Building enhanced environmental traceability solutions: From Thing-to-Thing communications to Generalized Cyber-Physical Systems

Borja Bordel[1]*, Ramón Alcarria[2], Miguel Ángel Manso[2] Antonio Jara [3]
[1]Department of Telematics Systems Engineering. Universidad Politécnica de Madrid, Spain
bbordel@dit.upm.es
[2]Department of Topographic Engineering and Cartography. Universidad Politécnica de Madrid
ramon.alcarria@upm.es, m.manso@upm.es
[3]Institute of Information Systems. University of Applied Sciences Western Switzerland
jara@ieee.org

Abstract

In the last decade, many different paradigms related to the named "next-generation technological systems" have appeared: from the Internet-of-Things to Cyber-Physical Systems and Machine-to-Machine communications. Traditionally these systems only consider hardware devices in their designs. However, the experience has proved that the really valuable solutions are which are human-focused or environment-focused (biological signal monitoring, people traceability, assisted-living, etc.). In this context, previous machine-focused paradigms have to be redefined. Therefore, this paper analyzes the requirements of technological solutions for environmental monitoring and proposes a coherent framework for their design. Moreover, most important components are identified and some relevant problems in this field are addressed; mainly the identifier management and the system modeling. Finally, a prototype for people traceability based on the proposed paradigms and Bluetooth Beacons technology is described. Results showed that the quality of the provided information is much higher in these new systems than in traditional approaches.

Keywords: Thing-to-Thing communications, Generalized Cyber-Physical Systems, people traceability, ubiquitous computing, pervasive sensing, environmental monitoring

1 Introduction

Cyber-Physical Systems (CPS) are integrations of physical and computational processes [16]. Although there is not a unified definition, this paradigm refers to a new generation of embedded devices, being able to interact in an enhanced way with the physical world [9]. In this way, communications between elements in a CPS must be based on machine-to-machine (M2M) techniques (those totally and automatically managed by devices [17]). Other similar systems, such as the Internet-of-Things (IoT) or the Wireless Sensor Networks (WSN), also belong to this new generation of engineered solutions and are usually analyzed together. A typical architecture for any of these systems (see Figure 1) does not include humans or any other living creature or environmental element (total automatization is the final objective). However, in the last years, it has been proved that the really interesting applications in this new era are which have humans and their environment as central actor. Many works related to biological signal monitoring [28], human traceability [9], human activity analysis [21], assisted living [30], etc. have been

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 3, pp. 40-56

*Corresponding author: E.T.S.I. Telecomunicación. Universidad Politécnica de Madrid. Avenida Complutense n^{o} 30. 28040 - Madrid (Spain), Tel. (+34) 91 549 57 00 ext. 3035 reported; and several successful commercial applications in this field have been placed into the market [22]. In this context, some authors have identified a new problem named as “the human-in-the-loop problem” [36]. It refers to the introduction of humans in the new technological systems, primary designed to operate without considering any human factor. Different roles have been identified for humans in these new solutions, although it is not clear how supporting the human intervention.

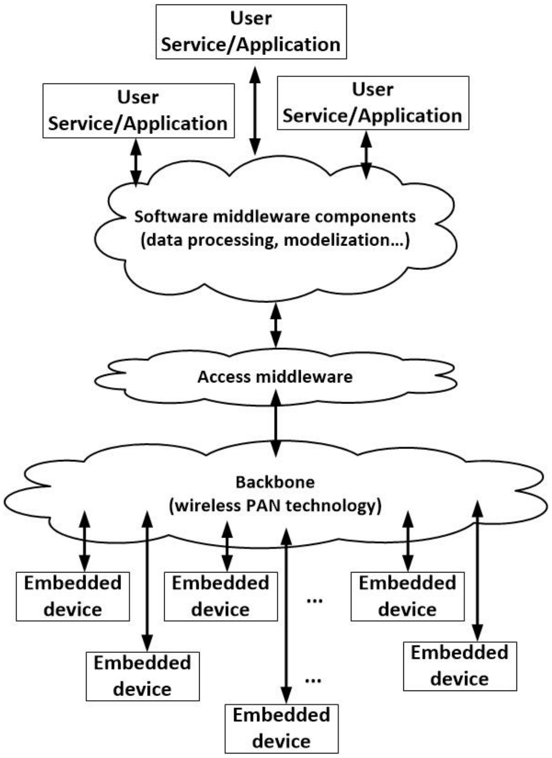


Figure 1: General architecture for a next-generation technological system

Some new paradigms, such as the humanized Cyber-Physical Systems [6], have been proposed, but they only cover some particular aspects of the problem (for example, the integration of humans as service providers). Many important issues, then, are not addressed (such as the way in which animals and other living creatures may be integrated into the system). Moreover, environmental monitoring or traceability solutions require specific instruments not usually included in traditional technological frameworks. In particular, it is required a representation and modeling instrument, and every element (or thing) in the environment must be provided with a hardware device (which cannot be seamless integrated because of obvious reasons) and an identifier.

Therefore, in this paper it is proposed a new concept named as Generalized Cyber-Physical Systems (GCPS) specially designed to support environmental traceability solutions using the CPS principles and other technological paradigms of the new era. In this context, Machine-to-Machine communications turn into Thing-to-Thing communications, as important information comes from living creatures and other physical elements, not from embedded machines (as occurs in WSN or IoT scenarios). Besides, the proposed framework and architecture consider different layers focused on representing the state of the environment being monitored (a UML model for this type of solutions is described).

The rest of the paper is organized as follows: Section 2 introduces the state of the art in studies about the integration of humans and other living creatures in technological systems. Section 3 proposes the concept of GCPS and a framework to design environmental control solutions, and analyzes the transition from the Machine-to-Machine (M2M) paradigm to the Thing-to-Thing (T2T) approach. Besides, the problem of the identifier management in these solutions is described and discussed. Section 4 provides an experimental validation based on a system designed following the described principles. Finally, Sections 5 and 6 describe some experimental results and some conclusions of our work.

2 State of the Art

Applications of CPS to traceability are numerous. Most of them are based on RFID (Radio Frequency Identification) solutions [37], where regular Things are provided with a miniaturized RFID chip [9]. However, recently, other proposals based on Wireless Sensor Networks [42] or Smart Transducers have been reported [6]. In general, nevertheless, all these papers consider CPS as a collection of physical objects which are operated by users, who are external participants. This vision is currently changing and each time more proposals of CPS including humans and other living creatures are reported.

Different proposals about human and other living creatures into CPS, WSN or IoT scenarios have been proposed.

As said in the Introduction, the "human-in-the-loop" systems are a special type of CPS which include humans in different roles. Basically, three different types of systems including people have been identified [29]: (i) systems directly controlled by humans, (ii) systems monitoring humans which take appropriate actions, and (iii) a combination of (i) and (ii). However, despite this exhaustive analysis, most works related to human-in-the-loop systems and applications are focused on monitoring humans [36, 18, 18], as it is the most challenging and revolutionary proposal. Any case, apart from the challenges identified for human integration into CPS, other aspects (such as animal traceability) are not addressed. Besides, in many applications humans are considered as a part of the environment instead of a new element in the CPS.

Some remarkable works in the field of human-in-the-loop systems are which are focused on univocally assigning identifiers to people [40]. These works may be used as the first step in traceability solutions, as they allow managers to change dynamically the identification of humans.

Other important proposals describe the called "Humanized Cyber-Physical Systems" [6]. This concept refers to CPS where humans are provided with the required instruments to be considered service providers, in the same way as sensors, actuators and the rest of hardware devices. Different proposals on the self-configuration of these systems [6], their design [44, 45] or about other similar ideas such as the "humanized cyber-physical services" [1] may be found.

