A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems

Volkan Gunes[1], Steffen Peter[1], Tony Givargis[1], and Frank Vahid[2]
[1] Center for Embedded Computer Systems, University of California
Irvine, CA 92697 - USA
[e-mail: {vgunes, st.peter, givargis}@uci.edu]
[2] Dept. of Computer Science and Engineering, University of California
Riverside, CA 92521 - USA
[e-mail: vahid@cs.ucr.edu]
*Corresponding author: Volkan Gunes

Received June 25, 2014; revised September 29, 2014; accepted October 29, 2014; published December 31, 2014

Abstract

The Cyber-Physical System (CPS) is a term describing a broad range of complex, multi-disciplinary, physically-aware next generation engineered system that integrates embedded computing technologies (cyber part) into the physical world. In order to define and understand CPS more precisely, this article presents a detailed survey of the related work, discussing the origin of CPS, the relations to other research fields, prevalent concepts, and practical applications. Further, this article enumerates an extensive set of technical challenges and uses specific applications to elaborate and provide insight into each specific concept. CPS is a very broad research area and therefore has diverse applications spanning different scales. Additionally, the next generation technologies are expected to play an important role on CPS research. All of CPS applications need to be designed considering the cutting-edge technologies, necessary system-level requirements, and overall impact on the real world.

Keywords: Cyber-Physical Systems, Embedded Computing Technologies, Physically-aware Engineered Systems, Model-Based Design, System-Level Requirements.

This work was supported in part by the National Science Foundation under NSF grant number 1016789 and 1136146.

http://dx.doi.org/10.3837/tiis.2014.12.001

1. Introduction and Motivation

Advances in digital electronics have led to a significant increase in the number of systems that couple the digital (cyber) systems with the physical world, namely what have become known as the Cyber-Physical System (CPS). The design of CPS requires a significant amount of reasoning with respect to unique challenges and complex functional, reliability, and performance requirements. A number of articles have addressed necessary problem formulations, system-level requirements, and arising challenges in CPS design. Baheti and Gill [1] introduce CPS concept and suggest research directions for CPS design. Lee [2] specifically points out the failure of standard abstraction layers, the need of reliable timing behavior, and lack of temporal semantics of existing programming language models for CPS design. Rajkumar [3] touches on system level aspects of CPS from the scientific and social impact standpoints. Lee [4] suggests two approaches, namely cyberizing the physical and physicalizing the cyber, for integrating the cyber systems with the physical systems.

A variety of existing surveys describe the holistic view of CPS. Shi [5] gives an outline of CPS features, challenges, and applications without going into the details. Sanislav and Miclea [6] describe CPS specifications, design, and research directions and briefly cover CPS applications and system level requirements. Horvath and Gerritsen [7] touch on CPS characteristics, design technologies (i.e. cyber, physical, and synergic technologies), and implementation principles.

The incentive for us to conduct this survey arises from a lack of unifying concepts, definitions, related terminologies, challenges, and applications. We aim to provide sufficient insight into CPS concepts and common applications. We make the following main contributions in this article. In this survey, we discuss the follwoings:

- CPS history, applications and challenges.
- Concepts similar to CPS.
- A glimpse of CPS application domains and existing efforts in each domain to realize CPS vision.

The rest of this paper is organized as follows. CPS history and definitions are presented in Section 2. CPS terminology and concepts relatively similar to CPS are explained in Section 3. Domains and applications of each domain are introduced in Section 4. CPS challenges are discussed in Section 5. Conclusions are provided in Section 6.

2. CPS History and Definitions

CPS is an emerging area that refers to the next generation engineered systems. The term CPS was coined at the National Science Foundation (NSF) in the United States around 2006 [8]. The CPS approach has been recognized as a paramount and prospective shift towards future networking and information technology (NIT) by the 2007 report of the President's Council of Advisors on Science and Technology (PCAST). PCAST recommends the reorganization of the national priorities in NIT research and development (R&D) and putting CPS at the top of the research agenda [9]. The National Science Foundation (NSF) has increasingly provided funding

opportunities to the scientific community to promote transformative research on CPS [10]. A special interest organization has been set up in the U.S., namely the Cyber-Physical Systems Virtual Organization (CPS-VO), to foster collaboration among CPS professionals in academia, government, and industry [11]. The European Union's joint technology initiative, called Advanced Research and Technology for Embedded Intelligence Systems (ARTEMIS), has invested in research and development (R&D) efforts on the next generation engineered systems with public-private partnership between European Nations and the industry to fulfill the vision of a world in which all systems, machines, and objects become smart and physically-aware, have a presence in the cyber-physical space, exploit the digital information and services around them, and communicate with each other as well as with the environment [12]. Moreover, the European Commission has launched a new research and innovation program, namely Horizon 2020, at the end of 2013 to develop new strategies for tackling societal challenges. Horizon 2020 is the biggest research and innovative program yet with a budget of nearly EUR 80 billion. Horizon2020 covers CPSs and advanced computing research and innovation [13].

CPS has been defined by the scientific community from different perspectives. Rajkumar [3] describes CPSs as "physical and engineered systems, whose operations are monitored, coordinated, controlled, and integrated by a computing and communicating core". Lee [14] describes CPSs as "integrations of computation with physical processes". Marwedel [15] describes them as "embedded systems together with their physical environment". Gill [16] describes them as "physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is deeply embedded into every physical component, possibly even into materials. The computational core is an embedded system, usually demands real-time response, and is most often distributed".

In summary, Cyber-Physical Systems (CPSs) are complex, multi-disciplinary, physically-aware next generation engineered systems that integrate embedded computing technology (cyber part) into the physical phenomena by using transformative research approaches. This integration mainly includes observation, communication, and control aspects of the physical systems from the multi-disciplinary perspective.

3. CPS Terminology and Relatively Similar Concepts

Although CPS is a relatively new concept, the system components are well-known. As shown in **Fig. 1**, CPS is composed of the physical world, interfaces, and cyber systems. The physical world refers to the physical phenomena wanted to be monitored or controlled. The cyber systems refer to the next generation embedded devices, which process information and communicate with their distributed environment. The interfaces refer to the communication network and other intermediate components, e.g. interconnected sensors, actuators, analog-to-digital converters (ADC), and digital-to-analog converters (DAC), responsible for bridging the cyber systems with the physical world. Sensors and actuators are responsible for converting other forms of energy to electricity (analog signal) and vice versa, respectively. ADC and DAC are responsible for converting continues analog signals to discrete digital signals and vice versa, respectively.

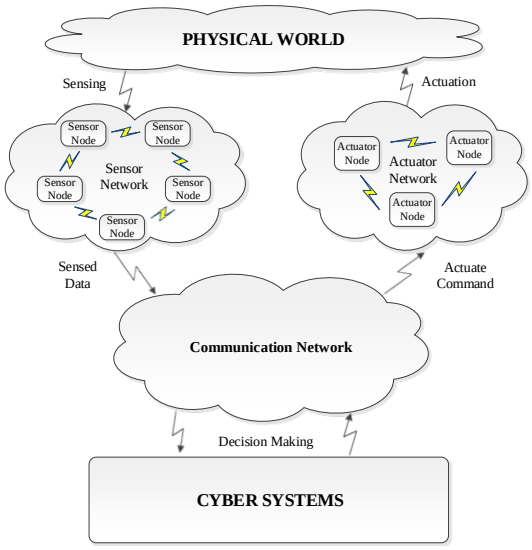

Fig. 1. CPS Holistic View

Resource scheduling in shared sensor and actuator networks (SANs) is a challenging task and plays an important role in CPS operation. In this regard, actuation coordination is essential to decide which actuators must be scheduled to perform a particular action or how to manage control actions properly. Various parameters, such as actuator capabilities, real-time guarantee, task completion time, energy consumption of each actuator, and the physical system requirements must be considered during control task allocation to particular actuator [17].

Regarding actuator scheduling, an important difference of CPSs compared to most cyber systems is the reversibility or preemption of actuator operations. While in most cyber systems, roll-back operations and preemption is available (e.g. databases or bus access protocols), physical operations executed by the actuators typically cannot be reversed. If an actuation is performed based on erroneous data, it is often very challenging or impossible to roll back the activity, as for instance discussed in [18] for specific healthcare applications. Additionally, non-reversibility challenge affects real-time scheduling in the cases where several jobs are managed on a shared platform. Even hard real-time tasks may be blocked by low-priority processes if a shared actuation resource access cannot be preempted or rolled back, as for instance discussed for a satellite communication system [19].

The control aspect of the physical phenomena and the theory behind control systems are the basis for all state-of-the-art continuous time dynamical systems and thus have a crucial role in CPS design. Conventionally, control policies are completely separate from the system infrastructure and implemented after manufacturing the system prototype [20]. Such an approach is not feasible to meet the demands expected from CPSs because of their complex and dynamic nature. To meet those demands and perform complex control laws, the physical system itself and its dependency relationship with those control laws should be well defined and modeled [21].

CPSs must operate in real-time. Real-time control is traditionally implemented through different forms of control mechanisms, namely open loop control, feed-forward control, and

feed-back control. The open loop strategy utilizes only the input signal (desired value) to actuate the output according to the control requirements and lacks a feedback mechanism to adjust the output of the system, therefore expects adjustments manually from the operator [22]. The feed-forward control strategy considers environmental effects measured via sensors over the physical system. Then, the control action is adjusted by the controller according to the anticipation of the relationship between the physical system and its environment [22]. The feed-back (a.k.a. closed loop) control strategy automatically refines the output based on the difference between the feed-back signal from the output and the input signal. Both the physical system and the controller affect each other, hence the name closed loop. All environmental effects (e.g. disturbance) on the physical system are taken into account via the feed-back signal [22]. Since CPS applications incorporate the physical systems/environments, and interact with them through their physical-awareness capability without human intervention, many of them are likely to adopt the feed-forward and the feed-back strategies together at the lowest level.

