Contributing to the Internet of Things

Luis M. Camarinha-Matos, João Goes, Luís Gomes, João Martins

Contributing to the Internet of Things

Luis M. Camarinha-Matos, João Goes, Luis Gomes, João Martins
Departamento de Engenharia Electrotécnica, Faculdade de Ciências e Tecnologia,
Universidade Nova de Lisboa, 2829-516 Caparica, Portugal
cam@uninova.pt

Abstract. The fast development of networked smart devices equipped with sensors and radio-frequency identification, connected to the Internet, is enabling the emergence of many new applications and the redesign of traditional systems towards more effective operation. Raising awareness among engineering PhD students for the potential of this new wave in their research work is a crucial element in their education. With this aim, the doctoral conference DoCEIS'13 focused on technological innovation for the Internet of Things, challenging the contributors to analyze in which ways their technical and scientific work could contribute to or benefit from this paradigm. The results of this initiative, which was reasonably successful, are briefly analyzed.

Keywords: Internet of Things, Cyber Physical Systems

1 Introduction

The fast development of the Internet of Things is enabling the emergence of many new applications and the redesign of traditional systems towards more effective operation. In fact, more and more objects are becoming embedded with sensors and gaining the ability to communicate. New smart devices, but also traditional machinery are "joining the Internet", facilitating the development of more integrated services and optimization of existing systems.

Some of the elements contributing to the wide potential of this area include: remote access / control, more effective monitoring and supervision thus allowing better performance, real-time access to data which supports timely decision making, wider systems integration, complemented with access to cloud-based resources, mobility without losing access to systems, access to large amounts of sensorial data, etc.

Nowadays, a substantial amount of technological innovation is the result of the research works of engineering PhD students. The very nature of the Internet of Things, combining the physical and the cyber worlds, requires the combination of a set of competencies typically covered by the area of Electrical and Computer Engineering. It is however necessary to call the attention of students in this area, which typically tend to focus on a specific research topic, for the potential of the "interconnected things" and the role they can play in this process.

The DoCEIS'13 conference was thus organized with this mission and some of the results are summarized in this paper.

2 Current Trends

The term "Internet of Things" was first proposed by Kevin Ashton in 1999 to describe a system where the Internet is connected to the physical world via ubiquitous sensors. The concept emerged in the context of the developments at the MIT Auto-ID Center on identification technologies.

According to some European views [1], **Internet of Things** (IoT) can be defined as "a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network".

Other definitions put more emphasis on technology: networked smart devices equipped with sensors and radio-frequency identification, connected to the Internet, all sharing information with each other without human intervention [2].

In this context, a "**thing**" could be defined as a real/physical or digital/virtual entity that exists and moves in space and time and is capable of being identified. Things are commonly identified either by assigned identification numbers, names and/or location addresses.

A related concept is represented by the term **Cyber-Physical Systems** (CPS). According to the US National Science Foundation (NSF), CPS are engineered systems that are built from and depend upon the synergy of computational and physical components [3].

Although some literature seems to use the two terms as synonyms, depending on the geographical origin of the authors, IoT can more properly be seen as a subset of CPS (Fig. 1). In fact, the notion of CPS includes not only things connected to the Internet, but also other physical systems embedding computational power. When these systems are geographically distributed and interconnected, they will likely resort to Internet.

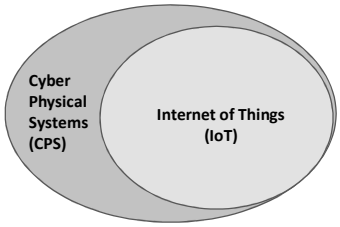

Fig. 1 - Relationship between CPS and IoT

A number of other related terms have emerged in the last decade to represent partial perspectives or focused application contexts. Some examples:

- ***Industrial Internet***. While focusing on industrial applications, it aims a global network connecting people, machines and data with the purpose of facilitating management, operation and maintenance of industrial facilities, and their improving performance. According to General Electric [4], "the full potential of Internet-based digital technology has yet to be fully realized across the global industry system. Intelligent devices, intelligent systems, and intelligent

decisioning represent the primary ways in which the physical world of machines, facilities, fleets and networks can more deeply merge with the connectivity, big data and analytics of the digital world". In this sense, the Industrial Internet can be seen as a subset of the IoT.

