DOI:10.1145/**tk**

Connected Things Connecting Europe

By Julie A. McCann, Gian Pietro Picco, Alex Gluhak, Karl Henrik Johansson, Martin Törngren and Laila Gide

It is estimated that personal computers, data centers, and other technologies constitute less than 1% of all microprocessor usage;[10] embedded systems represent the remaining percentage and can be found in our washing machines, microwaves, remote controls, PC peripherals (such as keyboards and mobile phones), with modern cars containing many tens of embedded microcontrollers.[18] Modern embedded-system microcontroller and transceiver technology advancements have brought forth the kinds of systems we have in the past defined as pervasive, ubiquitous, and embedded computing, and for some time in Europe, "embedded intelligence." However, today they are better known as the Internet of Things (IoT) and cyber-physical systems (CPS); see the figure here.

The jury is still out regarding a definition of the latter two terms or indeed how to differentiate them, but on the whole people tend to refer to IoT as embedded devices that connect to the Internet to exchange data, optimize processes, monitor environments, and typically consist of sensors, actuators, and low-power compute infrastructures. CPS is a term first coined in 2006 in the U.S. to characterize "the integration of physical systems and processes with networked computing" for systems that "use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems."[22] CPS is generally put forward as the more systems notion, while IoT emphasizes communication and analytics, yet IoT-like devices need not use Internet protocols to create a CPS, hence the ambiguity. The European Commission debated for two years whether to call its embedded intelligence programs CPS, with the latter winning out in the end. In this article, we embrace these terms fluidly and name them IoT/CPS; for other definitions see the sidebar "Some Definitions."

In essence, the terms represent different perspectives on the technological advancements that have led to creation of many related application terms—industry 4.0, smart cities, precision agriculture, smart transport, and autonomous vehicles—all representing new classes of technologically enabled systems. Recent studies have predicted the impact of IoT/CPS on the European Union's GDP in 2025 by sector, with "transportation" being forecast to create the greatest value, with a total of €245 billion alone; followed closely by "healthcare," "housing," and "industry."[1] As in the rest of the world, European countries and the European Commission have invested heavily in IoT/CPS research, almost €200 million, resulting in many cross-discipline, cross-country technology advancements unique in terms of their focus on the integration of such systems, particularly at scale; their underpinning communications substrates; and, more recently, their security and relationship to privacy. In this article we describe highlights of this work in more detail and present what we believe are the main outstanding challenges facing the field for Europe over the next decade.

The Integrated Approach

Two decades ago, a European named Kevin Ashton coined the phrase the "Internet of Things." His vision of connecting sensor- and actuator-based technology to the Internet unfolded an active area of technological advancement around the world that only in the past few years has begun to find larger-scale adoption and is finally becoming a commercial reality. In parallel, the University of California, Berkeley's TinyOS and Mote hardware combination dominated early academic experimental work on wireless sensor networks, also making its way into various commercial products. While the U.S. focused on designing new protocols and approaches to overcome the intrinsic limitations of resource-constraint IoT/CPS devices, the focus in Europe was more on the integration of such systems to fulfil real application needs. In particular, tools to aid the building of devices and, moreover, their applications became the European emphasis, resulting in mechanisms to ease programming and systems engineering and, more important, make such systems a natural extension of the Internet, the latter reaping the advantages of standardization and the software-engineering experience that programmers already had from other Internet systems.

Adam Dunkels of SICS in Sweden developed the Contiki operating system that has significantly grown in popularity, particularly over the past decade. As the technology matured, device hardware could pack more compute power for the same energy budget, and the resource savings TinyOS covered thus became less important. Exploiting this power, Contiki's advantage over its predecessors lay in its flexibility and ease of coding applications. Indeed, today hackers, academic institutions, and companies are using Contiki because it remains lightweight, mature, and free; for example, Texas Instruments (a U.S. company) ships many of its IoT/CPS devices (such as Sensortag) with the option of using Contiki.