In case the feedback loop is closed over wireless sensor and actuator networks (WSANs), passivity-based control design can be applied to make the control design insensitive to network uncertainties (e.g. time-varying delays) [23]. Fidelity-aware utilization control, which integrates data fusion with the feedback control, can be adopted in wireless cyber-physical surveillance systems to optimize system fidelity and adaptively adjust the control objective of CPU utilization in the presence of environmental variations (e.g. noise characteristics) [24]. The importance of control theory in CPS design has been addressed by a number of studies [1], [3], [8], [25], [26], [62], [69], [92], [93].

Conventionally, if the feedback control of a system is closed through a shared network, then that system is called a networked control system (NCS), in which the control input/plant output is passed through interconnected system components (such as sensors, controller, and actuators) [27]. Another type of control systems is called SCADA, which stands for supervisory control and data acquisition. These types of control systems are utilized to monitor and control processes, including but not limited to industrial, infrastructure, and facility-based processes that exist in the physical world. A SCADA system gathers data in real time from sensors in local and remote locations and transfers them to the central computers in order to control the equipment/conditions and take necessary actions [28]. CPS entails requirements far beyond the expectation of legacy control systems, such as NCS and SCADA.

Some core concepts in CPS can be traced back to the sensor network research and technologies related to sensor nodes and sensor networks. A sensor node integrates sensors, actuators, computing elements (e.g. processor, memory, etc.), communication modules, and a battery. The sensor network interconnects many small sensor nodes via wireless or wired connection [29]. Called as wireless sensor networks (WSN), a large number of sensor nodes equipped with wireless network connection can be deployed in the environment of the physical phenomenon. Those sensor nodes may provide raw data to the nodes responsible for data fusion or they may process the raw data by means of their computing capabilities and relay the required part of it to the other sensor nodes.

Various research areas and terminologies are relatively similar to CPS. A range of concepts similar to CPS is illustrated in **Fig. 2.** The term Big Data refers to the datasets that are too large and complex to capture, store, manage, and analyze with standard methods or database tools [30]. A large scale CPS can be envisioned as millions of networked smart devices, sensors, and actuators

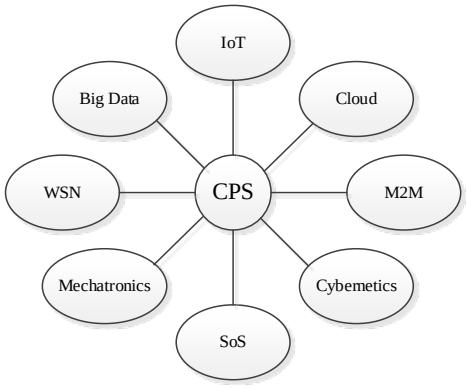

Fig. 2. Similar Concepts

being embedded in the physical world, which can sense, process, and communicate the data all over the network. Proliferation of technology-mediated social interactions via these highly featured and networked smart devices has allowed many individuals to contribute to the size of Big Data available. Depending on the size of data sets and number of smart devices involved, Big Data may be in the range of multiple terabytes to many petabytes (i.e. 1024 terabytes) [31].

Cloud is a paradigm shift in the Information and Communications Technology (ICT), through which businesses and users can have an on-demand network access to a shared pool of configurable computing resources (e.g. hardware, applications, services, etc.) [32], [33]. Cloud computing model promotes broad network access to a pool of resources, optimal usage and control of resources, minimal management effort of hardware and software resources, scalable computing capabilities, and on-demand services without human interaction with service providers [32]. Cloud computing provides new opportunities for CPSs in management and processing of aggregated sensor data and decision making methods based on a cloud model allow CPSs to enhance the system capability.

Systems of Systems (SoS) refers to large-scale, heterogeneous systems networked together for a common goal and composed of inherently autonomous components that can be operated and managed independently [34]. The term has been addressed by the systems engineering community and reflects the interest in large-scale systems that have considerable economical and societal impacts (e.g. critical infrastructures, intelligent transportation, emergency response, etc.) [35].

The term Mechatronics is the combination of “mecha”, referring to mechanical systems, and “tronics”, referring to electronic systems. The term was coined in the late 1960s. However, it has evolved over the decades comprising software and information technologies. Therefore, it can be considered as a systematic approach to design, develop, and implement complex engineering systems which incorporate information technologies into the physical domain [36], [37].

The term Cybernetics refers to an approach describing the study of communication and control characteristics in both machines and in living beings [38]. Broadly speaking, Cybernetics involves the qualitative analysis of the relationship between various system components and whole system behavior [39]. The theory of Cybernetics and the practice of mechatronic system design lay the foundations for the design of CPSs [40].

Inspired by the idea of interconnecting smart devices, the term the Internet of Things (IoT) was coined in 1999. IoT was envisioned as a future radio frequency identification (RFID) technology that enables the automatic identification of the physical objects via a small electronic chip called "RFID tag". IoT provides an opportunity to observe, identify, and understand the real world by capturing data about the things (i.e. RFID tagged objects) and help businesses achieve greater efficiency and accountability [41], [42].

IoT greatly overlaps with CPS, because IoT addresses observing the things in the physical world, exploiting communication capabilities, and capturing data needed to manage the things that aren't efficiently managed today [41], [43]. Even though IoT originally targeted identification and monitoring technologies, today IoT also applies to the control of the physical systems by the integration of RFID systems and Sensor Networks, namely RFID sensor networks [44].

The several important aspects of IoT are surveyed in detail in [45]. The survey includes different perspectives of IoT, revision of enabling technologies with the emphasis on what is being done and what needs to be done for further research. Besides IoT, the idea of interconnecting several heterogeneous CPS under a large-scale universal network (like the Internet) is addressed in [46] and referred to as the Cyber-Physical Internet (CPI).

Inspired by IoT, The Web of Things (WoT) integrates real world objects (things) into the World Wide Web using standard web technologies. In WoT, each physical object that contains an embedded device is identified as a standard Web resource with URI and can be accessed through Web APIs [47]. This provides connectivity of embedded devices at the application layer. A five-layer WoT framework to integrate WoT and CPS is studied in [47], using an intelligent vehicle system as a case study.

Machine-to-Machine (M2M) communication is another concept related to CPS. M2M refers to smart devices, such as computers, embedded processors, smart sensors, actuators, and mobile devices, talking to each other via a communication network [48], [49]. M2M is a communication standard that is a subset of both IoT and CPS. Existing research on M2M communications are surveyed in [50] from architecture, standard development, and representative application perspective. The authors also propose a solution to the integration of intelligent road and unmanned vehicle with wireless sensor networks (WSNs) navigation in the form of CPS. Enabling new business models, both M2M and IoT target data aggregation by offering smart services to customers to improve efficiency and provide automation and low-cost systems in the world of e-commerce [42], [49].

The above mentioned concepts clarify why the National Intelligence Council (NIC) foresees IoT/CPS as one of the six disruptive civil technologies with potential impacts on the U.S. interests [51]. The next generation Internet technologies are expected to play an important role on both IoT and CPS research. Therefore, how we interact with the real world will probably be revolutionized just like the traditional Internet revolutionized how we interact with one another [3], [52].

4. Domains and Applications

Various studies have addressed the domains and domain specific applications of CPS. In this section, we summarize a number of research efforts that address some of those domains, namely smart manufacturing, emergency response, air transportation, critical infrastructure, health care and medicine, intelligent transportation, and robotic for service. With this summary, we aim to cite

a few of the recent research efforts from CPS perspective for each application domain. **Table 1** provides an overview on the CPS applications according to their functionality. More details on the CPS applications are given in the following subsections.

Table 1. Functionality of CPS Domains

Type of Domain	Scale/Functionality
Smart Manufacturing	Medium Scale; optimizing productivity in the manufacture of goods or delivery of services.
Emergency Response	Medium/Large Scale; handling the threats against public safety, and protecting nature and valuable infrastructures.
Air Transportation	Large Scale; operation and traffic management of aircraft systems.
Critical Infrastructure	Large Scale; distribution of daily life supplies such as water, electricity, gas, oil.
Health Care and Medicine	Medium Scale; monitoring health conditions of the patients and taking necessary actions.
Intelligent Transportation	Medium/Large Scale; improving safety, coordination and services in traffic management with real-time info sharing.
Robotic for Service	Small/Medium Scale; performing services for the welfare of humans.

4.1 Smart Manufacturing (SM)

Smart manufacturing refers to the use of embedded software and hardware technologies to optimize productivity in the manufacture of goods or delivery of services [53]. Smart factory is another frequently mentioned concept to refer to the next generation smart manufacturing.

Smart manufacturing is one of the leading CPS application domains because of drivers like mass production, domestic and international marketing, economic growth, etc. A large effort on characterizing CPS for smart manufacturing has been undertaken in Europe and the U.S. The Industrie 4.0 project is a German strategic initiative, which represents a major opportunity for manufacturing of the future [54]. The Industrie 4.0 is aimed to take a pioneering role in manufacturing of the future. A non-profit organization, namely the Smart Manufacturing Leadership Coalition (SMLC), was established in the U.S. SMLC involves manufacturing supplier, practitioner, and consortia, technology companies, universities, and government labs that have expressed interest in realizing smart manufacturing of the future [55].

Over the years, manufacturing confronts with lots of demands for high flexibility. It is very challenging to meet those demands today because of safety reasons. Those safety reasons arise from close interactions and co-operations between machines and human experts in the absence of sufficient sensors and intelligent devices to avoid possible accidents [56]. CPS perspective on the future industrial revolution will improve safety, productivity, and efficiency by connecting embedded system production technologies to pave the way to highly flexible work flow and new forms of collaboration [57].

4.2 Emergency Response (ER)

Emergency response refers to handling the threats against public safety, health, and welfare and protecting the nature, properties, and valuable infrastructures. CPS can provide fast emergency response via large number of sensor nodes in the regions in case of the natural or man-made

disasters. However, this rapid response requires the nodes to collectively assess the situation and rapidly inform the central authority even in the frequently-changing environments. So robustness, effective resource utilization, adaptiveness, and timeliness come into play in this emergency response [58].