Some relevant works about CPS consider animals as an additional regular actor by default [5] . Animals are provided with sensing instruments [5] or are monitored using enhanced pattern recognition techniques [39] in the same way than humans. A similar research line is focused on animal control, using cyber-physical technologies. The basic idea of these proposals is to seamless integrate electronic devices (in particular, smart sensors and actuators) into animals with the objective of controlling their behavior [41] [43].

In respect to the inclusion of other living creatures in the system, different proposal may be found. Some of them are focused on the integration of miniaturized electronic devices into animals or plants [31]. However, these proposals are complicated to apply to uncontrolled or ad hoc scenarios. Most remarkable works analyzed natural emergency situation (for example, a forest fire [31]). In these works mathematical model to understand the living creature behavior are executed using cyber-physical instruments. These ideas are very valuable, as may support advanced services in traceability solutions. Finally, in the last group of works, animals are passive agents, whose lives are improved by means of specific services supported by a Cyber-Physical infrastructure [3, 14] (for example, they might be moved during grazing to enhance the nutrients in the field).

In comparison with all these previous proposals, our work proposes a coherent general framework, being able of considering both humans and other living creatures (in any of the possible roles). The basic idea is to monitor the environment and the activities of the creatures and humans; as well as to trace the aspect related to them which are considered relevant.

Considering these different approaches, different models and various modeling techniques for CPS have been described. Models based on semantic agents [26] are the most recent proposal. However, models based on matrix algebra [20] for pervasive sensing platforms based on CPS paradigm, and traditional solutions based on hybrid techniques [15] may be also found. In general , nevertheless, these proposals do not cover the entire stack of layers described for CP in the most common CPS reference architectures [9][8]. In this work, therefore, it is proposed a UML model covering all the relevant aspects of CPS [7].

3 A New Cyber-Physical Framework for Traceability

In this Section it is proposed a general framework for traceability, based on the integration of humans and other living creatures into CPS. This new type of systems is called Generalized Cyber-Physical Systems, and presents a specific architecture which is analyzed and described in the first subsection. In the second subsection it is presented the concept of Thing-to-Thing communications and discussed the identifier management. In the third subsection the system modeling is addressed.

3.1 General Framework: Analysis and Proposal

A generic traceability system is basically composed of two different sub-systems: the data acquisition and the information representation (see Figure 2 (a)). This division is also valid for Cyber-Physical Systems (see Figure 2 (b)) where the “Modeling” layer is specifically focused on information representation and “Sensors and actuators” on information acquisition.

As main difference, traditional traceability solutions consider elements to be monitored as external entities to the system, but CPS include all the creature or devices with interact with other components in the system. In this context, traceability solution in the new era (the Industry 4.0, as called as the era of the CPS [24]) must follow the principles of the Cyber-Physical infrastructures. In that way, traditional CPS are insufficient as they are only focused on environmental monitoring (temperature, humidity, etc.). Furthermore, other definition such as Humanized CPS [6], Industrial CPS [11], etc. present the same problem, as they only consider a certain part of the physical world.

In order to overcome these problems, a new definition is proposed: the Generalized Cyber-Physical Systems (GCPS). A GCPS is a CPS which integrates industrial production systems, humans, other living creatures, and any other desired element into its physical platform in the same way as embedded devices, sensors and actuators. These new elements must be able to provide services, execute processes, and perform any other activity which previously was supported only by hardware devices.

GCPS require including new components in the systems, specifically focused on adapting the new elements in the physical platform to the interfaces in the high-level layers. In that way, as User-focused components were defined in Humanized CPS; in GCPS we define the “Dedicated components” to fulfill these requirements (see Figure 3 (a)). Considering these definition, richer reference architecture for GCPS may be proposed (see Figure 3 (b)).

Basically, five different new layers have been included in the “Modeling level”. These new layers represent a virtual instance of the system (or system daemon, using the proposed terminology) which describe the state of the physical platform and the environment. Using this daemon the geographically sparse architecture of a GCPS (especially if the environment to be monitored occupies a large area) may

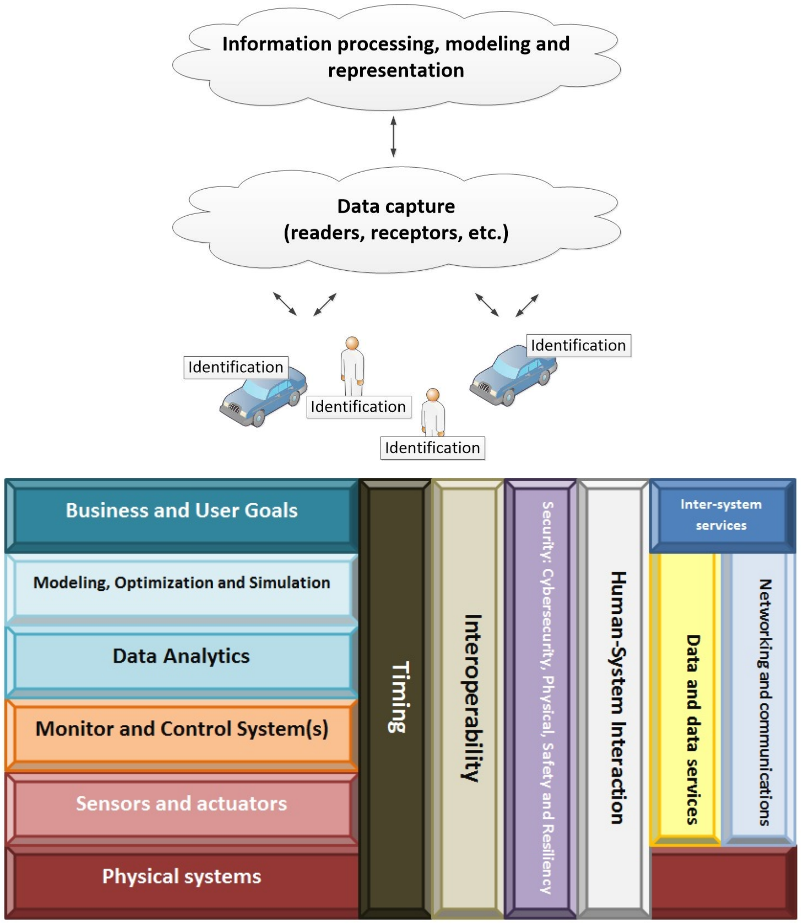


Figure 2: Basic architecture (a) traditional traceability systems (b) Cyber-Physical System

be managed in an easier way. Besides, other functionalities such automation, intelligence, etc. and other cognitive capabilities are supported in a centralized manner. Finally, this daemon allows user to obtain information about the current and past state of the system in a very fast way and, if required, future predictions about the CPS could be also calculated. Below, the five different new layers are analyzed [35]:

- Virtualization interface: This layer offers an interface to invoke virtualization functionalities (such as create a new daemon, halt an instance, etc.). This interface offers the possibility of automating the management of the system daemons (for example, to create dynamically one when required).
- Virtual services layer (VS layer): A virtual service (VS) is an abstract representation of real service offered at medium-level (usually named as ”production level” [32]). This layer allows managing the lifecycle of services, and (in our case) it contains the monitoring and traceability (and possibly prediction [10]) services employed in traceability solutions.
- Composite virtual devices layer (CVD layer): A composite virtual device is a virtual instance representing a group of virtual devices which work together in order to reach a common objective (for example, execute a service). These instances are managed at the appropriate layer. Examples of CVD are a set of sensors connected to a broker, or a subsystem including different embedded devices.

