Control Systems and the Internet of Things

Buzzwords are the drumbeat of technological progress. Casting an eye back over the last couple of decades in control, we are reminded of "hot topics" such as hybrid systems, embedded systems, cyberphysical systems (CPS), and systems of systems. The currency of some of our past buzzwords and catchphrases may have undergone devaluation, but others have maintained their mind share. Perhaps the lesson is to not always dismiss the hype.

In a field as mature as systems and control, most new developments are incremental—variations on well-honed themes and tweaks on established results. Transformative developments are infrequent, and when they occur they are not likely to be autogenic. The topics mentioned above are all multidisciplinary, requiring linkages with other disciplines, especially computer science, communications, and information technology. Control scientists and engineers have benefited from engaging with colleagues in other fields. Our tools and expertise have helped solve outstanding problems, control groups in industry and academia have been well funded for R&D explorations, and we have seen continuing growth in control journals and conferences. Control—as a discipline and as a community—is all the richer for having embraced multidisciplinary initiatives.

New things, or at least new buzzwords, are always coming up, of course. The buzz today is about the *Internet of Things* or IoT; for the last two years IoT has been at the peak of Gartner's "Hype Cycle for Emerging Technologies" [1]. I expect that many readers are working in or tracking developments in this area. Overlaps with other topics such as, and in particular, CPS are significant.

Digital Object Identifier 10.1109/MCS.2015.2495022
Date of publication: 19 January 2016

DEFINITIONS

What is the IoT anyway? All buzzwords resist crisp definition, but it may be helpful to review what a few sources have to say. To begin with, per *Wikipedia* [2]:

From an applications perspective, IoT solutions are being conceived of and implemented across the spectrum: homes and buildings, industrial plants, automotive and other vehicles, health care, and infrastructures.

> The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy, and economic benefit. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

I thought I would also share the following, from the global consulting company McKinsey [3]:

> In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What's revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention.

Finally, IEEE is also attempting to define the term. The IEEE IoT initiative published a white paper that discusses what IoT is as well as several definitions [4]. Rather than encapsulate the concept in one definition, though, separate definitions are offered based on the complexity of the implementation. First, for "low-complexity systems:"

> An IoT is a network that connects uniquely identifiable "Things" to the Internet. The "Things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "Thing" can be collected and the state of the "Thing" can be changed from anywhere, anytime, by anything.

This is extended to a "large-environment scenario":

> IoT envisions a self-configuring, adaptive, complex network that interconnects "things" to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature, and are uniquely identifiable. The representation contains information, including the thing's identity; status; location; or any other business, social, or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.

These definitions focus on technology. From an applications perspective, IoT solutions are being conceived of and implemented across the spectrum: homes and buildings, industrial plants, automotive and other vehicles, health care, and infrastructures—prominent examples of the last include smart grids, smart cities, and intelligent transportation systems. The motivating considerations in these and other domains are energy efficiency and productivity, safety and security, and comfort and convenience.

THE ROLE AND RELEVANCE OF CONTROL

In this "first wave" of IoT, attention has concentrated on wireless sensors, cloud connectivity, big data analytics, and mobile apps. As is evident from the definitions above, however, the vision of IoT extends to closed-loop control. Sensors connect through algorithms to actuators, with communication over the Internet. As noted above, the things of IoT "offer services, with or without human intervention, through the exploitation of . . . actuation capability."

These definitions are from the perspective of information and communication technologies (ICT), but closed-loop control in any context is not just, or primarily, an ICT challenge. Deep understanding of dynamics and control is essential. Feedback can qualitatively change the behavior of a dynamical system, for better or worse. A seemingly benign system can become unstable if feedback is inappropriately applied, and, on the other hand, automatic feedback control can enable unstable systems to reach levels of performance unattainable by stable systems. The closed-loop integration of physical systems with the Internet will require close collaboration of control experts with ICT experts.

TOPICS FOR CONTROL RESEARCH

Furthermore, IoT promises new vistas for the control research community. The fact that aircraft, cars, refineries, buildings, and medical devices function as well as they do is testament to the power and maturity of control science and engineering. But it's worth noting a few assumptions on which this success rests. The communication networks in control systems are generally assumed to be deterministic and reliable. Real-time operating-system platforms rely on predetermined, static schedules for computation and communication. Some control is now occurring over the Internet, but at a supervisory level—for power-grid distribution stations, wastewater treatment plants, some commercial buildings, and other applications. Closed-loop automation, more often than not, requires a dedicated, onsite end-to-end control system.

Control in the IoT imposes control-theoretic challenges that we are unlikely to encounter in our usual application domains. More research is needed in many areas, including [5]:

- *Control over nondeterministic networks*. Today's control systems assume deterministic communication and computation—in fact the execution and communication infrastructure is rigorously designed to ensure determinism. Nondeterminism—for example, unpredictability in sensor reading, packet delivery, or processing time—complicates closed-loop performance and stability.
- *Latency and jitter*. Control over the Internet and clouds will require much greater attention to latency (the end-to-end delay from sensor reading to actuation) and jitter (the variance in the intersampling interval). The techniques used in control applications today to deal with these phenomena are unlikely to suffice.
- *Bandwidth*. Many control applications are not demanding of communication bandwidth—a few sensor reads and actuator outputs a second can suffice. But even this level of network performance may not be assured with mobile and/or Internet connectivity. Furthermore, in the IoT, closed-loop control with feedback of video and other high-dimensional data is envisaged. The sophisticated signal- and image-processing algorithms involved will best be run on cloud platforms and will stress available bandwidth.
- *Cyber- and physical security, and resilience*. The physics of the "things" in IoT, if appropriately incorporated, can enhance detection and protection approaches for both cyber- and physical security. Conversely, physics and feedback can open the door to new attack scenarios: for example, a well-performing control system may be rendered unstable by introducing small delays in communication pathways.
- *Interoperable and plug-and-play sensors, models, and algorithms*. With current digital devices and platforms we have become accustomed to features such as auto-discovery, search, composition of services, and plug-and-play integration. These are not as yet available for control applications. To get there, interoperability will need to extend beyond the interface specification; "dynamic" compatibilities will also be critical.