At that time, the prevalent communications protocols operated over low-data-rate, local-area networking (up to approximately 50-meter distances) radio transmissions. 802.15.4-based protocols (such as ZigBee, designed in the U.S.) overcome these short distances by providing multi-hop communications allowing data to be relayed between devices to form longer-distance routes, hoping the data from device to device. However, in Europe, for researchers (such as Dunkels), the quest was now to push the Internet Protocol all the way down to small embedded devices themselves.[2] Early attempts include the work of Zach Shelby, an American, working at Oulu University,[3] but the now-ubiquitous 6LowPAN protocol has emerged to provide lightweight end-to-end Internet connectivity down to the smallest devices and has gradually replaced the previously popular ZigBee communications approach.

While 6LowPAN allowed for more efficient raw Internet communication, the next logical step was to make it Web friendly by replacing its heavy Web protocol with a more lightweight one. Work emanating from European large-scale mixed academic/industrial projects (such as SENSEI and FP7) focused on how such emerging wireless sensor and actuator networks can be more effectively integrated into a future Internet.4 Shelby worked with the Internet Engineering Task Force (IETF) and such companies as England's ARM low-power processor design company, ultimately producing the COAP protocol5 used to make applications on low-power devices easier to program. At about the same time, Dom Guinard at ETH Zurich and others advocated for such devices to become first-class citizens in the current Web. His pioneering work led to what is now known as the Web of Things, with active work as part of W3C receiving support from Siemens, Google, and other sources.[6]

The increasing investment in CPS/IoT throughout Europe, and the world, has meant an increase in the number of systems, protocols, and applications being built. Also, there was little integration between systems, as seen especially in the smart city domain. This fragmentation is thought to have undermined the confidence of stakeholders and market opportunities, affecting IoT adoption, thus causing Europe to become increasingly focused on the applications built on top of IoT/CPS systems and their integration.[7] Indeed the perception in Europe was that while U.S. IoT/CPS innovation focused on adoption environments based on individual business cases driven by economic return on investment, Europe's industry and academic researchers focused on the exploration of societal benefits and acceptance of CPS/IoT technology generally.

One major success resulting from the European joint research and industrial projects is FIWARE, a curated framework of open source-platform, market-ready components to accelerate development of IoT/CPS systems and their integration with cloud services.[8] Since its beginnings in 2012, FIWARE has evolved from a consortium of multinational telcos, including Telefónica (Spain), Orange (formally French Telecom), and others to a suite of more than 50 components to create value from real-world applications enabled by the ubiquity of heterogeneous and resource-constrained devices. Another example is from the ARTEMIS Industry Association,[9] with more than 170 members and associates from all over Europe, and the European IoT Platform Initiative Programme (IoT EPI), a €50 million programme with nine projects involving more than 40 different IoT platforms exploring multiple approaches to interoperability.[11]

An example of where Europe leads in living-lab deployments is the SmartSantander testbed in Santander, Spain, a prominent European experimental infrastructure for IoT/CPS. By embedding a large number of diverse sensor devices into a city environment, this testbed allowed a variety of smart city use cases to be explored. While initially useful for experiments with IoT protocols and data-driven services, the infrastructure is now part of the Santander's day-to-day operation, improving the lives of its citizens. Since its beginnings in 2010, more than 12,000 sensor devices have been deployed across the city to help the government operate as efficiently as possible through such applications as adaptive traffic management, smart parking, water management, intelligent streetlights, and waste disposal. SmartSantander went on to inspire other initiatives around the world, including the Array of Things project in Chicago.

Both testbeds and living labs[21] paved the way for IoT large-scale pilots in Europe, a €100M R&I program that commenced in 2017.[12] Examples of such projects include SynchroniCity (eight smart cities pilots[13]), MONICA (IoT technologies to manage sound and security at large, open-air cultural and sporting events[14]), and IoF2020 (Internet of Food and Farm 2020 with 70 partners from 16 European countries[15]); many of these projects are associated with, and continue to use, the FIWARE infrastructures.

