WSN and RFID Integration in the IoT scenario: an Advanced Safety System for Industrial Plants

Matteo Petracca, Stefano Bocchino, Andrea Azzarà,
Riccardo Pelliccia, Marco Ghibaudi, and Paolo Pagano

Original scientific paper

***Abstract*: The paper proposes and discusses the integration of WSN and RFID technologies in the IoT scenario. The proposed approach is based on the REST paradigm, thanks to which the two technologies can be seamless integrated by representing sensors, actuators and RFID related data as network resources globally addressable through state-of-the-art IoT protocols.**

The integration approach is detailed for the Smart Factory use case by proposing and developing an advanced IoT-based WSN and RFID integrated solution aiming at improving safety in industrial plants. The developed system can guarantee a safe access to factory dangerous areas in which safety equipments are required. In the paper, the system design is first presented, then, all the developed hardware and software solutions are described before presenting system performance results in a real test bed. System performance are reported in terms of response time and accuracy for authorization control and location tracking applications.

***Index terms*: IoT, WSN, RFID, Smart Factory, Safety.**

I. INTRODUCTION

In recent years, the worldwide spreading of Internet, in combination with the development of new miniaturized and low-cost embedded devices, has globally enabled the so called Internet of Things (IoT) vision [1]. The main idea behind the IoT concept is to have worldwide interconnected objects, each one individually discovered and addressed as a resource in the network. IoT devices will be remotely accessible, thus making available an enormous amount of data about the physical world which was previously inaccessible. In an IoT scenario innovative applications can be developed by using pervasive collected data and leveraging on the new control possibility offered by the IoT enabling solutions.

Albeit the IoT vision has been initially inspired by the success of the Radio-Frequency IDentification (RFID) technology [2], such a vision can be effectively enabled through a seamless integration of both RFID and Wireless Sensor Networks (WSNs)solutions in the Internet scenario. RFID is an extremely low-cost and low-power technology mainly characterized by passive devices, i.e., tags, which are able to send information when powered by electromagnetic fields generated by an RFID reader. It is a short-range radio technology mainly used for object identification [3] and tracking [4]. WSNs are composed by low-power embedded devices characterized by reduced computational capabilities that actively communicate among them to fulfill complex tasks. The transmission range of WSN devices is in the order of a hundred meters, and they are mainly used for real time environmental monitoring [5], tracking [6], and localization purposes [7]. The advantages provided by both technologies promote the design of an integrated solution in which the outstanding pervasiveness of RFIDs and the advanced sensing and communication features of WSNs are merged together to have pervasive and addressable resources in a worldwide network of objects.

Though an integration between RFID and WSN technologies has been already proposed in literature, the problem has been mainly addressed from an hardware point of view, while developing a custom application logic for the interoperability among devices. In the IoT scenario, the devices interoperability is one of the main strengths thanks to which new innovative applications can be developed. In this paper we propose a WSN and RFID integration according to the IoT spirit. The integration is proposed both at hardware and logic levels by discussing the use of IoT protocols at network and application layers. Moreover, the proposed approach is detailed, implemented, and assessed for the Smart Factory use case by developing an advanced safety system able to guarantee a safe access to factory dangerous areas in which safety equipments are required. This paper significantly extends an earlier version presented at the 20th IEEE International Conference on Software, Telecommunications and Computer Networks [8]. More in detail, in this version the integration between RFID and WSN technologies is not addressed only from an hardware point of view, but an IoT based interoperability is proposed, implemented and assessed.

The remainder of the paper is organized as follows. Section II describes the state-of-the-art in WSN and RFID integration by considering several application domains. In Section III the proposed IosT based WSN and RFID integration is presented. Section IV details the proposed integration solution in the Smart Factory use case, along with hardware and software implementation details. The performance of the developed

Manuscript received December 15, 2012; revised February 21, 2013.

M. Petracca and P. Pagano are with the National Laboratory of Photonic Networks, National Inter-University Consortium for Telecommunications, Pisa, Italy. E-mail: [matteo.petracca, paolo.pagano]@cnit.it

S. Bocchino, A. Azzarà, R. Pelliccia and M. Ghibaudi are with the Real-Time Systems Laboratory, Scuola Superiore Sant'Anna, Pisa, Italy. E-mail: [s.bocchino, a.azzara, r.pelliccia, m.ghibaudi]@sssup.it

1845-6421/03/8272

application in terms of accuracy and response times are presented in Section V. Conclusions follow in Section VI.

II. Related work

In the last several years, an increasing number of research activities have started to propose integrated WSN and RFID systems with the aim of providing new services or improving already available applications [9]. As already mentioned, the integration problem has been mainly addressed from an hardware point of view considering the benefits provided by an integrated solutions, and without proposing a full interoperability among devices according to the IoT paradigm. From the hardware point of view the integration between WSN and RFID can be reached by:

- Integrating RFID tags on WSN nodes;
- Integrating RFID readers on WSN nodes.

The former case consists in extending the sensing capabilities of a WSN node with those provided by RFID tags. In this scenario, the RFID tag can be used to provide location-aware services and for minimizing the WSN nodes power consumption giving to the node the capability to wake-up when triggered by RFID readers. If the integration consists in merging the RFID reader with a WSN node the main result is a low-cost pervasive extension of the WSN going towards the full accomplishment of the IoT vision.

