Imagineering an Internet of Anything

Irena Bojanova, *University of Maryland University College*
George Hurlburt, *STEMCorp*
Jeffrey Voas, *IEEE Fellow*

Today, the Internet of Things. Tomorrow, the Internet of Everything. Beyond that, perhaps, the Internet of Anything—a radically superconnected ecosystem where questions about security, trust, and control assume entirely new dimensions.

Increasingly, cyber-physical and cyber-biological systems function to interlink the cyber, physical, and biological worlds, creating what is currently called the Internet of Things (IoT). Every day, nearly a million new devices connect to the Internet, generating vast amounts of data—both device derived and input by people individually or through crowdsourcing the social networks on the Internet of Humans (IoH); http://mike2.openmethodology.org/blogs/information-development/2013/04/22/the-internet-of-humans.

As "things," or smart devices, add capabilities like context awareness, increased processing power, and energy-source independence, and as more people and new types of information are connected in a more relevant and valuable way, forecasters predict the advent of an Internet of Everything (IoE). Processes and data, in addition to things and people, will all be part of this greatly expanded paradigm. The recently proposed Industrial Internet (II) envisions an extension of the IoE.

From these concepts, we do some "imagineering"—a term associated with the Disney empire beginning in the 1950s, although it originated with Alcoa a decade earlier—to simultaneously "imagine" and "engineer" a further level of abstraction: the Internet of Anything (IoA). In the IoA, the imaginary isn't only about connecting new categories of things at exponential rates, but about envisioning a ubiquitous common software ecosystem, including an overarching "Internet Operating System" for which most engineering elements are already in place.

CYBER-PHYSICAL AND CYBER-BIOLOGICAL SYSTEMS

Cyber-physical systems (CPS) tightly interlink the cyber and physical worlds by integrating computational and physical processes, using sensors and actuators.[1] CPS are coordinated, distributed, and connected, and they must be robust and responsive. Examples include the smart grid, smart transportation, smart buildings, smart medical technologies, next-generation air-traffic management, and advanced manufacturing.[2]

Sensors or crowdsourcing applications generate data about the real world; that data is transferred into cyberspace, and cyberapplications and services use the data to interpret and affect the environment in real time, as shown in Figure 1.

Cyber-biological systems (CBS) add information to the

Published by the IEEE Computer Society

cybernetwork of things from the domain of living organisms. For example, marine animals in the oceans are tagged as network-connected sensors. DARPA has experimented with similarly connected sensors and possibly actuators that add insects to the grid. Implanted sensors in humans already allow physicians to remotely monitor patients' health via wireless devices; telemedical technologies have matured over several decades, so that human bodies are now cyber-integrated. Perhaps a patient, "enhanced" with an embedded insulin pump or a pacemaker or a neuro-connected prosthetic arm, could herself be considered a CBS.

The simple fact is many studies reveal that physical, biological, and cyber networks intertwine into vast, interconnected ecosystems best characterized as hypernets.

