Book Section:
Abiri Jahromi, A and Kundur, D (2020) Fundamentals of Cyber-Physical Systems. In: Anumba, CJ and Roofigari-Esfahan, N, (eds.) Cyber-Physical Systems in the Built Environment. Springer . ISBN 978-3-030-41559-4

https://doi.org/10.1007/978-3-030-41560-0_1

Chapter 1

Fundamentals of Cyber-Physical Systems

Amir Abiri Jahromi and Deepa Kundur

1.1. Introduction

Cyber-physical systems are permeating practical application to become an integral part of manufacturing, healthcare, agriculture, transportation, energy systems, financial systems, defense and smart infrastructure amongst other application spaces. It is expected that cyber-physical systems in 21st century gener-ate comparable innovation and drive for economic productivity and growth to the Internet revolution of the late 20th century. This is while educational and training programs, large scale testbeds, and skilled workforces are in short supply and are expected to remain a major challenge to innovation, develop-ment and adoption over the next decade.

The concept of cyber-physical systems (CPS) was first established over a decade ago as a next technological step in engineering. As such its evolution has arisen from multiple foundations resulting in a family of systems that have the potential to provide remarkable solution for traditional, contemporary and emerging areas of societal need.

A CPS essentially involves the integration of two subsystems: a computationally based subsystem involving sensors, communication infrastructure and computational elements and a physical one with components particular to the application context. For example, in power grid applications this would include electricity generation and transmission infrastructure, in transportation systems this could include power train and chassis control, in robotics applications it would include the motor units, gear box and arms. The cyber component represents, in some sense, the overall "central nervous system" of the CPS. It provides the "smarts" of the system essentially enhancing the operation of the physical system. A simple design mantra for CPS can be stated as *knowledge is power*. What distinguishes CPS is that the integration between the cyber and physical is considered tight. That is, these subsystems must intelligently work together and coordinate seamlessly.

This tight integration is aimed to facilitate attractive system properties including adaptability, autonomy, efficiency, functionality, reliability, safety and usability. Depending on the application and resources available, these properties are prioritized to different degrees. For example, in critical infrastructure, reliability and safety are of primary importance and in manufacturing, functionality may be a significant concern.

Figure 1.1 illustrates how the coupling of the cyber and physical components typically occur. The physical subsystem is comprised of components that are naturally linked physically. Often, they may be considered legacy system components of the original physical system prior to "cyber-enablement." The cyber subsystem is comprised of elements that are connected as well for the purpose of information flow. These could be through physical means such as two sensors connected through a physical communication wire or virtually through a wireless channel. In the physical and cyber subsystems, they are each individually coupled functionally as illustrated; typically, a graph-based model is effective in representing the connectivity.

The integration of the cyber and physical elements occurs at the *cyber-physical bridge*. Here, the physical-to-cyber link occurs at the sensors that convert observable and measurable physical quantities to data. The cyber-to-physical link occurs at the interface of actuation whereby information is processed to come up with decisions used to make physical change in the physical system. For example, this could be a storage device in a power system that employs information to decide if power should be absorbed or emitted for power grid stabilization. CPS can vary significantly in scale. The emerging trend is in the development of large-scale distributed networked systems.

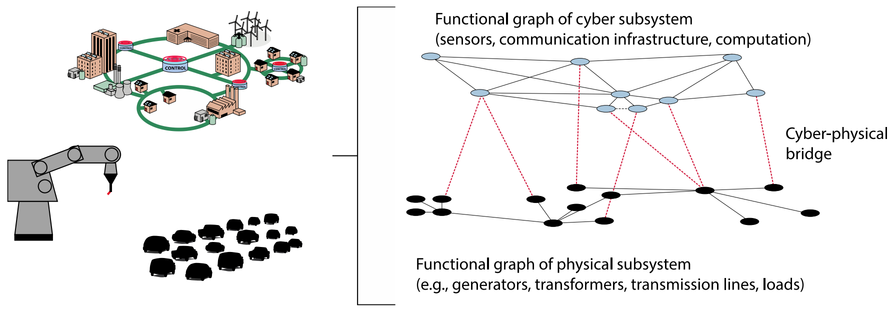

Fig. 1.1. Cyber-physical system description.