A first example of RFID and WSN integration is presented by Chen in [10] where a wireless localization system for monitoring children position in theme park is implemented. In the work, the integration is reached by installing an RFID reader on each WSN node, thus creating a hybrid localization system able to estimate the child position with a maximum error of 3 meters. The work presented by Xiong et al. in [11] can be classified in the same application scenario. In their paper a grid of RFID tags is used to enhance the positioning accuracy reached by standard well-known WSN localization algorithms based on the received signal strength indicator. In this latter case the integration of both technologies is reached again by installing RFID readers on WSN nodes. The RFID reader usually combines in a single physical device transmission (to the tags) and reception (from the tags) functions. In [12] an innovative approach is discussed by introducing a different device, called RFID listener, able to perform receive functions with the aim of realizing a distributed sensing. The integration of RFID listeners on low-cost and low-power WSN nodes allows to realize an architecture with a single transmitter and multiple listeners, enabling a denser deployment and increasing the localization accuracy. In the above mentioned works, RFIDs are mainly used for implementing a coarse grain localization while trying to optimize the power consumption of each WSN unit. Looking at the power consumption optimization scenario, Jurdak et al. proposed in [13] a low-cost system making use of IEEE802.15.4 transceiver as a fake RFID tag reader. In particular, their system transmits, through the installed IEEE802.15.4 transceiver, the electromagnetic energy necessary for triggering a tag and indirectly for waking up the associated WSN node.

More recently, integrated WSN and RFID solutions have been proposed in other application domains. In [14] Xiaoguang and Wei proposed the jointly use of WSN and RFID for the development of a smart warehouse management system. In the proposed application several possible network architectures are analyzed and discussed looking at the best trade-off between system reliability and deployment costs. The use of WSN and RFID in a smart home scenario is proposed by Hussain et al. in [15]. Leveraging on both WSN and RFID advantages the main idea provided by the authors is to assist elderly people by tracking their movements while providing personalized services to increase their comfort. In [16] the intelligent transport system scenario is considered. In their work Nasir and Soong propose to acquire pollutant emission levels gathered by hybrid WSN and RFID sensors installed near the vehicles. The pollutant levels are acquired only when an embedded RFID tag receives enough energy for waking up the sensors. The developed solution permits on one hand to acquire environmental data, and on the other hand, to correlate the pollutant emission level with a car identification number, i.e., the car license plate.

Albeit the above mentioned works greatly contribute in the design of an effective solution aiming at integrating both WSN and RFID technologies, none of them addresses the problem of a seamless integration going towards the full accomplishment of the IoT vision. The interoperability with devices compliant with Internet protocols is not taken into account, as well as possible solutions for managing resources made available by both WSN and RFID embedded devices.

III. IoT based WSN and RFID integration

A. IoT protocols

Over the past few years the research community has focused its activity on designing protocols for the IoT [17]. Indeed, well-known and widely used Internet protocols are often unsuited for IoT devices that are usually constrained in terms of computational power, memory, and transmission bandwidth. The main outcome of this research effort is an adaptation layer for the IPv6 protocol over Low-power Wireless Personal Area Networks (6LoWPAN) compliant with the IEEE802.15.4 [18] standard. 6LoWPAN [19], i.e., the adaptation of IPv6 for low-power devices, has proven to be a valid alternative to traditional proprietary WSN protocols [20]. Indeed, 6LoWPAN based networks can compete with traditional WSNs in terms of power consumption and network throughput, while achieving a seamless integration and interoperability with Internet. Fig. 1 depicts a 6LoWPAN network with its main components: (i) Host node (H); (ii) 6LoWPAN Router (6LR); (iii) 6LoWPAN Border Router (6LBR). The H node is a simple node of the network and does not provide any forwarding and routing service. The 6LR is a node with forwarding and routing capabilities, while the

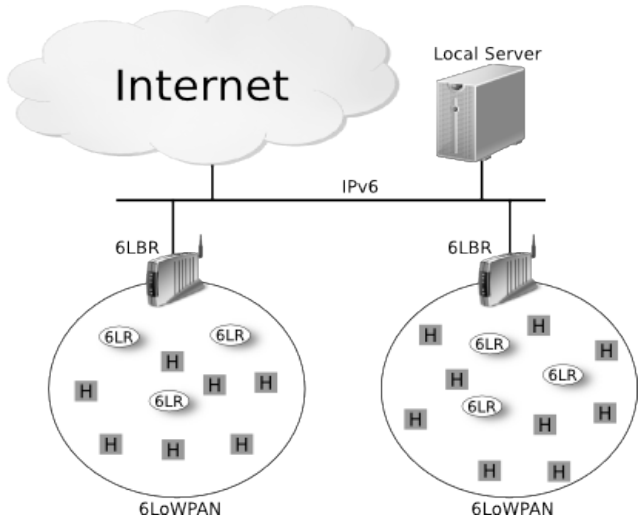

Fig. 1. 6LoWPAN network.

6LBRis in charge of connecting each subnet to Internet by translating 6LoWPAN into IPv6 packets and vice-versa.

The use of standard network protocols has been just the first step towards an effective IoT-based network implementation. Another important step is constituted by the on-going drafting of the Constrained Application Protocol (COAP) [21], an HTTP-like protocol especially designed for resource constrained devices. COAP permits to create embedded web services running on IoT nodes [22], thus extending the web architecture, based on the Representational State Transfer (REST) paradigm, to resource constrained devices. As HTTP, COAP is a working solution able to support machine-to-machine (M2M) communication, in the context of Web Services and Semantic Web Services [23].

B. WSN and RFID integration through the REST paradigm

REST is a software architecture for distributed systems presented by Fielding in his doctoral dissertation [24]. According to the REST architecture a distributed system is composed by clients and servers. Clients initiate requests to servers; servers process requests and return appropriate responses. Requests and responses are built around the transfer of representations of resources. Are source can be essentially any coherent and meaningful concept that may be addressed. A representation of a resource is typically a document that captures the current or intended state of the resource. The most significant example of a system conforming to the REST architecture is the World Wide Web, in which resources are manipulated by means of the HTTP protocol.

