Software Engineering for the Internet of Things

Xabier Larrucea, Tecnalia

Annie Combelles, inspearit

John Favaro, Intecs

Kunal Taneja, Google

0740-7459/17/$33.00 © 2017 IEEE

AKIN TO the mania of 1849 in the hills of California, we're witnessing a software developer's gold rush around the Internet of Things (IoT). Neither research nor industry (for example, HP[1] and IBM[2]) is immune to the fever. On one hand, researchers have been concentrating on aspects such as standardizing communication protocols[3] or even securing end-to-end communication.[4] On the other hand, reports from the gold fields are bringing disquieting news. An International Data Corporation (IDC) survey reported that 31.4 percent of the surveyed organizations had launched IoT solutions.[5] However a DZone survey reported that 87 percent of the surveyed developers were either unconcerned or only somewhat concerned about the new IoT paradigm.[6]

To understand the IoT's challenges and opportunities, *MIT Sloan Management Review* recently surveyed business executives, managers, and IT professionals from organizations around the world.[7] The data collected indicated several economic and technical issues to consider, such as these:

- *Customer satisfaction.* Managing networks of connected devices is influencing relationships between an organization, its customers, and suppliers in several ways. With connected devices, organizations can create and satisfy customer needs, including better quality.[8]
- *Organizational aspects.* Given the complexities of adding sensors and sensor data to a company's mix of products and operational processes, many organizations need additional expertise to take advantage of IoT projects, including expertise in data analytics and data security.
- *Variable costs.* Unlike in traditional IT projects, in which variable costs are extremely low, each additional device might bring considerable ongoing maintenance costs. The IoT is an actual network of real physical things that can grow unexpectedly.
- *Social implications.* It's still far from clear how people will react to IoT devices' growing presence. People will become more conscious of how the data they generate is used. Also, IDC's senior vice president and chief analyst Frank Gens predicted that by 2018, two-thirds of IoT networks will have a security breach.[9]

Confronted by the wildly diverse and unfamiliar systems of the IoT, many developers are finding themselves unprepared for the challenge. No consolidated set of software engineering best practices for the IoT has emerged. Too often, the landscape resembles the Wild West, with unprepared programmers putting together IoT systems in ad hoc fashion and throwing them out into the market, often poorly tested. Also, the academic sector is in danger of fragmenting into specialized, often unrelated research areas.

The industry needs guidance to engineer the new generation of scalable, highly reactive, often resource-constrained software systems characteristic of the IoT. Many of these systems are in mission-critical sectors such as medicine, industrial automation, and energy management.

Something Old, Something New

The term "IoT" embraces a variety of technologies and has been applied in several domains for different purposes. (For a comparison of IoT systems with cyber-physical systems, see the sidebar.) For example, researchers have proposed debugging approaches for IoT systems from an architectural viewpoint.[10] Companies sense that a new set of best practices is necessary but are unsure where to look for them. Some think that agile processes could help. For example, Michel Genard, Wind River's vice president and general manager of system simulation, said that developing IoT systems implies "new development processes," and that "embedded developers must increasingly adopt agile and continuous practices."[11]

However, more traditional research or techniques have much to offer. In a discussion of IoT research directions, John Stankovic described a situation in which two independently installed services in a single infrastructure (for example, light therapy for depression and an energy-saving motion detector in a smart home) could interfere with each other's functionality.[12] Veteran telecom software engineers recognize this as the feature interaction problem they've been working on for decades; they can draw inspiration from the body of research already available.

In short, past software engineering techniques can be harnessed and adapted to the challenges of today's IoT. Nevertheless, new approaches to standard software engineering techniques are also needed—for example, rethinking configuration management in the context of the extremely dynamic, continuously reconfiguring systems that are characteristic of the IoT.

A new generation of development environments is needed for software engineering for the IoT. One of the most exciting trends is development environments in the cloud—not for the cloud, but in the cloud—to enable the massively scalable verification and validation techniques (including simulation) that will be needed for most large mission-critical systems in the IoT. Some technology providers are now offering platforms that let software engineers quickly assemble systems that interact with sophisticated sensor devices yet preserve important system-level properties.

Most of all, we need to train the new generation of IoT software developers. We can't simply unleash them to develop IoT applications in an uncontrolled fashion and possibly endanger lives. The *IEEE Software* community, with its deep collective knowledge of both past and present practices, is uniquely positioned to lead the way and avoid costly reinvention of the wheel. This theme issue represents a step toward creating a core set of best practices that will guide the industry through the challenges of software engineering for the IoT.

In This Theme Issue

In "Model-Based Software Engineering to Tame the IoT Jungle," Bruce Morin, Nicolas Harrand, and Franck Fleurey discuss how to deal with distribution across heterogeneous nodes, how to deal with decentralized computing power, and how to build applications from an opportunistic viewpoint. They outline ThingsML, a modeling language that provides mechanisms to easily share variables among things and to link calls and callbacks. The authors also present an example of using ThingsML with the JavaScript Z-Wave library and report on their experience developing an e-health fall detection system.