Emergency response and disaster management have always drawn attention because of their societal implications. A White House Presidential Innovation Fellow project, namely the SmartAmerica Challenge, was launched in December of 2013 in the U.S [59]. The project is aimed to bring industry, academia, and the government together in the CPS agenda and to gather research efforts, projects, and activities from different domains together. Disaster response is one of the domains/challenges in the SmartAmerica Challenge.

The Strategic Foresight Initiative (SFI) was launched by the Federal Emergency Management Agency (FEMA) in the U.S. Department of Homeland Security (DHS). According to preliminary research results conducted by SFI, aging infrastructures pose a potential risk for the emergency management because they become less reliable and hinder disaster recovery [60].

Emergency management of the future should adopt emerging information technologies and social media use. Strong collaboration and cooperation among emergency management professionals, local and national authorities, and the community are needed. The use of effective forewarning, response, and recovery mechanisms are required in the future emergency management systems [61]. Unmanned aerial or ground vehicles can be deployed to provide efficient search and rescue efforts. Besides, new embedded technologies having physical awareness need to be integrated into the infrastructures to manage emergency response and disaster recovery in the future.

4.3 Air Transportation (AT)

Air transportation refers to any civil or military aviation systems and their traffic management. Smart air vehicles are expected to be predominant in the near future, especially for military service. The Unmanned Aerial Vehicle (UAV), commonly known as the drone, is just one of the well-known examples of smart air vehicles. Since physical-awareness is an important issue for the next generation air vehicles, CPSs are expected to make a profound impact on the future aviation and air traffic management (ATM) [1], [62].

Distributed control throughout the airspace is expected to become a substantial part of the next generation ATM systems. However, that would give rise to more scalability challenges since interactions between vehicles and infrastructure are becoming more complicated. Current capacity constraints at the major airports and airspace interactions between the airports and air vehicles in a multi-airport system limit the overall capacity of the system [62], [63].

The operation of aircrafts has been regulated over years by the procedures similar to those specified over 30 years ago [64]. Today, air traffic control is managed through radar towers and computing support systems have limited physical awareness. So, tight integration of the computational and physical capabilities is of paramount importance for the next generation air transportation systems.

As an existing effort to realize air transportation of the future, a vision of the next generation air transportation, namely NextGen, is introduced by the Federal Aviation Administration (FAA) in the U.S. Department of Transportation. NextGen is an approach transforming air traffic control

from routing over radar towers to routing over satellite-based technology [65]. Satellite navigation is used to provide the pilots with precise locations of surrounding airplanes. New system is being installed step by step and it is expected to see the outcomes of the approach (e.g. flight costs, enhanced safety, etc.) by the year 2018 [65].

4.4 Critical Infrastructure (CI)

Critical infrastructure refers to valuable properties and public infrastructures that are necessary for the survival or welfare of the nations. The Smart Grid is one of the appealing applications in the critical infrastructure domain. The Smart Grid incorporates central/industrial power plants, energy storage and transmission facilities, renewable energy resources (such as wind farms and solar cells), and energy distribution and management facilities in smart homes/buildings [66].

The Smart Grid describes the transformation from a centralized, producer-controlled network of electricity grid to a less centralized, more distributed, more cooperative, more responsive, and more consumer-interactive one by bringing future information and communication technologies and power system engineering together for grid modernization [67].

The Smart Grid provides real-time load monitoring, distribution, and planning at utility level; a balance of supply and demand at the device level; two-way flow of information (i.e. real-time communication between the consumer and utility); the integration of existing energy resources into the grid; large scale grid awareness and ability to switch between high level (e.g. state-wide) and low level (e.g. street-wide) grid exploration; real time integration of sensor data with geographical information; and power quality and blackouts monitoring as well as prevention or minimization of a potential outage [68].

Besides the Smart Grid, water distribution is another important service for the communities. The SmartAmerica Challenge project introduces an enhanced water distribution infrastructure challenge enabled by cellular based CPS that will eventually provide real-time monitoring of water quality and flow control; faster response to possible contamination; low cost and more secure water; and better leak detection [59].

4.5 Health Care and Medicine (HC&M)

Health care and medicine refers to the issues addressing multiple aspects of the patient's physiology. A special attention is drawn to medical applications in CPS research since they provide significant research opportunities for the CPS community. These opportunities include, but are not limited to, technologies related to home care, assisted living, smart operating room, smart medical devices (e.g. pace maker, medical ventilator, infusion pump etc.), and smart prescription [1], [69].

Current technological trends and challenges in the design of the Cyber-Physical Medical System (CPMS) are summarized in [70] along with promising research directions. These trends cover reliable software-based development to deliver new functionalities, increased connectivity of medical devices equipped with network interfaces, and demand for continuous patient monitoring (e.g. home care, assisted living, telemedicine, and sport-activity monitoring, etc.). Modeling and model-driven engineering will play an important role in the future CPMS development [70].

Interoperability as a system level requirement is of paramount importance in CPMS development. There have been joint efforts to satisfy that requirement, for example the Medical Device Plug-and-Play (MD PnP) Interoperability program [71] which was established in 2004. This program leads open platform and standard developments for medical device interoperability. These developments will allow heterogeneous systems to be composed in plug-and-play fashion, increase patient safety, and enable new treatment options and proliferation of technology [72].

Today, medical technology only provides limited access and integration of data along with manual coordination of medical devices and loops are not closed [73]. The Cyber-Physical Medical Systems of the future should provide extensive data integration and access, comprehensive data acquisition and analysis, closed loop control capabilities, energy efficiency, real-time visualization, and plug-and-play capability with interoperable medical devices.

4.6 Intelligent Transportation (IT)

Intelligent transportation refers to the advanced technologies of sensing, communication, computation, and control mechanisms in transportation systems to improve safety, coordination, and services in traffic management with real-time information sharing. Intelligent transportation facilitates both ground and sea transportation through information sharing over satellites and provides communication environment among vehicles, the infrastructure, and passengers' portable devices [74].

The intelligent transportation systems (ITSs) integrate pedestrians, vehicles, sensors, road-side infrastructures, traffic management centers, satellites, and other transportation system components by adopting different variation of wireless communication technologies and standards [75]. ITSs of the future allow real-time traffic monitoring; increase in transportation safety and comfort through information exchange among traffic users; optimal traffic management; collision avoidance; and utilization of satellite based technology to connect drivers, roads, and vehicles smoothly [76].

With the integration of CPS into infrastructures, vehicles, and roadways, ITSs can achieve driver assistance, collision avoidance or notification, improvements in travel time without fear of unexpected delays, reductions in congestion, and advanced control over infrastructure and vehicles for energy saving [64]. ITSs rely not only on advanced sensor and embedded computer systems technology but also on wireless, cellular, and satellite technologies for vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), and vehicle-to- infrastructure (V2I) communication to better manage complex traffic flow, ensure safety, and extend situational awareness.

4.7 Robotic for Service (RfS)

Robotic for service refers to deploying intelligent robots to perform services for the welfare of humans, and the equipment in a fully autonomous, semi-autonomous, or remotely controlled manner, excluding manufacturing operations [77]. Robotic for service is identified as one of the six disruptive civil technologies with potential impacts on the U.S. interests out to 2025 [51].

Robots can be deployed for several purposes, including but not limited to defense (e.g. explosive disposal, surveillance in prohibited areas, etc.), environment monitoring and control, assisted living, logistics, and so on. Since the next generation robots are likely to have close interactions with humans in the physical environment of their operation, learning and

interpretation of human activities by the robots comes into play as an important factor. From CPS perspective, integration of humans and smart robots is very important to enable all actors of CPSs to achieve better cooperation, collaboration, and organization to overcome complex duties [78].

To realize the vision of the next generation robotics, the National Science Foundation (NSF), in partnership with the National Institutes of Health (NIH), the U.S. Department of Agriculture (USDA), and the National Aeronautics and Space Administration (NASA) launched a new initiative, namely the National Robotics Initiative, and makes new investments totaling approximately $38 million in the development of the next generation robots to achieve cooperation and collaboration between humans and robots for enhanced productivity [79]. Another initiative, namely the Robotics Virtual Organization (Robotics-VO), has been launched in 2012 in the U.S. The initiative provides information for the members of the robotics community about funding opportunities, conferences, Principal Investigator (PI) meetings, robotics news and seminars, and educational resources [80].

4.8 Building Automation (BA)

Building automation refers to the deployment of various sensors, actuators, and distributed control systems to provide optimum control and automation of heating, ventilation, air conditioning (HVAC), lighting, fire prevention, and security systems in the buildings. Smart/intelligent building is a frequently mentioned concept to address the next generation buildings.

Smart buildings are needed to fulfill the vision of the Smart Grid and Smart City concepts. With the growing popularity, IoT/CPS provides great opportunities for new applications in the next generation building automation concept via a large range of smart building appliances including entertainment media as well, which in return brings diverse requirements and interaction patterns for realizing such systems [81]. Besides being applied in homes and offices, building automation from CPS perspective can be applied to laboratories. Since activities done in laboratories have been getting sophisticated due to technological advances, new arrangements and services, such as regulation of environmental conditions due to environment-sensitive equipment, accessing incidents or abnormalities, tracing dangerous materials, harvesting energy etc., are needed for the management of laboratories in the future [82].

In the future, smart buildings are expected to pick up the slack for fulfilling the needs of connecting the Smart Grid with smart living environments and learning their living patterns to ensure comfortable living environments. Smart house case models developed by a number of universities in the U.S. as prototypes are reviewed in [83]. Findings are that the applications of smart buildings are closely connected with the deployment of intelligent technologies as of such day. However, smart buildings must be designed as being adaptable and responsive not only to the short term but also to the long term needs of the users considering technological and social changes [83].