As previously introduced, the REST paradigm is also used in the IoT scenario, where resources usually represent sensors, actuators or other possible information. In such a context, the resources can be manipulated through the COAP protocol. Specifically, COAP provides four methods for manipulating resources: (i) PUT, to request that the resource identified by the URI is updated or created with the transmitted representation; (ii) POST, to request that the representation transmitted in the request is processed; (iii) GET, to retrieve a representation of the resource identified by the URI specified in the request; (iv) DELETE, to request the deletion of the resource identified by the specified URI. COAP additionally provides a resource observation mechanism [25] which allows a node to receive notifications about changes in resources it has previously subscribed to.

The possibility of representing sensors, actuators and other possible source of information as general resources identified by a global URI, i.e., the IPv6 address of the network interface plus a resource identification, allows to abstract the physical components of the system with a common operation logic. Considering a WSN and RFID integrated system, in which both RFID readers and RFID tags are integrated in hardware with WSN nodes, two new nodes should be added to those presented in Fig. 1: (i) Host Reader (HR), a WSN node in which an RFID reader has been integrated; (ii) Host Tag (HT), a WSN node in which an RFID tag is integrated. The two nodes are depicted in Fig. 2 as part of the 6LoWPAN network architecture, while representing the possible resource URIs exposed by nodes. An H node can expose a simple CoAP sensor or actuator resource (e.g., *coap://[aaaa::1]/sensor_resource* and *coap://[aaaa::2]/actuator_resource*), while HR and HT nodes can expose RFID related resources. More in detail, an HR node can expose an RFID reader relatedresource (e.g., *coap://[aaaa::3]/reader_resource*), while HT can expose an RFID tag related resource (e.g., *coap://[aaaa::4]/tag_resource*). As matter of example, a reader related resource can be an hardware configuration parameter or an aggregated information obtained by reading tags in the range. A tag related resource can be either the Electronic Product Code (EPC) memory content of a passive tag or a sensor value collected by a semi-passive tag.

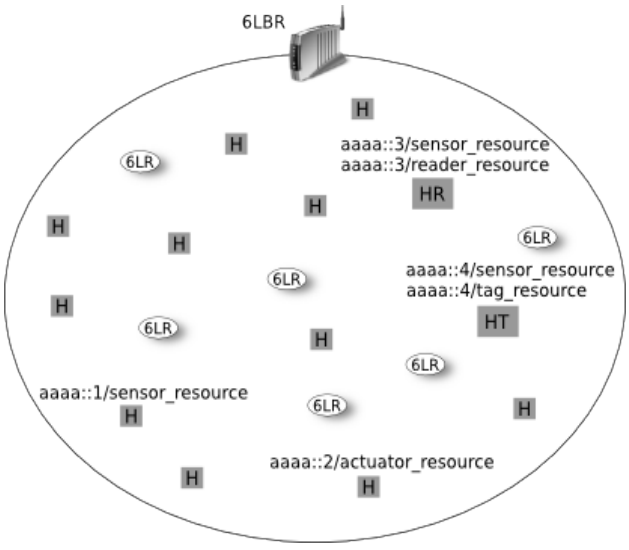

Fig. 2. IoT based WSN and RFID integrated network.

The proposed approach of extending the 6LoWPAN architecture with HR and HT nodes, while using the REST paradigm through the CoAP protocol is simple in its vision, yet powerful. Indeed, the proposed solution on one hand guarantees a full integration between WSN and RFID technologies, on the other hand achieves a seamless interoperability and integration with Internet according to the IoT vision.

IV. Advanced Safety System for Industrial Plants

The proposed approach of integrating WSN and RFID technologies by using IoT protocol solutions is detailed for the Smart Factory use case by proposing and developing an advanced safety system able to guarantee a safe access to factory dangerous are as in which safety equipments are required.

A. System design

Considering the industrial plant of a factory, the entire surface can be divided in several restricted areas, each of them characterized by a security access level. The access to each area must be taken under control to avoid possible dangerous situations. A minimum requirement to give access to an Area Under Control(AUC) is to check whether a worker asking for the access is wearing all necessary safety equipments. If the worker request is identified to be safe, then the AUC door can be opened and the worker can enter in the area. Though the selected use case can be considered quite simple, it is a real scenario in which WSN and RFID technologies can be integrated.

A pictorial sketch of the AUC area with its main componentsis depicted in Fig. 3. In the area, several 6LR and H nodesare deployed to collect data from the environment.

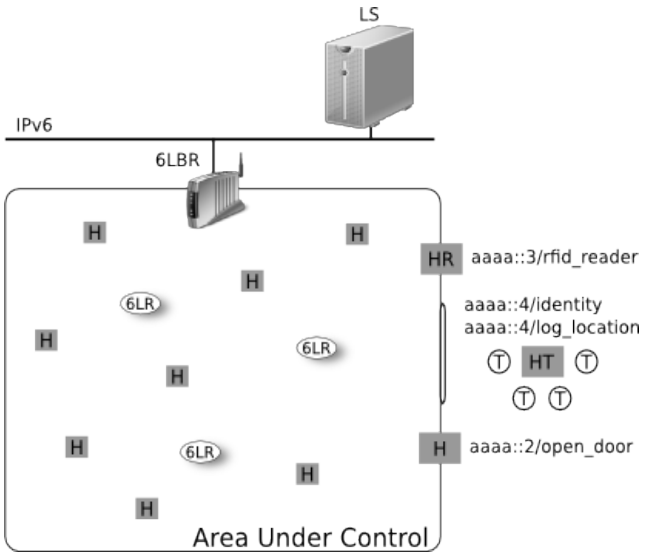

Fig. 3. System components and exposed resources.