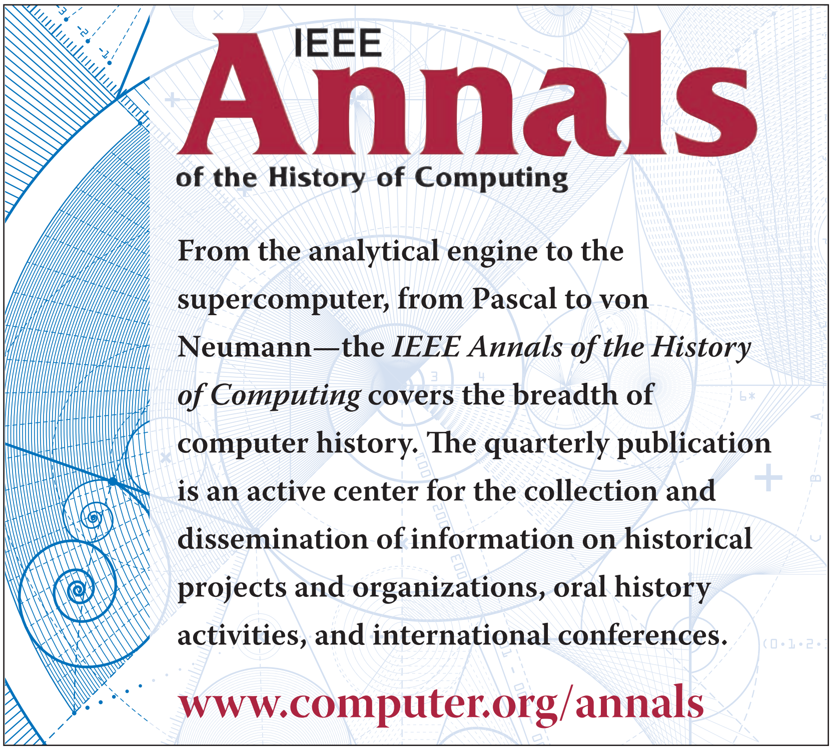
In "Key Abstractions for IoT-Oriented Software Engineering," Franco Zambonelli identifies key abstractions in IoT engineering that can represent a first small step toward a general disciplined approach for engineering IoT systems. Zambonelli highlights the stakeholders involved, the requirements involved, and avatars and coalitions, which abstract objects, places, and participants.

In "Model-Driven Engineering for Mission-Critical IoT Systems," Federico Ciccozzi and his colleagues discuss the technological challenges of IoT for critical systems. They propose model-driven engineering as a methodology to better support these technologies' adoption.

In this realm of diverse technologies, interoperability is critical. In "Enabling IoT Ecosystems through Platform Interoperability," Arne Bröring and his colleagues offer an architectural model for IoT ecosystems and highlight five common interoperability patterns.

In "Scalable Application Design for the IoT," Jaggannathan Venkatesh and his colleagues analyze the accuracy, complexity, and scalability of a modular approach to context-aware IoT applications. They provide a detailed comparison of their approach to the state of the art in a case study of four types of smart homes.

Finally, in "A Roadmap to the Programmable World: Software Challenges in the IoT Era," Antero Taivalsaari and Tommi Mikkonen distill their experience into an IoT system roadmap. They describe an emerging common end-to-end IoT architecture and predict the state of IoT systems in 2020 and 2025, from the data and programmability viewpoints. Only time will show whether they're right.



THE INTERNET OF THINGS AND CYBER-PHYSICAL SYSTEMS

Robert Minerva, the current director of the IEEE Internet of Things (IoT) Initiative, defines the IoT as

> made out of networked sensors and smart objects whose purpose is to measure/control/operate on an environment in such a way to make it intelligent, usable, and programmable and capable of providing useful services to humans.[1]

NIST defines cyber-physical systems (CPSs) or “smart” systems as “co-engineered interacting networks of physical and computational components.”[2] CPS technologies include

- the IoT,
- the Industrial Internet,
- smart cities,
- smart grids, and
- “smart” anything (for example, cars, buildings, homes, manufacturing, hospitals, and appliances).

We recognize a blurry separation between the IoT and CPSs. But by “IoT,” we include those situations in which smart objects or things interact with their environment intelligently and provide value to stakeholders or customers. So, all these aspects should be taken into account from a software engineering perspective. “CPS” is a more general term, as defined by University of California, Berkeley researchers.[3]

The European Commission’s CyPhERS (Cyber-physical European Roadmap and Strategy; www.cyphers.eu/project) project has been investigating the relationship between CPSs and IoT systems. Some techniques developed for CPSs can be the source of best practices for software engineering for the IoT. However, some factors, such as dynamicity and reliability, still require attention. In this sense, IoT systems tend to be extremely dynamic, where different devices can be added or removed in a specific IoT ecosystem during runtime while maintaining reliable communications.