Underpinning Communications Technologies

The communications substrate in an IoT/CPS architecture plays a crucial role, and low-power wireless connectivity is fundamental to balancing connectivity performance with low-power system capabilities and lifetimes. Freedom from power and data cables provides mobility and autonomy of devices that are readily deployed and relocated, can improve performance, and follow the users and objects they are attached to, or even move of their own volition, as with robots and drones. In recent decades, wireless communications was dominated by Wi-Fi and cellular communications that were ubiquitous yet energy-hungry; low-power alternatives had to emerge, as embodied by ZigBee in 2004. Today, the wireless communication landscape is significantly more fluid, with several technologies (both competing and complementary) offering disruptive opportunities unthinkable only a few years ago. Interestingly, several of these trends are the result of achievements by European researchers and companies, as we highlight here.

A prominent example is a new class of communications mechanisms described as "low-power wide-area networks" (LPWANs) that recently revealed trade-offs in the amount of power they require from the device, geographic coverage or distances they send data, and data rates. Until a few years ago, long-range communication was a privilege of cellular telephone communication where devices were fitted with SIM cards and communicated typically over 2G GPRS networks. This did not match with the low-power nature of CPS/IoT devices and meant they were required to be plugged into the mains, limiting where they could be placed or receive frequent battery changes, and many stakeholders were reluctant to rely solely on proprietary networks and devices owned by operators.

SigFox[16] based in France was in 2009 the first to use ultra-narrowband modulation to enable longer-distance communications while remaining low power. Since the first deployments that covered the entire country of France, SigFox showed its technology can provide coverage like cellphone communications but without the need for a SIM card and significantly less cost in terms of money and energy. But SigFox is still a telco operator, having to manage access to its own network and based on proprietary technology. In contrast, LoRa,[17] which was developed by Cycleo of Grenoble, France, and acquired by Semtech in 2012, used radio technology based on chirp spread spectrum modulation to effect low-power wide-area transmission. The LoRa Alliance then defined a public suite of protocol specifications (LoRaWAN) that allows a telco operator to deploy its own networks but also enables deployment and operation of privately owned networks operating side-by-side. Both SigFox and LoRa have their main center of gravity in Europe; for instance, of the 5,000+ gateways deployed today, 3,000+ are in Europe. This is also reflected in the surge of competing, industry-driven approaches, among which, arguably the most prominent, is Huawei's NB-IoT. Indeed, today's version of NB-IoT, which is being specified by the 3GPP, an international body of telcos, originated in early work by NEUL, a company from Cambridge, U.K., that developed the Weightless protocol and was bought out in 2014 by Hawaii. LPWA technologies are not being rolled out worldwide.

Where LPWA supports slow data over great distances, ultra-wideband (UWB) communications permits higher data volumes and speeds over short distances. Originally used for military applications, UWB became unlicensed in 2002, but a new wave of interest has followed a small Irish company called DecaWave[19] when it released the DW1000 chip, overcoming many of bulkiness and power-consumption issues and storming the field of real-time location-tracking systems. Indeed, the potential here is enormous, especially if UWB chips eventually find their way in smartphones where UWB could trigger a new wave of location-based IoT/CPS services with an impact comparable to (if not greater than) that achieved by GPS.

Trust, Safety, Security, Privacy (Guarantees)

CPS and IoT provide unprecedented capabilities and opportunities for the benefit of society. But it will be achieved through corresponding unprecedented technological complexity that also introduces new risks that need to be recognized, debated, and dealt with appropriately. This is essential since future CPS and IoT will be widespread and underpin a large number of critical societal infrastructures, including water, energy, transportation, and healthcare, all relying on the proper operation of the technologies.