- ***Internet of Events***. A perspective of the IoT that puts the emphasis on time dependency and discrete events handling [5]. As such, events modeling and management, time critical reactivity, and process modeling and supervision are the relevant issues here.
- ***Sensing Enterprise***. A concept introduced in the FInES (Future Internet Enterprise Systems) cluster of projects [6] to refer to an enterprise anticipating future decisions by using multi-dimensional information captured through physical and virtual objects and providing added value information to enhance its global context awareness. In other words, it particularly focuses on enriching enterprises' context awareness through intelligent, interconnected and interoperable smart components and devices to power enterprise systems, making them responsive to events in real time and aiming at reaching seamless transformation of (raw) data to (tailored) information and (experienced) knowledge.
- ***Ambient Intelligence***. A concept that represents electronic-enhanced environments which are sensitive and responsive to the presence of people [7]. Therefore it builds upon the notions of pervasive computing, embedded systems, context awareness, and human-centric computer interaction. One of the relevant application areas is the so-called ambient assisted living, which uses technology to assist elderly. IoT is naturally a way to materialize the vision of a technology that becomes invisibly embedded in our natural surroundings, present whenever we need it.

Due to its genesis, closely associated to communities involved in objects identification and logistics applications, IoT has been quite biased by RFID (Radio Frequency Identification) developments. Although RFID is an important enabling technology, it might also limit the vision, making it difficult to harness the full potential of the IoT. In fact, the "things" that can be connected to Internet are not only simple (passive) objects, but rather progressively more intelligent and autonomous "entities" with rich sensorial and acting capabilities. In terms of communications, a mix of wireless and wired forms co-exists. On the other hand, not all RFID applications represent cases of IoT. Under this more general perspective of "things", earlier examples of connection of devices to Internet - toaster, robots, like the Robotgarden, refrigerators, etc. - are important initial cases.

Recent advances in other enabling technologies, e.g. NFC (Near Field Communications), low power devices, embedded intelligence, sensor networks, and novel architectures for the support infrastructures, combined with easier access to resources through cloud computing, are creating the conditions for truly pervasive computing and ambient intelligence, and thus the emergence of a wave of novel applications with wide impact in all sectors of life.

A brief overview of the main milestones in the development of this area is represented in Fig.2.

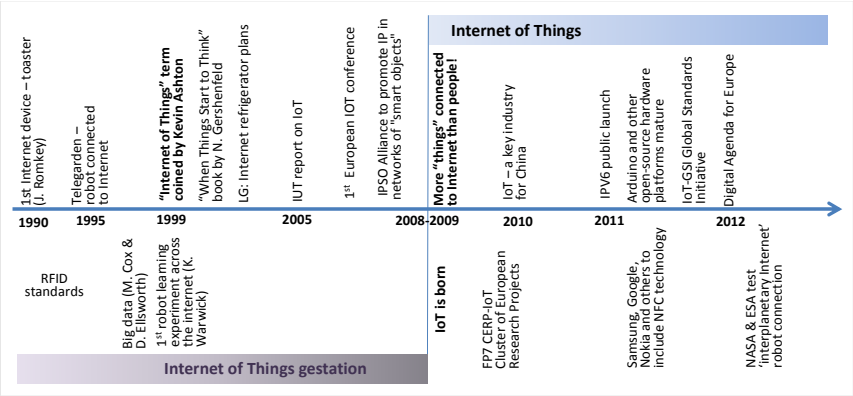

Fig. 2 – Some milestones in the development of the IoT

The area of Internet of Things has been growing in the last years, as represented by the large number of related projects (see [1]) and the Google trends graph (Fig.3).