Smart utility networks, such as home area networks (HANs), neighborhood area networks (NANs), wide area networks (WANs), and so on, can be deployed in the smart power distribution network of the future to provide two way flows of electricity and information. HAN communication can be utilized for building automation to deliver data traffic and control instructions not only between the smart utilities (e.g. smart meters) and the residents' smart devices but also between the residents' smart devices themselves [84].

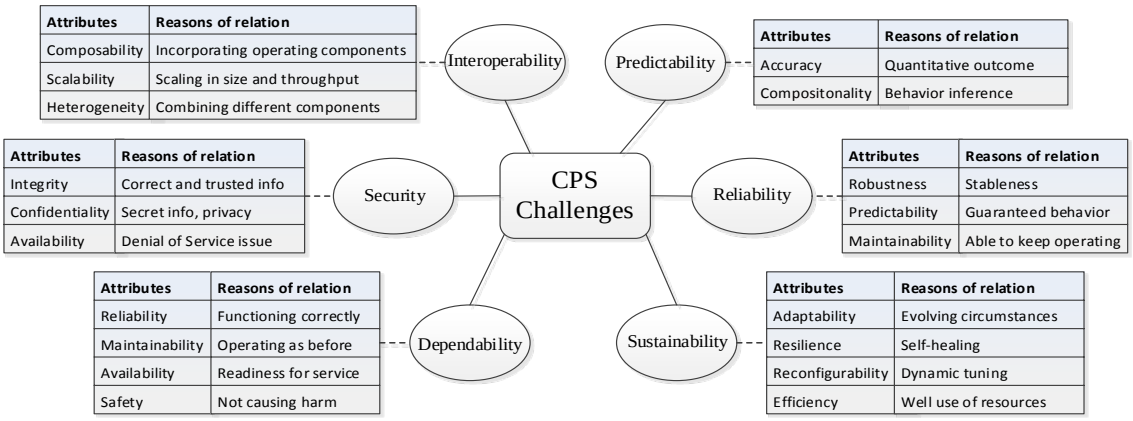

Fig. 3. CPS Challenges

5. CPS Challenges

Cyber-Physical Systems revolutionize our interaction with the physical world. Of course, this revolution does not come free. Since even legacy embedded systems require higher standards than general-purpose computing, we need to pay special attention to this next generation physically-aware engineered system requirements if we really want to put our full trust in them. Therefore, we want to clarify the definitions of some common CPS system-level requirements /challenges. We associate main CPS challenges with their attributes in **Fig. 3**. Brief definitions for the challenges are given in the following and an overview, linking challenges to applications, concludes this section.

Dependability refers to the property of a system to perform required functionalities during its operation without significant degradation in its performance and outcome. Dependability reflects the degree of trust put in the whole system. A highly dependable system should operate properly without intrusion, deliver requested services as specified and not fail during its operation. The words dependability and trustworthiness are often used interchangeably [85]. Assuring dependability before actual system operation is a very difficult task to achieve. For example, timing uncertainties regarding sensor readings and prompt actuation may degrade dependability and lead to unanticipated consequences. Cyber and physical components of the system are inherently interdependent and those underlying components might be dynamically interconnected during the system operation, which, in return, render dependability analysis very difficult. A common language to express dependability related information across constituent systems/underlying components should be introduced in the design stage [86], [87].

Maintainability refers to the property of a system to be repaired in case a failure occurs. A highly maintainable system should be repaired in a simple and rapid manner at the minimum expenses of supporting resources, and free from causing additional faults during the maintenance process. With the close interaction among the system components (e.g. sensors, actuators, cyber components, and physical components) underlying CPS infrastructure, autonomous predictive /corrective diagnostic mechanisms can be proposed. Continuous monitoring and testing of the

infrastructure can be performed through those mechanisms. The outcome of monitoring and testing facilities help finding which units need to be repaired. Some components, which happen to be the source of recurrent failures, can be redesigned or discarded and replaced with the ones with better quality [88], [57].

Availability refers to the property of a system to be ready for access even when faults occur. A highly available system should isolate malfunctioning portion from itself and continue to operate without it. Malicious cyber-attacks (e.g. denial of service attacks) hinder availability of the system services significantly. For example, in Cyber-Physical Medical Systems, medical data shed light on necessary actions to be taken in a timely manner to save a patient's life. Malicious attacks or system/component failure may cause services providing such data to become unavailable, hence, posing risk on the patient's life [89].

Safety refers to the property of a system to not cause any harm, hazard or risk inside or outside of it during its operation. A very safe system should comply with both general and application-specific safety regulations to a great extent and deploy safety assurance mechanisms in case something went wrong. For example, among the goals for smart manufacturing (SM), point-in-time tracking of sustainable production and real-time management of processes throughout the factory yield to improved safety. Safety of manufacturing plants can be highly optimized through automated process control using embedded control systems and data collection frameworks (including sensors) across the manufacturing enterprise. Smart networked sensors could detect operational failures/anomalies and help prevention of catastrophic incidents due to those failures/anomalies [55].

Reliability refers to the degree of correctness which a system provides to perform its function. The certification of system capabilities about how to do things correctly does not mean that they are done correctly. So a highly reliable system makes sure that it does the things right. Considering the fact that CPSs are expected to operate reliably in open, evolving, and uncertain environments, uncertainty in the knowledge, attribute (e.g. timing), or outcome of a process in the CPS infrastructure makes it necessary to quantify uncertainties during the CPS design stage. That uncertainty analysis will yield to effective CPS reliability characterization. Besides, the accuracy of physical and cyber components, potential errors in the design/control flow, cross-domain network connections in an ad-hoc manner limit the CPS reliability [90], [76].

Robustness refers to the ability of a system to keep its stable configuration and withstand any failures. A highly robust system should continue to operate in the presence of any failures without fundamental changes to its original configuration and prevent those failures from hindering or stopping its operation. In addition to failures, the presence of disturbances possibly arising from sensor noises, actuator inaccuracies, faulty communication channels, potential hardware errors or software bugs may degrade overall robustness of CPS. Lack of modeling integrated system dynamics (e.g. actual ambient conditions in which CPSs operate), evolved operational environment, or unforeseen events are other particular non-negligible factors, which might be unavoidable in run-time, hence the need for the robust CPS design [91].

Predictability refers to the degree of foreseeing of a system's state/behavior/functionality either qualitatively or quantitatively. A highly predicable system should guarantee the specified outcome of the system's behavior/functionality to a great extent every moment of time at which it is operating while meeting all system requirements. In Cyber-Physical Medical Systems (CPMS),

smart medical devices together with sophisticated control technologies are supposed to be well adapted to the patient's conditions, predict the patient‘s movements, and change their characteristics based on the context awareness within the surrounding environment [92]. Many medical devices perform operations in real-time, satisfying different timing constraints and showing diverse sensitivity to timing uncertainties (e.g. delays, jitters etc.). However, not all components of CPMS are time-predictable. Therefore, in addition to new programming and networking abstractions, new policies of resource allocation and scheduling should be developed to ensure predictable end-to-end timing constraints [93].

Accuracy refers to the degree of closeness of a system's measured/observed outcome to its actual/calculated one. A highly accurate system should converge to the actual outcome as close as possible. High accuracy especially comes into play for CPS applications where even small imprecisions are likely to cause system failures. For example, a motion-based object tracking system under the presence of imperfect sensor conditions may take untimely control action based on incorrect object position estimation, which in return leads to the system failure [94].

Compositionality refers to the property of how well a system can be understood entirely by examining every part of it. A highly compositional system should provide great insight about the whole from derived behaviors of its constituent parts/components. Achieving high compositionality in the CPS design is very challenging especially due to the chaotic behavior of constituent physical subsystems. Designing highly compositional CPS involves strong reasoning about the behavior of all constituent cyber and physical subsystems/components and devising cyber-physical methodologies for assembling CPSs from individual cyber and physical components, while requiring precise property taxonomies, formal metrics and standard test benches for their evaluation, and well-defined mathematical models of the overall system and its constituents [95].

Sustainability means being capable of enduring without compromising requirements of the system, while renewing the system's resources and using them efficiently. A highly sustainable system is a long lasting system which has self-healing and dynamic tuning capabilities under evolving circumstances. Sustainability from energy perspective is an important part of energy provision and management policies. For example, the Smart Grid facilitates energy distribution, management, and customization from the perspective of customers or service providers by incorporating green sources of energy extracted from the physical environment. However, intermittent energy supply and unknown/ill-defined load characterization hinders the efforts to maintain long-term operation of the Smart Grid. To maintain sustainability, the Smart Grid requires planning and operation under uncertainties, use of real-time performance measurements, dynamic optimization techniques for energy usage, environment-aware duty cycling of computing units, and devising self-contained energy distribution facilities (such as autonomous micro grids) [96], [66].

Adaptability refers to the capability of a system to change its state to survive by adjusting its own configuration in response to different circumstances in the environment. A highly adaptable system should be quickly adaptable to evolving needs/circumstances. Adaptability is one of the key features in the next generation air transportation systems (e.g. NextGen). NextGen's capabilities enhance airspace performance with its computerized air transportation network which enables air vehicles immediately to accommodate themselves to evolving operational

environment such as weather conditions, air vehicle routing and other pertinent flight trajectory patterns over satellites, air traffic congestion, and issues related to security [97].

Resilience refers to the ability of a system to persevere in its operation and delivery of services in an acceptable quality in case the system is exposed to any inner or outer difficulties (e.g. sudden defect, malfunctioning components, rising workload etc.) that do not exceed its endurance limit. A highly resilient system should be self-healing and comprise early detection and fast recovery mechanisms against failures to continue to meet the demands for services. High resilience comes into play in delivering mission-critical services (e.g. automated brake control in vehicular CPS, air and oxygen flow control over an automated medical ventilator etc.). Mission-critical CPS applications are often required to operate even in case of disruptions at any level of the system (e.g. hardware, software, network connections, or the underlying infrastructure). Therefore, designing highly resilient CPS requires thorough understanding of potential failures and disruptions, the resilience properties of the pertinent application, and system evolution due to the dynamically changing nature of the operational environment [86].