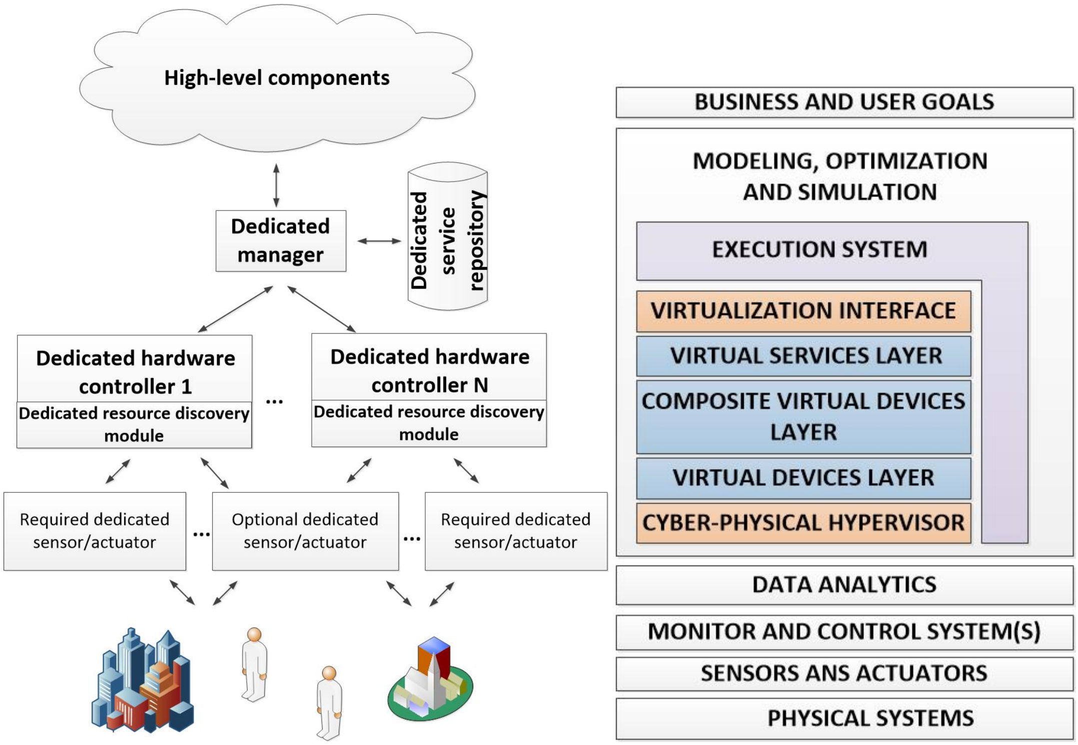

High-level components
Dedicated manager
Dedicated service repository
Dedicated hardware controller 1
Dedicated resource discovery module
...
Dedicated hardware controller N
Dedicated resource discovery module
Required dedicated sensor/actuator
...
Optional dedicated sensor/actuator
...
Required dedicated sensor/actuator
BUSINESS AND USER GOALS
MODELING, OPTIMIZATION AND SIMULATION
EXECUTION SYSTEM
VIRTUALIZATION INTERFACE
VIRTUAL SERVICES LAYER
COMPOSITE VIRTUAL DEVICES LAYER
VIRTUAL DEVICES LAYER
CYBER-PHYSICAL HYPERVISOR
DATA ANALYTICS
MONITOR AND CONTROL SYSTEM(S)
SENSORS ANS ACTUATORS
PHYSICAL SYSTEMS

Figure 3: Architecture of a GCPS (a) functional (b) reference

- Virtual devices layer (VD layer): Virtual devices refer to a representation of the embedded devices in the system (usually sensors and actuators, but also the called "self-managed devices" -see Section 3.3-). This functionality is useful in scenarios considering a geographically sparse infrastructure (for example, a company with different locations which desirers a complete description about the state of the entire company in the headquarters, such as it is offered in SCADA systems).
- Cyber-Physical hypervisor: This layer represents a specific hypervisor technology, focused on turning independent the real infrastructure from the virtual instance. Different virtualization techniques for CPS have been reported [19, 4].
- Apart from the previously cited layers, an execution system has to be also considered, in order to execute the user applications and services, described at the highest level. This system has been presented in previous works [32].

Finally, in order to create the daemon and the contained VD and CVD, it is necessary to acquire the required information to create a successful virtual representation of the system. Moreover, it is needed a model to represent all devise and elements in the system, used as base for the creation of the system daemon.

In the next subsections, both solutions are described: data acquisition and system modeling.

3.2 Data Acquisition: T2T Communications

In traditional traceability systems, every element to be monitored is provided with an electronic device containing a unique identifier which describes the identity of the element. In this context, the same identifier (for example when using RFID tags) allows the element to be identified, to be identified the embedded electronic device, to manage communications, etc. In that way, communications are (at the end) described as Machine-to-Machine communications (M2M) as the objective is to communicate the embedded device with a remote machine in an automatic and self-managed way. Thus, information is provided by the embedded device, not by the element to be monitored.

When using GCPS, this vision changes. Now, not every object, human or element (hereinafter "Thing" in a global way) is provided with an embedded device, as "Things" may be monitored using many other types of techniques and data analysis algorithms (such as implicit interactions [23]). Nevertheless, each Thing has to be provided, in the same way, with a unique identifier (which is part of its identity). In this new paradigm M2M communications are not valid, as information is directly provided by the Thing to be monitored. Then, we use the new concept of Thing-to-Thing communications (T2T).

T2T communications [38] is an emerging term, typical from Industry 4.0, next-generation IoT systems and CPS applications, describing a scenario where a physical Thing (including humans and any other living creature) communicates with some remote physical Things (in an automatic, implicit and self-managed way) through a technological infrastructure (typically a communication network).

In the analyzed traceability systems, T2T communications are used by environmental things to inform the central system about their position, presence, state, etc. Then, the provided information is collected and employed to instantiate the system daemon.

In this new context, however, identity management is a very complicated task. As not every Thing is provided with an embedded device containing a unique identifier, the identity of a monitored Thing is composed (at least and necessarily) of four different numbers (identifiers):

- *Monitored Thing ID (MT_ID)*: This identifier it is associated with the Thing to be monitored and characterizes it. It is created, defined and assigned by the system managers. In general no global or international organism is in charge of the management of these identifiers.
- *Associated device ID (AD_ID)*: In order to be able to communicate with other remote elements, each Thing has to be associated a device providing this functionality. This device has to be also provided with an identifier. A same device may be associated with different Things at different moments. In computer sciences, these identifiers are called OUI (Organizationally Unique Identifier). They are composed by 24 bits and are managed by the IEEE (such as MAC addresses, which could be also employed as AD_ID).
- *Communication management ID (CM_ID)*: This identifier depends on the network where the associated device and/or the monitored Thing are integrated. In global communication networks (such as Internet) they are manage by international organisms, although in local deployment (Bluetooth networks) might be assigned by system owners. IP addresses are the most common example.
- *Platform management ID (PM_ID)*: Finally, a provisional identifier is required to communicate and manage the associated device and the monitored Thing before to be integrated in a communication network. This identifier may be a specific address (or set of addresses) specifically booked for this purpose (as in the Internet) or a new and provisional identifier as in mobile networks.

The total identity of a monitored Thing, which changes dynamically, depends on the four previously named numbers. It is not clear how the four identifiers have to be composed and related (or even if they must be related in some way) in order to create the global Thing's identity. Proposals from the computer networks world usually deal with hierarchical constructions (in a similar way as in the IPv6 standard some identifiers are calculated from others) or the creation of Internet-like directions (for example, MT_ID@CM_ID/AD_ID). On the other hand, mobile communication experts usually prefer to employ the four identifiers in an independent way, considering four different registers and application scopes. In our case (see Section 4) we are using four independent numbers.

