Cyber-Physical Systems: Challenge of the 21st Century

Lukas Esterle, Radu Grosu

L. Esterle
Vienna University of Technology
Cyber-Physical Systems Group
Tel.: +43 (1) 58801 – 18219
E-mail: lukas.esterle@tuwien.ac.at

R. Grosu
Vienna University of Technology
Cyber-Physical Systems Group
Tel.: +43 (1) 58801 – 18210
E-mail: radu.grosu@tuwien.ac.at

Summary

Cyber-physical systems and the Internet-of-Things will be omnipresent in the near future. These systems will be tightly integrated in and interacting with our environment to support us in our daily tasks and in achieving our personal goals. However, to achieve this vision, we have to tackle various challenges.

Zusammenfassung

Cyber-physikalische Systems und das Internet-der-Dinge wird schon bald allgegenwertig sein. Durch die starke Integration und Interaktion mit unserer Umwelt können diese Systeme uns bei unseren täglichen Aufgaben unterstützen und behilflich sein, unsere Ziele zu erreichen. Um diese Vision zu verwirklichen, müssen jedoch noch einige Herausforderungen überwunden werden.

English Title: Cyber-Physical Systems: Challenge of the 21st Century

Deutscher Titel: Cyber-Physikalische Systeme: Herausforderung des 21sten Jahrhunderts

English Keywords: Cyber-Physical Systems, Internet-of-Things, Challenges, Revolution

German Keywords: Cyber-Physikalische Systeme, Internet-der-Dinge, Revolution, Herausforderungen

Cyber-Physical Systems: Challenge of the 21st Century

1. Introduction

Cyber-physical Systems (CPS) have their original roots in the early 1980ies with the development of microcontroller and emergence of embedded systems in the consumer area. Soon after, single embedded systems have been connected in networked embedded systems and with the vision of Weiser [1]pervasive computing, where individual embedded systems communicate and cooperated, started its triumph. However, these embedded systems rarely interacted with the physical world *per se*. It was until the late 2000s when computational systems were defined to interact with and control the physical environment [2, 3, 4].

We can consider the development from embedded systems towards CPS like the developments in transportation. The embedded system triggers the single component of the car such as the airbag. The networked embedded system represents the entire car where single components interact with each other to keep the car safely on the road in case of turbulences. In this comparison, the CPS would not be a single car, indeed it would be the entirety of all cars interacting with each other in the real world.

CPS are spatially-distributed, time-sensitive, and multi-scale, networked embedded systems, connecting the physical world to the cyber world through sensors and actuators. Nevertheless, computational systems interacting with the physical world are not new and have long been designed to interact with the real world in order to support humans to achieve their goals. However, only in recent years the physical world has been explicitly considered during the development process of such systems. This new paradigm sparked novel systems and entire research areas such as autonomous driving, industry 4.0, smart cities, or the Internet of Things. The Internet of Things (IoT) can be considered as the backbone of CPS. It connects the swarm of Sensors and Actuators to the nearby Gateways through various protocols, and the Gateways to the Fog and the Cloud.

The goal of these researches in CPS are manifold such as increasing reliability and safety, reducing resource consumption, or improving the overall performance of a given process. Autonomously driving vehicles ranging from cars and trains to planes yield in zero traffic fatalities. Smart cities increase public safety in general but also introduce smart transportation to reduce congestions. Resource conservation is achieved through energy aware buildings reducing the waste of power, water, and heat. On-the-fly production allows to adjust to the requirements of the individual consumer and make large storage space obsolete. And in agriculture a maximum output is achieved through constant monitoring of the environment and its impact on the crop.