Control in the IoT imposes control-theoretic challenges that we are unlikely to encounter in our usual application domains.

ISN'T THIS JUST CPS?

This is a question that will have occurred to the informed reader. Indeed, here's how a brief on CPS from the U.S. National Institute of Standards and Technology begins [6]:

> Cyber-physical systems (also referred to as the Internet of Things) feature a tight integration between the physical elements and the computational elements of a system.

This overstates the linkage, though. Not all CPS are IoT systems, but CPS can also rely on IoT. For a discussion of differences see Section 5.1 of [4]. Here is an example mentioned in [4]:

> For example, many wireless sensor networks monitor some aspect of the environment and relay the processed information to a central node so that the central node can make decisions with more reliable data collected from numerous distributed sources.

There's no question that such networks are CPS, but, in the absence of an Internet connection, there is no question that they are not IoT systems.

A more pragmatic distinction is that the CPS term has been embraced by the research community but has gained little traction in industry. IoT has been widely adopted by and is being promoted by industry. I know, or know of, a few people in major companies who have IoT in their title, but I haven't encountered a "VP of CPS" as yet!

Indicative of the industry interest is the establishment and growth of the Industrial Internet Consortium (http://iiconsortium.org). The IIC was formed in 2013 by five founding members: AT&T, Cisco, GE, IBM, and Intel. Membership has now grown to over 200 companies, including several major suppliers of control systems, tools, and equipment: ABB, Bosch, Honeywell, Mitsubishi Electric, National Instruments, Schneider Electric, and Siemens. Several universities and government organizations are also involved.

The "many faces of control" are well prepared to serve on multidisciplinary teams to develop a better understanding of these issues.

CONCLUSION

I hope this column has convinced readers of three things: that IoT is more than a buzzword, that control expertise will be required to realize the visions of IoT that the promoters of the field are promising, and that IoT brings new and exciting opportunities for research and development in control science and engineering. To illustrate the last assertion, here are some prospects that can motivate our research [5]:

- Systems that are not physically connected or collocated could be coordinated in real time.
- Optimized performance (such as energy efficiency) could be achieved for small-scale systems that cannot afford dedicated control systems.
- High-fidelity models could be widely applied for real-time control via cloud-based implementations.
- Global networks of sensors and actuators could be implemented and coupled with sophisticated control and optimization algorithms.
- Greater redundancy and fault tolerance could be achieved across critical infrastructures.

IEEE has launched an IoT initiative (http://iot.ieee.org), supported by several IEEE Societies including the IEEE Control Systems Society (CSS). All IEEE Members can join the IEEE IoT Technical Community and subscribe to the free IoT newsletter published by IEEE IoT. The CSS engagement is through the Technical Committee (TC) on Networks and Communications (http://networks-and-communications.ieeecss.org/). The TC chair, Daniel Quevedo, is a member of the IEEE IoT Steering Committee (as am I). Readers interested in being involved in control systems and the IoT are encouraged to participate in the TC.

ACKNOWLEDGMENTS

My thanks to Jonathan How, Kirsten Morris, and Daniel Quevedo for their comments and encouragement.

REFERENCES

[1] Gartner. (2015, Oct. 2). Gartner's 2015 Hype Cycle for Emerging Technologies identifies the computing innovations that organizations should monitor. [Online]. Available: http://www.gartner.com/newsroom/id/3114217

[2] (2015, Sept. 22). Wikipedia, Internet of things. [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_Things

[3] M. Chui, M. Löffler, and R. Roberts. (2015, Sept. 23). The Internet of things. *McKinsey Quarterly*. [Online]. Available: http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things

[4] R. Minerva, A. Biru, and D. Rotondi. (2015, Sept. 23). Towards a definition of the Internet of things (IoT). [Online]. Available: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[5] T. Samad. (2015, Sept. 23). The Web of things and cyberphysical systems: Closing the loop. presented at W3C Workshop Web Things. Berlin. [Online]. Available: http://www.w3.org/2014/02/wot/papers/samad.pdf

[6] (2015, Sept. 23). National Institute of Standards and Technology. *Cyber Phys. Syst.* [Online]. Available: http://www.nist.gov/itl/ssd/cyber-physical-systems.cfm

Tariq Samad

» PRESIDENT'S MESSAGE

(continued from page 8)

naturally to control and systems approaches, including the production of sustainable energy, the implementation of affordable and effective health care, automated manufacturing, and the societal implications of the growing databases that live in the cloud. Some of the themes that link these seemingly disparate challenges are the reliance on "big data," the need for more effective sensors, requiring novel materials for hardware, and the characterization and management of uncertainty.

The "many faces of control" are well prepared to serve on multidisciplinary teams to develop a better understanding of these issues and, furthermore, to formulate and develop solutions for these challenging opportunities. I will return to this theme over the course of the year in this column, and I welcome comments from this community on novel classes of problem that are yielding to systems and control solutions.

REFERENCES

[1] (2015, Sept. 30). List of systems engineering universities. [Online]. Available: https://en.wikipedia.org/wiki/List_of_systems_engineering_universities

[2] INCOSE. (2015, Sept. 30). [Online]. Available: http://www.incose.org/Home

[3] F. Borrelli. (2015, Sept. 30). MPC course materials. [Online]. Available: http://www.mpc.berkeley.edu/mpc-course-material

Francis J. Doyle III