Each one of them can expose a sensing or actuating resource which can be manipulated through COAP methods by the Local Server (LS)connected to the 6LBR. Close to the door two main actors of the system are installed: (i) the HR node, in charge of detecting whether a worker identified by its own identity device, HT, is wearing all the necessary equipments, and (ii) the H node able to open the door in case the access is authorized. The HR node is exposing a *coap://[aaaa::3]/rfid_reader* resource from which the LS can receive detection events. In the system design the HR and H nodes have been kept separate to consider cases in which a remote actuation is required (e.g., two consecutive doors in a corridor must be opened). However, in the case reported in Fig. 3 the functionality of the H node could be embedded in HR, thus having a node with multiple functionality.

To better explain the proposed safety access system design a sequence diagram has been reported in Fig. 4 to show the main messages exchanged in the setup and operational phases of the system. In the setup phase, LS activates the subscriptions to the necessary resources (e.g., *coap://[aaaa::3]/rfid_reader*) by sending a COAP message (a) to the HR node by means of the COAP observe protocol. The HR node maintains a list of the active subscriptions, while in LS an event handler is installed at run-time and associated to received notification messages. During the operational phase, when the HT node is in the HR range, the worker identity, as well as the list of the equipments to wear, is read by accessing the memory of the tag embedded on it (b and c messages). At the same time a new COAP resource *coap://[aaaa::3]/tag_aaaa_4* is created in HR. The new resource logically represents the memory of the HT tag, and creates a virtual access to the COAP resources exposed by HT (e.g., *coap://[aaaa::4]/identity* and *coap://[aaaa::4]/log_location*). When all the required equipments are detected by reading their own passive T tags, the HR node sends an authorized request event (d) to LS using a COAP method. The event is then automatically handled by LS which sends an open door request (e) to the actuator node exposing the *coap://[aaaa::2]/open_door* resource. The list of all necessary equipments is stored in the HT node in order to keep the safety

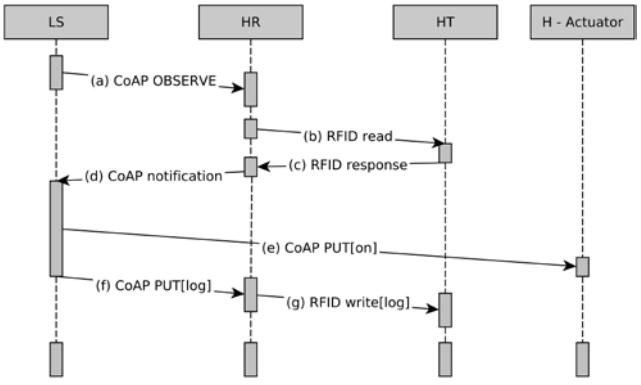

Fig. 4. Messages exchanged among network devices.

requirements as much as close to the worker, thus enabling multiple checks in case several HR nodes are installed in the AUC area. If the HT node exposes multiple RFID related resources more checks and applications can be realized. In the proposed system, after the authorization phase, the tag_aaaa_4 resource is handled (f and g messages) to store in the tag memory of the HT node the identification number of the AUC which the worker is entering, thus creating a per AUC tracking application. The tag_aaaa_4 resource virtually access to the *coap://[aaaa::4]/log_location* resource.

In the above described system design, malicious cases in which unauthorized workers enter the dangerous area when the door has been opened by a previous successful authorization have not been taken into account. The management of such situations is considered outside the scope of this work. In any case, the problem can be easily managed by installing again several HR nodes in the AUC, thus enabling periodic checks of the safety requirements. The problem of associating a safety equipment to the wrong worker identity has been solved by storing a worker identification number on both HT and T tags. When the identity of a worker is read from HT, the HR node discards all the equipment tags in the same operational range showing a different identification number. In case of several HT nodes have been detected, the check for authorizing the entrance in the AUC area is performed sequentially for each worker, discarding not valid equipments.

B. Hardware components

The main hardware components of the system are, according to Fig. 3, the LS, the 6LBR, the H node with an actuation resource, and the two new nodes HR and HT. To develop all the integrated hardware components, as well as for the 6LBRand H nodes, the selected WSN device is the Seed-eye [26]board. The board, depicted in Fig. 5, is equipped with a 32-bitmicrocontroller, an IEEE802.15.4 transceiver, Ethernet interface and various expansion connectors. The microcontroller is a 32-bitMicrochip™ PIC32MX795F512L microcontroller based on the MIPS architecture and able to reach a maximum clock speed of80 MHz, it embeds 128 Kbyte of RAM and 512 Kbyte of Flash memory. Wireless communication capabilities are provided by the Microchip™ MRF24J40MB transceiver, characterized by a transmission frequency of 2.4 GHz with a transmission power ranging from -46 dBm to +20 dBm. Seed-eye presents a small form factor, and can be powered by either batteries or through the USB port. The Seed-eye, as it is, can be used for the 6LBRnode by connecting them to an IPv6 network through the Ethernet interface, while the H node with the actuation capabilities has been created by embedding a relay with two exchange connectors on the board, and operating it via a serial connection. The Hactuation node is reported in Fig. 6.