A key concern is that current engineering methodologies are generally viewed as inadequate for next-generation CPS. Consequently, multiple calls have been issued from the E.U. for new methodologies, including Platform4CPs,[25] AENEAS,[26] and the Acatech National Academy of Science and Engineering.[27] The full potential of future CPS can be obtained only when new engineering methodologies are in place to ensure future CPS systems are sufficiently safe, secure, available, privacy-preserving, and overall trustworthy. A science for CPS engineering is needed. Europe is positioned well in this regard to address the key challenges of complexity management, safety, and security by design and privacy.

Complexity management of IoT/CPS systems is important because they inherit the complexity of their cyber and physical parts. There is a lack of approaches to systematically accomplish "composability" of CPS components, meaning achieving integration of CPS components is difficult without negative, sometimes unknown, side effects, or emerging behaviors.[28] Composability for CPS must address the multifaceted dependencies in CPS across components, functions, and system-level properties. An example of a European stronghold is the effort driven by Kopetz on composable time-triggered architectures, with research funded through several E.U. projects that have influenced many communication protocols for CPS, delivered reusable architectural services for exploitation across platforms of different domains (INDEXYS project in 2008), and paved the way for successful companies like TTTech.[20]

The use of machine learning, particularly deep learning, provides a novel technology within CPS. While such technologies enable entirely new types of applications, they raise concerns about how to deal with transparency (black-box behavior), robustness, predictability (such as when data is outside a training set), and how to cost-efficiently verify, validate, and assure such systems.[29,30] In addition, CPS systems must function in increasingly complex environments, as in automated driving. Describing such varying environments and systematically dealing with uncertainty represent further key challenges that have been addressed in such European research projects as Pegasus[31] and the U.K. EPSRC-funded S4: Science for Sensor Systems in 2016.[32]

Safety and security engineering concerns the connectivity and spread of CPS and provides new attack surfaces that could exploit vulnerabilities in the cyber and/or physical side, as well as among human stakeholders. This implies that existing security approaches are not suitable. Moreover, security may affect safety, thus calling for integrated and balanced security and safety trade-offs and development of new methodologies. The widespread use of CPS systems and their increasing automation imply that existing safety-engineering approaches are not sufficient, and, in particular, that future CPS will need to deal with risk explicitly, incorporating measures of dynamic risk, as compared, again, with automated driving. An example of security research in Europe comes from the £23M PETRAS Research Hub in the U.K., which involves 60 projects researching the various aspects of IoT/CPS security, from devices to social practice, and have produced a landmark report, *The Internet of Things: Realising the Potential of a Trusted Smart World*,[33] co-produced with the Royal Academy of Engineering.

It is infeasible to predict all possible faults, threats, and failure modes for future CPS. Systems will have to be resilient, with built-in build monitors and error handlers to ensure cost-efficient dependability. Examples of European efforts include the MBAT project that gave European industry a leading-edge affordable and effective validation-and-verification technology in the form of a Reference Technology Platform (the MBAT RTP) and the AQUAS project, which is developing solutions for safety/security/performance co-engineering, as in Sillitto.[34] Europe has a strong tradition in dependability and engineering of trustworthy systems, notably through the ARTEMIS and ECSEL private-public partnerships. Example projects include Pegasus, funded by the German Federal Ministry for Economic Affairs and Energy and involving all major German OEMs and Tier 1 companies to produce mechanisms to test and formally verify autonomous vehicles. And SCOTT is examining frameworks to enabler development of secure and connected trustworthy things primarily for the rail-transport industries.[35] Separately, the TrustLite security framework from the Intel Collaborative Research Institute for Secure Computing (a collaboration by TU Darmstadt, University of Helsinki, and other European security institutes) have produced an Execution-Aware Memory Protection Unit (EA-MPU) that provides programmable operating system-independent isolation of software modules at runtime for low-cost embedded devices.