1.2. Cyber-Physical Systems Characteristics

CPS are safe and interoperable smart networked systems with distributed and deeply integrated cyber and physical components including sensing, control, processing and computing, communication and actuating elements that are capable of interacting with physical world and human users in real-time [NSF (2013); Schätz et al (2015); NIST (2013a)]. A cyber-physical system can be a small and local system such as a building management system or a highly connected, complex, and large system integrated over several domains such as a city-scale autonomous transportation system or a smart electric grid which is spanned over a continent.

The sensing, actuating and human-interactive features of CPS in combination with their highly distributed and networked intelligence and computational power have the potential to significantly increase efficiency, flexibility, and autonomy while improving the situational awareness, robustness and resiliency of the present systems that are loosely coupled or manually operated [National Academies of Sciences, Engineering, and Medicine (2016)]. Yet, safety, security and reliability remains the top priority for CPS given the integral role that CPS plays in mission oriented and safety-critical systems like transportation systems and healthcare. CPS are closely related to other fields including embedded systems, robotics, Internet-of-things, and big data [National Academies of Sciences, Engineering, and Medicine (2016)].

Embedded Systems: The field of embedded systems is focused on the integration of cyber elements such as processors and software to purely electrical and mechanical systems to perform a specific task. The generalization of the concept of embedded systems to perform multi-tasking in real-time through the integration of distributed sensing, computation, control, and actuation over a communication network has led to the notion of CPS.

Robotics: The field of robotics is focused on the seamless integration of sensors, actuators, processors and control to perform a task autonomously or semi-autonomously. Although similar elements are present in both fields of robotics and CPS, the strong emphasis on distributed sensing, processing, control, actuation and networking is a distinguishing feature of a cyber-physical system.

Internet-of-things: Internet-of-things is focused on dynamic communication network infrastructure with standard interoperable protocols that autonomously communicate data amongst entities with well-defined and unique identifiers. These entities include physical equipment, virtual elements, computing devices and human users. In contrast to CPS, the concept of Internet-of-things does not place emphasis on the aspects of control or regulation, computational power and human-machine interaction.

Big data: The field of big data is focused on the systematic analysis, storage, and visualization of a large volume of data. Although the field of big data has applications in CPS, its focus is limited in comparison to CPS and does not address the limitations of CPS for data management and analysis.

1.3. Drivers for the Development of Cyber-Physical Systems

The main drivers for the development of CPS include security, economic competitiveness, societal needs and technical drivers [NIST (2013b)]. As the cost of sensing, control, processing and computing, communication and information technologies continue to drop and the levels of connectivity between systems continue to grow, the vulnerability of systems and the number of attacks and intrusions is expected to grow. Thus, it is expected that the expense of security consume significant share of expenditures in all sectors. In this environment, security will be the main motivation for the development and adoption of trustworthy, cyber-resilient, safe and reliable CPS.

The higher levels of consumer demand and the need for improved efficiency will generate an economic competitive driving force for innovation, development, and adoption of CPS. As the interoperability, modularity and high functionality of CPS combined with their safety, security and reliability advances and become more evident, their application in all sectors become more prevalent. Deregulation of electricity markets is a prime example where the need for higher levels of efficiency and competitiveness became a motivation for innovation and development of smart grid concept. Growing competitiveness of businesses in combination with the increased deployment of cost-effective sensing, processing, information and communication technologies is also a major incentive for pushing forward the innovation in CPS and shaping the future deployment and adoption of these systems in all sectors.

The endeavor for improving life quality and standard is another driving force for innovation and development of CPS. CPS play a key role in domains that involve human interaction and cover both societal and technical aspects. Moreover, cyber-physical technologies are capable of performing tasks that are either dangerous or difficult for humans and significantly reduce accidents caused by human error. For example, it is expected that the application of CPS grow dramatically in sectors like transportation, healthcare, and mining as they become more affordable.