Reconfigurability refers to the property of a system to change its configurations in case of failure or upon inner or outer requests. A highly reconfigurable system should be self-configurable, meaning able to fine-tune itself dynamically and coordinate the operation of its components at finer granularities. CPSs can be regarded as autonomously reconfigurable engineered systems. Remote monitoring and control mechanisms might be necessity in some CPS application scenarios such as international border monitoring, wildfire emergency management, gas pipeline monitoring etc. Operational needs (e.g. security threat level updates, regular code updates, efficient energy management etc.) may change for such scenarios, which call for significant reconfiguration of sensor/actuator nodes being deployed or the entire network to provide the best possible service and use of resources [98].

Efficiency refers to the amount of resources (such as energy, cost, time etc.) the system requires to deliver specified functionalities. A highly efficient system should operate properly under optimum amount of the system resources. Efficiency is especially important for energy management in CPS applications. For example, smart buildings can detect the absence of occupants and turn off HVAC (heating, ventilation, and air conditioning) units to save energy. Further, they can provide automated pre-heating or pre-cooling services based on the occupancy prediction techniques [99].

Security refers to the property of a system to control access to the system resources and protect sensitive information from unauthorized disclosures. A highly secure system should provide protection mechanisms against unauthorized modification of information and unauthorized withholding of resources, and must be free from disclosure of sensitive information to a great extent. CPSs are vulnerable to failures and attacks on both the physical and cyber sides, due to their scalability, complexity, and dynamic nature. Malicious attacks (e.g. eavesdropping, man-in-the-middle, denial-of-service, injecting fake sensor measurements or actuation requests etc.) can be directed to the cyber infrastructure (e.g. data management layer, communication infrastructure, decision making mechanisms etc.) or the physical components with the intent of disrupting the system in operation or stealing sensitive information. Making use of a large-scale network (such as the Internet), adopting insecure communication protocols, heavy use of legacy systems or rapid adoption of commercial off-the-shelf (COTS) technologies are other factors which make CPSs easily exposed to the security threats [100], [101].

Integrity refers to the property of a system to protect itself or information within it from unauthorized manipulation or modification to preserve correctness of the information. A high integrity system should provide extensive authorization and consistency check mechanisms. High integrity is one of the important properties of a CPS. CPSs need to be developed with greater assurance by providing integrity check mechanisms on several occasions (such as data integrity of network packets, distinguishing malicious behaviors from the ambient noise, identifying false data injection and compromised sensor/actuator components etc.). Properties of the physical and cyber processes should be well-understood and thus can be utilized to define required integrity assurance [100], [102].

Confidentiality refers to the property of allowing only the authorized parties to access sensitive information generated within the system. A highly confidential system should employ the most secure methods of protection from unauthorized access, disclosure, or tampering. Data confidentiality is an important issue that needs to be satisfied in most CPS applications. For example, in an emergency management sensor network, attacks targeting confidentiality of data transmitted may degrade effectiveness of an emergency management system. Confidentiality of data transmitted through attacked sensor nodes can be compromised and that can cause data flow in the network to be directed over compromised sensors; critical data to be eavesdropped; or fake node identities to be generated in the network. Further, false/malicious data can be injected into the network over those fake nodes. Therefore, confidentiality of data circulation needs to be retained in a reasonable degree [103].

Interoperability refers to the ability of the systems/components to work together, exchange information and use this information to provide specified services. A highly interoperable system should provide or accept services conducive to effective communication and interoperation among system components. Performing far-reaching battlefield operations and having more interconnected and potentially joint-service combat systems, Unmanned Air Vehicles (UAVs) call for seamless communication between each other and numerous ground vehicles in operation. The lack of interoperability standards often causes reduction in the effectiveness of complicated and critical missions [104]. Likewise, according to changing needs, dynamic standards should be developed and tested for devices, systems, and processes used in the Smart Grid to ensure and certify the interoperability of those ones being considered for a specific Smart Grid deployment under realistic operating conditions [105].

Composibility refers to the property of several components to be merged within a system and their inter-relationships. A highly composable system should allow recombination of the system components repeatedly to satisfy specific system requirements. Composibility should be examined in different levels (e.g. device composibility, code composibility, service composibility, system composibility). Certainly, system composibility is more challenging, hence the need for well-defined composition methodologies that follow composition properties from the bottom up. Additionally, requirements and evaluations must be composable accordingly. In the future, it will probably be of paramount importance to incrementally add emerging systems to the system of systems (e.g. CPS) with some predictable confidence without degrading the operation of the resulting system [106].

Heterogeneity refers to the property of a system to incorporate a set of different types of interacting and interconnected components forming a complex whole. CPSs are inherently heterogeneous due to constituent physical dynamics, computational elements, control logic, and

deployment of diverse communication technologies. Therefore, CPSs necessitate heterogeneous composition of all system components. For example, incorporating heterogeneous computing and communication capabilities, future medical devices are likely to be interconnected in increasingly complex open systems with a plug-and-play fashion, which makes a heterogeneous control network and closed loop control of interconnected devices crucial. Configuration of such devices may be highly dynamic depending on patient-specific medical considerations. Enabled by the science and emerging technologies, medical systems of the future are expected to provide situation-aware component autonomy, cooperative coordination, real-time guarantee, and heterogeneous personalized configurations far more capable and complex than today's [93].

Scalability refers to the ability of a system to keep functioning well even in case of change in its size/increased workload, and take full advantage of it. The increase in the system throughput should be proportional to the increase in the system resources. A highly scalable system should provide scatter and gather mechanisms for workload balancing and effective communication protocols to improve the performance. Depending on their scale, CPSs may comprise over thousands of embedded computers, sensors, and actuators that must work together effectively. Scalable embedded many-core architectures with a programmable interconnect network can be deployed to deliver increasing compute demand in CPS [107]. Further, a high performance and highly scalable infrastructure is needed to allow the entities of CPS to join and leave the existing network dynamically. In the presence of frequent data dissemination among those entities, dynamic software updates (i.e. changing the computer program in run-time) can help update CPS applications dynamically and use CPS resources more productively [108].

In fact, all system requirements/attributes are related to each other although we point out the general requirements and their direct/immediate attributes. We aimed to highlight the holistic view of system requirements for CPS applications in **Fig. 3**. CPS is a very broad research area and therefore has diverse applications spanning different scales. All of CPS applications need to be designed considering its impact on the real world and necessary system-level requirements.

Table 2 addresses existing studies that touch upon the importance of those requirements for the application domains. Even though it cannot reflect the overall CPS research, it gives us a notion that the trend of CPS research is on Critical Infrastructures, specifically the Smart Grid, and security aspects of them.

Table 2. References' table that touches on the importance of the subject challenges for CPS application domains

Domain	Dependability	Sustainability	Security	Reliability	Interoperability	Predictability
AT	[101], [109]	[96], [112]	[96], [109], [117], [118]	[104], [112], [123]	[63], [104]	[92], [118]
CI	[101], [92]	[66], [96]	[66], [92], [96], [117], [119], [120], [121], [122]	[66], [92], [124]	[66], [92], [105]	[66]
ER	[101]	[113]	[96], [103], [113], [125]	[125], [126], [127]	[125], [127]	[126]
SM	[92], [101]	[114]	[92]	[92], [128]	[92], [128]	[128]
HC&M	[93], [101], [110]	[92], [96]	[58], [96], [117]	[93]	[92], [93], [130]	[93]
IT	[92], [111]	[92]	[111], [119]	[129]	[92]	[92]
RfS	[101]	[115], [116]	[116]	[131]	[115]	[132]

6. Conclusions

The Cyber-Physical System (CPS) is a promising paradigm for the design of current and future engineered systems and is expected to make an important impact on our interactions with the real world. The idea behind CPS places the focus on the integrated system design instead of on the cyber or the physical system independently. In order to shed some light on the origins, the terminology, relatively similar concepts, and today's challenges in CPS, we presented this survey on related literature discussing practical applications and dominant research domains. Since CPS is a very broad research area, CPSs span diverse applications in different scales. Therefore, each application necessitates strong reasoning capabilities with respect to unique system-level requirements/challenges, the integration of cutting-edge technologies into the related application, and overall impact on the real world. We conclude that existing legacy systems have limited awareness of the CPS requirements, and that revolutionary design approaches are necessary to achieve the overall system objectives.

References

[1] Radhakisan Baheti and Helen Gill, "Cyber-physical systems," *The Impact of Control Technology, IEEE*, pp. 161-166, 2011.

[2] Edward A. Lee, "Cyber Physical Systems: Design Challenges," in *Proc. of 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing*, pp. 363–369, 2008. Article (CrossRef Link)

[3] Ragunathan (RAJ) Rajkumar, Insup Lee, Lui Sha, and John Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. of 47th IEEE/ACM Design Automation Conf.*, pp. 731–736, 2010. Article (CrossRef Link)

[4] Edward A. Lee, "CPS Foundations," in *Proc. of 47th IEEE/ACM Design Automation Conf*. 2010. Article (CrossRef Link)

[5] Jianhua Shi, Jiafu Wan, Hehua Yan, Hui Suo, "A Survey of Cyber-Physical Systems," in *Proc. of the IEEE Int. Conf. on Wireless Communications and Signal Processing*, 2011. Article (CrossRef Link)

[6] Teodora Sanislav and Liviu Miclea, "Cyber-Physical Systems - Concept, Challenges and Research Areas," *Journal of Control Engineering and Applied Informatics*, vol. 14, no. 2, pp. 28-33, 2012.

[7] Imre Horvath and Bart H. M. Gerritsen, "Cyber-Physical Systems: Concepts, Technologies and Implementation Principles," in *Proc. of the Tools and Methods of Competitive Eng. (TMCE) Symposium*, pp. 19-36, 2012.

