EDITOR CHUCK WALRAD
Davenport Consulting; cwalrad@daven.com

Standards for the Internet of Things: A Case Study in Disaster Response

Phillip A. Laplante, Pennsylvania State University
Jeffrey Voas, IEEE Fellow
Nancy Laplante, Widener University

For life-critical systems like disaster response, standards are essential to ensure safety and reliability.

The Internet of Things (IoT) is, potentially, the next great technological revolution, promising fantastic economic benefits, improved quality of life, and even the easing of human suffering. However, the IoT also raises unprecedented security and privacy concerns as well as safety issues. Standardizing IoT devices and connections is the key to fully realized economic benefits and safe interoperability, particularly among systems.

There will be hundreds of thousands, if not millions, of IoT applications—some interconnected, some not, and some connecting with others in unintended or anticipated ways. Therefore, defining IoT standards is extremely important. But what exactly is the IoT, and what are the standards that best define it? To illustrate possible challenges the IoT will present, we describe a case study and suggest a path forward.

NOT ENOUGH STANDARDIZATION

There's no set definition of the IoT, but many descriptions exist.

For instance, the European Research Cluster defines IoT as a "dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" (www.internet-of-things-research.eu/about_iot.htm).

ITU, the UN's specialized agency for information and communication technologies, describes the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable

information and communication technologies" (www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx).

The Organization for the Advancement of Structured Information Standards (OASIS) refers to the IoT as a system "where the Internet is connected to the physical world via ubiquitous sensors."[1]

According to the Worldwide Web Consortium, the IoT "includes sensors and actuators, physical objects and locations, and even people. [It's] essentially about the role of Web technologies to facilitate the development of applications and services for things and their virtual representation" (www.w3.org/WoT).

Many other definitions can be found in Wikipedia, Techopedia, Webopedia, and so on. But all of these definitions incorporate some notion of diverse systems interoperating—sometimes even opportunistically by connecting to any available system within range.

Typical applications for the IoT include smart homes, smart cities, transportation, healthcare, and critical infrastructure systems such as power generation and distribution. IoT applications will be found almost everywhere, from industrial and government settings to the home. OASIS predicts that IoT sensors will exist in "every mobile device, every auto, every door, every room, every part, on every parts list, every sensor in every device in every bed, chair or bracelet in every home, office, building or hospital room in every city and village on Earth."[1] To date, however, most IoT systems are experimental and small in scale as platform builders and end users discover the challenges of building systems.

CASE STUDY: DISASTER SCENARIO

Despite the lack of an agreed-upon definition for the IoT, many standards are emerging for IoT devices, communications, networks, and applications, and more raising the question of interoperability across these standards. Nothing better illustrates this challenge than an IoT-enabled disaster emergency response system. For example, in the US, such a system would represent the convergence of systems requiring compliance with not only applicable IoT standards but also standards from the National Institute of Standards and Technology (NIST), Occupational Safety and Health Administration, Federal Emergency Management Administration, Health Insurance Portability and Accountability Act, and more.

9/11 disaster

Disasters can be caused by weather events, through accidents, and intentionally by humans (for example, bombings, arson, and bioterrorism). One of the most infamous human-caused disasters is the September 11, 2001, plane crashes into the World Trade Center Towers in New York City and the Pentagon building in Washington, DC. For those too young to remember, you can easily find images and videos of the scenes depicting the attack on the World Trade Center Towers and struggles for survival in the aftermath as first responders rushed to aid victims.

In New York City, the initial impact of the first plane was followed by smoke and fire in the North Tower. It was apparent that those on the plane were dead, as no one could have survived the impact and heat from the crash. Concern also mounted for those who were in the tower, as the workday had begun. News media and bystanders were shocked, unsure if some terrible accident had occurred or if this was an intentional attack. Very soon after the first plane hit, a second plane crashed into the South Tower, making it apparent that the event was human caused.

From the moment of the first attack and through the next several days, rescuers frantically worked to locate victims, evacuate the wounded, and find bodies in the wreckage. For many more days, the victims' families awaited either the happy announcement that their loved ones were found in a nearby hospital, or the devastating news that they were dead or missing.

In addition to the threats from fire, smoke, and unstable buildings, concern spread to the surrounding area as the first tower collapsed into rubble, followed by the second, taking many adjacent buildings with them. First responders who had rushed into a building to help save lives became victims themselves in the collapse of the towers. Local hospitals waited for the wounded to arrive, and triage areas were set up on site to immediately care for survivors. Unfortunately, few victims could be rescued, and the collateral impact on the area soon spread. More than 2,700 people died and nearly 7,000 were treated in area hospitals for injuries received in the New York City attacks.[2]

IoT to the rescue?