The need for improved reliability, reduced installation costs, automation, seamless human-machine interaction and higher levels of connectivity and remote access in industry is another reason for innovation and development of CPS. CPS provides an advanced platform for flexible, adaptive and autonomous systems that are compatible with heterogonous systems containing legacy systems and human users.

1.4. Applications of Cyber-Physical Systems

CPS are used for various applications in different sectors including manufacturing, transportation, energy, agriculture, smart buildings/structures, emergency response, defense and healthcare. This section briefly discusses the application of CPS in these sectors. A more detailed overview of CPS applications in industries other than the built environment will be provided in Chapter 3.

Manufacturing: CPS will play a vital role in keeping up with fast-changing and complex needs of consumers by providing smart, flexible and networked manufacturing production lines. The smartness, flexibility and connectivity of CPS also reduces the lead times required for changing the size and production level of manufacturing systems. In the present global market place, it is imperative for manufacturing industries to rely on CPS in order to maintain their economic competitiveness [Monostori et al (2016)].

Transportation: CPS can significantly reduce air and vehicle traffic and improve public transportation system by introducing smarter traffic control mechanisms and intelligent/autonomous transportation systems. Moreover, CPS can eliminate accidents caused by human error by improving the autonomy and intelligence of transportation systems [Deka et al (2018)].

Energy: CPS play a vital role in realizing smart energy systems for a sustainable future. CPS with their connectivity, smartness, interoperability, flexibility and self-healing properties can provide a platform to improve efficiency, sustainability and resiliency in energy sector. Moreover, the interdependency of different energy sectors like gas and electricity on other related infrastructures such as transportation, water and telecommunications highlights the critical role that CPS can play in energy security. For example, the massive integration of renewable energy resources like wind and solar, electrification of road transportation, and continuously aging power system legacy assets coupled with more frequent natural disasters and possibility of cyber-physical attacks demand higher levels of situational awareness, autonomy, adaptability, flexibility, resiliency and self-healing properties in the electric energy systems which is achievable through CPS [Kezunovic et al (2016)].

Agriculture: Climate change and higher needs for agricultural products due to growing population is expected to become a major challenge in the following decades. CPS will play a key role in addressing the pressing need for smarter, more efficient and sustainable supply chain of agricultural products while providing opportunities for higher levels of productivity.

Smart buildings/structures: Building management systems are becoming smarter and connected with external infrastructures such as first responders and law enforcement. Moreover, structures like bridges, highways and tunnels use different sensors to improve sustainability and resiliency as well as safety and reliability. CPS in smart buildings can significantly improve energy efficiency by measuring different quantities like temperature, occupancy, light intensity and humidity in real-time and adjusting energy consumption. Moreover, CPS can play a vital role in improving the security of building management systems [Schmidt and Ahlund (2018)].

Emergency Response: Climate change has already resulted in more frequent natural disasters such as hurricanes, tornados and wild fires. CPS can significantly improve situational awareness and support first responders during natural disasters through their sensor networks, surveillance systems, intelligence, automation and robotics [Zander et al (2015)].

Defense: Defense systems are becoming more reliant on complex, adaptable and autonomous CPS such as unmanned aerial vehicles, robotics and surveillance systems for meeting the military and national defense needs to reduce the human involvement. Moreover, cyberwarfares which rely of CPS has become an important part of offensive and defensive operations.

Healthcare: CPS are becoming prevalent in medical devices like artificial pancreas since they can autonomously monitor and react to abnormal body conditions. Moreover, CPS are expected to play a vital role in providing supporting systems for elderly people, people with disabilities and patients that need 24/7 care [NITRD (2009)].

1.5. Evolution of Cyber-Physical Systems

The transformation of purely electrical and/or mechanical engineering systems with physical implementation of sensing, actuating, control, and decision making to physical systems with cyber elements in the form of sensors, processors and software resulted in the emergence of embedded systems which are designed for a specific purpose. Afterwards, the need for the development of networked and multi-purpose monitoring, surveillance, and control systems in various applications including defense, energy systems, transportation systems, healthcare, and first responders resulted in the emergence of sensor networks and secure networked control systems. The notion of CPS is then developed and emerged out of the generalization of the concept of embedded systems and by parallel contributions from the fields of sensor networks, embedded systems and secure networked control systems. CPS are realized by the seamless and secure integration of a spatially distributed and networked sensors, actuators, computing devices, and feedback control systems that are interacting with each other, the physical world and human users over a communication network in real-time.

