Standards for Things

OMG Standards in the Age of the Industrial Internet of Things

Julie Pike

September 24, 2014

The Object Management Group® (OMG®) – an international, not-for-profit, technology standards consortium – has been working on Industrial Internet of Things standards long before the "Internet of Things" became an industry buzzword. This paper outlines these various standardization efforts.

Introduction

The world is quickly becoming a small place thanks to technology. In the past few years, the pace of change has become even more rapid due to the emergence of a technological phenomenon known as the "Internet of Things" ("IoT"). IoT is the convergence of machine and intelligent data – enabled by cheap computing, universal connectivity, and better real-time, predictive analytics. These connected devices are allowing smart machines and systems to perform functions that were simply not possible before.

When talking about IoT connected devices, many people think about self-driving cars that connect with the road to communicate upcoming traffic or refrigerators that send notifications to your smartphone when you're running low on a particular grocery staple. But the possibilities of the IoT go much deeper than that. Think about airplanes that can alert ground crew about upcoming maintenance requirements *and* have already scheduled the delivery of needed parts. Or perhaps homebound patient monitoring systems that connect directly to the hospital so doctors can monitor patients' health. This particular subset of the IoT is known as the Industrial Internet. Think of it as the Internet Revolution finally impacting the Industrial Revolution. According to a report by General Electric, roughly 46% of the global economy ($32.3 trillion in global output) can benefit from the Industrial Internet.[1]

In March 2014, OMG® announced it would be managing the Industrial Internet Consortium™ (IIC). The IIC is an open membership organization formed to catalyze and coordinate the priorities and enabling technologies of the Industrial Internet. While not a standards organization, the IIC works with numerous standard organizations – including the OMG, of course, and many others. IIC testbeds are focused on discovering and taking advantage of disruptive new products and services, though requirements and priorities for new standards will also spin off of these efforts – and no organization is better placed to manage standardization in that space than the OMG itself.

In fact, OMG has been active in Industrial Internet of Things standardization efforts long before the IIC's founding. In this paper, we will discuss the different standards and standardization activities that the OMG already has in place that address the IoT. We'll discuss these few examples, but do keep in mind that the real action in the Industrial Internet is, and will be, capturing the semantics of industrial systems so that you can fulfill the Industrial Internet pattern: integrate thousands of sensors, perform real-time, predictive analytics on that data, and deliver visualization and decision support to policymakers.

1. Data Distribution Service (DDS)
2. Threat Modeling
3. Structured Assurance Case Metamodel
4. Unified Component Model

[1] Annunziata, Marco and Evans, Peter C., *Industrial Internet: Pushing the Boundaries of Minds and Machines,* General Electric (GE), 2012. http://www.ge.com/docs/chapters/Industrial_Internet.pdf

5. Dependability Assurance Framework For Safety-Sensitive Consumer Devices
6. Automated Source Code CWE-SANS Top 25-Based Security Measure
7. Oil and Gas Risk Management

Data Distribution Service (DDS)

OMG's Data Distribution Service (DDS) standard is a protocol for the IoT. Already, the standard has been widely deployed in hundreds of IoT application domains, including Industrial Control, Healthcare, Aerospace, Telecommunications, Defense, Energy, Smart Cities, and Transportation. DDS and its predecessor specifications power the connectivity of literally billions of devices worldwide.

DDS enables network interoperability for connected machines, enterprise systems and mobile devices. It provides scalability, performance, and Quality of Service that is required to support IoT applications. DDS can be deployed in platforms ranging from low-footprint devices to the Cloud and supports efficient bandwidth usage as well as agile orchestration of system components. It provides a global data space for analytics and enables flexible IoT real-time system integration.

Threat Modeling

Ever since the IoT was first established, critics' concerns have centered on the security issues of devices connecting with and having access to information from other devices. Without stringent measures in place, hackers can easily delve into personal information, including an individual's bank account and credit card information, where they are currently located, and when their home is empty (and how to get past any home security systems). The possibility for attack through the IoT is alarming.

For the past year, the OMG Systems Assurance Task Force has been working on a standard for threat information sharing (or "threat modeling"). This enables system engineers and architects to build systems-of-systems that implement and leverage the capabilities to share threats and security attacks across different devices, IT systems, and standards.

With first results expected in 2015, this effort is already key to creating trustworthy, secure IoT systems with appropriate protection of privacy. Although the effort is led by commercial concerns dependent on highly-secure financial systems, there are already significant contributions from national government bodies, especially in the intelligence field.

Structured Assurance Case Metamodel

The different devices and networking capabilities making up the IoT and related concepts are manufactured by thousands of companies – all with different standards on safety, integrity, reliability, privacy and security properties and behaviors. One device in an exchange may have

strict safety and integrity measures while the other's requirements and assumed behavior may be more lax in comparison. In addition, when a new IoT-like capability enters the marketplace, the manufacturers will need to prove that their offering is as secure, safe, resilient, and trustable as they claim to avoid any product recalls, integration disasters, or media fallout.

The OMG Structured Assurance Case Metamodel defines a way for assurance tools to create and exchange sets of "assurance cases" with auditable claims, arguments, and the supporting evidence about a system or service's attributes like safety, security, reliability, integrity, or the ability to adhere to privacy requirements. This standard ensures that end users in manufacturing, healthcare, transportation, and related industries are not only making good investments in their individual devices and networking options – but a good investment in their IoT-like capabilities as a whole.

