Cyber-Physical Systems - Concept, Challenges and Research Areas★

Teodora Sanislav, Liviu Miclea

Automation Department, Technical University of Cluj-Napoca, Cluj-Napoca, Romania (e-mails: Teodora.Sanislav@aut.utcluj.ro, Liviu.Miclea@aut.utcluj.ro)

Abstract: Cyber-Physical Systems (CPSs) represent an emerging research area that has attracted the attention of many researchers. Starting from the definition of CPS, the paper discusses the need for these systems implementation in various application domains and the research challenges for defining an appropriate formalism that represent more than networking and information technology - the information and knowledge will be integrated into physical objects. As CPSs are expected to play a major role in the design and development of future engineering systems, a short state of the art regarding the main CPS research areas (generic architecture, design principles, modeling, dependability, and implementation) ends the paper.

Keywords: Cyber-physical systems, architecture, modeling, design, dependability.

1. INTRODUCTION

Using the Internet we can interact with people and get useful information from wide world in a very short time. Thus, the Internet has transformed the way we do our researches, studies, we manage our business and services and even our fun way. However, there is a gap between the cyber world in which information is transmitted and modified and the physical world in which we live. Also, the last two decades have brought a digital revolution that has transformed the industry. This change is not a choice, but it is determined by fundamental economic and technological long term trends, that have created an environment which allows and requires a wide and varied range of new capabilities.

The technological advances from the recent decades has led to some early examples of a new systems generation (e.g. quality, safety and efficiency critical infrastructure; integrated, self optimizing transportation systems and vehicles; air planes and automobiles that are environmentally friendly and energy efficient; advanced health care via increased automation, integrating smart devices, and providing safe access to electronic medical records; new biotechnologies). These early examples demonstrate the need for a new generation of systems - *Cyber-Physical Systems (CPSs)* - to represent more than networking and information technology, information and knowledge being integrated into physical objects. By integrating perception, communication, learning, behavior generation, reasoning into such systems a new generation of intelligent and autonomous systems may be developed (see CPS-Steering-Group (2008)).

The paper is structured as follows. Section 2 discusses the concept recently appeared - CPS from the following points of view: various definitions, characteristics, properties. Section 3 highlights the need for the CPSs implementation in various application areas and their characteristics for several of these domains. Section 4 presents the research challenges in order to define an appropriate formalism for these classes of systems (CPSs). A presentation, as a state of the art, regarding the main CPSs research areas: generic architecture, design principles, modeling, dependability and some implemented examples, represents the core of the paper and the subject of the section 5. Section 6 concludes the paper.

2. CPS CONCEPT

The recently appeared *CPS* term will have to enable the development of a modern vision for the social services that transcend time and space to dimensions never seen before (see CPS-Steering-Group (2008)). CPS is an integration of computation with physical processes, is about intersection, not the union of the physical and the cyber (see Lee and Seshia (2011)). Also a complex CPSs definition was given by Shankar Sastry from University of California, Berkeley in 2008: "A cyber-physical system (CPS) integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safety, securely, efficiently and real-time".

CPSs are not: the traditional embedded systems or the real-time systems, the today's sensor networks and only desktop applications, but they have certain characteristics that define them, as mentioned in Huang (2008) and presented below: (1) Cyber capabilities in every physical component; (2) Networked at multiple and extreme scale; (3) Dynamically reconfiguring/reorganizing; (4) High degrees of automation, the control loops must close; (5) Operation must be dependable and certified in some cases; (6) Cyber and physical components are integrated for learning and

★ This paper was supported by the project "Improvement of the doctoral studies quality in engineering science for development of the knowledge based society-QDOC" contract no. POSDRU/107/1.5/S/78534, project co-funded by the European Social Fund through the Sectorial Operational Program Human Resources 2007-2013. Both authors are main authors.

adaptation, higher performance, self-organization, auto-assembly.