1.5.1. Foundations of Cyber-Physical Systems

- **Sensor Networks**

Sensors connect the physical world with the cyber world by converting the real-world phenomena into signals that can be processed, stored, visualized and acted upon in the cyber world. Therefore, they can be integrated into many devices and used in numerous applications. The rapid advancements in the design of low-power, and inexpensive sensors have contributed to the emergence of distributed sensor networks (DSNs) over the past decade.

DSNs are comprised of low-cost unattended groups of densely placed sensor "nodes" that observe, communicate (often using wireless means), and coordinate to collectively achieve high-level inference tasks. DSNs represent a conceptual shift in the way humans and machines monitor, and interact with the physical environment and have found a wide range of applications including surveillance, safety, condition monitoring, and process automation. For example, DSNs can be employed to monitor and protect civil infrastructure such as bridges and tunnels by collecting structural health information using spatially distributed vibration sensors.

The spatially distributed and collaborative nature of DSNs introduces several challenges and benefits. The challenges facing the development and adoption of DSNs include safety, security, real-time performance and energy consumption as well as availability, reliability and robustness in harsh environments. The major benefits associated with DSNs include cost effectiveness, flexibility, efficiency, autonomy, redundancy and distributed nature. The DSNs can be considered as the first building block of CPS which provides a cost-effective, flexible, and reliable platform for monitoring and interacting with physical world in real-time.

- **Embedded Systems**

Embedded systems can be broadly defined as devices that contain tightly coupled physical (mechanical and/or electrical) and cyber (processor and software) components to perform a specific task. Most of embedded systems operate in constrained environments and interact with physical world in real-time which imposes limitations on available resources like memory size, processing power and power consumption.

Embedded systems are present in almost all the devices around us like microwave oven, refrigerator, dishwasher, printers and even our watch just to name a few. In CPS, distributed embedded systems perform multiple tasks in a coordinated and collaborative way in real-time. Although embedded systems form the computational foundation for CPS, the need for distributed, coordinated and collaborative computations in real-time create challenges that are specific to CPS such as the need for asynchronous computational models. The challenges facing the transformation of embedded systems to CPS are discussed in the Section on distinguishing features of CPS.

- **Secure Networked Control Systems**

The rapid deployment of distributed sensors, actuators, communication networks and processors in control systems resulted in the emergence of networked control systems. Networked control systems are central or distributed control systems that exchange information with distributed sensors and actuators over communication networks. In comparison to traditional control systems, networked control systems provide several benefits including reduced costs, improved flexibility, reliability and interoperability. Yet, the uncertainty in the integrity of data received from distributed sensors and commands transmitted to actuators as well as the potential unavailability of communication networks introduces new challenges for the design of networked control systems. For example, the unavailability of the feedback loop signals due to communication channel loss may cause instability problems for control systems with drastic consequences.

The efforts to address these challenges resulted in the emergence of the secure networked control systems. The field of secure networked control systems is concerned with the design of control systems that can survive conditions where the availability and integrity of data is compromised [Cardenas (2008)]. The design of distributed, secure, robust, and fault-tolerant control systems form the foundation of secure networked control systems which are necessary for the development of CPS.

1.5.2. Principles of Cyber-Physical Systems

CPS consists of physical, cyber and control/decision making elements. The physical elements in CPS refer to the electrical and mechanical components as well as the physical world that CPS is interacting with in real-time. The physical elements follow the principles of the physical world which includes physics, mathematics and mathematical modeling, probability, statistics and stochastic processes, logic, linear algebra and analysis. The cyber elements in CPS refer to the software, data structures, databases and networks as well as the processors and computational devices. The cyber elements follow the principles of computer engineering and computer science which includes software programming, computational hardware, processors and embedded computation, and networking. The control/decision making elements refer to cyber and physical elements that process and monitor incoming information from sensors and commands the actuators to perform various tasks through feedback control loops. The control and decision making elements follow the principles of control theory, adaptive and robust control, distributed and fault-tolerant control, stability, optimization, hybrid systems, digital and real-time systems [National Academies of Sciences, Engineering, and Medicine (2016)].