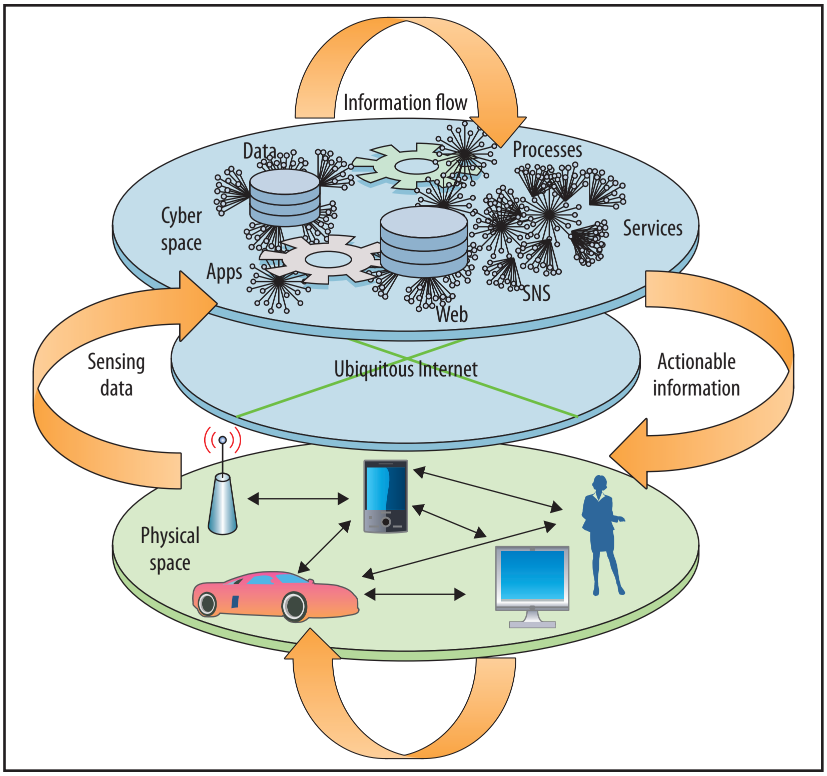

Figure 1. Information flow between the cyber and physical worlds. Data generated in the physical world is transferred to cyberspace for interpretation, which, in turn, affects the physical environment. (Source: E. Simmon et al., "A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems," NIST, Aug. 2013; www.nist.gov/customcf/get_pdf.cfm?pub_id=914023; used by permission.)

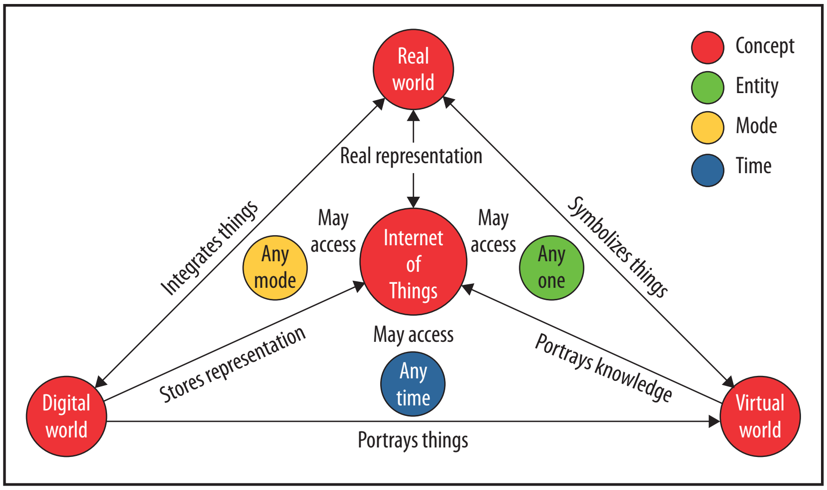

Figure 2. The Internet of Things: a conceptual view, integrating concepts, entities, modes, and time from the real, the digital, and the virtual worlds.

THE INTERNET OF THINGS

Mark Weiser envisioned the technology behind CPS in the early 1990s,[3] and as it has evolved the concept has been called ubiquitous computing, pervasive computing, ambient computing—and now the Internet of Things, a term RFID pioneer Kevin Ashton claims to have coined in 1999.[4]

The IoT is essentially a conglomeration of networked entities attached to sensors that can register and react to vibration, temperature, vital signs, liquidity, light, and much more. Gartner defines the IoT as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (www.gartner.com/it-glossary/internet-of-things). The European Research Cluster on the Internet of Things (IERC) defines it 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, use intelligent interfaces, and are seamlessly integrated into the information network" (www.internet-of-things-research.eu/about_iot.htm).

Figure 2 illustrates the IoT as we conceive it.