The HT node has been developed by embedding a semi-passive RFID tag into the Seed-eye. A picture of the node is reported in Fig. 7. The selected embedded tag is the IDS

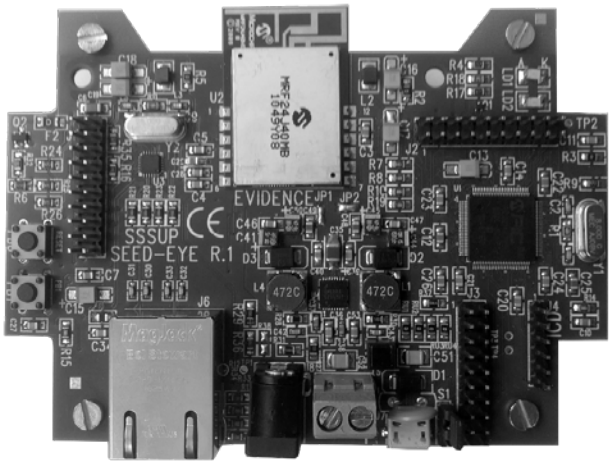

Fig. 5. Seed-eye board.

SL900A chip able to communicate in the UHF bands ranging from 860 MHz to 960 MHz, and usable as passive or semi-passive RFID tag. Indeed, thanks to an internal real time calendar, the SL900A chip can be operated as data-logger by connecting external sensors to dedicated pins. The SL900A has been connected to the Seed-eye board trough a serial peripheral interface, from which it is possible to read both the EPC memory of the device and the values of possibly connected external sensors.

Last key component of the system is the HR node, depicted in Fig. 8. It has been created by interconnecting an RFID reader to the Seed-eye. The selected reader is the module Sensor ID Discovery UHF OEM which has been connected to the Seed-eye by means of a simple serial interface. The reader supports the EPC standard for reading data from tag memories, while reaching a transmission power of +27 dBm. Thanks to the selected omni-directional antenna, and transmission power, the reader is able to read tags at a distance

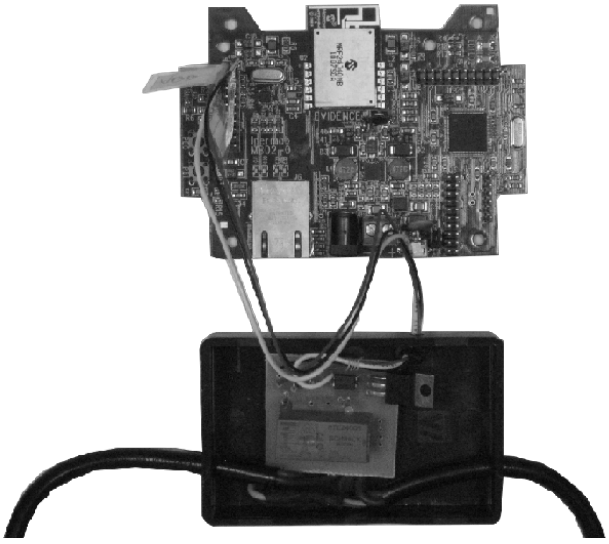

Fig. 6. H node with actuation resource.

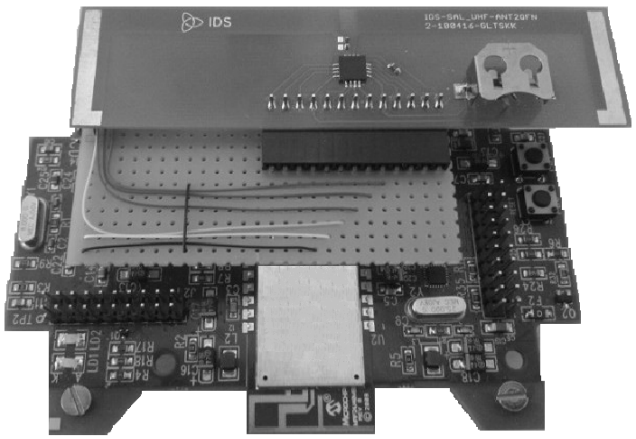

Fig. 7. HT node embedding a semi-passive tag.

of around 5 meters. The choice of using RFID hardware equipments working in the frequency band ranging from 860 MHz to 960 MHz avoids any possible interference with the selected WSN devices. It must be stressed that the Seed-eye is equipped with a radio transceiver operating in the 2.4 GHz frequency band. However, the interference between RFID and WSN is still an open issue to be solved in large integrated networks operating in the same frequency band [27].

Regarding the passive tags used on safety equipments, the Alien ALN-9654 G have been selected. This choice has been mainly done due to their extreme low-cost and compliance with the EPC standard.

C. Software components

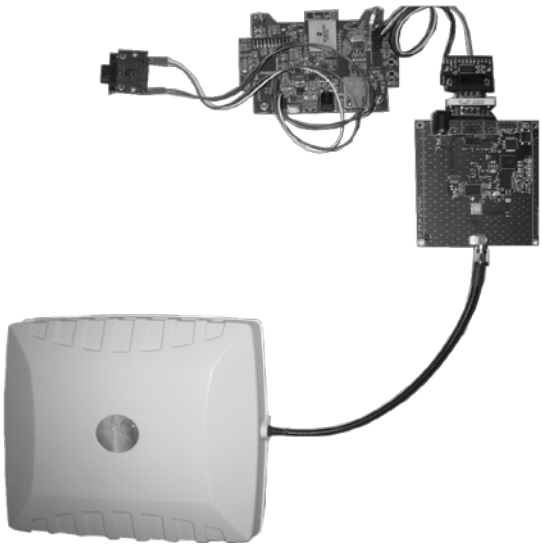

Fig. 8. HR node embedding an RFID reader.