CPSs, as all information and communication systems, are characterized by the following fundamental properties: (1) Functionality; (2) Performance; (3) Dependability and security; (4) Cost. Other properties that affect the system dependability and security are: usability, management and adaptability. The main features of the CPSs are following: (1) Input and feedback from/to the physical environment - the existence of the secured communication channels; (2) Management and distributed control - a federated approach; (3) Real-time performance requirements; (4) Large geographical distribution without physical security components in various locations; (5) Very large scale control systems (SystemOfSystems - SoS).

3. APPLICATION DOMAINS

Cyber-physical systems present a set of advantages: they are efficient and safe systems, they allow individual entities to work together in order to form complex systems with new capacities. Cyber-physical technology can be applied in a wide range of domains, offering numerous opportunities: critical infrastructure control, safe and efficient transport, alternative energy, environmental control, telepresence, medical devices and integrated systems, telemedicine, assisted living, social networking and gaming, manufacturing, agriculture (see Huang (2008), Lee (2008)). Critical infrastructure, assets that are essential for the functioning of a society and economy, includes facilities for: water supply (storage, treatment, transport and distribution, waste water); electricity generation, transmission and distribution; gas production, transport and distribution; oil and oil products production, transport and distribution; and telecommunication.

The paper Wan et al. (2010) presents some requirements that CPSs should meet according to the business sectors where they will be used: automotive, environment monitoring/protection, aviation and defense, critical infrastructure, healthcare (Table 1). The physical platforms, support for CPSs, provide the following five capabilities: computing, communication, precise control, remote cooperation and autonomy.

Unlike the traditional embedded systems, the CPSs interface directly with the physical world, making the detection of environmental changes and the system behavior adaptation to be considered the key challenges in the design of such systems.

Table 1. CPSs Characteristics and their Application Domains

Application Domain	CPSs Characteristics
Automotive	CPSs for the automotive industry require high computing power, due to complex traffic control algorithms that calculate for example the best route according to traffic situation.
Environment	CPSs for environment monitoring, distributed in a wide and varied geographical area (forests, rivers, mountains) must operate without human intervention for long time periods with minimal energy consumption. In such an environment, the accurate and in time data collection provided by the ad-hoc network with low power consumption, represent a real research challenge.
Aviation, defense	CPSs for aviation and defense require a precise control and high security and not least high power computing. In this scope, the development of the security protocols will be the main research challenge.
Critical infrastructure	CPSs for energy control, water resources management, etc. require a precise and reliable control, leading to application software methodologies to ensure the quality of the software.
Healthcare	CPSs for healthcare and medical equipments require a new generation of analysis, synthesis and integration technologies, leading to the development and the application of the interoperability algorithms.

4. RESEARCH CHALLENGES

Currently, the research is divided into isolated sub-discipline, such as: communications and networking, systems theory, mathematics, software engineering, computer science, sensors. Thus, digital systems are designed and analyzed using a variety of modeling tools and formalisms. Each representation brings out some features and doesn't take into account the other in order to make malleable analysis. Usually, formalism represents either the cybernetic processes, or those physical, but not both, as necessary to achieve CPSs. The following paragraphs present the main directions of research needed in CPSs domain that is still in its early-stage:

Abstraction and Architectures - Innovative approaches to abstractions (formalisms) and architectures to enable control, communication and computing integration for the rapid design and implementation of CPSs have to be developed. They should allow the integration and interoperability of heterogeneous systems that composed the CPSs in a modular, efficient and robust manner (see Baheti and Gill (2011)).

Distributed Computations and Networked Control - refers to new frameworks, algorithms, methods, and tools related to time-and event-driven computing, software, variable time delays, failures, reconfiguration, and distributed decision support systems to satisfy the high reliability and security requirements for heterogeneous cooperating components that interact through a physical environment (see Baheti and Gill (2011)).

Verification and Validation - Hardware and software components as well as the systems they form, have to overcome their actual stage and to achieved a high degree of dependability, re-configurability, and when is required to be certified. New models, algorithms, methods, and tools to verify and validate software components and also entire system from early design stage represent the research directions addressed to the scientific community (see Baheti and Gill (2011)).