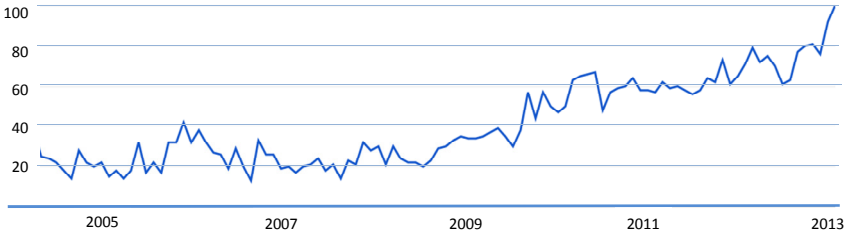

Fig. 3 - Google trends graph for Internet of Things

In terms of application cases, many implementations and futuristic scenarios have been designed for a large spectrum of domains. Some relevant examples are summarized in Table 1.

Table 1: Applications examples

Application domain	Example features
Aerospace and aviation	▪ Fighting counterfeiting - introducing electronic pedigrees for certain categories of aircraft parts: decentralized database, RFID tags, etc. ▪ Wireless monitoring of the aircraft – sensors network detecting various conditions such as pressure, vibrations, temperature etc.
Airports and other hubs	▪ Safety – RFID tags associated to luggage; building security monitoring. ▪ Indoor location systems. ▪ Interaction with customers gadgets: NFC for check-in, payments, etc.
Automotive	▪ Real-time locating systems and connecting with other IoT sub networks, improving vehicle tracking and management. ▪ Dedicated Short Range Communication – Vehicle-to-vehicle and vehicle-to-infrastructure communications (Intelligent Transportation Systems). ▪ The vehicle itself as a 'thing', enabling it to make automatic emergency calls

	or breakdown calls when appropriate, collecting as much data as possible from surrounding 'things'. ▪ Interactions between the vehicle and user's gadgets.
Driving insurance	▪ Pay-as-you-drive: Electronic recorders in the car, which are able to record *acceleration*, *speed*, and other parameters, and communicate this information to the insurer -> cheaper rate or premium. ▪ Similar approach applied to buildings, machinery, etc.
Environment monitoring	▪ Environment surveillance: earth quakes, tsunami, forest fires, floods, pollution (water and air).
Food traceability and agribusiness	▪ Food traceability. ▪ Traceability of agricultural animals and their movements. ▪ Real time detection of animals during outbreaks of contagious disease. ▪ Counting animals in a farm (for subsidies).
Independent Living support	▪ Detecting the activities of daily living, particularly in the case of elderly or people with special needs, using wearable and ambient sensors, monitoring social interactions using wearable and ambient sensors, monitoring chronic diseases using wearable vital signs sensors, and in body sensors. ▪ "Things" can learn regular routines and raise alerts or send out notifications in anomaly situations.
Intelligent / smart cities	▪ Environment monitoring, public safety, urban analytics, emergencies handling, participatory governance, etc. ▪ Integrated multi-modal transportation management (mobility networks), Energy and water management, Waste collection management, etc. ▪ City level social networks (& interaction with gadgets).
Intelligent buildings	▪ Home automation, operation of home appliances. ▪ Sensors for temperature, humidity provide the necessary data to automatically adjust the comfort level and to optimize the use of energy for heating or cooling (ubiquitous sensor networks). ▪ Smart metering for measuring energy consumption and transmitting this information to the energy provider electronically. ▪ Monitoring and reacting to human activity, such that exceptional situations could be detected and people can be assisted in everyday activities e.g. supporting the elderly. ▪ Building security infrastructure.
Intelligent transportation infrastructures	▪ Tolling and vehicle monitoring. ▪ Roads and highways with warning messages and diversions according to traffic and climate conditions and unexpected events like accidents or jams. ▪ Smart parking, traffic congestion management, etc.
Manufacturing & Product Life Cycle management	▪ Embedded smart devices or the use of unique identifiers and data carriers that can interact with an intelligent network infrastructure and information systems: optimization of processes, refine schedules, and improve logistics. ▪ Product's usage history along its life cycle (from cradle to grave). ▪ Remote maintenance and updating of manufacturing equipment.
Medical technology, healthcare	▪ Measurement and monitoring methods of vital functions (temperature, blood pressure, heart rate, cholesterol levels, blood glucose etc). ▪ Implantable wireless identifiable devices could be used to store health records that could save a patient's life in emergency situations. ▪ Edible, biodegradable chips could be introduced into the body and used for guided action.
Operation in dangerous environment	▪ Tele-operation and tele-presence, Tele-supervisory control, etc. ▪ Detection of gas levels and leakages in industrial environments. ▪ Under water exploration, fire fighting, etc.
Retail, Logistics,	▪ RFID-equipped items and smart shelves: automatically checking of goods receipt, real time monitoring of stocks, tracking out-of-stocks or the