1.5.3. Distinguishing Features of Cyber-Physical Systems

CPS are founded by bridging the cyber and physical elements including distributed sensing, communication, computing, control and actuation elements which are interacting with physical world and human users in real-time. Accordingly, CPS demand distinguishing features as follows [National Academies of Sciences, Engineering, and Medicine (2016)].

- **Advanced Computational Models and Concepts**

CPS rely on distributed sensor networks that provide variable number of inputs about changing physical environment and human user needs in real-time and demand adaptive control and decision making and variable number of outputs. This characteristic demands novel computational models that are different in two respects from classical computational models.

First, computational models with adaptive and variable number of inputs/outputs are essential for CPS. For example, consider time-varying number of electric vehicles at a charging station that should negotiate and decide how to charge/discharge their batteries depending on the need of their users and the availability of power from the electric grid. In this scenario, the electric vehicle charger receives input signals from various number of agents including the electric vehicle owner and should make correct decisions about charging/discharging of the battery. Another example is a set of autonomous vehicles that should change their speed depending on the traffic status and passenger needs. This is in complete contrast to the classical computational models where models are developed based on fixed and known number of inputs/outputs.

Second, distributed, and collaborative computational models are required that are coordinated in a synchronous or asynchronous fashion. In classical computational models, the computations are performed sequentially. In contrast, in CPS distributed and variable number of processors perform computations and communicate data collaboratively which can be coordinated in a synchronous or asynchronous fashion depending on the application. In synchronous computational models, the processors work in harmony and exchange messages in synchronized rounds. This is while, the processors in asynchronous computational models work at independent speeds and exchange messages on an as-needed basis. In both examples of electric vehicles and autonomous vehicles asynchronous computational models are required where each vehicle optimizes its objective and exchanges information with other vehicles on an as-needed basis.

- **Discrete and Continuous Mathematics and Modeling**

An important difference between CPS and classical systems is that both discrete and continuous mathematics and modeling are needed for CPS. Such systems which require both discrete and continuous modeling and mathematics are called hybrid systems. For instance, cyber elements in CPS follow event-driven models and discrete time mathematics while physical elements follow continuous time evolving models and continuous time mathematics. Thus, the knowledge about the integration of discrete and continuous models and mathematics are critical. This is while either continuous or discrete mathematics and modeling is used in classical systems. Smart grids are prime examples of CPS where communication networks and power systems constitute the cyber and physical elements which respectively function based on discrete and continuous modeling and mathematics.

- **Real-Time Computing for PhysicalWorld**

The real-time characteristic of CPS distinguishes them from conventional systems. In a real-time system the accuracy and correctness of the system behavior depends not only on the correctness and accuracy of the results, but also on the time instant at which these results are available to be applied. As such, specific operating systems, computing architectures, and programming languages are required with the ability to address the requirements of CPS for real-time computing. Moreover, sophisticated models should be developed with the ability to predict and consider time delays while performing real-time control and decision making. For example, autonomous vehicles need to recognize the boundaries of the road, distance from different objects and adjust the speed accordingly while taking into account the time delays for receiving and processing data from sensors, as well as necessary time for computations and communication of commands to actuators.

- **Interaction with Physical World**

Interactions of CPS with physical world imposes complex design constraints on all elements of these systems. For example, type of sensors, processors, control systems, communication networks, and actuators that can be used will be imposed by the characteristics of the physical world that CPS interacts with. Moreover, other factors such as memory size, processing power and power consumption as well as redundancy and fault tolerance of elements may become decisive depending on the physical world constraints and cause unpredictable failures. This feature highlights the need for various testbeds to examine the CPS design requirements in a safe and controlled environment which is discussed next.