Also, the scientific challenges in the CPSs field were highlighted in the CPS Steering Group Report from March 2008 (CPS-Steering-Group (2008)) and are the following: (1) The *realignment of the abstraction layers in design flows* - the abstractions must include physical concepts such as time and energy. These changes related to the layers of abstraction will allow the synthesis of computations with physical properties and physical system dynamics that are robust against implementation uncertainties; (2) The development of the *semantic foundations for composing heterogeneous models and modeling languages* that describe different physics and their associate logics; (3) The development of a *new understanding of compositionality in heterogeneous systems* that allows the creation of large, networked systems that satisfy essential physical properties and deliver the required functionality in a reliable way; (4) The development of a *technology for achieving the predictability in partially compositional properties*; (5) The development of a *model-based, precise, and predictable technology foundation for system integration*; (6) The development of a new *infrastructure for agile design automation* of CPSs; (7) The development of *new open architectures* for CPSs that will allow the building of the national-scale and global-scale capabilities; (8) The development of *architectures and tools for reliable CPSs* from unreliable components and *resilient CPSs* that will tolerate malicious attacks from either the cyber or physical domains. These architectures should leverage open systems technologies to reduce design times and increase confidence of the CPSs. In CPS-Steering-Group (2008) the Table 2[1] highlights the importance of some of the challenges mentioned above for some areas covered by the CPSs: aviation, defense, automotive, energy and healthcare.

Table 2. Research Directions for Several CPSs Application Domains

	Aviation Defense	Auto	Energy	Healthcare
New abstraction layers for design	V.I.	V.I.	V.I.	V.I.
Semantic foundations for composing models	V.I.	V.I.	I.	I.
Composition platforms for heterogeneous systems	V.I.	V.I.	V.I.	V.I.
Foundation for system integration	V.I.	V.I.	V.I.	V.I.
Infrastructure for automatic design	V.I.	V.I.	L.I.	I.
Open architectures	I.	I.	V.I.	I.
Dependability and security	V.I.	V.I.	V.I.	V.I.

5. RESEARCH AREAS

At international level, the CPSs researches are in the following areas: the definition of a generic architecture, the definition of the CPSs design principles in their application domains, the modeling of the CPSs, the ensuring of the CPSs dependability, and the CPSs implementation (for critical infrastructure control and beyond).

5.1 Generic Architectures for CPSs

Architecture of a CPS should provide uniform treatment of cyber and physical elements. The software architecture provides a good starting point but the concept should be extended to CPS by using new vocabulary for physical and cyber-physical elements necessary to analyze the system behavior.

The paper "A Prototype Architecture for Cyber-Physical Systems" (Tan et al. (2008)) presents a representative prototype architecture of the CPS concept, which highlights cyber world represented by events/information as an abstraction of the real physical world governed by semantic laws, evolving the typical architecture of the embedded systems and align it to current technological requirements. This architecture reveals the following: (1) *Global Reference Time* - provided by the next generation network and should be accepted by all CPS components; (2) *Event/Information Driven* - the events are "raw facts" reported by sensor units/humans or "actions" made by actuator units/humans and the information represents the abstraction of the physical world made by system control units or humans through event processing; (3) *Quantified Confidence* - a standard method to calculate the confidence of the events/information at any point in time; (4) *Publish/Subscribe Scheme* - each CPS control unit subscribes to interesting events/information based on its system goal, and also publishes event/information when necessary; (5) *Semantic Control Laws* - having the event-condition-action form, the laws precisely control system behaviors related to the environment context according to user defined conditions or scenarios; (6) *New Networking Techniques* - provide the global reference time, new event/information routing and data management schemes.

The paper "A Software Architecture for Next-Generation Cyber-Physical Systems" (West and Parmar (2006)) proposes to develop a CPS based on a software architecture composed of a collection of *application-specific services*, which organizes itself with the most appropriate methods of communication and isolation between services. The software architecture must take into account the automatic composition of services in order to satisfy the application constraints, given underlying hardware limitations, and also the hardware heterogeneity in the generation and verification of a software system for a given application.