Supply Chain Management	detection of shoplifting. ▪ Improving logistic processes with RFID data. ▪ Guidance in the shop according to a preselected shopping list, fast payment solutions like automatically check-out using biometrics.
Safety and security monitoring	▪ Building monitoring: water leaks, gases, vibrations, fire, un-authorized entry, vandalism. ▪ Personnel: mugging alarm, equipment surveillance, payment systems, identity security.
Smart grid	▪ Advanced metering, supporting more effective energy management. ▪ Interaction with smart appliances. ▪ Intelligent monitoring. ▪ Demand response and value added services

As it becomes clear in the above application examples, the Internet of Things is a multi-disciplinary subject that requires the integration of contributions from multiple technologies. Table 2 lists the most relevant ones and summarizes the key issues to be addressed in each one.

Table 2: Involved technologies

Technology	Illustrative key issues
Communication technology	Energy efficient bi-directional communications, Multi-frequency, wireless sensor networks, message-queue based communications targeting cloud environment, etc.
Network technology	Protocol gateways, Scalable architectures, Secure & reliable wireless communication protocols, service based network, etc.
Network discovery	Automated discovery mechanisms and mapping capabilities (new "things" continuously appear / disappear, some "things" evolve)
Software and algorithms	Micro operating systems, Service oriented computing, Applications in cloud environments, Self-adaptive software (autonomic systems), Bio-inspired algorithms, Energy-aware systems, Context aware software, Events management, Balancing local vs. cloud intelligence and decision making, Objects' representation (services, agents), etc.
Hardware devices	Nano-electronic smart devices, Energy harvesting, Polymers electronics, Embedded intelligence, Low cost tags, Smart devices, Multi-standard protocols, Heterogeneous architectures, Low cost devices, etc.
Data and signal processing technology	Semantic interoperability, Data sharing, Data aggregation, Stream processing, Big data processing, etc. Making sense of the massive amounts of data that can be generated by intelligent devices (big data) is one of the key components of the IoT.
Discovery and search engine technologies	Device discovery, Distributed repositories, Positioning and localization, Terrestrial mapping, Location awareness, etc.
Power and energy storage technologies	Batteries / micro-batteries, Energy harvesting, Energy consumption mapping, Energy-based priority scheduling, dynamic tariffs, etc.
Security and privacy technologies	Privacy for heterogeneous devices, Decentralized authentication and trust, Energy efficient encryption, Anonymity mechanisms, Data ownership, etc.
Standardisation	Standards for cross interoperability, Standards for intelligent devices, Languages for things interaction, Standard infrastructure architectures, etc.
Relationship network management technologies	Identity, relationship and reputation management, Organizational structures, Collaborative models and functions, Collective intelligence, Traceability of distributed decision making, etc.

A comprehensive research and development agenda for IoT can be found in [1]. In addition to the purely technological issues, there are other relevant aspects to be properly addressed in order to let the full potential of IoT be achieved. These include: Legal and regulatory aspects, Socio ethical aspects, and Economical aspects.