Innovations driven by advances in mobility, cloud computing, and big

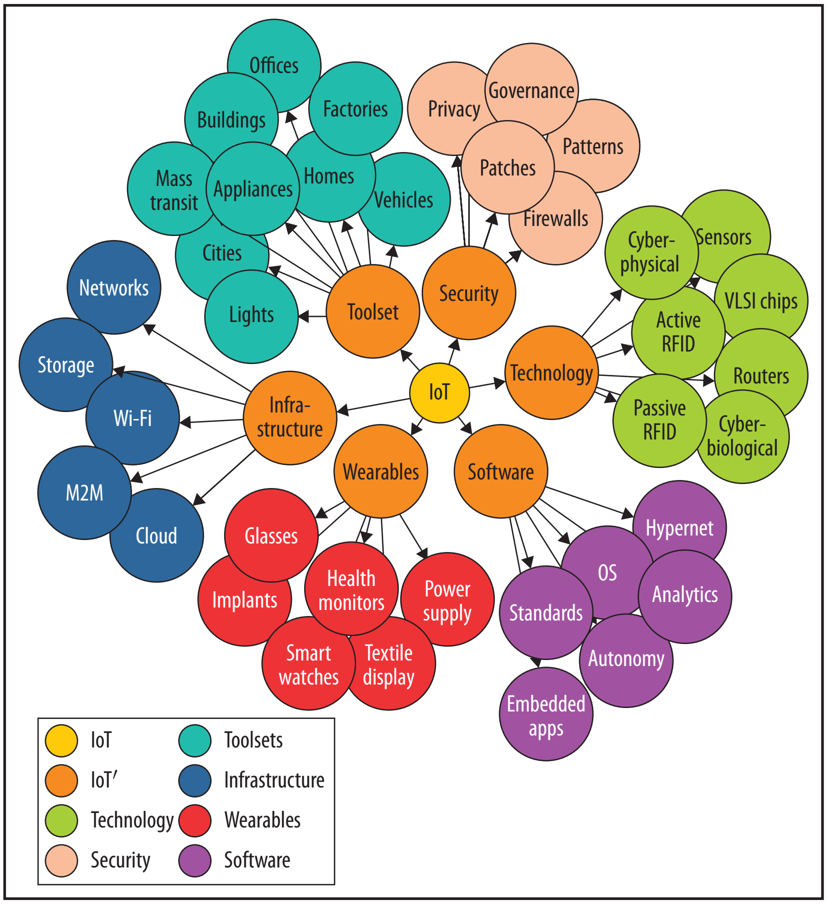

Figure 3. Conceptual rendering of the vast IoT ecosystem. We break down the IoT into six functional parts, comprising an intricately connected array of entities, systems, and units.

data analytics increase the number and kinds of networked connections, as well as the opportunities for people and machines to derive unprecedented value from these connections.[5] The basic tenets of the IoT may be summarized as follows:

- Things communicate.
- Things can sense.
- Things should be physical—for example, software shouldn't be considered a "thing."
- Communication is mostly wireless due to scaling and the natural limitations of wired infrastructures.
- On-board algorithms and software implementations own and control sensor I/O.
- Things are likely heterogeneous.

By 2020, it's predicted that between 30 billion and 50 billion objects will be connected to the Internet.[6] As we illustrate in Figure 3, the IoT ecosystem is vast.

THE INTERNET OF EVERYTHING AND THE INDUSTRIAL INTERNET

Almost as soon as the IoT had taken root conceptually, the idea morphed into the more broadly conceived Internet of Everything—a term first used in print by Dave Evans, chief futurist at Cisco, in 2012[7] and then reaching widespread popularity after the 2013 Gartner Symposium/ITxpo.[8]

Cisco's marketing materials describe the IoE as "bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before—turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries" (http://share.cisco.com/IoESocialWhitepaper/#/0/2).

Closely related to the IoE, but another level up in abstraction, is the Industrial Internet (II), the brainchild of the Industrial Internet Consortium (IIC) founded by AT&T, Cisco, IBM, and Intel earlier this year. The II is the vehicle through which "technology leaders drive industry ecosystem[s] to accelerate more reliable access to big data to unlock business value" (www.iiconsortium.org/press-room/03-27-14.htm). The goal of the IIC is to assure open interoperability standards and common architectures for connecting smart devices, machines, people, processes, and data.

In his recent president's column for IEEE's *The Institute* titled "Coming Next: The Internet of Everything," IEEE President and CEO J. Roberto Boisson de Marca envisions "a complex, self-configuring, and adaptive system of networks of sensors and smart objects whose purpose is to connect all things, including commonplace and industrial objects."[9] By extension, this concept has much in common with the emerging idea of hypernetworks—all-encompassing nonlinear ecosystems in which discrete, nonlinear networks federate to produce a veritable network of networks.

THE INTERNET OF ANYTHING

The IoE, as well as the II, fundamentally inhibit managing big data, as their contextual basis lacks ontological reference: "everything" implies whatever already exists, whatever is already known, whatever "is" according to business interests.

The "anything" of the IoA, however, implies not only whatever is known, but also whatever can possibly be *imagined* as part of the networked or connected ecosystem. The IoA envisions an overarching Internet operating system—a common software ecosystem capable of accommodating any and all sensor inputs, system states, operating conditions, and data contexts. It will be an exceedingly reliable, highly scalable, widely distributed (and fragmented), and eminently adaptive universal environment, sensitive to data in context.

The components for such architecture are already emerging: flash memory, persistent magnetic disk, NoSQL, Sync, mobile and wearable computing, Hadoop, object storage, virtual computing, cloud computing, software-defined networks, and converged infrastructure abstractions.[10]

Based on a statistically controlled interaction among many diverse software networks, this ecosystem would have to work within carefully tailored parameter-bound patterns, intentionally designed to prevent failure, maintain security, and optimize flow. While "everything" subtly suggests business as usual—merely at a larger scale and floating in a sea of ubiquitous quasi-related sensors—"anything" transcends IPv6 and TCP/IP, extending further up the classic open systems interconnection stack. Figure 4 presents our vision of the IoA ecosystem.