3.3 Modeling a Generalized Cyber-Physical System

In order to represent in a correct way the system state using the functionalities of the system daemon, it is required a model for GCPS including all the possible elements in those system. Figure 4, Figure 5, and Figure 6 represent a UML model describing an entire GCPS. In order to propose and validate the describe model, it has been taken into account different sources: the Berkeley's conceptual map about CPS [13], relevant works about CPS modeling [15, 25, 27], and previous practical experiences on next-generation technological systems simulation [2, 33]. Below the most important aspects are explained.

First, as can be seen, GCPS are made of two different types of elements: cyber elements and physical elements (but both belong to the system). Some examples of physical elements are provided (some of the most important) but others could be considered. On the other hand, cyber elements correspond to the layer in the reference architecture showed on Figure 2.

Sometimes transducers are implemented in a same physical device together with control components, creating a self-managed device. If a self-managed device, besides, is able to execute scripts and processes described at prosumer level, then it is said the device is a sub-system. Sub-systems are very typical in humanized systems, as people are able to understand prosumer language without problems (for example, if natural language is considered as prosumer description language). In other cases, sensors and actuators could be connected among them through a wireless broker, acting as control component.

In respect to processes, their classification, descriptions and decomposition have been analyzed in detail in the state of the art [32]. Same considerations may be done in respect to physical object and variables [34].

Considering the proposed UML diagram, and the previously described architecture, the activity diagram of the proposed tool is presented on Figure 7. As can be seen, the described UML model is instantiated in two steps. During the first phase, physical constraints are generated: the number of involved people, the physical configuration of the scenario, etc. In order to create the corresponding simulation script, information from users and the real deployment is collected. All interaction between the real deployment and the virtualized platform are performed trough the cyber-physical hypervisor, which provides the adequate interface. During second phase, cyber elements are instantiated (as well as services) and system operation starts. The system state is constantly updated considering the events coming from the real deployment. When timer expires, for example at end of a working day, statistical results are showed to managers.

4 Experimental Validation

An experiment was designed in order to validate the proposed solution as a valid technology for creating enhanced traceability solutions. In order to perform the experiment a traceability systems based on Bluetooth Beacons was constructed.

Fourteen (14) people were provided with an independent hardware device storing a 16-bits number acting as humans' identity. Each device, besides, was provided with a MAC address by the manufacturing company (Samsung, in this case), so this identifier was employed as Associated device ID.

As hardware platform, it was selected the Artik 020 architecture, consisting on C-programmable microprocessor and a Bluetooth Low-Energy communication module. In that way, communications management ID was selected by experts among all the available addressed (in this case it was selected a broadcast address, so the same identifiers could be used as CM_ID and PM_ID). Devices were configured to act as Beacons (see Figure 8).

The system was deployed in an open laboratory of the Technical University of Madrid, where people provided with electronic devices were asked to perform a certain itinerary. A one square kilometer area was employed to perform the experiments. Different obstacles were deployed in the area, so it

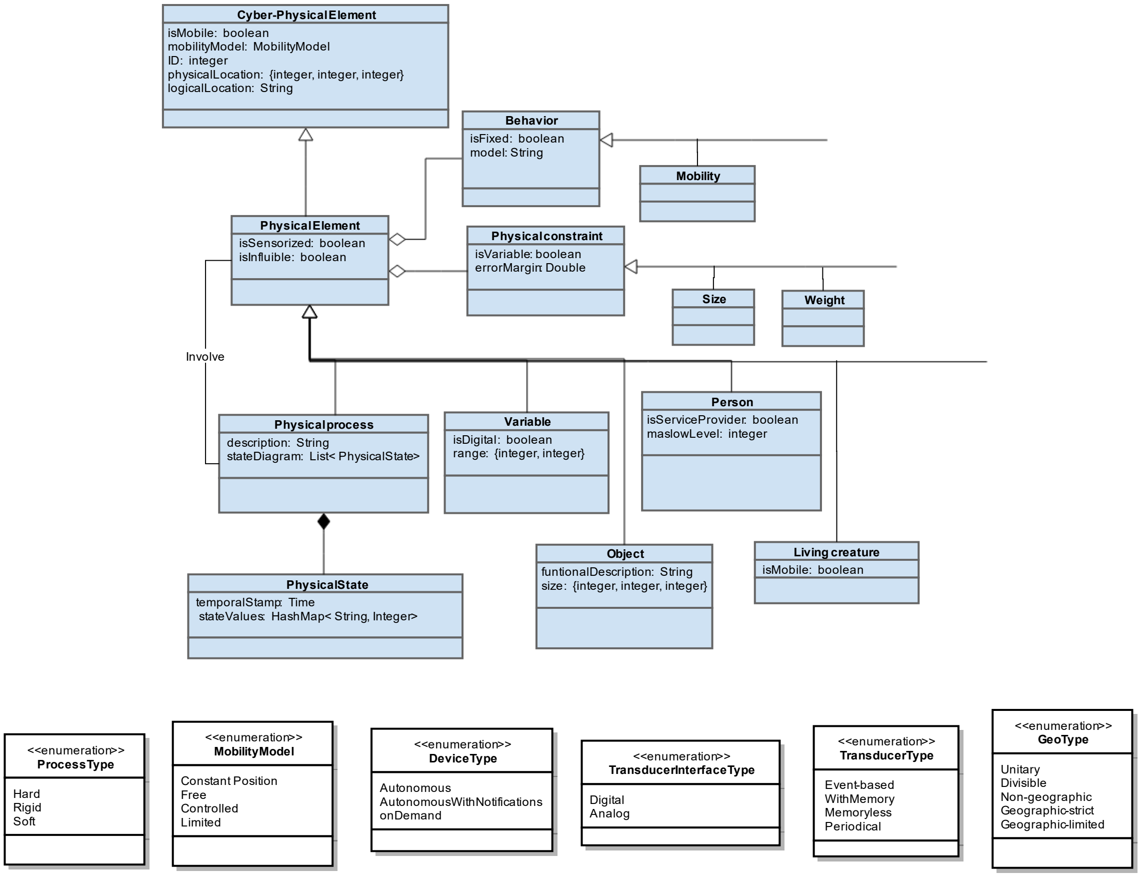


Figure 4: UML description of a GCPS (part 1)

was monitored if people were able to cross them, the time they employed, etc. In order to monitor the people actuation, different Artik 530 platform were deployed around the environment. These machines, in addition to Bluetooth communications, they are able to use WiFi technology. Using this interface, data about people were sent to a remote host, were a Java application was running. That application was described in different previous works about traditional traceability systems [9]. At the same time, data were introduced in a system daemon, previously configured using the Libvirt library (as Samsung Artk 530 platform is based on Linux machines).

Selected traditional traceability systems were exhaustively described in the state of the art [9]. It consists of a system involving some RFID-powered elements such as gloves and tables. These devices are connected with a central server where information from hardware devices is collected and processes in order to track the itinerary of the object under study. A second system was also deployed, based on a pre-CPS view [12]. In particular, in this system, regular workers are in charge of evaluating the quality and evolution of the product, employing different media to notify changes to the control system.

Records created using both methods (Java application as in traditional traceability systems and a virtual instance of the system as proposed in GCPS) were stored. At the end of the experiment, people were asked to describe their itinerary as much detailed as possible. The three information sources were compared.