5.2 CPSs Design Principles

Because the CPSs are just at the beginning, there are in the specialized literature, mainly scientific papers that attempt to define certain design principles of these systems in their fields of application (Sha et al. (2008), Huang (2008), Lee (2008), Baheti and Gill (2011)).

The paper "Cyber-physical Systems in Industrial Process Control" (Wang et al. (2008)) analyses the design principles of large-scale systems composed of heterogeneous components which can be solved by a new unifying network and control theory. The paper approaches the real-time

[1] Notation: V.I. - very important; I - important; L.I. - less important.

operation in a heterogeneous system which requires a unified theory of real-time operation that includes existing results and novel solutions. Also, the cross-layer design is reached, specifying that each device should be designed based on hardware, operating system, middleware, sensing, actuation, as well as communication as a whole. The cross-design approach of the CPSs is borrowed from the cross-layer communication techniques used in wireless sensor networks.

The design of complex systems and CPSs increasingly require the involvement of three major disciplines: control, systems and software engineering. Considering that, the paper "Composition of Cyber-Physical Systems" (Sztipanovits (2007)) notes that the design decomposition by orthogonal aspects of the problem cannot be applied in case of CPSs due to the heterogeneity of these systems. Also the strong interdependences between the CPSs components limit the compositionality in the design process. The abstraction of the system interdependencies is needed and this procedure can be achieved by the development of new modeling techniques.

5.3 CPSs Modeling

The CPSs modeling represents the key of these systems implementation. In recent years the modeling has evolved, leading to the apparition of the "meta-modeling" techniques and of the suite of tools called "meta-programmable", that allow the introduction of domain-specific modeling language, giving to the system designers the modeling concepts and notation adapted to the application domain. These modeling techniques are shown in Sztipanovits (2007) for their usage in CPSs modeling.

There is also a semantic representation of the CPS interdependencies using semantic models implemented with multi-agent techniques (see Talcott et al. (2008)). The paper "Cyber-Physical Systems and Events" (Talcott et al. (2008)) proposes event-based semantics, as foundation for CPSs semantics. The event-based semantics were chosen for the following reasons: (1) The events concern interactions between components and observations rather that internal state. This enables specification and reasoning at higher-levels while integrating easily with more detailed information. (2) The events are the notion of causal partial order that reflects the physical reality that for events separated in space does not allow us to decide a linear order (and should not depend on it). The paper Talcott et al. (2008) presents two compositional models, one for autonomous agents and the other for interactive agents. The model based on interactive agents seems to provide the forms of interaction such as needed in CPSs. The CPSs modeling should consider the interaction between the physical and cyber components and communications and therefore a formal framework for studying these systems have to be invented.

The paper "An Integrated Specification Logic for Cyber-Physical Systems" (Bujorianu and Barringer (2009)) proposes a formal approach called "Hilbertean formal methods" to provide a denotational semantics for these systems. The approach combines the denotational semantics with an algebraic model for physical processes in order to evidence the holistic perspective of the CPSs paradigm and has the following key points: (1) It provides uniformity in treating deterministic and stochastic models; (2) It is based on a domain theoretic semantics; (3) The environment characteristics are formalized as specific classes of types.

5.4 CPSs Dependability

Dependability represents the ability to deliver service that can justifiably be trusted (see Avizienis et al. (2004)). There is another definition for the dependability concept from the criterion for deciding if the service is dependable point of view: the dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable (see Avizienis et al. (2004)). A systematic exposure of the dependability highlights three concepts: the attributes that define it (reliability, availability, safety, integrity, confidentiality, and maintainability), the means by which it is achieved (fault prevention, fault tolerance, fault removal, fault forecasting) and the threats which it must cope (fault, error, failure).