- **Safety-Critical Applications**

Testing, validation and certification for systems and devices whose failure do not result in serious consequences are normally performed at the final stage before deployment. This is while most of CPS are safety-critical systems whose failure could result in loss of life, significant property damage or damage to the environment. Thus, their safety, reliability and security has higher priority over other objectives such as cost and performance. The safety-critical applications of CPS in sectors like healthcare, transportation, and defense demand novel testing, validation and certification procedures and testbeds from planning to deployment stage including design, assembly, implementation, and delivery stages.

- **Cross-Cutting Technologies**

CPS are underpinned by cross-cutting technologies that facilitate the following characteristics.

- Abstractions, modularity, and composability
- Standard and interoperable
- Adaptable and predictable
- Hierarchical and secure networked control and decision making
- Distributed sensing, communications, control and actuation
- Redundancy, resilience, survivability and self-healing properties
- Novel testing, validation, and certification mechanisms,
- Autonomy and human interaction
- Cybersecurity
- Resource constrained

1.6. Challenges and Opportunities

1.6.1. Challenges

The major challenges facing innovation, development and adoption of CPS can be classified into technological, educational and legal challenges [Schätz et al (2015); National Academies of Sciences, Engineering, and Medicine (2016)].

- **Technological Challenges**

The technological challenges partly stem from the distinguishing features of CPS compared to classical systems. For example, technological advancements are required for the development of distributed, interoperable, autonomous and reliable systems that can protect safety, privacy, dependability and cybersecurity of CPS.

The development of interoperable systems with certain level of modularity, and composability that can be combined and integrated with legacy systems has been initiated in industry a decade ago but it is still at the embryonic stage in terms of deployment, testing and validation. In addition, the safety and reliability concerns are still the main barriers in front of the adoption of autonomous systems in different sectors. Considering the volume of data that will be generated, gathered and processed by CPS, development of various mechanisms for protecting the data privacy is another technological challenge that should be addressed properly. Lastly, cybersecurity is the most important technological challenge that must be addressed while designing CPS considering the critical role that they play in safety-critical systems like defense and transportation systems [Schätz et al (2015)].

The other two contributing factors to technological challenges are the economic and scientific aspects. A good share of benefits associated with the CPS may not be quantifiable using classical business models since in many cases they only contribute to facilitating the processes or providing services rather than resulting in a product. Thus, new business models and cost/benetit analysis tools must be developed to justify the investment in CPS. Moreover, considering the transdisciplinary nature of the CPS, innovations in this field require scientific contributions from several domains. Therefore, a body of knowledge with suitable breadth and depth from several domains should be established for modeling, design and implementation of CPS. Finally, socio-technical aspect of CPS play a key role for their adoption in the society which demands a special attention.

- **Educational Challenges**

The skilled workforces, knowledgable experts, professionals and educational trainers with a deep understanding of CPS are in short supply and are expected to remain as a major challenge in front of innovation, development and adoption of CPS at least over the next decade. This is mainly because the field of CPS requires the integration of knowledge from multiple areas of engineering such as computer science, computing engineering, civil, mechanical or electrical engineering, systems engineering with a right balance between theory and practice. The breadth and depth of knowledge required for innovation and development of CPS makes the education in this field challenging. Therefore, new education/training systems should be designed and implemented based on the requirements of CPS [National Academies of Sciences, Engineering, and Medicine (2016)].

The lack of cyber-physical laboratories and testbeds in educational institutions and industry is another obstacle which hampers the provision of the required education/ training in the field of CPS. Individuals in the field of CPS need access to testbeds with different levels of complexity and integration of physical and cyber components so that they can develop relevant programming, simulation and experimentation skills.

- **Legal Challenges**

The application of the CPS in different sectors demands different legislations and regulations concerning the privacy of data, safety and security of systems and users, and liability as well as testing and certification of CPS. Moreover, considering that CPS may span over different states, provinces or even continents, new legal standards and terms may be needed to specifically address the needs of CPS [Schätz et al (2015)].

