implementation of supporting services to ensure the sensor program's success. The list of recommendations can be augmented with other recommendations proposed by the roundtable participants.

FIGURE 3 Improving interoperability, cybersecurity, and enabling sensors for IoT



13.1. FOUNDATIONAL DATA

The following is a review of important foundational data to consider:

- *Sensor vocabulary:* Sensor arguments/parameters will use standard format to capture and exchange data. This will remove ambiguity and will greatly improve interoperability.
- *Sensor unique ID:* This will help identify each sensor device. It is not a manufacturer ID. It could be assigned to a sensor by an implementer. Typical unique IDs are 96, 128, or 256 bits. The number can contain context data such as barcode data and a sequential number to make it unique. The roundtable participants will recommend the best structure for such a number.
- *Sensor taxonomy:* Standard sensor classes are needed to facilitate queries and analysis of sensor

data. There are several existing taxonomies such as those implemented in Google APIs that could be recommended by roundtable participants.

- *Sensor events:* The events are a unit of data that will be used to store and share sensor data. The events will be made up of standard vocabulary elements. It will have additional context information added, such as the sensor unique ID, taxonomy or class type, date time frame, location, values, and other data.
    - Sensor events will help convey the following information: what, when, where, and why.
    - Sensor events will improve interoperability and will help realize the benefits of IoT.

13.2. CYBERSECURITY PROTECTION PROFILES

Profiles can be created by observing some of the following procedures and topics:

- The roundtable security experts will propose how to make physical devices and data secure.
- The recommendations might include writing protection profiles (PPs) for the following:
    - Silicon
    - Gateways

Protection profiles (PPs) might be differentiated by a level of assessment rigor, for example:

- Basic PPs might be performed by manufacturers themselves (self-testing).
- Advanced PPs would require third-party lab testing.

13.3. APPLICATION PROGRAMMING INTERFACES

APIs are the primary ways applications communicate. Sensor developers have made comments about a need for standard APIs that will immediately improve interoperability. Google APIs are the predominant APIs for sensors, and they are available as open source. The roundtable participants will make recommendations on the course of action: adopt or develop a new one.

13.4. IMPLEMENTATION GUIDELINES

The implementation guidelines are deliverables that will be developed in the near term. They will convey best practices for setting up sensors, communication protocols, encryption, gateways, firewalls, and applications. Implementation guidelines are common in many markets, such as medical devices. The guidelines should contribute to mitigating current interoperability and cybersecurity issues and will permit IEEE to set up certification programs.

13.5. STANDARDS

The specifications will address emerging technology or existing technology where too many proprietary solutions exist.

- IEEE Std 802.11bf, a wireless local-area network (WLAN) standard, has great potential to enhance the reliability and efficiency of WLAN sensing and establish interoperability of wireless devices to enable a wide range of new and useful applications.
- IEEE P1451.99™ will position sensors to take advantage of IoT.[24]

Standards take a little longer to develop but given the importance of the topics, IEEE will make every effort to fast-track them.

13.6. LIST OF PROPOSED RECOMMENDATIONS

The Roundtable Participants have recommended to conduct a survey to validate the recommendations and to narrow down the scope. The survey should include the following questions:

a. What are the most widely used wireless communications protocols, should they be in scope and why?
b. What standard should be used to define parameters and data?
c. What cyber protocols for IoT standards exist, or guidance exists?

[24] IEEE P1451.99™, Draft Standard for Harmonization of Internet of Things (IoT) Devices and Systems is currently in the drafting process and is not an approved IEEE Standard.

TABLE 4 Proposed recommendations

Number	Recommendations	Details	Scope
1	Standardize sensor data vocabulary and publish it on the web	Based on IEEE Std 2700 (can be harmonized with Google's APIs) and TEDS-specific IEEE Std 1451.4. In text, JSON, and XML formats	Foundational data
2	Establish global unique identifier for each sensor device	Options: based on IEEE Std 1451-2-2010 or GS1 EPC (This could be associated with certificate.)	Foundational data
3	Develop sensor events	a. Sensor events will be used to transmit, store and query data. b. Query language can be developed (e.g., GS1/ISO EPCIS standard)	Foundational data New standard
4	Establish standard taxonomy for sensor categories	Similar to Google APIs	Foundational data
5	Develop IoT sensor standard and test specification	a. Based on IEEE Std 802.11bf (WLAN sensing) b. Test specification	New standard
6	Develop/adopt RESTful APIs	Adopt Google's APIs or create open-source new APIs	Source code
7	Develop Interoperability Data Sheet	A scaled down version focused on interoperability	Guide
8	Develop implementation guides for sensor devices (MEMS sensors, initially)	a. Profile for MEMS Sensors b. Test specification (Start with BLE and use vocabulary)	Implementation guide
9	Develop cybersecurity protection profiles for sensor devices	Cybersecurity protection profiles for silicon and gateway (start with basic PP for silicon).	Cybersecurity protection profiles
10	Develop protection mechanisms for storing and accessing data (from sensor to cloud)	Encryption, PKI, or other Encryption: EAS 128, 256 or the strongest possible Compression: ZIP, RAR,7Z, MP3. Compression ration should be greater than 75%	Cybersecurity
11	Product certification program	a. IEEE Conformity Assessment Program (based on approved recommendations) b. Cybersecurity evaluation program	IEEE Conformity Assessment Program
12	Professional certification program	Implementer's certification	Certification
13	Promote certified sensors	a. IEEE organizations (Sensors Council, ICAP, SA) b. List certified devices on IEEE Sensors Registry	IEEE Sensors Registry and IEEE services

Number	Recommendations	Details	Scope
14	Establish educational program	IEEE Sensors Council: webinars, training, best practice guides.	IEEE services
15	Technology with human touch	Electronic hardware design to easy interoperability, reuse and repair and fabricated using easily available materials and sustainable and resource efficient processes.	IEEE services

These recommendations, if implemented, will significantly increase interoperability, and will mitigate cybersecurity attacks or their effects.

14. SUMMARY AND CALL TO ACTION

IEEE has listened to its members asking for better IoT sensor/actuator devices interoperability, protection from cybersecurity attacks, and preparations for industry to take full advantage of the internet.

This paper lists the most common issues that plague the industry and recommendations to resolve or mitigate them. These issues and recommendations were discussed at the roundtable meeting of industry leaders. With the roundtable participants' support, IEEE will propose a plan to implement them.

It is hoped that roundtable participants will promote this effort, provide experts to work on the solutions, and be the first to adopt or implement them.

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571