To develop the firmware to be installed on all the nodes of the system the Erika Enterprise OS [28] has been selected. Erika OS is characterized by an extremely reduced Flash footprint, although it can provide advanced scheduling policies (e.g., fixed priority, earliest deadline first) for organizing tasks execution, as well as resources and semaphores for implementing preemption policies. We choose to use Erika OS, instead of other popular operating systems, such as Contiki and TinyOS, because of its real time features that allow the integration of background monitoring and maintenance tasks on system nodes. These tasks may run in the node at a low priority level, while preserving the required QoS for high priority activities, such as those related to RFID authorization. As matter of example, the HR node can embed additional sensor resources constantly monitored in background without interfering with high priority activities, thus allowing to reduce the number of nodes to be deployed. Furthermore, Erika OS comes with a fully compliant, lightweight IEEE802.15.4 software stack, µWireless, that can be configured for performing time accurate, periodic and a periodic packet transmissions. The full 6LoWPAN network stack, as well as the COAP protocol, are part of the Erika communication stack. They have been implemented following the IETF recommendations. In the 6LoWPAN stack both flooding and geographical routing protocols have been implemented, namely 6LoWPAN Ad-Hoc On-Demand Distance Vector (AODV) and 6LoWPAN SPEED. Implementation details of all the above protocols can be found in previous works of the authors [29], [30].

In the WSN and RFID integrated solution proposed in Section III all the RFID based capabilities have been abstracted as device resources. In order to accomplish such a vision the RFID based software components have been implemented in Erika OS as system drivers. For the HR node several functions to set hardware parameters have been implemented, as well as functions for configuring the serial communication interface and for managing the EPC memory of read tags. The HT node driver consists of several functions able to configure the semi-passive tag parameters and to get values from possible sensors embedded into the tag.

Regarding the LS software solutions, these have been developed as custom applications able to provide web-based services for data storage, resource discovery, nodes configuration, and automatic event handling. Detailed architectural and implementation solutions can be found in [31].

V. PERFORMANCE EVALUATION

The performance of the proposed system have been evaluated by means of a real deployment reflecting the scenario depicted in Fig. 3. Both HR and H actuator nodes have been installed close to the entering door of an AUC area, while inside the area three 6LR nodes have been deployed, as well as a 6LBR and a laptop working as LS. In the deployed test bed two main experiments have been conducted with the aim of evaluating: (i) the system response time and its accuracy in authorizing the access in the AUC, and (ii) the

system response time in logging AUC identification data on the HT node.

A. System response time and accuracy in authorization control

The system response time for authorizing a worker to enter in the AUC area has been evaluated by connecting a laptop to both HR and H actuator nodes. When the HR node sends an authorization request a timer starts, for being stopped when the open door request is received by the H actuator node. The response time has been evaluated as a function of the total number of transmission hops necessary for sending the various requests from HT to LS and from LS to H, thus simulating a real system in which multi-hop communications are necessary. The number of communication hops has been modified by forcing a static routing in the 6LR nodes, i.e., a static routing table has been written for all nodes for each experiment. In the case of two hops no 6LR nodes are allowed to forward messages, and HR and H communicate directly with the 6LBR. Routing protocols such as those previously mentioned (e.g., 6LoWPAN AODV or6LoWPAN SPEED) have not been used to avoid to consider possible routing delays in the evaluation of the system response time. Results of the performed experiments are summarized in terms of mean (95% confidence interval) and standard deviation values in Table I. The overall performance result figures reported in the table have been obtained by performing one thousand authorization requests for each considered network configuration. In Fig. 9 the response time probability density functions for the cases of 2 and 5 hops are shown.

TABLE I
RESPONSE TIME AS A FUNCTION OF THE NUMBER OF HOPS

Number of hops	Response time [ms]	
	μ	σ
2	147.59±1.54	24.75
3	150.79±2.02	29.72
4	156.18±1.58	32.04
5	165.32±3.76	58.40

The time values reported in Table I include all the elaboration times spent in each system node, and the network stack delays for receiving and sending COAP messages. As it is easy to expect, the whole response time increases, in average, as a function of the number of hops. In any case, the overall time in authorizing the entrance in the AUC is bounded and completely acceptable by a worker. Regarding the time distribution for each experiment, its behavior shows a Gaussian shape with a second peak slightly pronounced at higher time values. The observed behavior has been further investigated, and it is mainly due by Erika OS policies in managing tasks in the network stack. Bigger amount of time correspond to cases in which higher priorities tasks preempt tasks with lower priority levels, e.g., an incoming packet task preempts the data transmission task, thus increasing the total system response time. The phenomenon occurs for each

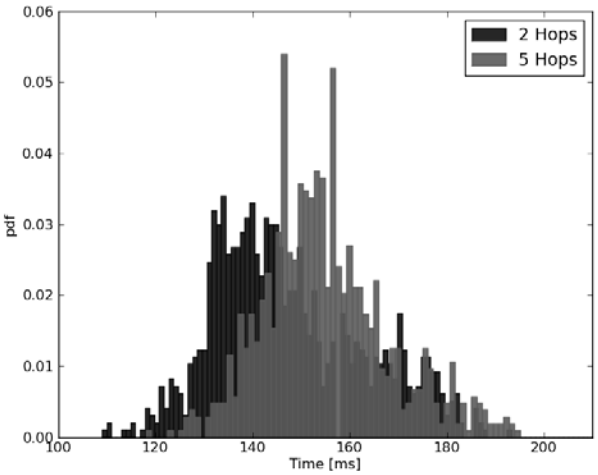

Fig. 9. Response time pdfs for the cases of 2 and 5 hops.

experiment, and it is more evident for higher numbers of transmission hops, see Fig. 9. The behavior is quantitatively revealed by the standard deviation, which increases according to the number of hops.