Although considerable research and practical developments were made during the last two decades, it is likely that substantial efforts are still needed in this area, as illustrated by the Gartner's hype cycle (Fig. 4). According to this forecast, it will still take more than 10 years to reach the "plateau of productivity" in this area.

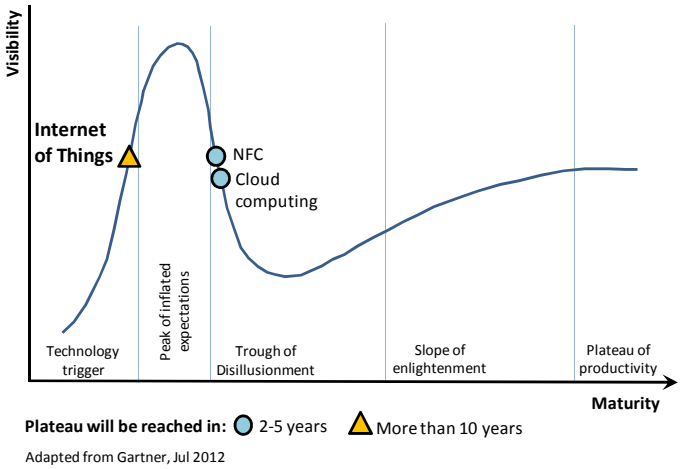

Fig. 4 - Hype cycle for Internet of Things (adapted from Gartner's [8])

3 Example Contributions

IoT is a particularly relevant topic for Electrical and Computer Engineering (ECE) researchers and professionals. In the last decades the scope of ECE has expanded so widely that it risks some "fragmentation". Most professionals (and students) focus on a specialization sub-field, rarely mastering a comprehensive view of the whole field. Since IoT requires a "strong dialogue" among the various sub-fields of electrical and computer engineering (and other areas), it represents a potential gluing element to bring them together.

Under this assumption, a challenge was presented to DoCEIS'13 conference participants [9] (doctoral students from various countries and different sub-fields) as summarized in the following questions:

- *In which aspects your research can contribute to the development of the Internet of Things?*

or

- *In which aspects your area of work could be affected / influenced in the future by the development of the Internet of Things?*

As a result, all contributors made an effort to analyze the relationship between their specific research work and the IoT. Among the accepted papers there is an almost balanced distribution between those that contribute to the development of support technologies for IoT and those that can benefit from IoT adoption [9], as summarized in Fig. 5. The size of the rectangles is proportional to the number of contributions in each specific sub-field.