[8] Edward A. Lee and Sanjit A. Seshia, "Introduction to Embedded Systems: A Cyber-Physical Systems Approach," 1st Edition, 2011.

[9] CPS Steering Group, "Cyber-Physical Systems Executive Summary," 2008. Retrieved on June 25, 2014 from http://iccps.acm.org/2011/_doc/CPS-Executive-Summary.pdf

[10] President's Council of Advisors on Science and Technology (PCAST), "Leadership Under Change: Information Technology R&D in a Competitive World," 2007. Retrieved on June 25, 2014 from http://www.nitrd.gov/Pcast/reports/PCAST-NIT-FINAL.pdf

[11] Cyber-Physical Systems Virtual Organization (CPS-VO). Retrieved on June 25, 2014 from http://cps-vo.org/

[12] The Artemis Embedded Computing Systems Initiative. Retrieved on June 25, 2014 from http://www.artemis-ju.eu/home_page

[13] The EU Framework Program for Research and Innovation (Horizon2020). Retrieved on June 25, 2014 from http://ec.europa.eu/programmes/horizon2020/

[14] Edward A. Lee, "Cyber-Physical Systems - Are Computing Foundations Adequate?," Position Paper in

NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, 2006.
[15] Peter Marwedel, Embedded System Design, *Springer*, 2nd Edition, 2010. Article (CrossRef Link)
[16] Helen Gill, "Cyber-Physical Systems: Beyond ES, SNs, and SCADA," Presentation in *the Trusted Computing in Embedded Systems (TCES) Workshop*, 2010. Retrieved on June 25, 2014 from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1724&context=sei
[17] Lei Mo, Xianghui Cao, Jiming Chen, and Youxian Sun, "Collaborative Estimation and Actuation for Wireless Sensor and Actuator Networks," in *Proc. of the 19th World Congress the International Federation of Automatic Control*, pp. 5544-5549, Cape Town, South Africa, August 24-29, 2014.
[18] Luo, Yan, Krishnendu Chakrabarty, and Tsung-Yi Ho, "A cyberphysical synthesis approach for error recovery in digital microfluidic biochips," in *Proc. of the IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2012. Article (CrossRef Link)
[19] Tom Springer, Steffen Peter, and Tony Givargis, "Resource Synchronization in Hierarchically Scheduled Real-Time Systems using Preemptive Critical Sections," in *Proc. of the IEEE Workshop on Software Technologies for Future Embedded & Ubiquitous Systems (SEUS)*, Reno, June 2014.
[20] E.Y. Erdem, et al. "Thermally actuated omnidirectional walking microrobot," *Journal of Microelectro-mechanical Systems*, vol. 19, no. 3, pp. 433–442, 2010. Article (CrossRef Link)
[21] Yuchen Zhou and John S. Baras, "CPS Modeling Integration Hub and Design Space Exploration with Application to Microrobotics," Control of Cyber-Physical Systems, *Lecture Notes in Control and Information Sciences*, vol. 449, pp. 23-42, 2013. Article (CrossRef Link)
[22] Adrian A. Hopgood, "Intelligent Systems for Engineers and Scientists", *CRC Press*, 3rd Edition, 2012.
[23] Xenofon Koutsoukos, et al., "Passivity-Based Control Design for Cyber-Physical Systems," in *Proc. of the International Workshop on Cyber-Physical Systems - Challenges and Applications (CPS-CA)*, 2008.
[24] Jinzhu Chen, Rui Tan, Guoliang Xing, Xiaorui Wang, Xing Fu, "Fidelity-Aware Utilization Control for Cyber-Physical Surveillance Systems," in *Proc. of the 31st IEEE Real-Time Systems Symposium (RTSS)*, pp. 117-126, 2010. Article (CrossRef Link)
[25] Danielle C. Tarraf (Ed.), "Control of Cyber-Physical Systems," in *Proc. of Lecture Notes in Control and Information Sciences*, vol. 449, March 2013. Article (CrossRef Link)
[26] Manuel Mazo Espinosa, "Contributions to the Control of Networked Cyber-Physical Systems," *a PhD dissertation at the University of California, Los Angeles*, 2010.
[27] Rachana A. Gupta and Mo-Yuen Chow, "Networked Control System: Overview and Research Trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527-2535, 2010. Article (CrossRef Link)
[28] Supervisory Control and Data Acquisition (SCADA) systems, *Technical Information Bulletin 04-1*, 2004. Retrieved on June 25, 2014 from http://scadahacker.com/library/Documents/ICS_Basics/SCADA Basics - NCS TIB 04-1.pdf
[29] Frank Golatowski, et al., "Service-Oriented Software Architecture for Sensor Networks," in *Proc. of International Workshop on Mobile Computing (IMC)*, pp. 93-98. 2003.
[30] James Manyika, et al., "Big data: The next frontier for innovation, competition, and productivity," *McKinsey Global Institute (MGI)*, 2011. Retrieved on October, 31, 2014 from http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights and pubs/MGI/Research/Technology and Innovation/Big Data/MGI_big_data_full_report.ashx
[31] Amit Sheth, Pramod Anantharam, and Cory Henson, "Physical-Cyber-Social Computing: An Early 21st Century Approach," *IEEE Intelligent Systems*, vol. 28, no. 1, pp. 78-82, 2013. Article (CrossRef Link)
[32] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *Recommendations of the National Institute of Standards and Technology*, 2009.
[33] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation*

Computer Systems, vol. 25, no. 6, pp. 599–616, 2009. Article (CrossRef Link)
[34] Mohammad Jamshidi (Ed.), "System of Systems Engineering: Innovations for the 21st Century," *John Wiley &Sons*, vol. 58, 2011.
[35] Tariq Samad and Thomas Parisini, "Systems of Systems," *the Impact of Control Technology*, pp. 175-183, 2011.
[36] William Bolton, "Mechatronics: Electronic Control Systems in Mechanical and Electrical Engineering," *Pearson Education*, 5th Edition, 2013.
[37] David Bradley and David W. Russell, "Mechatronics in Action," *Springer*, 2010. Article (CrossRef Link)
[38] Norbert Wiener, "Cybernetics," *Bulletin of the American Academy of Arts and Sciences*, vol. 3, no. 7, pp. 2-4, 1950. Article (CrossRef Link)
[39] H. S. Tsien, "Engineering Cybernetics," *McGraw-Hill*, 1954.
[40] Sang C. Suh, U. John Tanik, John N. Carbone, Abdullah Eroglu (Editors), "Applied Cyber-Physical Systems," *Springer*, 2013. Article (CrossRef Link)
[41] Kevin Ashton, "That 'Internet of Things' thing", *RFID Journal*, 2009.
[42] Ramon Caceres and Adrian Friday, "Ubicomp Systems at 20: Progress, Opportunities, and Challenges," *Pervasive Computing, IEEE*, vol.11, no.1, pp.14-21, 2012. Article (CrossRef Link)
[43] Mark Roberti, "The Internet of Things Revisited," *RFID Journal*, 2010.
[44] Ashraf E. Al-Fagih, Sharief M. A. Oteafy, and Hossam S. Hassanein, "A pricing scheme for porter based delivery in integrated RFID-Sensor Networks," in *Proc. of 37th IEEE Conf. on Local Computer Networks Workshops*, pp. 827-834, 2012. Article (CrossRef Link)
[45] Luigi Atzori, Antonio Iera, and Giacomo Morabito, "The Internet of Things: a Survey," *Elsevier Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. Article (CrossRef Link)
[46] Anis Koubaa and Bjorn Andersson, "A Vision of Cyber-Physical Internet," in *Proc. of 8th International Workshop on Real-Time Networks (RTN)*, 2009.
[47] Tharam S. Dillon, Hai Zhuge, Chen Wu, Jaipal Singh and Elizabeth Chang, "Web-of-things framework for cyber-physical systems," *Concurrency and Computation Practice and Experience*, vol. 23, no. 9, pp. 905-923, 2011. Article (CrossRef Link)
[48] David S. Watson, et al., "Machine to machine (M2M) technology in demand responsive commercial buildings," in *Proc. of the ACEEE 2004 Summer Study on Energy Efficiency in Buildings: Breaking out of the Box*, pp. 22–27, 2004.
[49] Syed Gilani, "The Promise of M2M: How Pervasive Connected Machines are Fueling the Next Wireless Revolution," White Paper, *Mentor Graphics*, 2009.
[50] Min Chen, Jiafu Wan and Fang Li, "Machine-to-machine communications: architectures, standards, and applications," *KSII Trans. on Internet and Information Systems*, vol. 6, no. 2, pp. 480-497, 2012. Article (CrossRef Link)
[51] Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests out to 2025. *Conference Report CR 2008-07*, 2008. Retrieved on June 25, 2014 from http://www.fas.org/irp/nic/disruptive.pdf
[52] Subharthi Paul, Jianli Pan, and Raj Jain, "Architectures for the Future Networks and the Next Generation Internet: A Survey," *Elsevier Computer Communications*, vol. 34, no. 1, pp. 2-42, 2011. Article (CrossRef Link)
[53] Heiko Koziolek, et al., "Towards software sustainability guidelines for long-living industrial systems," in *Proc. of 3rd Workshop of GI Working Group Long-living Software Systems (L2S2): Design for Future*, 2011.
[54] Henning Kagermann, Wolfgang Wahlster, and Johannes Helbig, "Recommendations for implementing the strategic initiative INDUSTRIE 4.0," *Final report of the Industrie 4.0 Working Group*, 2013. Retrieved on June 25, 2014 from

