# IOT STANDARDS

This column will look at different segments of the IoT market as it relates to implementation and use of standards. Each column will select a particular vertical, and lay out the relevant standards and technologies that affect the evolving IoT hyperspace. The pace of the columns will start broadly with the vision of narrowing the subject of subsequent articles toward more specific applications of standards, whether in the development, application, test, or commissioning of IoT technologies.

# IoT Standards Matters

by Mike Violette
Washington Laboratories, USA

The universe of standards issues that affect IoT development and implementation is vast and complicated, involving many organizations, technologies and interests. This article discusses the intersection of three elements of the IoT Standards Ecosystem, namely: the principal organizations that drive Global Standards Development, Standards for Functionality and Compatibility, and Standards for Security and Privacy. These topics are evolving rapidly and, like the Internet of Things, constantly morphing as technology solutions are developed and implemented.

Not being able to swallow the whole thing, our plan is to eat the standards watermelon a bit at a time over the next several issues of *IEEE Internet of Things Magazine*.

So, for this inaugural article, I've chosen to briefly introduce the standards players by some admittedly subjective, broad, divisions: The Standards Development Organizations (SDO) Space, the Government Space and the Industry Space. A sample of some of the players will be described and further explored in future installments.

## SDOs

Standards Development Organizations SDOs or Standards Settings Organizations SSOs operate, in general, according to certain defined processes. Many organizations operate through a consensus process that is characterized by openness, transparency, balance, and due process or mechanisms for ensuring adherence to organizational procedures, including provision for appeals."[1] The global standards eco-system is varied and vast with a mix of players with various, and sometimes opposing, agendas.

Figure 1 represents a cross-section of standards-setting bodies that are involved in various IoT standards (among other things, such as EMC, Electrical Safety, Radio/Wireless and Cyber-Security) involved with formally-recognized national standards bodies, committees and global organizations as well other "fora and consortia."

The availability of the standards depends largely on the funding strategies. Many SDOs charge for their standards (IEC, ISO, IEEE, etc.) while others distribute the standards for free (ETSI, e.g.) as part of government-sponsored efforts to promulgate the information. In many of the standards-development models, much of the work is performed by volunteers who presumably have a stake in the outcome of the end-product, whether promoting a certain technology, protecting a bit of existing "real estate" or staying connected for other reasons. (I have met many standards "nerds" who do this for fun!)

How big is the standards universe? Just a brief perusal of the IEEE Standards Association website[2] shows a "partial listing" of IEEE standards that are related to IoT. This listing has over 70 standards, from base standards like IEEE 802.3-2012 "IEEE Standard for Ethernet" to more esoteric and specific **IEEE 1609.11™-2010** — "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)."

Editor's Note: Text appearing in bold indicates a live link in the online version.

The IEEE is, obviously, an active contributor to the standards world, with many of the IEEE outputs being elevated to National Standards under the American National Standards Institute (ANSI), which is celebrating 100 years since its founding in May 1918, and whose mission is to "administer and coordinate the U.S. voluntary standards and conformity assessment system."

A sister initiative under the aegis of the IEEE is the 5G Initiative, and the overlap of 5G and IoT is significant. One resource that has been developed under that initiative is the IEEE 5G Standards Database, found here: **https://5g.ieee.org/standards/standards-database**. This database is a collaborative effort aimed at collecting, in one place, standards that have "something to do with 5G," and is a crowd-sourced kind of effort. Contributions are welcome and encouraged from interested parties.

Clearly, the efforts undertaken to create this broad range of specifications and methods over the past decades has led to fundamental changes in our way of life. It is certainly expected to proceed apace and shows no sign of easing as various influencers cooperate and compete with each other for standards territory.

The interaction between the various SDOs are varied and complex and involve a mix of face-to-face get-togethers requiring many gallons of coffee as well as significant virtual efforts, where draft versions of documents whirl about on the Internet as part of consensus efforts that aim to include many voices. Often, it works well. Not infrequently the process may not work so well and there are often winners and losers in the standards race (think the long-ago VHS vs BETA square-off).

## Standards for Functionality

A second layer of this standards-dive includes functionality. This is a pretty critical aspect of the standards biome, and winners and losers are also defined in this space.

With so many players in the IoT space, it's a little dizzying to determine the dominant drivers for IoT functionality; in fact, to be honest, the task is a bit overwhelming. Major players in the industry, from software and hardware developers to government to network operators, have already staked out decades of operating methods that drive IoT functionality.

This space includes consensus-driven efforts as well as private and proprietary standards. One organization that has an open, consensus-based structure is the Internet Engineering Task Force (IETF), which is a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture."

This particular group has over 100 working groups aimed at improving "the smooth operation of the Internet." The working groups have defined areas that range from HTTP to Video Codecs to IPv6 Operations to Software Updates for Internet of Things. This group is open to anyone who is interested in contributing to the IETF's core mission and there are no membership fees. **https://www.ietf.org/about/participate/**.

The development and improvement in standards and specifications are conducted through mail lists and collaborative tools, while face-to-face meetings serve the purpose of putting faces with email addys.