The Unified Component Model for Distributed, Real-Time and Embedded Systems

Component-based systems engineering has proven to be a key enabler of software reuse and reduced time to market for Software Intensive products. One adopted OMG standard is the CORBA Component Model (CCM), which was designed to support Information Systems using OMG's CORBA standard (used worldwide in hundreds of thousands of devices). Since its adoption, CCM has evolved to support domains beyond CORBA. For example, Lightweight CCM (LwCCM) was designed to support domains with more stringent real-time requirements and resource constraints. However, IoT systems need more than what LwCCM can provide; they need component models that aren't tied to a specific type of middleware, but can be used with multiple middleware standards offering different communication models, quality of service guarantees, and memory footprints. IoT systems need a simple, lightweight, middleware-agnostic, and flexible component model.

In 2013, OMG issued a Request for Proposal for a Unified Component Model for Distributed, Real-Time and Embedded Systems (UCM for DRE) that will be independent from and compatible with any communication middleware. UCM for DRE will support allow many different interaction models, including publish-subscribe and request-reply. Doing so will permit the use of multiple protocols in a single system to provide communications – or the use of only one without requiring the memory footprint of the others.

Dependability Assurance Framework for Safety-Sensitive Consumer Devices

"Consumer devices" is a newly coined term which refers to a new category of industrial products used by end users including automobiles, service robots, consumer electronics, and smart houses. Unlike traditional industrial machineries, consumer devices are used in diverse, open and dynamic environments. Furthermore, as accountability of manufacturing companies becomes more and more crucial, they need to assure that their products are dependable whenever required during the development and operational phases.

The Request for Proposal (RFP) for the Dependability Assurance Framework for Safety-Sensitive Consumer Devices proposes a process model of simultaneous development of embedded control software and dependability cases. In the process, control software and the dependability case are simultaneously refined and updated.

The most notable place where the Dependability Assurance Framework will be seen is in automobiles where the standard will ensure that vehicles do not crash into other vehicles, pedestrians, buildings, etc. With the IoT, automotive is transforming itself from a personal vehicle to a terminal of the Internet so that any information from an automobile or the Internet can be transmitted to each other for more convenience. No longer are automobiles' sole purpose to carry people from place to place – they will now carry *information*.

Automated Source Code CWE-SANS Top 25-Based Security Measure

According to the Common Weakness Enumeration (CWE) – a cybersecurity community repository – there are over 800 known weaknesses in software that can be exploited by attackers to make your software do things you didn't intend and could damage your organization. With such an overwhelming number of ways software can be attacked, it can be a daunting task for developers to protect and review for all weaknesses in a new system.

The Automated Source Code CWE-SANS Top 25-Based Security Measure (Top 25 CWEs) defines a method for automating the measurement of an application's security posture regarding violations of secure architectural and coding practice in source code with the violations being drawn from the CWE repository. The specification was developed from the CWE/SANS Institute Top 25 most commonly exploited weakness, 19 of which can be detected in source code.

This standard is part of a suite of specifications that the Consortium for IT Software Quality (CISQ) – an independent IT industry leadership group – is developing with OMG to automate measuring software source code quality characteristics. Not only can these measures be used by IT organizations, IT service providers, and software vendors, but they can also be applied to the software of the systems in the Industrial Internet. With the adoption of the Top 25 CWEs, Industrial Internet and IoT software developers will be able to check against commonly exploited weaknesses before products go to market thus ensuring their product's integrity, resilience, and safety for the marketplace.

Oil and Gas Risk Management

Nowadays, Oil and Gas exploration and production are both domains in which large amounts of instrumentation are used to continuously report back on the conditions of the oil well:

- During seismic surveys, tens of thousands of geophones or hydrophones capture acoustic signals as well as accurately report their exact position

- During drilling, information about what's happening near the drill bit (including the vibration, rotation, inclination, and many other parameters) is continuously recorded as part of "measurement while drilling" (MWD) or "logging while drilling" (LWD) operations.
- During production, sensors embedded in the production casing in electrosubmersible pumps or in the well-head equipment report pressures, temperatures, flow rates, pump motor speeds and vibrations, and more.

There are two main purposes to monitoring this information. If everything in the process is going as it should, the main purpose of monitoring is to optimize operations – drilling faster and more accurately, replacing the drill when it is absolutely necessary, and optimizing reservoir production. However, there is also a key safety imperative: many of these same measurements can be used to predict and prevent failures or generate alarms for – what the industry calls – "process safety events" – instances where deviations from the intended course of events portends a potential incident or accident.

In recent years, the concept of remote monitoring of operations has also been extended to the surveillance of unmanned production platforms, including oil spill detection, and to the visual monitoring of pipelines over distances of hundreds of miles, in order to detect not only accidental leaks, but also acts of sabotage or theft in real-time.

This network of sensors and actuators, and the analytics that interpret the data and enable smart decisions, predate the emergence of the IoT, but it nevertheless constitutes a very important example of a network of connected devices that interact with a very real and sometimes hostile physical world.

Conclusion

Though the emergence of the Internet of Things is a fairly recent technological shift, OMG has consistently been at the forefront of the movement with IoT-related standardization activities stretching back to the early 2000s. And with the addition of managing the Industrial Internet Consortium, OMG is taking a front row seat to the development of testbeds and use cases for the IoT.

For more information on IoT standards that OMG is working on, visit www.omg.org. To learn more about the OMG-managed Industrial Internet Consortium, visit www.iiconsortium.org.

Acknowledgements

The author would like to thank the following OMG members and supporters for their expertise on the various standardization efforts discussed in this paper. In particular, we extend our sincerest gratitude to Claude Baudoin, Gerald Beuchelt, Laura Clark, Naoya Ishizaki, Robert Martin, and Virginie Watine.

About OMG

Celebrating its 25th anniversary in 2014, the Object Management Group® (OMG®) is an international, open membership, not-for-profit technology standards consortium. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. OMG's modeling standards enable powerful visual design, execution and maintenance of software and other processes. Visit www.omg.org for more information.