With a forecast of 50-bn devices connected by 2020 and $15-tn business in next 20 years, all big industrial players are dedicating vast resources to IoT. In the US alone, Amazon, Siemens, Apple, Cisco, Bosch General Electric, Google, IBM, Intel, Kuka, Microsoft and many others compete for a piece of the IoT.
Four pillars drive industrial forecasts: Connectivity, Monitoring, Prediction, and Optimization. The first two are already in progress, enabled by recent technological advances. Last two pillars are expected to radically change our society. The huge number of sensors to be deployed in manufacturing, transportation, energy and utilities, buildings and urban planning, health care, environment, or jointly in smart cities, will allow the collection of terabytes of information (Big-Data), which can be processed for predictive purposes. Moreover, the huge number of actuators will enable the optimal control of these areas and drive market advantages. For example, the predictive maintenance of assets is expected to save up to 12% in scheduled repairs, reducing maintenance costs up to 30%, and eliminating breakdowns up to 70% [5].
According to the report by General Electric (2015), 73% of companies are already investing more than 25% of their technology budget in big-data analytics. Moreover, ¾ of executives expect that level to increase just in the next year. Across the industries surveyed, 80% to 90% of companies indicated that big-data analytics is either the top priority (61% in aviation industry) or in the top three (28% for power distribution, 31% for power generation, 31% for oil and gas, 24% for mining). In 53% of companies the board of directors is the primary influencer of their IoT adoption strategy. Strong board-level support can also be seen in manufacturing (67%), rail (60%) and wind (45%). A staggering 89% say that companies not adopting IoT and big-data analytics in the next year risk losing market share and momentum.

This large number of devices, to be operational in the near future, gives rise to various technical challenges regarding different aspects of CPS such as the required architecture, handling uncertainty, or how to introduce smartness to these systems. In the remainder of this article, we will discuss these technical challenges in more detail. We conclude this article with an outlook on what the future might hold for us and cyber-physical systems.

2. Technical challenges

In cyber-physical systems, an enormous amount of sensors and actuators come together to interact with each other as well as with the environment. This huge complexity gives rise to various technical and scientific challenges that need to be addressed in order to achieve the vision of pervasive and ubiquitous cyber-physical system.

2.1. Mathematics

When computer systems interact with the real world, we have to deal with the continuously changing environment within the discrete processes of a computer. This requires us to harmonize models reflecting the continuous environment, possibly having an infinite amount of states, with models for the discrete computing system with a finite amount of states. This requires novel mathematical approaches handling the discrete-continuous duality of such a situation. Such a situation already occurred in the physics, with the particle-wave (that is, discrete-continuous) duality. This showed that light and elementary components of atoms are neither particles, nor waves, but both. In this case, the harmonization happened within quantum mechanics by using a probabilistic approach, where discrete probability distributions model the discrete aspects, and the continuous probability distributions model the continuous aspects. An intriguing aspect of this theory is the use of complex numbers in order to model the wave-function of the elementary components, and the question is, when such numbers are going to enter the arena of computer science, too.

2.2. Architecture

Due to the enormous amounts of devices expected to interact with each other in the near future, currently used approaches for architectures will not be sufficient to deal with the arising complexity [6, 7]. Additionally, the functionality of the individual devices is increasing at the same time. Therefore, we will have to work towards new ways of building applications with an incomprehensive number of devices with currently unknown capabilities. Furthermore, we require special operating systems for cyber-physical systems. A so called cyber-physical system has to deal with various problems which need to be tackled by the CPS-OS such as:

- **Openness**: Allow interaction with possibly new devices entering the system to achieve common goals. If the current device has spare resources, it may accept tasks from other devices in the network.
- **Isolation**: Allow a device to isolate itself in order to achieve its own goals within the given time. This is important to ensure a device cannot be hijacked by other devices and their offloaded tasks.
- **Safety**: CPS/IoT will be pervasive, and our lives are going to depend on it. As a consequence, we have to make sure that it will behave as intended. This is especially important when we think of safety-critical applications and its implications such as autonomous driving.
- **Security**: The CPS-OS is required to safeguard the data that is being transferred to other devices. This is especially important when offloading tasks to other devices with sensible data. Alternatively, the CPS-OS has to ensure that sensible data does not leave the device unauthorized.
- **Privacy**: There should be no way to identity of owner of a device without proper authorization. This includes information that might be used to reveal the identity of the owner of the device.
- **Extensibility and Discovery**: Allow new devices to join network in order to achieve common goals faster. New devices need to be discovered autonomously by the already joined devices in the network. In addition, the network has to be able to learn about the capabilities of these newly joined devices in order to utilize it as a new resource. At the same time, the new device has to be able to gain knowledge about the capabilities already available in the network.
- **Robustness**: Removing devices from the application, may not affect the performance of the system. If applications or processes rely on specific devices, the network has to be able to deal with failing or removing of such devices using respective mechanisms.
- **Self-protecting**: Detect and fend off attacks from the outside as well as malicious or contra-productive devices trying to join the network. This is obviously problematic as it is contradicting the openness aspect of the CPS-OS. Hence the network requires clear protocols, reasons, and taxonomies to lock out specific devices. These taxonomies and reasons might be defined and negotiated by the devices of the network at runtime.
- **Self-maintenance**: Ensure functionality in standard as well as in uncertain situation. This includes handling resources such as memory or battery levels but also that performed actions achieve the expected outcome. If this outcome is not achieved, the process might be adapted accordingly. This may happen through autonomous adaptation but also through coordinated software updates.
- **Self-awareness**: The individual devices have to be aware of their own capabilities and the corresponding impact of own action on the environment and other devices. Additionally, they need to be able to handle actions performed by other devices in the network, whether these actions are beneficial or disadvantageous for their own goals.
- **Connectivity**: The devices in the networks are not operating in isolation but should also have the capability to connect to the web and cloud services.
- **Location**: The individual devices might need to be able to localize other devices. This can be done only relative to their own location or in absolute space. Furthermore, this can only be a semantic proximity. In any case, this proximity can further be exploited for improving collaboration between the individual nodes.