http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf
[55] Smart Manufacturing Leadership Coalition (SMLC), "Implementing 21st Century Smart Manufacturing," *Workshop Summary Report*, 2011. Retrieved on June 25, 2014 from https://smart-process-manufacturing.ucla.edu/about/news/Smart Manufacturing 6_24_11.pdf
[56] Laila Gide (Editor), "Embedded / Cyber-Physical Systems ARTEMIS Major Challenges: 2014-2020," *Draft Addendum to the ARTEMIS-SRA 2011*, 2013. Retrieved on June 25, 2014 from http://www.artemis-ia.eu/publication/download/publication/910/file/ARTEMISIA_SRA_Addendum.pdf
[57] Germany Trade&Invest, "Industrie 4.0 - Smart Manufacturing for the Future," December 2013. Retrieved on June 25, 2014 from http://www.its-owl.de/fileadmin/PDF/News/2014-01-14-Industrie_4.0-Smart_Manufacturing_for_the_Future_German_Trade_Invest.pdf
[58] John A. Stankovic, Insup Lee, Aloysius Mok, and Raj Rajkumar, "Opportunities and obligations for physical computing systems," *IEEE Computer Society*, vol. 38, no. 11, pp. 23–31, 2005. Article (CrossRef Link)
[59] The SmartAmerica Challenge, *A White House Presidential Innovation Fellow project*, December 2013. Retrieved on June 25, 2014 from http://smartamerica.org/about/
[60] The Federal Emergency Management Agency (FEMA), "A report on Critical Infrastructure," *The Strategic Foresight Initiative (SFI)*, 2011. Retrieved on June 25, 2014 from http://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf
[61] The Federal Emergency Management Agency (FEMA), "Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty," *Progress Report Highlighting the 2010-2011 Insights of the Strategic Foresight Initiative*, 2012. Retrieved on June 25, 2014 from http://www.fema.gov/media-library-data/20130726-1816-25045-5167/sfi_report_13.jan.2012_final.docx.pdf
[62] Radha Poovendran, et al., "A Community Report of the 2008 High Confidence Transportation Cyber-Physical Systems (HCTCPS) Workshop," 2009. Retrieved on June 25, 2014 from http://www.ee.washington.edu/research/nsl/aar-cps/NCO_June_2009.pdf
[63] Philippe A. Bonnefoy, "Scalability of the Air Transportation System and Development of Multi-Airport Systems: A Worldwide Perspective," *Ph.D. dissertation*, Massachusetts Inst. of Technology, 2008.
[64] Networking and Information Technology Research and Development (NITRD) Program, "Winning the Future with Science and Technology for 21st Century Smart Systems," Retrieved on June 25, 2014 from http://www.nitrd.gov/nitrdgroups/images/1/12/CPS_OSTP_ResponseWinningTheFuture.pdf
[65] The Federal Aviation Administration (FAA), NextGen. Retrieved on June 25, 2014 from http://www.faa.gov/nextgen/
[66] James A. Momoh, "Fundamentals of Analysis and Computation for the Smart Grid," in *Proc. of IEEE Power and Energy Society General Meeting*. pp. 1–5, 2010. Article (CrossRef Link)
[67] Hassan Farhangi, "The path of the smart grid," *IEEE Power Energy Mag*. vol. 8, no. 1, pp. 18-28, 2010. Article (CrossRef Link)
[68] The U.S. Department of Energy, "The Smart Grid: An Introduction". Retrieved on June 25, 2014 from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf
[69] Kyoung-Dae Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," in *Proc. of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287-1308, 2012. Article (CrossRef Link)
[70] Insup Lee and Oleg Sokolsky, "Medical Cyber Physical Systems," in *Proc. of 47th Design Automation Conference*, pp. 743-748, 2010. Article (CrossRef Link)
[71] The Center for Integration of Medicine and Innovative Technology. Medical Device Plug-and-Play

Interoperability program. Retrieved on June 25, 2014 from http://mdpnp.org/
[72] David Arney, et al., "Plug-and-Play for Medical Devices: Experiences from a Case Study," *Biomedical Instrumentation and Technology*. vol. 43, no. 4, pp. 313-317, 2009. Article (CrossRef Link)
[73] Julian M. Goldman, "Medical Device CPS Testbeds: Candidate Testbed for Research and Development on Cyber-Physical Medical Device Systems," *NSF CPS PI Meeting* held in Arlington, VA, USA, 2013.
[74] The U.S. Department of Transportation. The Intelligent Transportation Systems (ITS) Program's Research. Retrieved on June 25, 2014 from http://www.its.dot.gov/research.htm
[75] Fengzhong Qu, Fei-Yue Wang, and Liuqing Yang, "Intelligent Transportation Spaces: Vehicles, Traffic, Communications, and Beyond," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 136-142, 2010. Article (CrossRef Link)
[76] Acatech - National Academy of Science and Engineering, "Cyber-Physical Systems Driving force for innovation in mobility, health, energy and production," *Position Paper*, December 2011. Retrieved on June 25, 2014 from http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_POSITION_CPS_Englisch_WEB.pdf
[77] Service Robots-IFR International Federation of Robotics. Retrieved on June 25, 2014 from http://www.ifr.org/service-robots/
[78] Abdelghani Chibani, Yacine Amirat, Samer Mohammed, Eric Matson, Norihiro Hagita, and Marcos Barreto, "Ubiquitous robotics: Recent challenges and future trends," *Robotics and Autonomous Systems*, 2013. Article (CrossRef Link)
[79] The National Science Foundation (NSF), National Robotics Initiative (NRI), October 2013. Retrieved on June 25, 2014 from http://www.nsf.gov/news/news_summ.jsp?cntn_id=129284
[80] Robotics Virtual Organization (Robotics-VO). Retrieved on June 25, 2014 from http://www.robotics-vo.us/
[81] Ioannis Chatzigiannakis, Jan Philipp Drude, Henning Hasemann, Alexander Kröller, "Developing Smart Homes Using the Internet of Things: How to demonstrate Your System," *Distributed, Ambient, and Pervasive Interactions, Springer International Publishing*, vol. 8530, pp. 415-426, 2014. Article (CrossRef Link)
[82] Chi-Un Lei, et al., "Building an Intelligent Laboratory Environment via a Cyber-Physical System," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013. Article (CrossRef Link)
[83] AmirHosein GhaffarianHoseini, et al., "The essence of future smart houses: From embedding ICT to adapting to sustainability principles," *Renewable and Sustainable Energy Reviews*, vol. 24, pp. 593–607, August 2013. Article (CrossRef Link)
[84] Weixiao Meng, Ruofei Ma, Hsiao-Hwa Chen, "Smart grid neighborhood area networks: a survey," *IEEE Network*, vol. 28, no.1, pp.24-32, January-February 2014. Article (CrossRef Link)
[85] Kaiyu Wan and Vangalur Alagar, "Dependable Context-sensitive Services in Cyber Physical Systems," in *Proc. of International Joint Conference of IEEE TrustCom-11, ICESS-11/FCST-11*, pp. 687-694, 2011. Article (CrossRef Link)
[86] Grit Denker, Nikil Dutt, Sharad Mehrotra, Mark-Oliver Stehr, Carolyn Talcott, and Nalini Venkatasubramanian, "Resilient dependable cyber-physical systems: a middleware perspective," *Journal of Internet Services and Applications*, vol. 3, no. 1, pp. 41-49, 2012. Article (CrossRef Link)
[87] Kai Höfig, "A vehicle control platform as safety element out of context," at *HiPEAC Computing Systems Week*, Barcelona, Spain, May 15, 2014. Retrieved on October 31, 2014 from http://rts.eit.uni-kl.de/hipeac-ws-0514/Presentations/KaiHoefig.pdf
[88] Santiago Ruiz-Arenas, Imre Horváth, Ricardo Mejía-Gutiérrez, and Eliab Z. Opiyo, "What is with the Maintenance Principles of Cyber-Physical Systems?," *Journal of Mechanical Engineering*, 2014. Article (CrossRef Link)

[89] Shah Ahsanul Haque, Syed Mahfuzul Aziz, and Mustafizur Rahman, "Review of Cyber-Physical Systems in Healthcare," *Int'l Journal of Distributed Sensor Networks*, vol. 2014, 2014. Article (CrossRef Link)
[90] "Strategic R&D Opportunities for 21st Century Cyber-Physical Systems," *Report of the Steering Committee for Foundations in Innovation for Cyber-Physical Systems*, Retrieved on September 26, 2014 from http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf
[91] Matthias Rungger and Paulo Tabuada, "A Notion of Robustness for Cyber-Physical Systems," *eprint arXiv:1310.5199*, 2013. Retrieved on October 31, 2014 from http://arxiv.org/abs/1310.5199
[92] "Cyber Physical Systems: Situation Analysis of Current Trends, Technologies, and Challenges," in *Proc. of NIST CPS Workshop*, 2012. Retrieved on September 26, 2014 from http://events.energetics.com/NIST-CPSWorkshop/pdfs/CPS_Situation_Analysis.pdf
[93] High Confidence Software and Systems Coordinating Group, "High-confidence medical devices: Cyber-physical systems for 21st century health care," *A Research and Development Needs Report, NCO/NITRD*, 2009. Retrieved on June 25, 2014 from http://www.whitehouse.gov/files/documents/cyber/NITRD - High-Confidence Medical Devices.pdf
[94] V. Gunes, S. Peter, and T. Givargis, "Modeling and Mitigation of Faults in Cyber-Physical Systems with Binary Sensors," in *Proc. of the 16th IEEE International Conference on Computational Science and Engineering (CSE)*, pp. 515-522, Sydney, December 2013. Article (CrossRef Link)
[95] "Foundations for Innovation in Cyber-Physical Systems," *Workshop Report prepared by Energetics Incorporated for the National Institute of Standards and Technology (NIST)*, 2013. Retrieved on September 26, 2014 from http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf
[96] Ayan Banerjee, et al., "Ensuring safety, security and sustainability of mission-critical cyber physical systems," in *Proc. of the IEEE*, vol. 100, no. 1, pp.283-299, 2011. Article (CrossRef Link)
[97] Ramesh K. Agarwal, "Review of technologies to achieve sustainable (Green) aviation," *Recent Advances in Aircraft Technology, Intechopen*, Chapter 19, pp. 427-464, 2012. Article (CrossRef Link)
[98] Misra, Sanjay, and Emmanuel Eronu, "Implementing Reconfigurable Wireless Sensor Networks: The Embedded Operating System Approach," *Embedded Systems - High Performance Systems, Applications and Projects, Intechopen*, Chapter 11, pp. 221-232, 2012. Article (CrossRef Link)
[99] James Scott, et al., "PreHeat: controlling home heating using occupancy prediction," in *Proc. of the 13th ACM international conference on Ubiquitous computing*, pp. 281-290, 2011. Article (CrossRef Link)
[100] "Designed-In Cyber Security for Cyber-Physical Systems," *Workshop Report by the Cyber Security Research Alliance (CSRA) and Co-sponsored with NIST*, 2013. Retrieved on September 26, 2014 from http://www.cybersecurityresearch.org/documents/CSRA_Workshop_Report.pdf
[101] Raja Waseem Anwar and Saqib Ali, "Trust Based Secure Cyber Physical Systems," in *Proc. of Workshop Proceedings: Trustworthy Cyber-Physical Systems, Tech Report Series*, Computing science, Newcastle Uni., 2012.
[102] Yilin Mo and Bruno Sinopoli, "Integrity Attacks on Cyber-Physical Systems," in *Proc. of the 1st ACM international conference on High Confidence Networked Systems (HiCoNS)*, pp. 47-54, 2012. Article (CrossRef Link)
[103] George Loukas, Diane Gan, and Tuan Vuong, "A review of cyber threats and defense approaches in emergency management," *Future Internet*, vol. 5, no. 2, pp. 205-236, 2013. Article (CrossRef Link)
[104] Jeremiah Gertler, "U.S. Unmanned Aerial Systems," *CRS Report for Congress, Congressional Research Service*, 2012. Retrieved on September 26, 2014 from http://fas.org/sgp/crs/natsec/R42136.pdf
[105] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, *NIST Special Publication 1108R2*, 2012. Retrieved on September 26, 2014 from http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf

[106] "A Roadmap for Cybersecurity Research," *the U.S. Department of Homeland Security*, 2009. Retrieved on September 26, 2014 from http://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf
[107] V. Gunes and T. Givargis, "XGRID: A Scalable Many-Core Embedded Processor," in *Proc. of 11th IEEE International Conference on Embedded Software and Systems (ICESS)*, Paris, August 2014.
[108] Mi Jeong Park, Dong Kwan Kim, Won-Tae Kim, and Seung-Min Park, "Dynamic software updates in cyber-physical systems," in *Proc. of IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 425-426, 2010. Article (CrossRef Link)
[109] Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," in *Proc. of the IEEE*, vol. PP, no.99, pp.1-22, 2013. Article (CrossRef Link)
[110] Junbeom Hur and Kyungtae Kang, "Dependable and secure computing in medical information systems," *Computer Communications*, vol. 36, no. 1, pp. 20-28, 2012. Article (CrossRef Link)
[111] Farinaz Koushanfar, Ahmad-Reza Sadeghi, and Herve Seudie, "EDA for Secure and Dependable Cybercars: Challenges and Opportunities," in *Proc. of the 49th Design Automation Conference*, 2012. Article (CrossRef Link)
[112] Mark D. Moore, "Aviation Frontiers on-Demand Aircraft," in *Proc. of 10th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference*, 2010. Article (CrossRef Link)
[113] Ashton Rohmer, "Emergency Response in Large-Scale Disasters: Lessons Learned and Implications for National Security", *Government Honors Papers*, Page 9, 2010. Retrieved on September 26, 2014 from http://digitalcommons.conncoll.edu/govhp/9/
[114] Smart, Safe, and Sustainable Manufacturing, *Rockwell Automation 2013 Corporate Responsibility Report*, 2013. Retrieved on September 26, 2014 from http://literature.rockwellautomation.com/idc/groups/literature/documents/br/esap-br018_-en-p.pdf
[115] Pedro F. Santana, Jose Barata, and Luis Correia, "Sustainable robots for humanitarian demining," *International Journal of Advanced Robotics Systems (ARS-journal)*, vol. 4, no. 2, pp. 207-218, 2007. Article (CrossRef Link)
[116] Bernd Scholz-Reiter, Moritz Rohde, Stefan Kunaschk, Michael Lütjen, "Towards automation of low standardized logistic processes by use of cyber physical robotic systems (CPRS)," in *Proc. of WSEAS Int. Conf. on Mathematical and Computational Methods in Science and Eng*, pp. 293-298, 2011.
[117] Nabil Adam, "Workshop on future directions in cyber-physical systems security," *Report on workshop organized by Department of Homeland Security (DHS)*, 2010. Retrieved on September 26, 2014 from http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf
[118] Rosa N. Weber, and Eric Euteneuer, "Avionics to enable UAS integration into the NextGen ATS," *AIAA Guidance, Navigation, and Control Conference*, 2010. Article (CrossRef Link)
[119] Sajal K. Das, Krishna Kant, and Nan Zhang, "Handbook on Securing Cyber-Physical Critical Infrastructure," *Morgan Kaufmann*, Chapter 25, 2012. Article (CrossRef Link)
[120] Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and C. L. Philip Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981-997, 2012. Article (CrossRef Link)
[121] Wenye Wang and Zhuo Lu, "Cyber security in the Smart Grid: survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, 2013. Article (CrossRef Link)
[122] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," in *Proc. of the IEEE*, vol. 100, no. 1, pp. 210-224, 2012. Article (CrossRef Link)
[123] Keerti K. Bhamidipati, Daniel Uhlig, and Natasha Neogi, "Engineering Safety and Reliability into UAV Systems: Mitigating the Ground Impact Hazard," in *Proc. of AIAA Guidance, Navigation and Control Conf*. pp. 2007-6510, 2007. Article (CrossRef Link)
[124] Alejandro D. Dominguez-Garcia, "Reliability modeling of cyber-physical electric power systems: A

system-theoretic framework," *the IEEE Power and Energy Society General Meeting*, 2012. Article (CrossRef Link)

[125] Joseph Vincent Treglia, et al., "Interoperability by 'Edgeware': Wireless Grids for Emergency Response," in *Proc. of the IEEE Hawaii International Conference on System Sciences (HICSS)*, 2011. Article (CrossRef Link)

[126] Jesper Andersson, Rogerio de Lemos, Sam Malek, Danny Weyns, "Modeling Dimensions of Self-Adaptive Software Systems," *Springer Software Engineering For Self-Adaptive Systems*, pp. 27-47, 2009. Article (CrossRef Link)

[127] Janet Marsden, Joseph Treglia, and Lee McKnight, "Dynamic Emergency Response Communication: The intelligent Deployable Augmented Wireless Gateway (iDAWG)," in *Proc. of IEEE Int. Multi-Disciplinary Conf. on Cognitive Methods in Situation Awareness and Decision Support*, pp. 279-286, 2012. Article (CrossRef Link)

[128] Detlef Zühlke and Lisa Ollinger, "Agile Automation Systems Based on Cyber-Physical Systems and Service-Oriented Architectures," *Advances in Automation and Robotics*, vol. 1, pp. 567-574, 2012. Article (CrossRef Link)

[129] Prithviraj Patil, "Towards Reliable Communication in Intelligent Transportation Systems," in *Proc. of the 31st IEEE International Symposium on Reliable Distributed Systems (SRDS)*, pp.485-486, 2012. Article (CrossRef Link)

[130] Min-Woo Jung and Jeonghun Cho, "Interoperability and Control Systems for Medical Cyber Physical Systems," *IT Convergence and Security 2012, Lecture Notes in EE, Springer*, vol. 215, pp. 283-291, 2013. Article (CrossRef Link)

[131] Jeongmin Park, et al., "Intelligent Service Robot and Application Operating in Cyber-Physical Environment," *Embedded and Multimedia Computing Technology and Service*, vol. 181, pp. 301-310, 2012. Article (CrossRef Link)

[132] Zhenyu Ye, Henk Corporaal, and Pieter Jonker, "PhD forum: A cyber-physical system approach to embedded visual servoing," in *Proc. of IEEE Int. Conf. on Distributed Smart Cameras*, pp. 1-2, 2011. Article (CrossRef Link)

Volkan Gunes received his M.S. degree in Computer Science from the University of California, Irvine. He is currently a Ph.D. candidate in the Department of Computer Science and Graduate Student Researcher in the Center for Embedded Computer Systems, at the University of California, Irvine. His research interests include Embedded Computer Systems, Cyber-Physical Systems, and Embedded Many-core System-on-a- Chip Architectures.

Steffen Peter received his diploma in Computer Science (2006) and his PhD (Dr.-Ing) in Computer Engineering (2011) from the Brandenburg University of Technology at Cottbus (BTU) in Germany. From 2006 to 2012 he worked in the IHP Microelectronics research institute on trustworthy embedded systems. Since August 2012, he is Postdoctoral Researcher in the Information and Computer Science department at UC Irvine, where he works in the Design Science for Cyber Physical Systems Project. His research interests include modeling of timing, network and dependability aspects in cyber physical systems and wireless sensor networks.

Tony Givargis received his Computer Science MS and PhD degrees from University of California, Riverside in 1997 and 2001 respectively. He is currently a Professor in the Department of Computer Science and faculty in the Center for Embedded Computer Systems, at the University of California, Irvine. His research interests include all aspects of system software design, in particular, embedded software. He has published over 90 peer-reviewed conference and journal papers, over 11 issued patents, and a number of best paper awards. He is the coauthor of two popular textbooks on embedded system design and has received the prestigious Frederick Emmons Terman Award in 2011 for his research and teaching contributions to the field.

Frank Vahid (Ph.D. C.S. UC Irvine 1994) is a Professor of Computer Science and Engineering at the Univ. of California, Riverside, and co-founder and CTO of Zyante.com. His research interests include embedded systems programming and design, and development of interactive online learning material for engineering education.