In the system design, an event is sent from HR to LS only when a worker is wearing all the necessary safety equipments, which means that all the passive tags T read by HR are in the equipments list stored in the HT node. The event based approach permits to have a certain percentage of false access rejections, while no false access acceptances are allowed. Must be stressed that, while the absence of false acceptances depends on the system design, possible false rejections strictly depends on the hardware equipments used for reading the RFID tags. RFID readers able to reach higher output power levels, as well as directive antennas with higher gains can greatly reduce the phenomenon, thus significantly reducing the possibility of a false rejection. However, the detailed phenomenon can be experienced in a real scenario, thus its impact has been evaluated in the case of one or two safety equipments are necessary to enter in the AUC area. Situations in which more equipments are necessary(i.e., a bigger number of tags must be read by the reader)are characterized by worst hardware dependent performance and have not been further analyzed. More in detail, the system false an authorization event, e.g., all the tags are installed in the HR range at a distance of one meter from the antenna, and counting the number of reading attempts necessary to generate the event. The results of the performed analysis have been reported in Table II for the two considered cases. For each of them one thousand experiment shave been performed. With the selected hardware equipments the false rejection rate is equal to 0 % after four attempts in case one passive tags plus HT have to be read, while it has a residual value of 1.5 % after six attempts in the case in which two passive tags plus the HT node are necessary to generate the authorization event.

False rejections in generating the authorization event increase the overall response time of the system. Combining

the response time results in sending the authorization event with the additional delay for generating the event itself, a figure of merit about the overall system response time can be obtained. Considering the maximum delay of a five hop communication, and the highest event generation time experienced in the case of one HT node and one T tag the overall response time is less than 400 ms, which slightly increases in case of two T tags are used. In both cases the value is bounded and completely acceptable by the worker.

TABLE II
FALSE REJECTION RATE VERSUS NUMBER OF READING ATTEMPTS

Number of reading attempts	False rejection rate [%]	
	HT=1, T=1	HT=1, T=2
1	10.8	49.3
2	2.6	24.9
3	0.2	13.6
4	0.0	6.7
5	0.0	2.8
6	0.0	1.5

B. System response time in logging location data

As previously described, by accessing to the log location resource of the HT node, a per AUC tracking application can be implemented. In the system design, the AUC identification data are stored in the EPC memory of the HT node when the involved resource is accessed by LS through HR. The log location request is sent immediately after the open door request. To evaluate the system response time in logging location data on HT, a laptop has been connected to the HR node. When the log location request coming from the LS is received by HR a timer starts, for being stopped when HR is able to read a formal acknowledgment for the successfully performed operation in the HT memory. The experimental setup does not take into account transmission delays due to multi-hop communications between LS and HR, in any case an overall value can be extracted by data in Table I by considering the number of hops from LS to HR. Each measured value is the necessary time for sending an EPC write memory request by the RFID reader, and for reading an acknowledgment in the memory of the semi-passive tag embedded in the HT node. With the adopted hardware solutions, by installing HT at distance of one meter from the antenna, the average experienced logging time is 289.41±1.73 ms (95% confidence interval),again completely acceptable by a worker waiting for entering the AUC area. The above reported result has been obtained by performing one thousand experiments. Even in this case several attempts can be necessary before reading from HT the expected acknowledgment. This behavior can be noticed in Fig. 10, wherein the pdf distribution two main Gaussians can be noticed, the first with a peak around 280 ms and the second with a peak around290 ms. Moreover, values around 300 ms have been measured a few times. Better performance results can be reached by using improved RFID hardware equipments.

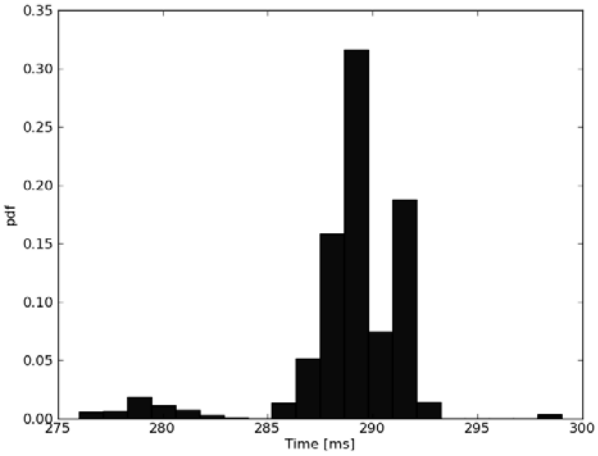

Fig. 10. Response time pdf for logging location data.

VI. CONCLUSIONS

In this paper an integration between WSN and RFID technologies in the IoT scenario is presented. In the first part of the paper the problem is first analyzed in respect of IoT enabling solutions, by proposing an integration between WSN and RFID through the REST paradigm. By representing sensors, actuators and RFID related data as network resources, addressable through COAP protocol methods, a seamless integration between the two technologies can be reached. The result is a final integrated solution in which the outstanding pervasiveness of RFIDs and the advanced sensing and communication features of WSNs are merged together to have pervasive and addressable resources in a worldwide network of objects. To fully support the IoT based integration, the reference 6LoWPAN architecture is extended by defining two new IoT nodes: (i) the Host Reader, a WSN node in which an RFID reader has been integrated, and (ii) the HostTag, a WSN node embedding an RFID tag.

In the second part of the paper the proposed integration approach in the IoT scenario is detailed for the Smart Factory use case by proposing and developing an advanced safety system able to guarantee a safe access to factory dangerous areas in which safety equipments are required. In the selected use case the system design is presented by detailing COAP resources and describing their interactions. In a real test bed deployment the adopted hardware and software solutions are first described, then the system performance in respect of two main experiments is presented. In the first experiment the system response time and accuracy in the authorization control is analyzed, showing that in case of multi-hop communications the overall response time is completely acceptable by a worker waiting for entering the area. Thanks to the event based approach no false acceptances are allowed,

while the system false rejection rate quickly decreases by increasing the number of reading attempts. In the second experiment the system response time in logging location data on HT nodes is analyzed, showing the feasibility of new integrated tracking applications that leverage popular IoT protocols.