This ecosystem, clearly based on distributed automation, must create identity controls and address serious management questions for interaction among entities, including some of the following:

- Are you a thing, a human, or another living organism?
- If you are human, must you have an identity as such?
- Where is where (the geo-location)?
- When is when (time being tamper-able)?

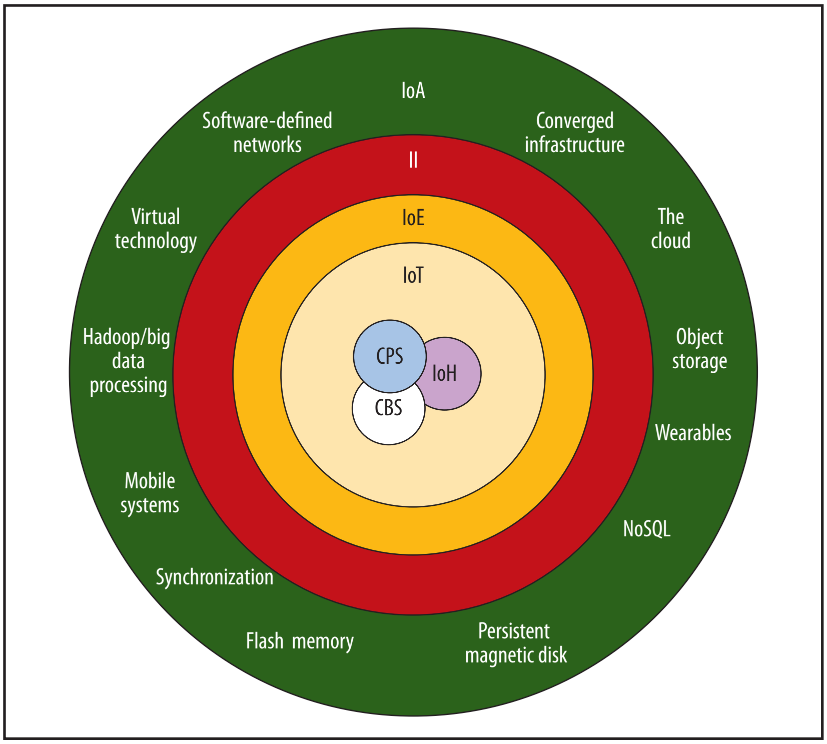

Figure 4. The Internet of Anything (IoA) ecosystem. Cyber-physical systems (CPS), cyber-biological systems (CBS), and the "Internet of Humans" (IoH) comprise the IoT. The Internet of Everything (IoE) and the Industrial Internet (II) grow out of the IoT and combine with distributed, automated systems to become the IoA.

Questions like these point to fundamental concerns about how we determine "trust" in IoA terms. Although truth isn't malleable, trust is. And even in the IoT, that malleability is troubling.

And all this begs the question: Should an IoA be separate from the IoH if it's to be trustworthy? Is an IoA (even an IoA bounded and reduced in size) trustable? And how far must you restrict, or bound, it to make it trustable? Further, is that trust even verifiable?

We offer the following observations as true:

- Trust in the IoA is, minimally, a function of algorithms, sensors, interfaces, interoperability, security, and privacy in a wireless hypernetworked environment.
- Scalability in terms of network effects (according to Metcalfe's law, the value of a network increases proportionately to the square of the number of users) compounds the difficulties for defining trust—even when only a few nodes/hops/branches are involved.
- Heterogeneity exacerbates the problems associated with interoperability.
- Privacy as a concept falls victim to sensors and wireless communication, and so should be redefined.
- Whoever or whatever owns the IoA's limitless data (a nation? a company?) ultimately owns the IoA—assuming they can analyze it.
- Within a wireless reality, an IoA is prone to drastic malicious attacks.

Such issues require our attention sooner rather than later. A recent Pew Research report, based

THE DIGITAL FUTURE: SOME MORE HOPEFUL AND LESS HOPEFUL THESES

The following predictions for the digital future come from Pew Research Center, *Digital Life in 2025*, 11 Mar. 2014 (www.pewinternet.org/files/2014/03/PIP_Report_Future_of_the_Internet_Predictions_031114.pdf).