IoT/CPS systems are constantly monitoring homes, factories, cars, and more, and while understanding these processes can make them more efficient, sustainable, and safe, they can expose privacy concerns. The most prominent European initiative affecting IoT/CPS data gathering is that of the General Data Protection Regulation (GDPR) regarding data protection for individuals in the E.U. and its economic area.[36] The European approach to privacy is that, through GDPR, all the requirements of data domains and territories are consolidated into a single coherent and well-defined regulation. One aspect of this is that a data owner must prove its data protection reasonably matches the current state of the art, which in turn uniquely drives practical anonymization research. Researchers aim to demonstrate privacy shortfalls to make schemes more robust. For example, U.K. and Belgium researchers[37] were able to prove it took only four location points to be able to uniquely identify someone 95% of the time and that data coarsening and noise addition do not help. This was followed by Gadotti et al.,[23] who showed privacy techniques using “sticky noise” could be infiltrated easily. All European citizens, as well as those only visiting Europe, are covered by GDPR, meaning its effect reaches much farther than just Europe.

Conclusion

We have drawn out three views of IoT/CPS systems the European approach to research contributes to in its own unique way, though European researchers continue to collaborate across the globe to address the many challenges associated with these systems. This subject continues to grow and, with it, new problems. For example, as such systems contribute to the autonomy of cars, water networks, precision farms, and more, the more we need to be able to understand how to engineer them and provide guarantees regarding their operation. However, as we do not fully understand how digital systems interact with the physical world, we do not yet have such guarantees. We thus need a science of cyber-physical interaction; related design principles will then emerge, much as they have in other engineering disciplines. Given the importance of the communications substructure for such systems, the jury is still out as to which protocol (or set) will win.

There are many players in the LPWA game, but the big question is what will be the effect of the promised 5G suite of solutions? Finally, as these systems take more control of our lives, their ethical approach is key, including the ability to maintain privacy while still being useful. Indeed, their security is of paramount importance, as being able to hack a water network or autonomous vehicle could mean disaster. Plenty of research for Europe and beyond to consider.

References

1. https://www.statista.com/statistics/686173/iot-s-impact-on-gdp-in-the-european-union-eu-by-sector/
2. Dunkels, D. Full TCP/IP for 8-bit architectures. In *Proceedings of the 1st ACM/Usenix International Conference on Mobile Systems, Applications and Services* (San Francisco, May 2003).
3. Shelby, Z., Mahonen, P., Riihijarvi, J., Raivio, O., and Huuskonen, P. NanoIP: The Zen of embedded networking. In *Proceedings of the IEEE International Conference on Communications* (Anchorage, AK, 2003), 1218–1222.
4. https://tools.ietf.org/id/draft-shelby-core-coap-req-01.html
5. http://coap.technology/
6. http://www.usa.siemens.com/en/about_us/research/web-of-things.htm and https://github.com/google/physical-web
7. http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Semantic_Interoperability_Final.pdf
8. https://www.fiware.org/about-us/
9. https://artemis-ia.eu/project/59-3car.html
10. Turley, J. Embedded processors by the numbers. *EE Times* (May 1, 1999); https://www.eetimes.com/author.asp?section_id=36&doc_id=1287712
11. https://iot-epi.eu/
12. https://european-iot-pilots.eu/
13. https://synchronicity-iot.eu/
14. https://european-iot-pilots.eu/project/monica/
15. https://european-iot-pilots.eu/project/iof2020-2/
16. https://www.sigfox.com
17. https://lora-alliance.org/
18. Fleming, B. Microcontroller units in automobiles. *IEEE Vehicular Technology Magazine 6,* 3 (2011), 4–8.