Simulation description language was based on a objet-orient programming language, such as C++ (employed in other popular simulator such as NS3). Figure 9 shows a fragment of the proposed sce-

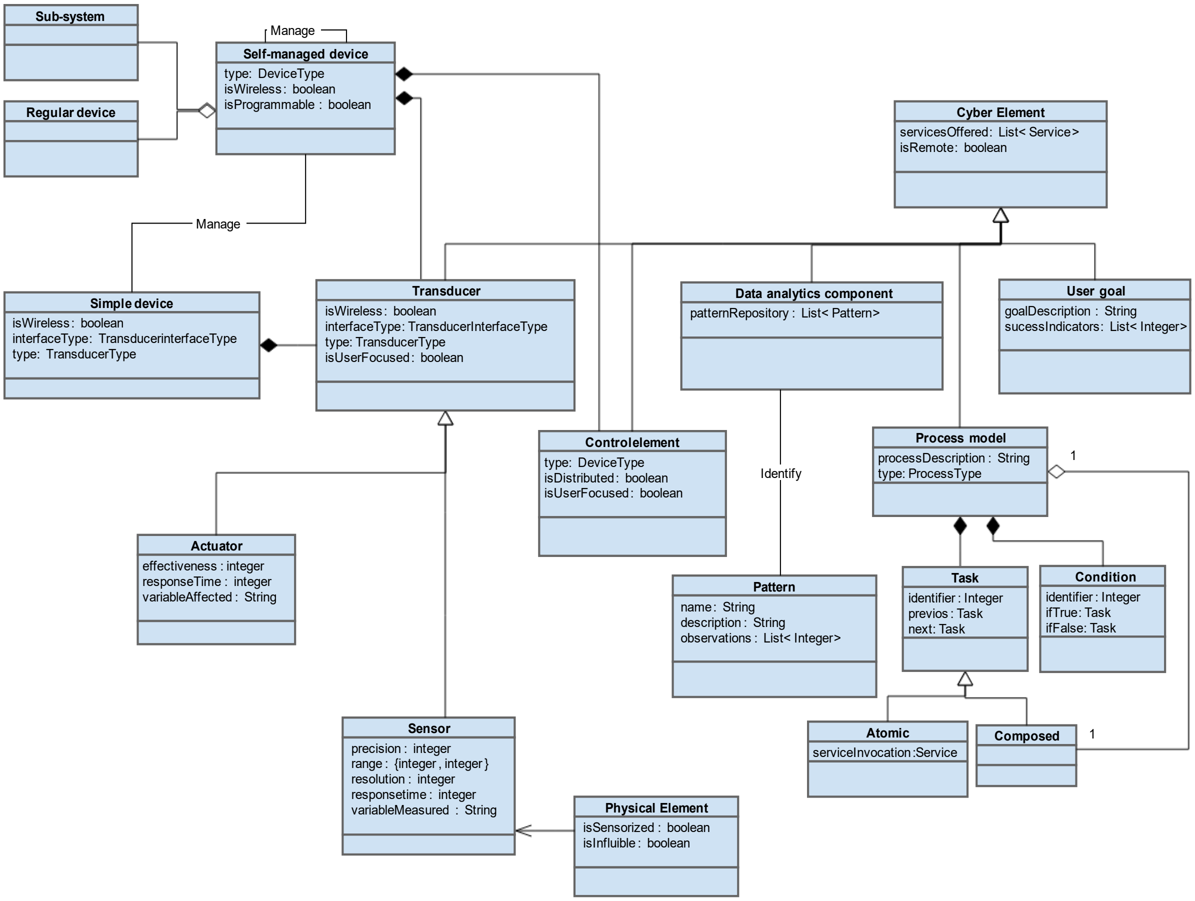


Figure 5: UML description of a GCPS (part 2)

nario. Programming tasks were performed using a regular Integrated Development Environment (IDE) specifically designed for the selected language.

5 Results and Discussion

In this Section a comparison about the three different obtained records of information is performed. Figure 10 shows a comparison between the number of errors found the record of the traditional traceability systems compared to the number of errors when using the proposed GCPS.

The difference is small between systems based on CPS but two factors may be considered as the cause of the seen improvement in the case of GCPS. First, errors in the management of information are more common in traditional systems. As traditional systems consist of a database containing the state of the different monitored people, errors occurring when accessing or writing into the database turn into traceability errors. Nevertheless, GCPS are supported by a virtualized platform, so the data structure as much more complex and secure. Second, traditional traceability systems do not include consistency checks (for example, a person cannot walk 3 kilometers in one minute). Thus, some errors which are detected by the consistency control policies in the system daemon are accepted by traditional traceability systems (which, for example, cannot ask for confirmation to the hardware platform when receiving incoherent data).

If systems which are not based on CPS paradigm are considered, differences are much greater.

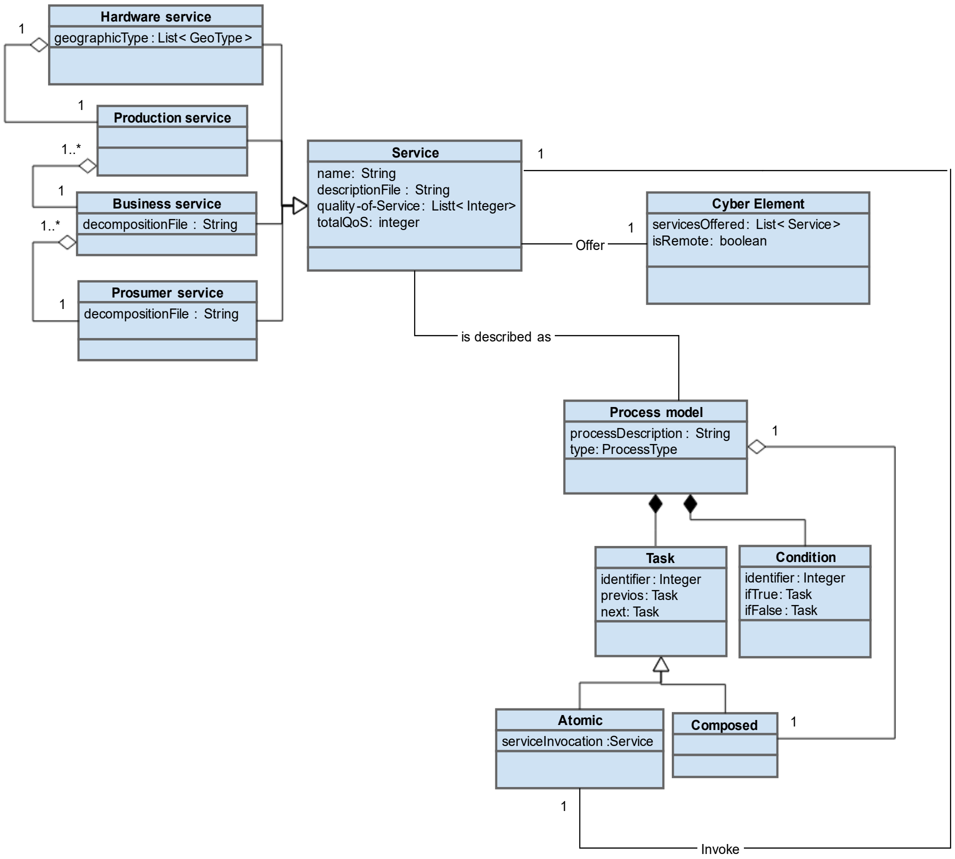


Figure 6: UML description of a GCPS (part 3)