References

1. R. Minerva, “IoT and Its Challenges”; http://iot.ieee.org/images/files/pdf/iot_and_its_challenges_roberto_minerva.pdf.
2. “Cyber-physical Systems,” NIST; www.nist.gov/cps.
3. “Cyber-physical Systems”; cyberphysicalsystems.org.

The articles we’ve selected for this theme issue illustrate only some of the many concerns that software engineering for the IoT must address. A further example is cybersecurity, and the stakes are high: in October 2016, the Internet was subjected for the first time to a massive distributed denial-of-service attack by an army of infected IoT devices.[13] The attack provided ample evidence that the IoT will bring not only enormous opportunities but also enormous challenges. It’s up to the software community to equip itself to face these challenges.

References

1. *Internet of Things Research Study: 2015 Report*, Hewlett Packard Enterprise, 2015; www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.
2. “Watson Internet of Things,” IBM, 2016; www.ibm.com/internet-of-things.
3. S.N. Han et al., “Service Composition for IP Smart Object Using Realtime Web Protocols: Concept and Research Challenges,” *Computer Standards & Interfaces*, Jan. 2016, pp. 79–90.
4. H.-C. Chen et al., “A Security Gateway Application for End-to-End M2M Communications,” *Computer Standards & Interfaces*, Feb. 2016, pp. 85–93.
5. “IDC’s 2016 Global IoT Decision Maker Survey Finds Organizations

ABOUT THE AUTHORS

XABIER LARRUCEA is a senior project leader (PMP) and research scientist at Tecnalia and a part-time lecturer in information systems and quality assurance at the University of the Basque Country. His research interests include safety-critical software systems, software quality assurance, software process improvement, empirical software engineering, and metamodeling technology strategy. Larrucea received a PhD in software engineering from Universidad del País Vasco and an Executive MBA from the ESIC Business and Marketing School. He's an IEEE senior member and a member of the *IEEE Software* initiatives team. Contact him at xabier.larrucea@tecnalia.com.

ANNIE COMBELLES is the president and founder of the advisory company inspearit. Her research interests are software quality, agile methods, value-added agile management, and customer experience. Combelles received an engineering master's from Ecole Nationale Supérieure de l'Aéronautique et de l'Espace and an Executive MBA from Hautes Etudes Commerciales Management. She received the 1980 Aerospace and Aeronautics medal for Innovation in France. Combelles has served on the *IEEE Software* editorial board and industry advisory board. Contact her at annie.combelles@inspearit.com.

JOHN FAVARO is a senior consultant at Intecs in Pisa. His research interests include intelligent transportation systems, cybersecurity, and functional safety for mission-critical software systems. Favaro received an MSc in computer science from the University of California, Berkeley. He's a member of the *IEEE Software* editorial board. Contact him at john.favaro@intecs.it.

KUNAL TANEJA is a software engineer at Google. Previously, he was a researcher in Accenture Technology Labs' Internet of Things (IoT) Group, focusing on architecting scalable IoT platforms. Taneja received a PhD in computer science from North Carolina State University. Contact him at kunalltaneja@google.com.

Moving past Pilot Projects and toward Scalable Deployments," Int'l Data Corp., 2016; www.idc.com/getdoc.jsp?containerId=prUS41788916.

6. *The DZone Guide to the Internet of Things*, DZone, 2015; dzone.com/guides/internet-of-things-1.
7. S. Jernigan, S. Ransbotham, and D. Kiron, "Data Sharing and Analytics Drive Success with IoT," *MIT Sloan Management Rev.*, 8 Sept. 2016; sloanreview.mit.edu/projects/data-sharing-and-analytics-drive-success-with-internet-of-things.
8. R. Hackbarth et al., "Improving Software Quality as Customers Perceive It," *IEEE Software*, vol. 33, no. 4, 2016, pp. 40–45.
9. C. Wong, "IDC's 2016 Predictions: IoT Headed for Huge Growth (and Security Headaches)," *itbusiness.ca*, 5 Nov. 2015; www.itbusiness.ca/news/idcs-2016-predictions-iot-headed-for-huge-growth-and-security-headaches/60954.
10. P. Eugster, V. Sundaram, and X. Zhang, "Debugging the Internet of Things: The Case of Wireless Sensor Networks," *IEEE Software*, vol. 32, no. 1, 2015, pp. 38–49.
11. "Wind River Simics Advances Agile Practices for IoT Development," Wind River, 30 June 2015; www.windriver.com/news/press/pr.html?ID=13829.
12. J.A. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things J.*, vol. 1, no. 1, 2014, pp. 3–9.
13. D. Sanger and N. Perlroth, "A New Era of Internet Attacks Powered by Everyday Devices," *New York Times*, 22 Oct. 2016.

See www.computer.org/software-multimedia for multimedia content related to this article.