But what would have happened if the IoT had made it possible to track the people in the towers, in the wreckage, and fleeing on foot or being taken away in emergency vehicles? The result could have been better victim location and identification as well as more effective resource allocation and patient triage. Victims who made it to the triage area could have received a bracelet with a bar code or another type of device and have been registered in a system for passive or active tracking. Entering victims into a central system would allow for tracking to various acute care facilities from the disaster site. Victims who had succumbed to their injuries could have also been tracked for expeditious identification and transfer off site.

This capability already exists: Tia Gao and her colleagues developed a prototype real-time patient-monitoring system that "integrates vital signs sensors, location sensors, ad-hoc networking, electronic patient records, and Web portal technology to allow remote monitoring of patient status," including those still at disaster scenes.[3]

First responders who rush to the scene could also be tracked. In the New York City attacks, if tracking devices had been part of the first responders' gear, they could have assisted in locating specific personnel or those who became victims themselves. For healthcare teams, tracking could have assisted in ensuring appropriate staff in triage areas as well as in monitoring locations for safety purposes.

These kinds of systems are also being developed. For example, more than 10 years ago, Konrad Lorincz and his colleagues developed a system called CodeBlue that dynamically integrates sensors and other wireless devices in a disaster response setting.[4] They also developed an RF-based technology called MoteTrack that locates responders and patients within buildings during a disaster.

Tracking supplies and equipment in a disaster scenario is also very important. Networks of hospital systems already communicate about available supplies, such as ventilators and blood infusion products; however, a disaster site IoT could enhance and expand this functionality. A central command that inventories available supplies could benefit from tracking supply use and equipment relocation. The supplies could also be linked to victim tracking. Standards for such systems are already under development; for example, IEEE's Big Data New Initiative (http://bigdata.ieee.org/standards) has a medical IoT effort that's developing portable medical devices standards, such as the IEEE 11073 family of standards.[5]

However, these IoT system benefits would be predicated on effective and reliable interoperability of all systems involved, including the victims' personal trackable devices, such as phones or wearable IoT-enabled devices.

STANDARDS HARMONIZATION

Beyond standardizing the definition of the IoT, process interoperability, and systems and components, we need standards that help organize opportunistic IoT configurations. There are such standards underway. For example, LoRaWAN—a Low Power Wide Area Network specification intended for wireless battery-operated things in regional, national, and global networks—incorporates secure bidirectional communication, mobility, and localization services for continuous interoperability among smart devices.[6] Competing standards such as Sigfox (www.sigfox.com) and LTE[7] are also emerging. These kinds of standards are needed, but they must be harmonized, particularly for life-critical applications such as disaster response.

> Standardization is needed for all IoT devices but is essential in disaster response scenarios.

NIST recently released draft Interagency Report (IR) 8063, which offers a scientific foundation for the IoT and harmonization of related standards.[7] This work posits that communication, computation, and sensing are IoT technologies' core activities and defines a set of basic distributed system components called primitives and a class of elements that form the basis for all IoT systems. The following primitives have been proposed:[7]

- *sensor*: an electronic utility that digitally measures physical properties (for example, temperature, acceleration, weight, and sound) and outputs raw data;
- *aggregator*: a software implementation based on mathematical function(s) that transforms/consolidates groups of raw data into intermediate data;
- *communication channel*: a medium by which the data is transmitted (for example, physical via USB, wireless, wired, or verbal) between sensor, aggregator, communication channel, decision trigger, or eUtility;
- *eUtility* (external utility): a software or hardware product or service, providing computing power that aggregators will likely need in the IoT; and
- *decision trigger*: an if–then rule that creates the final results needed to satisfy the purpose, specification, and requirements of a specific IoT.

The elements that play a major role in fostering the degree of interoperability in IoTs are as follows:[7]

- *environment*: the universe that all primitives in a specific network of things operate in; this is essentially the operational profile of an IoT;
- *cost*: the expenses (time and money) that a specific IoT incurs in terms of nonmitigated reliability and security risks;
- *geographic location*: the physical place where a sensor or eUtility operates or was manufactured;
- *owner*: the person or organization that owns a particular sensor, communication channel, aggregator, decision trigger, or eUtility;
- *device ID*: a unique identifier for a particular sensor, communication channel, aggregator, decision trigger, or eUtility; and
- *snapshot*: an instant in time, utilized for synchronization of events fired by sensor, aggregator, communication channel, decision trigger, or eUtility.