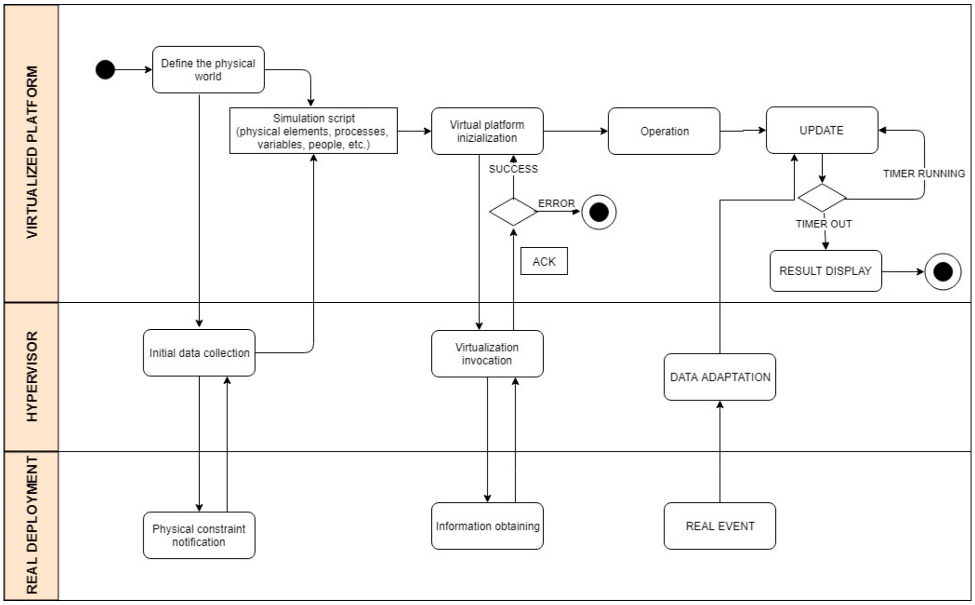

VIRTUALIZED PLATFORM
HYPERVISOR
REAL DEPLOYMENT
Define the physical world
Simulation script (physical elements, processes, variables, people, etc.)
Virtual platform inizialization
Operation
UPDATE
TIMER RUNNING
TIMER OUT
RESULT DISPLAY
SUCCESS
ERROR
ACK
Initial data collection
Virtualization invocation
DATA ADAPTATION
Physical constraint notification
Information obtaining
REAL EVENT

Figure 7: Activity diagram of the proposed tool

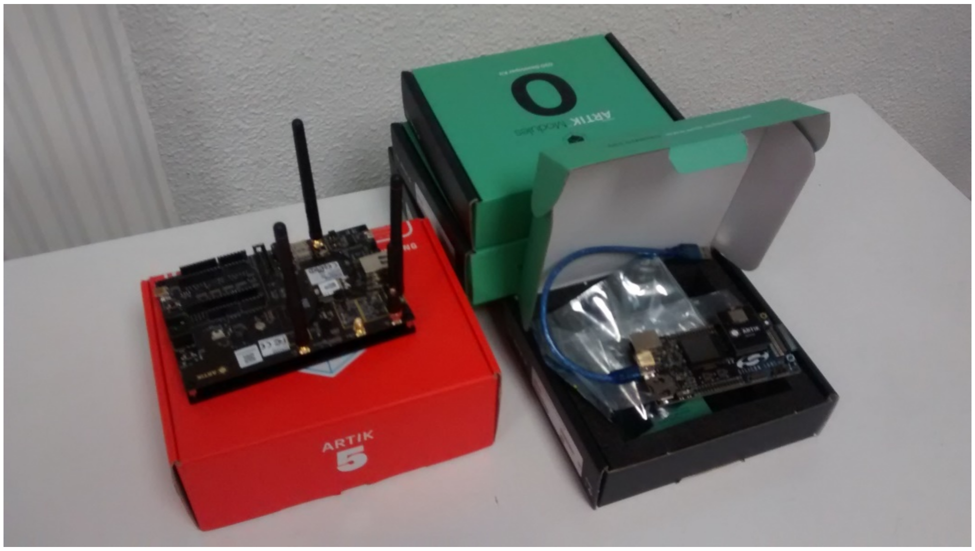
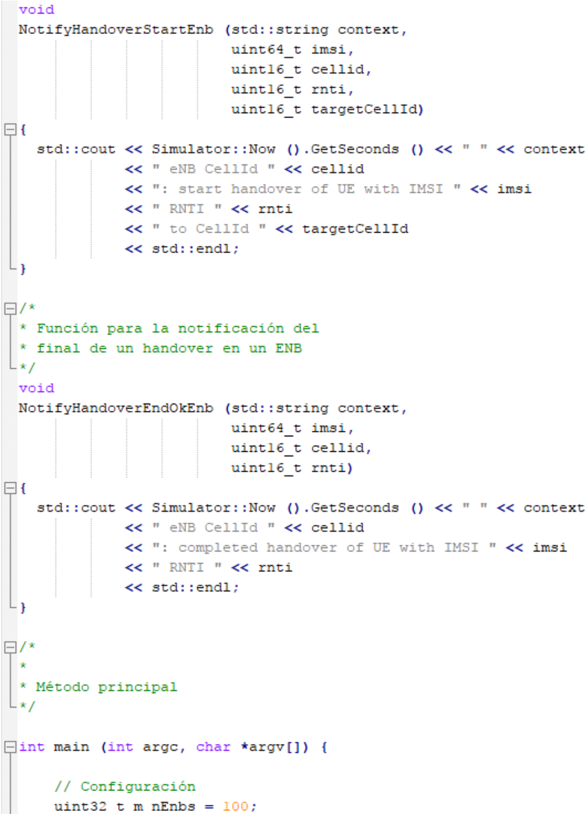


Figure 8: Deployed system



```
void
NotifyHandoverStartEnb (std::string context,
                        uint64_t imsi,
                        uint16_t cellid,
                        uint16_t rnti,
                        uint16_t targetCellId)
{
  std::cout << Simulator::Now ().GetSeconds () << " " << context
            << " eNB CellId " << cellid
            << ": start handover of UE with IMSI " << imsi
            << " RNTI " << rnti
            << " to CellId " << targetCellId
            << std::endl;
}

/*
* Función para la notificación del
* final de un handover en un ENB
*/
void
NotifyHandoverEndOkEnb (std::string context,
                        uint64_t imsi,
                        uint16_t cellid,
                        uint16_t rnti)
{
  std::cout << Simulator::Now ().GetSeconds () << " " << context
            << " eNB CellId " << cellid
            << ": completed handover of UE with IMSI " << imsi
            << " RNTI " << rnti
            << std::endl;
}

/*
*
* Método principal
*/

int main (int argc, char *argv[]) {

    // Configuración
    uint32 t m nEnbs = 100;
```

Figure 9: Screenshot of the employed IDE

Causes for this increase have been analyzed previously in other works [9], and in general are related to the possibility of obtaining real-time information from the system, as well as the possibility of implementing predictive techniques in order to obtain some information about the future.

Figure 11 compares the number of parameters maintained for each human in the traceability system,