A team of researchers from the University of Science and Technology, Missouri, United States of America is concerned with CPSs dependability and intends to create a framework for its qualitative and quantitative understanding. The papers "A General Framework for Quantitative Modeling of Dependability in Cyber-Physical Systems: A Proposal for Doctoral Research", "Towards Integrated Simulation of Cyber-Physical Systems: A Case Study on Intelligent Water Distribution", "A Semantic Agent Framework for Cyber-Physical Systems", "Modeling Cyber-Physical Systems with Semantic Agents" (Lin et al. (2009a, b), Lin et al. (2010), Lin et al. (2011)) present the model build by this team using multi-agent techniques. The development of models for CPSs is difficult because the complexity of that kind of system, the fundamental differences in the operation of cyber and physical components and the interdependencies between these components. The agents-based model meets these problems through flexible software agents, which are autonomous, intelligent and decision making entities. The agents-based model has semantic capabilities presented as a semantic ontology for errors detection in water resources management application domain. The ontology represents the physical entities of the CPS (e.g. sensors), as well as the information retrieval, analysis and processing taking place between these entities. Based on the defined ontology, a semantic service model using events was developed, that allows agents to annotate the semantics of data exchanged between the services of the each ontology entity, and to verify and automatically convert semantic data whenever possible. The model implementation was done using the C++ programming language.

The paper "Optimal Adaptive System Health Monitoring and Diagnosis For Resource Constrained Cyber-Physical Systems" (Zhang et al. (2009)) proposes a proactive health monitoring and management (HMM) system that monitors the health condition of a CPS, and diagnoses and identifies the faulty components in case of failures. The HMM adaptive system uses the fault signature matrix (FSM) to associate the CPS components with the rules of the CPS normal behavior and a Diagnosis Quality driven Adaptive Health Monitoring (DQAHM) system model that includes several parameters that can be specified for achieving effective real-time HMM for a CPS, including the CPS resource constraints, the criticality of each CPS component, the resource requirements of the HMM system, and the required diagnosis quality. All these are used to control the sensors activation frequency in order to optimize the overall system diagnosis quality. Also a decision making process is developed to dynamically determine the adaptive HMM system configurations (sensor activation patterns).

The CPSs dependability is also addressed by the paper "Design and Development Methodology for Resilient Cyber-Physical Systems" (Woo et al. (2008)) which proposes a methodology for the design and the development of the CPSs in order to meet all classes of failures (both the hardware and software failures). The failures, affecting the system's ability to properly control its physical actions, represent a challenge that can be achieved using the meta-level monitoring and the response capacity in order to allow high performance and reliable post-failure operations. The design and development methodology unifies in a formal way the software engineering with a series of feedback control laws and with the efficient resources monitoring.

5.5 CPSs Examples

Even if the CPSs foundations are not still finalized, there are research centers that have developed earlier examples of CPSs or have formulated CPSs development challenges in some applications areas. Two examples are described in this subsection.

There are researches on implemented CPSs managing critical infrastructure control (see Flores et al. (2008), Morris et al. (2011). The paper "Engineering Future Cyber-Physical Energy Systems: Challenges, Research Needs, and Roadmap" (Flores et al. (2008)) presents the researches regarding the CPS for energy infrastructure monitoring and control from the north of the United States. This system requires the integration of several heterogeneous physical levels and several networks of decision control, mediated by decentralized and distributed structures of sensors/actuators coupled with an intelligence level, leading to the development of new modeling paradigm for advanced CPSs for energy with embedded security and distributed control.

The paper "Cyber-Physical Systems for Real-Time Hybrid Structural Testing: A Case Study" (Huang et al. (2010)) presents a CPS for real-time hybrid testing of civil structures. The hybrid testing integrates the physical components of the structure with the computation models of other known structural components, thereby significantly improving the purely numerical or empirical approaches. The novelty of the CPS lies in its reusable architecture and its efficient implementation in C++ programming language, within which both cyber and physical components can be integrated flexibly through XML-based configuration specifications.