More Hopeful Theses

- The Internet will enhance global connectivity, fostering more planetary relationships and less ignorance.
- The IoT, artificial intelligence, and big data will make us more aware of the world and our own behavior.
- Augmented reality and wearable devices will monitor and give quick feedback on daily life (for example, to enhance personal health).
- Political awareness and action will be facilitated. More peaceful change and public uprisings will emerge.
- The spread of the "Ubernet" will diminish the meaning of borders, and new "nations" of those with shared interests may emerge.
- The Internet will become "the Internets" as access, systems, and principles are renegotiated.

Less Hopeful Theses

- Dangerous divides between haves and have-nots may expand, resulting in resentment and possible violence.
- Abuses and abusers will "evolve and scale." Human nature isn't changing; laziness, bullying, stalking, stupidity, pornography, dirty tricks, and crime will continue, and those who practice them have new capacity to make life miserable for others.
- Pressured by these changes, governments and corporations will try to assert power—and at times succeed—as they invoke security and cultural norms.
- People will continue—sometimes grudgingly—to make tradeoffs, favoring convenience and perceived immediate gains over privacy. Privacy will become something only the upscale enjoy.
- Humans and their current organizations may not respond quickly enough to challenges presented by complex networks.
- Most people haven't yet noticed the profound changes today's communications networks are already bringing about; these networks will be even more disruptive in the future.

on interviews with 2,558 experts and technology builders about the digital world of 2025, suggests that in the near future "the Internet will become 'like electricity'—less visible, yet more deeply embedded in people's lives for good or ill."[5] The sidebar "The Digital Future: Some More Hopeful and Less Hopeful Theses" summarizes several of its main findings, which mirror our vision and concerns.

To conclude our attempt at imagineering, we posit that "things" can form communities, similar to clouds. These things can be rogue. A global clock will need to be devised to keep "things" organized and in check. On Walt Disney's original *Mickey Mouse Club* television show, Wednesday was "Anything Can Happen" day. With the IoA, every day would be Wednesday. ◼

References

1. E. Simmon et al., *A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems*, NIST, Aug. 2013; www.nist.gov/customcf/get_pdf.cfm?pub_id=914023.
2. National Science Foundation, "Cyber-Physical Systems: Program Solicitation," NSF doc. 14-542, 2014; www.nsf.gov/pubs/2014/nsf14542/nsf14542.pdf.
3. M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, vol. 265, no. 3, 1991, pp. 94–104.
4. K. Ashton, "That 'Internet of Things' Thing," *RFID J*, 22 June 2009; www.rfidjournal.com/articles/view?4986.
5. Pew Research Center, *Digital Life in 2025*, 11 Mar. 2014; www.pewinternet.org/files/2014/03/PIP_Report_Future_of_the_Internet_Predictions_031114.pdf.
6. M. Ceniceros, "The Internet of Things Ecosystem: The Value Is Greater than the Sum of Its 'THINGS,'" *Business 2 Community*, 1 Apr. 2014; www.business2community.com/business-innovation/internet-things-ecosystem-value-greater-sum-things-0829370#!DmBAi.
7. D. Evans, *The Internet of Everything: How More Relevant and Valuable Connections Will Change the World*, white paper, Cisco ISBG, 2012; www.cisco.

com/web/about/ac79/docs/innov/IoE.pdf.

8. Gartner Newsroom, “Gartner Identifies the Top 10 Strategic Technology Trends for 2014,” 8 Oct. 2013; www.gartner.com/newsroom/id/2603623.
9. J.R.B. de Marca, “Coming Next: The Internet of Everything,” *IEEE The Institute*, Mar. 2014; http://theinstitute.ieee.org/opinions/presidents-column/whats-coming-next-the-internet-of-everything.
10. L. Leung, “The New Computing Architecture Is Here,” blog, 2 Apr. 2014; www.linkedin.com/today/post/article/20140402185604-756499-the-new-computing-architecture-is-here.

***Irena Bojanova** is a professor and program director of information and technology systems at the University of Maryland University College (UMUC). You can read her cloud computing blog at www.computer.org/portal/web/Irena-Bojanova. Contact her at irena.bojanova@umuc.edu.*

***George Hurlburt** is chief scientist at STEMCorp, a nonprofit that works to further economic development via adoption of network science and to advance autonomous technologies as useful tools for human use. Contact him at ghurlburt@change-index.com.*

***Jeffrey Voas,** Security column editor, is an IEEE Fellow and a Fellow of the American Association for the Advancement of Science (AAAS). Contact him at jeffrey.m.voas@gmail.com.*

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