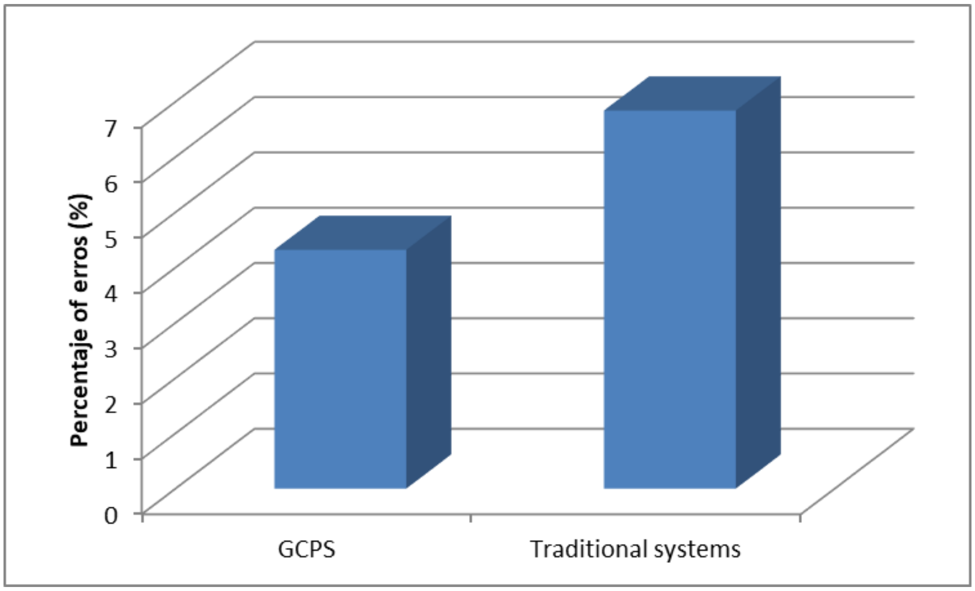


Figure 10: Comparison in the number of traceability errors

in both, traditional solutions and GCPS. As can be seen, in this case, the number of parameters is much greater (a 40% higher in the case of GCPS). That is because of the capability of the system daemon to extract new information from received one from the physical platform (functionality not included in traditional solutions). System which are not based on CPS paradigm require a high level of human intervention, and (usually) controlled parameters per item are much lower (in order to do profitable the system deployment).

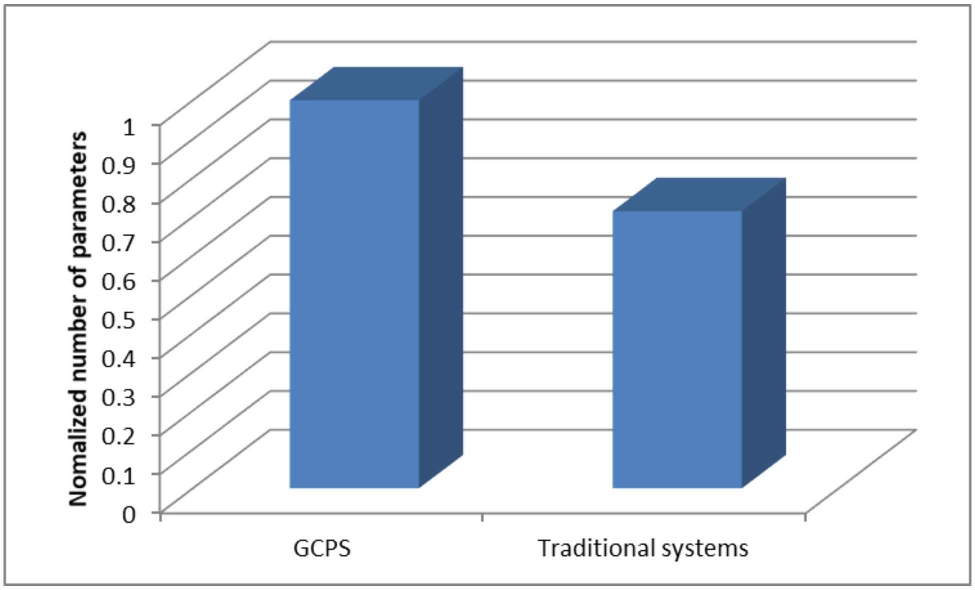


Figure 11: Comparison in the number of parameters per person

Finally, in order to show a more detailed comparison, Table 1 shows the values of some remarkable parameters.

Parameter	GCPS	Traditional systems (CPS)	Traditional systems (no CPS)
Maximum number of parameters per entity	154	107	5 (estimated)
Maximum number of entities in the system	Undefined	1024	200 (estimated)
Mean calculation delay (s)	17	34	52
Mean initialization period (s)	72	24	Not applicable
Integration with supervisory control systems	Yes	Yes	No

Table 1: Parameter comparison

6 Conclusions

Enhanced traceability solutions belong to the new era, usually named as the Industry 4.0 or the Cyber-Physical Systems era. Traditionally, technological systems look for the total automation, maintaining humans and other living creatures outside the system. This situation is incompatible with the creation of next-generation traceability solution following the CPS principles. Therefore, in this paper it is proposed a new concept named as Generalized Cyber-Physical Systems, being able of including not only embedded devices, but also any other important or relevant element (including, humans, animals, etc.). Moreover, it is described the evolution of Machine-to-Machine communications to Thing-to-Thing communications, due to the integration of new elements into CPS. Finally, as GCPS are based on a virtualized instance of the system, it is proposed a simulation model. The experimental validation showed that the quality of the provided information is much higher in these new systems than in traditional approaches.

Acknowledgments

The research leading to these results has received funding from the Ministry of Economy and Competitiveness through SEMOLA project (TEC2015-68284-R) and by the Centre for the Development of Industrial Technology (CDTI) through PERIMETER SECURITY project (ITC-20161228). Borja Bordel has received funding from the Ministry of Education through the FPU program (grant number FPU15/03977). Ramon Alcarria thanks the Ministry of Education, Culture and Sport for the professor's mobility program.

References

[1] A. Ahmad, A. Paul, M. M. Rathore, and H. Chang. Smart cyber society: Integration of capillary devices with high usability based on Cyber–Physical System. *Future Generation Computer Systems*, 56:493–503, 2016.

[2] A. T. Al-Hammouri. A comprehensive co-simulation platform for cyber-physical systems. *Computer Communications*, 36(1):8–19, dec 2012.

[3] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili. On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, 58:1060–1069, 2016.

[4] R. F. Babiceanu and R. Seker. Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. *Computers in Industry*, 81:128–137, sep 2016.

[5] R. Baheti and G. H. Cyber-physical systems: The Impact of Control Technology. 2011.

[6] B. Bordel, R. Alcarria, D. Martín, T. Robles, and D. S. de Rivera. Self-configuration in humanized Cyber-Physical Systems. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–12, sep 2016.

[7] B. Bordel, R. Alcarria, D. Martín, T. Robles, and D. S. de Rivera. Self-configuration in humanized Cyber-Physical Systems. *Journal of Ambient Intelligence and Humanized Computing*, 8(4):485–496, aug 2017.

[8] B. Bordel, R. Alcarria, M. Pérez-Jiménez, T. Robles, D. Martín, and D. S. de Rivera. Building Smart Adaptable Cyber-Physical Systems: Definitions, Classification and Elements. pages 144–149. Springer, Cham, dec 2015.

[9] B. Bordel Sánchez, R. Alcarria, D. Martín, and T. Robles. TF4SM: A Framework for Developing Traceability Solutions in Small Manufacturing Companies. *Sensors*, 15(11):29478–29510, nov 2015.

[10] B. Bordel Sánchez, R. Alcarria, D. Sánchez de Rivera, and A. Sánchez-Picot. Predictive algorithms for mobility and device lifecycle management in Cyber-Physical Systems. *EURASIP Journal on Wireless Communications and Networking*, 2016(1):228, dec 2016.

[11] A. W. Colombo. *Industrial cloud-based cyber-physical systems : the IMC-AESOP approach*.

[12] I. E. Commission. International standard iec 62264-1: Enterprise-control system integration part 1: Models and terminology. IEC: Geneva, Switzerland, 2003.

[13] B. U. C. concept map. Available online: `http://cyberphysicalsystems.org`, last viewed May 2017.

[14] C. Coopmans, B. Stark, A. Jensen, Y. Q. Chen, and M. McKee. Cyber-Physical Systems Enabled by Small Unmanned Aerial Vehicles. In *Handbook of Unmanned Aerial Vehicles*, pages 2835–2860. Springer Netherlands, Dordrecht, 2015.

[15] P. Derler, E. A. Lee, and A. S. Vincentelli. Modeling Cyber–Physical Systems. *Proceedings of the IEEE*, 100(1):13–28, jan 2012.