Defining IoT systems in this way allows for the trustworthy interoper-

ability of systems built from any IoT components, services, and commercial products.

THE WAY FORWARD

Whereas standards harmonization seeks to reconcile the differences in two or more standards, standards blending means selecting the components of each standard that best fit specific IoT technical combinations.[8] Because NIST IR 8063 defines the basic pieces of any IoT, it can be used as a basis for blending two or more standards (see Figure 1).

For example, suppose standards A and B are IoT standards for some devices or systems used in an emergency response scenario (such as those in our disaster response example). The primitives and elements of NIST IR 8063 can be extracted from standards A and B, reconciled into an intermediate representation, and then translated into a blended standard (call it A/B).

Standardization is needed for all IoT devices but is essential in disaster response scenarios because first responders, doctors, nurses, and others come from various different locations and facilities, uniting themselves with IoT-enabled equipment. But there are still many unresolved challenges. For example, what about other IoT-enabled systems (such as those carried by the victims, or in nearby buildings, or even on first responders) that opportunistically interact in this setting? These could be helpful (for instance, by allowing rapid access to a victim's medical history) or problematic (for instance, by triggering a security response that could block signals). What about nearby noncritical systems that might inadvertently interact with a critical system in an IoT and cause a catastrophic failure? What about security standards?

Noncritical systems, such as those for emergency response, might interoperate with critical IoT systems without regard to protocol, and we might find out at the worst time—during the disaster.

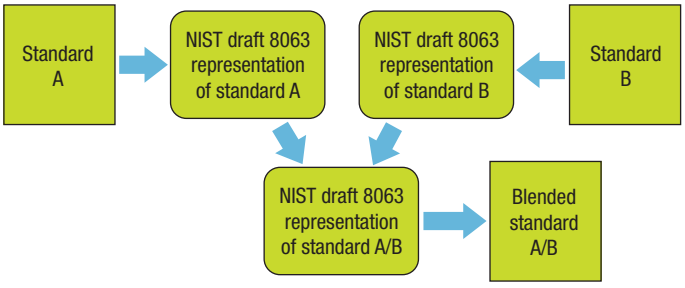

Figure 1. An intermediate representation for standards blending. The primitives and elements of the draft National Institute of Standards and Technology (NIST) Interagency Report 8063 can be extracted from standards A and B, reconciled into an intermediate representation, and then translated into a blended standard, A/B.

In the IoT, especially for life-critical systems like disaster response, harmonious and blended standards are essential.

REFERENCES

1. C. Cosgrove-Sacks, "Open Protocols for an Open, Interoperable Internet of Things," Org. for Advancement of Structured Information Standards, 18 Feb. 2014; www.oasis-open.org/presentations/open-protocols-and-internet-of-things-oasis.ppt.
2. J.R. Lawson and R. Vettori, *Emergency Response Operations*, NIST NCSTAR 1-8, Nat'l Inst. Standards and Technology, 1 Dec. 2005; www.nist.gov/customcf/get_pdf.cfm?pub_id=101049.
3. T. Gao et al., "Vital Signs Monitoring and Patient Tracking over a Wireless Network," *27th Ann. IEEE Conf. Engineering in Medicine and Biology Society* (EMBS 05), 2006, pp. 102–105.
4. K. Lorincz et al., "Sensor Networks for Emergency Response: Challenges and Opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, 2004, pp. 16–23.
5. A.F. Martins et al., "IEEE 11073 and Connected Health: Preparing Personal Health Devices for the Internet," *IEEE Int'l Conf. Consumer Electronics* (ICCE 14), 2014, pp. 274–275.
6. K. Tassin, "LTE and the Internet of Things," 3GPP, 2016; www.3gpp.org/news-events/3gpp-news/1607-iot.
7. J. Voas, "Draft: Primitives and Elements of Internet of Things (IoT) Trustworthiness," NIST IR 8063, Nat'l Inst. Standards and Technology, 16 Feb. 2016; http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8063.
8. J.M. Voas and P.A. Laplante, "Standards Confusion and Harmonization," *Computer*, vol. 40, no. 7, 2007, pp. 94–96.

PHILLIP A. LAPLANTE is a professor of software engineering at the Pennsylvania State University. Contact him at plaplante@psu.edu.

JEFFREY VOAS is a cofounder of Cigital and *Computer's* Cybertrust column editor. He's an IEEE Fellow. Contact him at jeffrey.m.voas@gmail.com.

NANCY LAPLANTE is an associate professor of nursing at Widener University. Contact her at nllaplante@mail.widener.edu.

Selected CS articles and columns are also available for free at **http://ComputingNow.computer.org**.