6. CONCLUSIONS

The paper presents a short state of the art regarding the development of the CPSs - future engineering systems, to which many countries (e.g. USA, EU) pay more attention by offering various funding opportunities. Starting with this study, which highlights the need to develop CPSs in various application domains, the research challenges and the early achievements in this field, the authors will try to build a framework to ensure the *dependability* property of these systems by their behavior evaluation. The evaluation consists of a CPSs event-driven multi-agent model development, able to combine the physical and cyber components and to facilitate the correct study of their interdependences.

REFERENCES

Avizienis, A., Laprie, J.C., Randall, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions On Dependable And Secure Computing*, 1, 11-33.

Baheti, R. and Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology*, 161-166.

Bujorianu, M. and Barringer, H. (2009). An integrated specification logic for cyber-physical systems. In *Proceedings of 14th IEEE International Conference on Engineering of Complex Computer Systems*, 291-300.

CPS-Steering-Group (2008). Cyber-physical systems - executive summary. URL http://varma.ece.cmu.edu/summit.

Flores, A., Quiles, E., and et. al. (2008). New formulation through arti_cial neural networks in the diagnosis of faults in power systems - a modular approach. In *Electronics, Robotics and Automotive Mechanics Conference 2008*, 411-416.

Huang, B. (2008). Cyber physical systems: a survey.

Huang, H.M., Tidwell, T., and et. al. (2010). Cyber-physical systems for real-time hybrid structural testing: a case study. In *Proceedings of ICCPS10*, 69-78.

Lee, E.A. (2008). Cyber physical systems: design challenges. *Technical report no. UCB/EECS-2008-8*.

Lee, E.A. and Seshia, S.A. (2011). *Introduction to embedded systems - a cyber-physical systems approach*. LeeSeshia.org.

Lin, J., Sedigh, S., and et.al. (2011). A semantic agent framework for cyber-physical systems.

Lin, J., Sedigh, S., and Miller, A. (2009a). A general framework for quantitative modeling of dependability in cyber-physical systems: a proposal for doctoral research. In *2009 33rd Annual IEEE International Computer Software and Applications Conference, 668-671.*

Lin, J., Sedigh, S., and Miller, A. (2010). Modeling cyber-physical systems with semantic agents. In *Proceedings of 34th Annual IEEE Computer Software and Applications Conference Workshops*, 13-18.

Lin, J., Sedigh, S., and Miller, A. (2009b). Towards Integrated Simulation of Cyber-Physical Systems: A

Case Study on Intelligent Water Distribution. In *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 690-695*.

Morris, T.H., Srivastava, A.K., and et. al. (2011). Engineering future cyber-physical energy systems: challenges, research needs, and roadmap.

Sha, L., Gopalakrishnan, S., and et.al. (2008). Cyber-physical systems: a new frontier. In *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*.

Sztipanovits, J. (2007). Composition of cyber-physical systems. In *Proceedings of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07)*.

Talcott, C., Wirsing, M., and et. al. (2008). Cyber-physical systems and events. *Software-Intensive Systems*, 101-115.

Tan, Y., Goddard, S., and Perez, L.C. (2008). A prototype architecture for cyber-physical systems. *SIGBED Review*, 5(1).

Wan, K., Man, K.L., and Hughes, D. (2010). Specification, analyzing challenges and approaches for cyber-physical systems (CPS). *Engineering Letters*, 18(3).

Wang, Y., Vuran, M.C., and Goddard, S. (2008). Cyber-physical systems in industrial process control. *ACM SIGBED Review - Special issue on the RTSS forum on deeply embedded real-time computing*, 5(1).

West, R. and Parmar, G. (2006). A software architecture for next-generation cyber-physical systems. In *Position Paper at the NSF Cyber-Physical Systems Workshop*.

Woo, H., Yi, J., and et. al. (2008). Design and development methodology for resilient cyber-physical systems. In *Proceedings of The 28th International Conference on Distributed Computing Systems Workshop*, 525-528.

Zhang, Y., Yen, I., and et. al. (2009). Optimal adaptive system health monitoring and diagnosis for resource constrained cyber-physical systems. In *Proceedings of the 20th International Symposium on Software Reliability Engineering*, 51-60.