- **Data Storage**: Data needs to be stored in a distributed fashion among the devices. At the same time, neither the user or the applications need to be concerned about the actual location of the data.
- **Communication**: The devices have to be able to communicate with each other. How this is implemented may not affect the performance of the application running on the devices or the user using them.
- **Time**: Timing might be crucial for certain applications. This is with respect to communication as well as with sensing. In sensing, important events may not be missed. In communication, it might require the devices to synchronize and operate with time constraints.

2.3. Space-time

One of the biggest challenges of CPS is not space-time in general, representing events at certain times in space, but rather how they are conceived by the number of varying systems. In a CPS with heterogeneous systems, there can be three different problems: synchronicity, frequency, and granularity. Synchronicity can be a problem if we consider a sine wave where two sensors measure the system with a frequency of but are off by a certain time. This would result in completely contrary measurements. In a similar fashion, frequencies are problematic when results should be compared or combined and hence need to be considered explicitly. Granularity refers to how well the environment can be sensed. If fine granular sensors are combined with coarse granular sensors, a mechanism has to be devised in order to achieve meaningful results. While this can be solved manually for two arbitrary sensors, however, given the large number of sensors in a CPS, this needs to be automated. Hence, each device has to be aware of its own sensors capabilities.

2.4. Uncertainty

In CPS, multiple systems are combined to form a larger system, operating in the real environment. This requires the CPS to deal with the inherent uncertainty of this environment coming about two main reasons. First, the CPS only has partial knowledge of its environment. This can happen either due to insufficient distribution of sensors, the frequency of the sensing units not being high enough, or the granularity not being sufficient in order to sense an event. Second, the CPS only has limited resources to observe the environment. This means, events might have been disregarded as to conserve resources. This ranges from conceptual models on how to deal with uncertainty [8] to approaches on how to use the available information to overcome the obstacles of uncertainty [9, 10].

2.5. Safety

While the safety of a CPS might be achieved through the sheer number of sub-systems involved, developers have to consider techniques to ensure safety of the system in case important sub-systems fail during runtime [11]. This can be achieved through self-healing processes and autonomous integration of new systems in the CPS. This capability will inevitably lead towards emergent behavior---behavior the designer of the system has not originally intended but is a result of its capabilities and interactions. On how to detect and control such a behavior, especially when it is not beneficial for the user, is a very hard challenge that needs to be solved. However, the interplay between guaranteeing safety and ensuring security of the system is an important aspect to be considered CPS [12].

2.6. Security

In large-scale cyber-physical systems, the gathered information needs to be secured on all levels. Weather it is on the sensor level monitoring the general environment or personalized sensors (e.g. heart rate) but also on the network level, where data is exchanged among sensors and aggregation nodes up to the cloud storage. The system has to guarantee that no unauthorized person is able to access the devices or the generated data. This is of particular importance when devices or machines in direct interaction with humans. Having insufficient security may give access to unauthorized persons which may cause not only financial but also human damage [13, 14].