19. https://www.decawave.com/
20. http://www.indexys.eu/
21. Open Living Labs; https://enoll.org/
22. Lee, E.A. and Seshia, S.A. *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*. MIT Press, Cambridge, MA, 2016.
23. Gadotti, A., Houssiau, F., Rocher, L., and de Montjoye, Y.A. When the signal is in the noise: The limits of Diffix's sticky noise. 2018; *arXiv preprint arXiv:1804.06752*
24. Istomin, T. et al. Data prediction + synchronous transmissions = ultra-low-power wireless sensor networks. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems,* 2016.
25. Platforms4CPS: Final recommendations;
https://www.platforms4cps.eu/fileadmin/user_upload/E-Book_-_Platforms4CPS_Key_Outcomes_and_Recommendations.pdf
26. AENEAS, ARTEMIS Industry Association, EPoSS. *Strategic Research Agenda for Electronic Components and Systems*, 2018; https://efecs.eu/publication/download/ecs-sra-2018.pdf
27. Acatech National Academy of Science and Engineering. *Living in a Networked World. Integrated Research Agenda Cyber-Physical Systems,*
2015; http://www.cyphers.eu/sites/default/files/acatech_STUDIE_agendaCPS_eng_ANSICHT.pdf
28. Törngren, M. and Grogan, P.T. How to deal with the complexity of future cyber-physical systems? *Journal of Designs 2,* 4, 2018; http://www.mdpi.com/2411-9660/2/4/40
29. Wagner, M. and Koopman, P. *A Philosophy for Developing Trust in Self-driving cars. In Road Vehicle Automation*, G. Meyer and S. Beiker, Eds. Lecture Notes in Mobility. Springer, Cham, Switzerland, 2015, 163–171.
30. Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., and Mané, D. *Concrete Problems in AI Safety*. 2016; arXiv:1606.06565
31. https://www.pegasusprojekt.de/en/about-PEGASUS
32. Calder M., Dobson, S., Fisher, M., and McCann, J. *Making Sense of the World: Models for Reliable Sensor-Driven Systems,* Mar. 28, 2018; arXiv preprint arXiv:1803.10478
33. http://www.oerc.ox.ac.uk/news/Centre-contribution-IoT-reports
34. Sillitto, H. *Architecting Systems: Concepts, Principles and Practice. Volume 6: Systems*. College Publications, London, U.K., 2014.
35. https://www.indracompany.com/en/indra/scott-secure-connected-trustable-things
36. https://eur-lex.europa.eu/eli/reg/2016/679/oj
37. De Montjoye, Y.-A. et al. Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports 3* (2013), 1376;
http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

Julie A. McCann is a professor of computer systems, Department of Computing at Imperial College, London, U.K.

Gian Pietro Picco is a professor in the Department of Information Engineering and Computer Science (DISI) at University of Trento, Italy.

Alex Gluhak is head of technology at Digital Catapult, Guildford, U.K.,

Martin Törngren is a professor of embedded control systems in the Department of Machine Design at KTH Royal Institute of Technology, Stockholm, Sweden.

Karl Henrik Johansson is a professor in the School of Electrical Engineering and Computer Science at KTH Royal Institute of Technology, Stockholm, Sweden.

Laila Gide is Past-President, ARTEMIS Industry Association, and Past-Director, Advanced Studies Europe in the Corporate Strategy, Marketing and Technical Directorate, Amsterdam, The Netherlands.

PQs/

We thus need a science of cyber-physical interaction; related design principles will then emerge, much as they have in other engineering disciplines.

Given the importance of the communications substructure for such systems, the jury is still out as to which protocol (or set) will win.

SB/

Some Definitions

Microcontroller. Computer on a single chip with one or more processor cores, memory, and input/output peripherals.

Sensor nodes/mode. Generic way to describe sensor-based devices typically consisting of several sensors and radio communications module(s) governed by a microcontroller. Different from phones and traditional computers, they are a few centimeters in size without keyboard or screen. An example is the University of California, Berkeley, TMote Sky sensor node consisting of the CC2420 ZigBee near-range communications, an MSP430 low-power microcontroller packed into a matchbox-size form factor.

Actuator. A device that controls other devices (such as valves and switches.

European Research Council. A body that funds technological research in the E.U. Its framework funding programs include FP7 (Framework Programme) finished in 2013, giving way to H2020 (Horizon 2020). On top of this, each E.U. country also has national funding infrastructures, as in EPSRC in the U.K. and DFG in Germany.

IETF. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and smooth operation of the Internet; for more, see https://www.ietf.org/about/