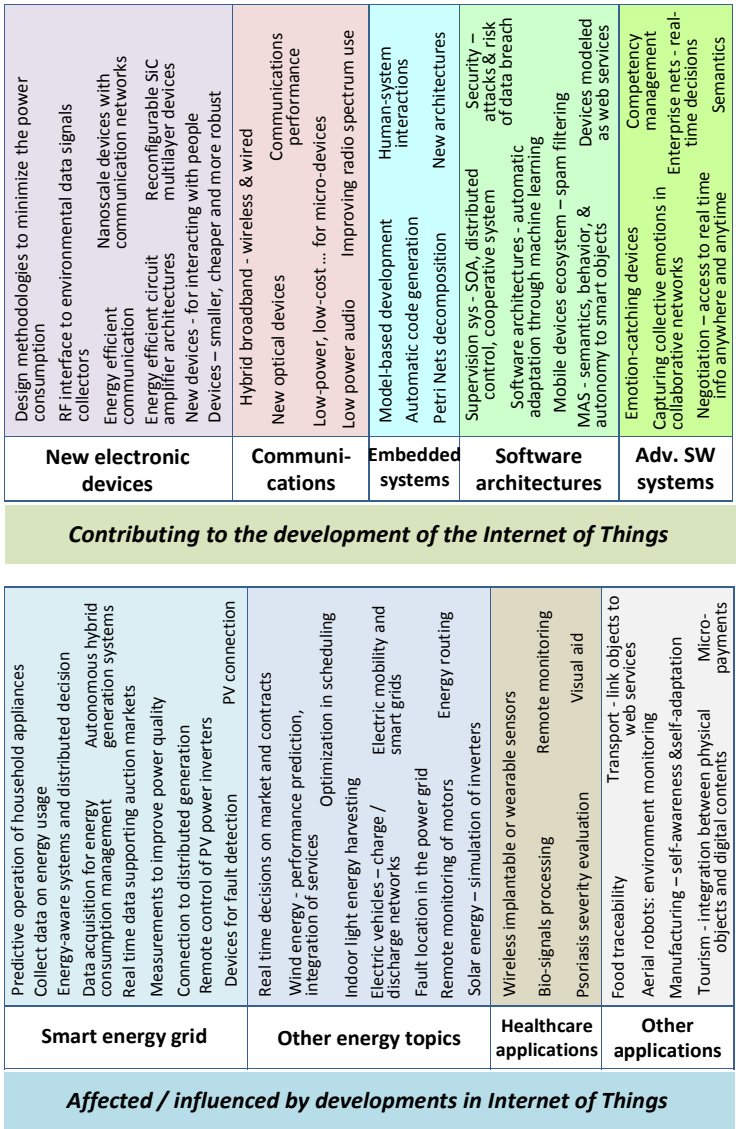

Fig. 5 – DoCEIS'13 contributions to IoT

4 Open challenges

From the analysis of the state of the art and also considering the sample of contributions to DoCEIS'13, it becomes evident that more attention needs to be devoted to the system level. Such system perspective is needed in order to better understand and manage complex IoT environments.

More and more we live surrounded by large numbers of devices with growing (embedded) intelligence / sensing and computational power, connected to Internet, and forming complex inter-dependent systems. These devices can typically be "represented" in the cyber-space by service entities (or agents). The combination of physical devices with their "cyber representatives" constitutes a cyber-physical system. In this environment, devices / representatives can "appear and disappear" from the cyber-space.

Devices / sub-systems typically have an "owner"; therefore, in addition to the growing autonomy of such entities (which comes from the growing intelligence / cognitive capabilities), they also have to "obey" to their owners, which introduces a new dimension to the problem of designing such systems. When systems involve a large number of entities (hundreds? thousands? millions?), flat organizational structures are not appropriate. Therefore some "structural thinking" is necessary, leading to the organization of such entities in "communities" or "societies" ("ecosystems") of cyber-physical artifacts (Fig. 6). Important issues in these "communities" are the definition of "borders" / membership, roles, and evolution.