The IETF's IoT efforts include melding IoT needs with existing standards, such as the first WG chartered in 2005 (6LoWPAN) which defined methods for adapting IPv6 to IEEE 802.15.4 (wireless personal area networks (WPANs)). Other wireless technologies are similarly adapted, including flavors of Blue-

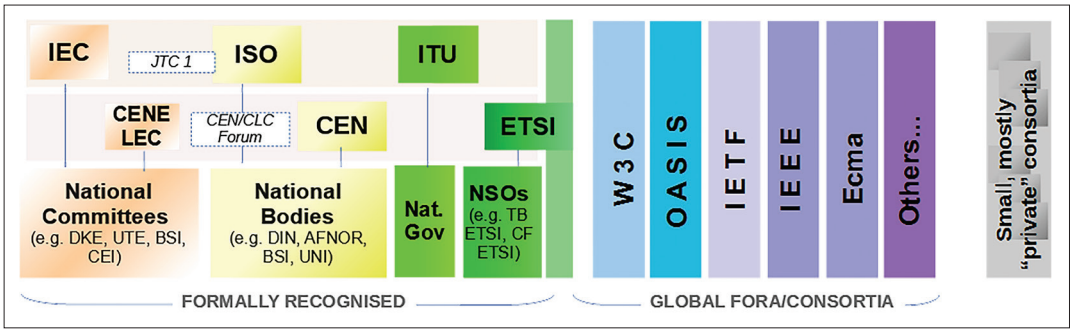


FIGURE 1. A cross-section of standards-setting bodies that are involved in various IoT standards Figure credit: Dr. Jochen Friedrich, IBM Europe.

tooth and Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) cordless phones. The intent is to make efficiency and reliability a prime feature of the IoT.

Naturally, the carriers and big data folks have evolved their own practices and standards. Verizon, for example, has a strong interest in connectivity for Machine-to-Machine (M2M) connections and the revenue that equates to the many billions of over-the-air connections that are growing on its networks. The major themes of its IoT services include the role of M2M connectivity in Smart Cities, route planning and dispatch for delivery services, mobile commerce and asset tracking.

From Verizon's report, "State of the Market: Internet of Things 2017: Making Way for the Enterprise,"[3] the subject of standards comes up on page 1: "An absence of industry-wide IoT standards, coupled with security, interoperability and cost considerations make up over 50 percent of executive concerns around IoT, according to Verizon's survey."

Clearly, major players are working in many spaces to make this uncertainty diminish, and the importance of security is at the top of the list.

## Standards for Security and Privacy

The National Institute of Standards and Technology (NIST) issued a voluntary "Cybersecurity Framework"[4] that "consists of standards, guidelines, and best practices to manage cybersecurity-related risk." This guidance is broad and intended to be flexible and adaptable to the many different needs of the IoT space. The word "standard" appears over 30 times in the document, and thus highlights the importance echoed in the words of the Verizon report.

The framework lays out tools to reach certain desirable outcomes and is designed to give a methodology for managing and reducing cyber threats. The key part of the framework relies on implementing these five functions: Identify, Protect, Detect, Respond and Recover, and can be further broken down into Categories and Subcategories with references that may be used to inform an entities' structure. Some examples of Categories include: "Asset Management, Access Control and Detection Processes."

How an organization implements this framework depends on the needs and implementation of whatever operations it is engaged in. Coupled with this methodology is a need for Risk Assessment to be overlaid in an organization's operation.

Other, international, standards for cyber security exist. One example of this is the series of standards under IEC 62443. This particular standard morphed from an ANSI standard (ANSI/ISA-99 or ISA99) to a standard under the International Electrotechnical Committee (IEC). It was originally developed by the International Society for Automation (ISA) and includes four general components or categories, namely: General, Policies and Procedures, System, and Component. The structure is meant to guide the development of a compliant and secure process, whether it involves software, hardware or a mix.

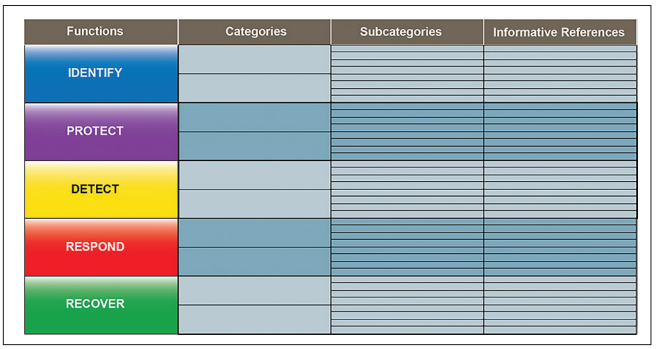


FIGURE 2. NIST cybersecurity framework.

One aspect of the IEC 62443 structure includes the opportunity for systems to be evaluated under a Conformity Assessment process and certification by Certification Bodies accredited for the discipline. Certification has most broadly been applied to devices, either evaluation for conformance with safety requirements, spectrum use and related physical conformance. The IEC 62443 Conformance Certification reviews the processes by which an organization has assured that their processes, code and security measures properly implement the applicable IEC 62443 requirements.

On a global basis, one of the challenges is to bring a necessary level of conformance that realistically manages the risks of cyber-threats without impeding the functioning of the Internet of Things. This requires reasonable standards and, for the foreseeable future, will be an active area of development across the entire IoT space.

Michael Violette (mikev@wll.com) is president of Washington Laboratories and director of the American Certification Body. He has over 25 years of experience in the field of EMC evaluation and product approvals, and has overseen the development of engineering services companies in the United States, Europe, and Asia. He is a Professional Engineer, registered in the State of Virginia. He has given numerous presentations on compliance topics and is a regular contributor to technical and trade magazines.

FOOTNOTES

[1] Overview of International Cybersecurity and Privacy Standards Development. Elaine Newton, PhD. Oracle Corporation
[2] http://standards.ieee.org/innovate/iot/stds.html
[3] http://www.verizonenterprise.com/verizon-insights-lab/state-of-the-market-internet-of-things/2017/
[4] https://www.nist.gov/cyberframework