[16] Edward A. Lee. Cyber-Physical Systems - Are Computing Foundations Adequate? In *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, Austin, TX, 2006.

[17] Geng Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson. M2M: From mobile to embedded internet. *IEEE Communications Magazine*, 49(4):36–43, apr 2011.

[18] M. Gillham, G. Howells, and S. Kelly. Assistive Trajectories for Human-in-the-Loop Mobile Robotic Platforms. In *2015 Sixth International Conference on Emerging Security Technologies (EST)*, pages 56–61. IEEE, sep 2015.

[19] J. He, Y. Geng, Y. Wan, S. Li, and K. Pahlavan. A Cyber Physical Test-Bed for Virtualization of RF Access Environment for Body Sensor Network. *IEEE Sensors Journal*, 13(10):3826–3836, oct 2013.

[20] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura. Modeling of Future Cyber–Physical Energy Systems for Distributed Sensing and Control. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 40(4):825–838, jul 2010.

[21] M. P. Jimenez, B. B. Sánchez, and R. P. A. Garrido. T4ai: A system for monitoring people based on improved wearable devices. *Research Briefs on Information & Communication Technology Evolution (ReBICTE)*, 2:1–16, 2016.

[22] Jody Ranck. Gigaom — The wearable-computing market: a global analysis. Technical report, Gigaom Pro, 2012.

[23] W. Ju and L. Leifer. The Design of Implicit Interactions: Making Interactive Systems Less Obnoxious. *Design Issues*, 24(3):72–84, jul 2008.

[24] H. Lasi, P. Fettke, T. Feld, and M. Hoffmann. Industry 4.0. *Business & Information Systems Engineering*, 6(4), 2014.

[25] E. A. Lee. Cyber Physical Systems: Design Challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369. IEEE, may 2008.

[26] J. Lin, S. Sedigh, and A. Miller. Modeling Cyber-Physical Systems with Semantic Agents. In *2010 IEEE 34th Annual Computer Software and Applications Conference Workshops*, pages 13–18. IEEE, jul 2010.

[27] P. Marwedel. *Embedded System Design*. Springer Netherlands, Dordrecht, 2011.

[28] I. Mohino-Herranz, R. Gil-Pita, J. Ferreira, M. Rosa-Zurera, and F. Seoane. Assessment of Mental, Emotional

and Physical Stress through Analysis of Physiological Signals Using Smartphones. *Sensors*, 15(10):25607–25627, oct 2015.

[29] S. Munir, J. A. Stankovic, C.-J. M. Liang, and S. Lin. Cyber physical system challenges for human-in-the-loop control. In *Presented as part of the 8th International Workshop on Feedback Computing*, San Jose, CA, 2013. USENIX.

[30] P. Rashidi and A. Mihailidis. A Survey on Ambient-Assisted Living Tools for Older Adults. *IEEE Journal of Biomedical and Health Informatics*, 17(3):579–590, may 2013.

[31] V. Ruchkin, V. Fulin, B. Kostrov, A. Taganov, and A. Kolesenkov. Forest fire monitoring by means of cyber-physical system. In *2016 5th Mediterranean Conference on Embedded Computing (MECO)*, pages 30–34. IEEE, jun 2016.

[32] B. Sánchez, R. Alcarria, D. Sańchez-De-Rivera, and Á. Sańchez-Picot. Enhancing process control in industry 4.0 scenarios using Cyber-Physical systems. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 7(4), 2016.

[33] B. B. Sanchez, A. Sanchez-Picot, and D. S. D. Rivera. Using 5G Technologies in the Internet of Things Handovers, Problems and Challenges. In *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 364–369. IEEE, jul 2015.

[34] A. Sanchez-Picot, D. Martin, D. S. de Rivera, B. Bordel, and T. Robles. Modeling and Simulation of Interactions Among People and Devices in Ambient Intelligence Environments. In *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 784–789. IEEE, mar 2016.

[35] C. Sarkar. Virtualizing the internet of things. Available online: `http://www.es.ewi.tudelft.nl/phd-theses/2016-Sarkar.pdf`, last viewed May 2017.

[36] G. Schirner, D. Erdogmus, K. Chowdhury, and T. Padir. The Future of Human-in-the-Loop Cyber-Physical Systems. *Computer*, 46(1):36–45, jan 2013.

[37] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher. *Cyber-physical systems : foundations, principles and applications*. Academic Press, 2017.

[38] T. to-Thing standardization initiative. Available online: `https://datatracker.ietf.org/rg/t2trg/about/`, last viewed May 2017.

[39] K. Wan, D. Hughes, K. L. Man, and T. Krilavicius. Composition challenges and approaches for cyber physical systems. In *2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications*, pages 1–7. IEEE, nov 2010.

[40] H. Wang, S. Gong, X. Zhu, and T. Xiang. Human-In-The-Loop Person Re-Identification. dec 2016.

[41] T. Wark, K. Prayaga, J. O'Grady, M. Reed, A. Fisher, C. Crossman, W. Hu, Y. Guo, P. Valencia, P. Sikka, P. Corke, C. Lee, and J. Henshall. The design and evaluation of a mobile sensor/actuator network for autonomous animal control. In *Proceedings of the 6th international conference on Information processing in sensor networks - IPSN '07*, page 206, New York, New York, USA, 2007. ACM Press.

[42] F.-J. Wu, Y.-F. Kao, and Y.-C. Tseng. From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile Computing*, 7(4):397–413, aug 2011.

[43] F. Xia and Feng. QoS Challenges and Opportunities in Wireless Sensor/Actuator Networks. *Sensors*, 8(2):1099–1110, feb 2008.

[44] X. Yue, H. Cai, H. Yan, C. Zou, and K. Zhou. Cloud-assisted industrial cyber-physical systems: An insight. *Microprocessors and Microsystems*, 39(8):1262–1270, nov 2015.

[45] Z. Zhang, X. Li, X. Wang, and H. Cheng. Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0. pages 127–171. Springer International Publishing, 2017.

Author Biography

Borja Bordel received the B.S. degree in telecommunication engineering in 2012 and the M.S. telecommunication engineering in 2014, both from Technical University of Madrid. He is currently pursuing the Ph.D. degree in telematics engineering at Telecommunication Engineering School, UPM. His research interests include Cyber-Physical Systems, Wireless Sensor Networks, Radio Access Technologies, Communication Protocols and Complex Systems.

Ramón Alcarria received his M.S. and Ph.D. degrees in Telecommunication Engineering from the Technical University of Madrid in 2008 and 2013 respectively. Currently, he is an assistant professor at the E.T.S.I Topography of the Technical University of Madrid. He has been involved in several R&D European and National projects related to Future Internet, Internet of Things and Service Composition. His research interests are Service Architectures, Sensor Networks, Human-computer interaction and Prosumer Environments.

Miguel Manso received a M.S. in Telecommunication Engineering and Ph.D. in Geographic Engineering degrees from Technical University of Madrid in 2003 and 2009 respectively. He is an Associate Professor on Geomatics Engineering at the Technical University of Madrid since 1992. He has participated in some national and international projects related to Geospatial Data and Cartography. His research areas are Sensor Networks and Web Enablement, Spatial Data Infrastructure and Spatial Databases.

Antonio Jara received his Ph.D. at the Intelligent Systems and Telematics Research Group of the University of Murcia (UMU) from Spain. He is the Vice-chair of the IEEE Communications Society Internet of Things Technical Committee, CTO and co-founder of the Smart Cities company viBrain Solutions, Assistant Prof. PostDoc at University of Applied Sciences Western Switzerland (HES-SO). His research interests are WSNs (6LoWPAN and ZigBee) and RFID applications in building automation and healthcare.