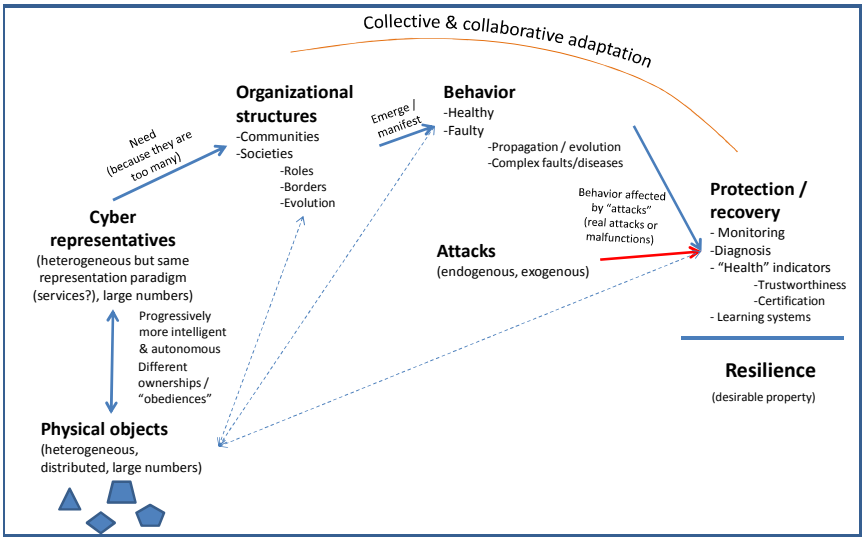

Fig. 6 - Toward sustainable IoT-based systems

In organized communities – and depending on their design / purpose – different behaviors can emerge. Some behaviors are consistent with the system's purpose (healthy behaviors). But we can also have faulty / deviating behaviors. These are particularly critical as complexity increases and we become more dependent on such systems. Understanding (and detecting) faulty behaviors is thus critical. How do these

behaviors propagate / extend over "different regions" of the communities? How do they evolve? How can systems adapt to faulty situations? Collaborative networks and collective adaptive systems principles are important here.

Faulty behaviors can have an endogenous source (component's malfunctioning, interoperability "frictions", non-collaborative behavior, etc.) or result from exogenous attacks (e.g. terrorist cyber-attacks). It is therefore necessary to develop adequate protection / recovery approaches and mechanisms. This involves distributed monitoring, (collective) diagnosis of detected faulty behaviors, and launching recovery / self-healing processes. Considering the complex nature of such systems, it is important to first elaborate some "health indicators", including system's trustworthiness indicators, system's certification, etc. How much can we trust in systems that we do not fully understand and over which we do not have full control (as they are complex, evolving, components belonging to different owners, etc.)? Learning mechanisms should be an intrinsic functionality here.

5 Concluding Remarks

Developments in the Internet of Things are having a strong impact in all sectors of society and their importance is likely to grow in the coming years.

The needed technological components and approaches to connect the physical and the cyber worlds open important expansion opportunities for the area of Electrical and Computer Engineering. This is clearly reflected in the contributions to the DoCEIS'13 (4th Doctoral Conference on Computing, Electrical and Industrial Systems).

References

1. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. (Eds.) (2010). Vision and Challenges for Realising the Internet of Things. CERP-IoT, European Commission.
2. Pretz, K. (2013). The Next Evolution of the Internet. *The Institute*, IEEE, 7 Jan 2013, http://theinstitute.ieee.org/technology-focus/technology-topic/the-next-evolution-of-the-internet.
3. NFS (2012). Cyber-Physical Systems (CPS). http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286, accessed on 4 Feb 2013.
4. Evans, P.C.; Annunziata, M. (2012). Industrial Internet: Pushing the boundaries of minds and machines. *GE report*, Mar 2012. www.ge.com/docs/chapters/Industrial_Internet.pdf
5. Ortner, E.; Schneider, T. (2008). Temporal and Modal Logic Based Event Languages for the Development of Reactive Application Systems. In: *Proc. 1st International workshop on Complex Event Processing for the Future Internet*, 28-30 Sep 2008, Vienna, Austria.
6. FInES (2011). A European Innovation Partnership for Catalysing the Competitiveness of European Enterprises. Position Paper on Orientations for FP8, European Commission, http://cordis.europa.eu/fp7/ict/enet/documents/fines-position-paper-fp8-orientations-final.pdf
7. Cooky, D.; Augustoz, J.; Jakkula, V. (2009). Ambient Intelligence: Technologies, Applications, and Opportunities. *Pervasive and Mobile Computing*, 5(4), pp 277-298.
8. LeHong, H.; FennKey, J. (2012). Trends to Watch in Gartner 2012 Emerging Technologies Hype Cycle. http://www.forbes.com/sites/gartnergroup/2012/09/18/key-trends-to-watch-in-gartner-2012-emerging-technologies-hype-cycle-2/
9. Camarinha-Matos, L.M.; Tomic, S.; Graça, P. (2013). Technological Innovation for the Internet of Things. *Proceedings of DoCEIS 2013*, Springer, IFIP AICT Series 394.