2.7. Privacy

Similar to security, privacy is a big issue in upcoming cyber-physical systems. If personalized data is exchanged among multiple sensor nodes or aggregated for further analysis, it has to be impossible to map the gathered data to a specific person. While in many situations, it is important to be able to map information to a specific person, in a cyber-physical system this may only happen in an anonymized fashion. There is a lot of ongoing research tackling the different problems and issues arising with shared information and privacy in IoT and CPS [15, 16, 17].

2.8. Smartness

Having large number of sensors and actuators in single cyber-physical system, inevitably requires the individual devices to feature some kind of smartness. Having such large number of devices in the near future requires us to develop approaches which allow the individual devices operate autonomously without the interaction of an operator. This includes self-localization, self-organization, self-identification, self-configuration, self-healing, self-optimization, and self-aware capabilities [18, 19, 20, 21]. While the individual device may only have very limited capabilities, in combination with other devices the system is expected to exhibit a more rational behavior.

These capabilities may reach from simple discovery and self-localization mechanisms to more complex such as learning, information exchange and integration/aggregation, and self-adaptation mechanisms to deal with changing environments.

Additionally, we consider the large number of devices introducing different levels of smartness as a benefit as different situation might require different capabilities. The heterogeneous mix of abilities allows to cope with different problems and select the most appropriate ones for the given situation without wasting resources by too powerful approaches [22]. In this respect, there is a lot to learn from biology, and we have made huge strides in this direction.

3. Discussion

Cyber-physical systems will be ever-present in our environment in the near future. While the initial systems are already deployed, we still have quite a long way to go until we can unleash its full potential.

The Cyber-Physical Systems group at the Vienna University of Technology is laying out the foundation for cyber-physical systems. The main focus of the group is on the specification, design, analysis, and monitoring and control of the behaviors of such systems. To specify emergent behavior combinations of ideas from spatial-temporal logics and signal processing are used [23, 24]. The design of generic architectural frameworks is based on probabilistic hybrid systems. The development of novel hardware/software system design processes are supported by automatic formal methods on model checking and recent advances on machine learning techniques [25, 26]. When analyzing a system's behavior symbolic as well as stochastic model checking approaches and techniques for adaptive verification at runtime are employed [27, 23, 28]. Using information from the analysis process, different control strategies, such as simple PID, biological-inspired, supervisory or optimal control, are applied to guide the systems behavior efficiently towards its goals [29]. The international impact of the Cyber-Physical Systems group on science and technology is documented by a large number of national and international projects such as Cyber Heart (USA-NSF) [24], ARRiVE (USA-AFOSR) [27], EMC2 (EU Artemis-JU, AT-FFG) [30], AMADEOS (EU-FP7) [29], Harmonia (AT-FFG) [28], or RiSE (AT-FWF) [25], among others [31].

The CPS/IoT paradigm will without any doubt lead to a much higher productivity, will lead for all of us to a better health, and to a cleaner environment, through its continuous monitoring and advanced techniques to disposed residues. Moreover, many of our routine tasks are going to be automated, which will give us more time for our family, more time for ourselves, more time for our elderly, more time for vacation, and more flexibility in conceiving our own work. However, this will be only possible, if our knowledge and capabilities will be continuously enhanced (note that we are infinitely more intelligent and adaptive than our most advanced intelligent agents), and this will require more learning. In fact, we will be required to learn all our life.

References

[1] M. Weiser, "The Computer for the 21st Century," Scientific America, pp. 94-104, 1991.

[2] E. A. Lee, "Cyber Physical Systems: Design Challenges," in International Sysmposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008.

[3] W. Wolf, "Cyber-physical Systems," IEEE Computer, pp. 88 - 89, 2009.

[4] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, "Cyber-physical systems: the next computing revolution," in Design Automation Conference (DAC), 2010.

[5] A. General Electric, "Industrial Internet Insights Report for 2015," Online: http://www.ge.com/digital/sites/default/files/industrial-internet-insights-report.pdf, 2015.

[6] S. Bensalem, K. Goossens, C. Kirsch, R. Obermaisser, E. A. Lee and S. J., "Time-predictable and composable architectures for dependable embedded systems," in International Conference on Embedded software., 2011.