1.6.2. Opportunities

CPS improve the efficiency, flexibility, reliability, autonomy and self-healing properties of systems while providing higher levels of situational awareness, robustness, resiliency and interoperability. Moreover, CPS enable better coordination, collaboration and control of large and complex systems. In addition, CPS provide opportunities for higher levels of connectivity and remote access. Finally, CPS provide numerous opportunities for skilled workforce to design, develop and deliver new devices, systems and services.

1.7. Conclusions

Cyber-physical systems are establishing themselves as a critical element of modern engineering systems design. Their multidisciplinary roots have helped to spur on interdisciplinary collaborations and results. Rich innovations exist at the intersection of traditionally siloed fields. As such CPS represent a paradigm shift in the way in which engineering systems are developed in terms of empirical and mathematical modelling, real-time computing, interaction with the physical world and safety. As their technologies become intrinsic to the operation of smart societies, it will become imperative to not only address technological challenges, but those related to shortage of an appropriately trained workforce.

References

Cardenas, A. A., Amin, S. and Sastry, S. (2008). "Secure Control: Towards Survivable Cyber-Physical Systems," 2008 The 28th International Conference on Distributed Computing SystemsWorkshops, pp. 495–500, Beijing, 2008.

Deka, L. , Khan, S., Chowdhury, M., and Ayres, N. (2018). "Transportation Cyber-Physical Systems and its Importance for Future Mobility," *Trans. Cyber-Physical Syst.*, Elsevier, pp. 1–19, 2018.

Kezunovic, M., Annaswamy, A., Dobson, I., Grijalva, S., Kirschen, D., Mitra, J., and Xie, L. (2016). Energy Cyber-Physical Systems: Research Challenges and Opportunities, Report from NSF workshop, Arlington, Virginia, Dec. 2013.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., and Ueda†, K. (2016). Cyber-physical systems in manufacturing, CIRP Annals, Volume 65, Issue 2, 2016, pp: 621-641, Available: https://doi.org/10.1016/j.cirp.2016.06.005

National Academies of Sciences, Engineering, and Medicine (2016). *A 21st Century Cyber-Physical Systems Education*. Washington, DC: The National Academies Press. https://doi.org/10.17226/23686.

National Institute of Standards and Technology (NIST) (2013a). Foundations for Innovation: Strategic R&D Opportunities for 21st Century Cyber-physical Systems: Connecting Computer and Information Systems With the Physical World, Report of the Steering Committee for Foundations in Innovation for cyberphysical systems, National Institute of Standards and Technology, vol. 28, Jan. 2013. Available: https://www.nist.gov/system/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf

National Institute of Standards and Technology (NIST) (2013b). Strategic Vision and Business Drivers for 21st Century Cyber-Physical Systems, Report from the Executive

Roundtable on Cyber-Physical Systems, January 2013. Available: https://www.nist.gov/el/upload/Exec-Roundtable-SumReport-Final-1-30-13.pdf.

National Science Foundation (NSF) (2013). Cyber Physical Systems NSF10515, Arlington, VA, USA, 2013. [Online]. Available: https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm.

Networking and Information Technology Research and Development (NITRD) (2009). High Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care, 2009. Available: https://www.nitrd.gov/About/MedDevice-FINAL1-web.pdf.

Schätz, B., Törngren, M., Passerone, R., Bensalem, S., Sangiovanni-Vincentelli, A., McDermid, J., Pfeifer, H., and Cengarle, M. (2015). Cyber-pHysical European Roadmap & Strategy -- Research Agenda and Recommendations for Action, produced by the CyPhERS project, March 2015, www.cyphers.eu. [Online]. Available: https://cyphers.eu/sites/default/files/d6.1+2-report.pdf.

Schmidt, M. and Ahlund, C. (2018). "Smart buildings as cyber-physical systems: Data-driven predictive control strategies for energy efficiency," *Renewable and Sustainable Energy Reviews*, vol. 90, pp. 742–756, 2018.

Zander, J., Mosterman, P., Padir, T., Wan, Y. and Fu, S. (2015). "Cyber-physical Systems can Make Emergency Response Smart", *Procedia Engineering*, vol. 107, pp. 312–318, 2015.