[7] J. Lee, B. Bagheri and H.-A. Kao, "Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," Manufacturing Letters, pp. 18 - 23, 2015.

[8] M. Zhang, B. Selic, S. Ali, T. Yue, O. Okariz and R. Norgren, "Understanding Uncertainty in Cyber-Physical Systems: A Conceptual Model," in European Conference on Modelling Foundations and Applications, 2016.

[9] E. Bartocci and R. Grosu, "Monitoring with Uncertainty," ArXive. arXiv:1308.5329, 2013.

[10] E. Bartocci, R. Grosu, A. Karmarkar, S. A. Smolka, S. D. Stoller, E. Zadok and J. Seyster, "Adaptive Runtime Verification," in International Conference on Runtime Verification: Revised Selected Papers, Springer, 2013, pp. 168 - 182.

[11] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems," Proceedings of the IEEE, pp. 283 - 299, 2012.

[12] M. Sun, S. Mohan, L. Sha and C. Gunter, "Addressing safety and security contradictions in cyber-physical systems," in Workshop on Future Directions in Cyber-Physical Systems Security, 2009.

[13] K. K. Venkatasubramanian, S. Nabar, S. K. Gupta and R. Poovendran, "Cyber physical security solutions for pervasive health monitoring systems," Information Resources Management Association. User-Driven Healthcare: Concepts, Methodologies, Tools, and Applications, 2013.

[14] G. Loukas, Cyber-physical attacks: A growing invisible threat, Butterworth-Heinemann, 2015.

[15] D. Kozlov, J. Veijalainen and Y. Ali, "Security and privacy threats in IoT architectures," in International Conference on Body Area Networks, 2012.

[16] R. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, pp. 23 - 30, 2010.

[17] C. Medaglia and A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," in The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer, 2010, pp. 289 - 395.

[18] J. O. Kephart and D. Chess, "The vision of autonomic computing," IEEE Computer, pp. 41 - 50, 2003.

[19] R. P. Würtz (Ed.), Organic computing, Springer, 2008.

[20] C. Müller-Schloer, H. Schmeck, and T. Ungerer (Eds.), Organic computing—A paradigm shift for complex systems, Springer, 2011.

[21] P. Lewis, M. Platzner, B. Rinner, J. Tørresen, and X. Yao (Eds.), Self-aware Computing Systems: An Engineering Approach, Springer, 2016.

[22] L. Esterle, J. Simonjan, G. Nebehay, R. Pflugfelder, G. Domínguez and B. Rinner, "Self-aware Object Tracking in Multi-Camera Networks," in Self-aware Computing Systems: An Engineering Approach, Springer, 2016, pp. 261 - 278.

[23] "LogiCS (funded by AT-FWF)," 2016. [Online]. Available: http://logic-cs.at/phd/. [Accessed 9 2016].

[24] "CyberHeart (funded by USA-NSF)," 2016. [Online]. Available: http://cyberheart.cs.stonybrook.edu/. [Accessed 9 2016].

[25] "RiSE (funded by AT-FWF)," 2016. [Online]. Available: http://arise.or.at/. [Accessed 9 2016].

[26] "Industry 4.0 (funded by AT-Infineon)," 2016. [Online]. Available: http://ti.tuwien.ac.at/cps/research/projects. [Accessed 9 2016].

[27] "ARRiVE (funded by USA-AFOSR)," August 2016. [Online]. Available: http://arrive.cs.stonybrook.edu/. [Accessed 9 2016].

[28] "HARMONIA (funded by AT-FFG)," 2016. [Online]. Available: http://harmonia.vmars.tuwien.ac.at/. [Accessed 9 2016].

[29] "AMADEOS (funded by EU-FP7)," 2015. [Online]. Available: http://amadeos-project.eu/. [Accessed 9 2016].

[30] "EMC2 (funded by EU-ARTEMIS-JU, AT-FFG)," 2014. [Online]. Available: http://www.artemis-emc2.eu/. [Accessed 9 2016].

[31] "Projects of the Cyber-Physical Systems Group at TU Vienna," 2016. [Online]. Available: http://ti.tuwien.ac.at/cps/research/projects. [Accessed 9 2016].