REFERENCES

[1] J.P. Conti, "The Internet of Things," Communications Engineer, vol. 4, no. 6, pp. 20–25, January 2006.

[2] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart Objects as Building Blocks for the Internet of Things," IEEE Internet Computing, vol. 14, no. 1, pp. 44–51, December 2009.

[3] A. Bratukhin and A. Treytl, "Applicability of RFID and Agent-Based Control for Product Identification in Distributed Production," in Proceedings of International Conference on Emerging Technologies and Factory Automation, Prague, Czech Republic, September2006, pp. 1198–1205.

[4] P. Wilson, D. Prashanth, and H. Aghajan, "Utilizing RFID Signaling Scheme for Localization of Stationary Objects and Speed Estimation of Mobile Objects ," in Proceedings of International Conference on RFID, Grapevine, USA, March 2007, pp. 94–99.

[5] R. Lin, Z. Wang, and Y. Sun, "Wireless sensor networks solutions for real time monitoring of nuclear power plant," in Proceedings of World Congress on Intelligent Control and Automation, Hangzhou, China, June 2004, pp. 3663–3667.

[6] L.Q. Zhuang, W. Liu, J.B. Zhang, D.H. Zhang, and I. Kamajaya, "Distributed asset tracking using wireless sensor network," in Proceedings of IEEE International Conference on Emerging Technologies and Factory Automation, Hamburg, Germany, September 2008, pp. 1165–1168.

[7] R. Wang, Z. Zhang, J. Wang, and A. Xue, "A new solutions for staff localization in chemical plant ," in Proceedings of International Conference on System Science and Engineering, Macao, June 2011,pp. 503–508.

[8] C. Salvatore, S. Bocchino, M. Petracca, R. Pelliccia, M. Ghibaudi, and P. Pagano, "Wsn and rfid integrated solution for advanced safety systems in industrial plants," in International Conference on Software, Telecommunications and Computer Networks, Split, Croatia, September 2012, pp. 1–5.

[9] H. Liu, M. Bolic, and A. Nayakand I. Stojmenovic, "Taxonomy and challenges of the integration of rfid and wireless sensor networks, "IEEE Network, vol. 22, no. 6, pp. 26–35, November 2008.

[10] C. Chen, "Design of a Child Localization System on RFID and Wireless Sensor Networks," Journal of Sensors, vol. 2010.

[11] Z. Xiong, F. Sottile, M. Spirito, and R. Garello, "Hybrid Indoor Positioning Approaches Based on WSN and RFID," in Proceedings of International Conference on New Technologies, Mobility and Security, Paris, France, February 2011, pp. 1–5.

[12] D. De Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: towards distributed RFID sensing with software defined radio," in Proceedings of International Conference on Mobile Computing and Networking, Chicago, USA, September2010, pp. 97–104.

[13] R. Jurdak, A. Ruzzelli, and G. O'Hare, "Multi-hop rfid wake-up radio: Design, evaluation and energy tradeoffs," in Proceedings of International Conference on Computer Communications and Networks, St. Thomas, USA, August 2008, pp. 1–8.

[14] Z. Xiaoguang and L. Wei, "The research of network architecture in warehouse management system based on rfid and wsn integration", in Proceedings of IEEE International Conference on Automation and Logistics, Qingdao, China, September 2008, pp. 2556–2560.

[15] S. Hussain, S. Schaffner, and D. Moseychuck, "Applications of wireless sensor networks and rfid in a smart home environment", in Proceedings of Communication Networks and Services Research Conference, Moncton, Canada, May 2009, pp. 153–157.

[16] A. Nasir and B. Soong, "Environ sense: An integrated system for urban sensing using rfid based wsn's," in Proceedings IEEE Region10 Conference, Singapore, January 2009, pp. 1–5.

[17] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the internet of things: A survey," in International Conference on Software, Telecommunications and Computer Networks, Dubrovnik, Croatia, September 2011, pp. 1–6.

[18] "Wireless Medium Access Control (MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks(LR-WPAN)," The Institute of Electrical and Electronics Engineers, October 2003.

[19] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6over Low-Power Wireless Personal Area Networks (6LoWPANs):Overview, Assumptions, Problem Statement, and Goals," RFC4919, August 2007.

[20] J.W. Hui and D.E. Culler, "Ip is dead, long live ip for wireless sensor networks," in Proceedings of the 6th ACM conference on Embedded network sensor systems, Raleigh, USA, November 2008,pp. 15–28.

[21] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP)," CoRE Working Group, October2012.

[22] Z. Shelby, "Embedded web services," IEEE Wireless Communications, vol. 17, no. 6, pp. 52 –57, 2010.

[23] "Foundations for the web of information and services - a review of 20 years of semantic web research," in Foundations for the Web of Information and Services, D. Fensel, Ed. 2011, Springer.

[24] R.T. Fielding, Architectural styles and the design of network-based software architectures, Ph.D. thesis, 2000.

[25] K. Hartke, "Observing Resources in CoAP," IETF Internet-Draft, October 2012.

[26] "Seed-eye board. A Multimedia WSN device," rtn.sssup.it/index.php/hardware/seed-eye.

[27] A. Mitrokotsa and C. Douligeris, RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations, chapter Integrated RFID and Sensor Networks: Architectures and Applications, pp. 511–535, Wireless Networks and Mobile Communications. CRC Press, Taylor & Francis Group, 2009.

[28] P. Gai, E. Bini, G. Lipari, M. Di Natale, and L. Abeni, "Architecture For A Portable Open Source Real Time Kernel Environment," in Real-Time Linux Workshop and Hand's on Real-Time Linux Tutorial, Nairobi, Kenya, November 2000.

[29] S. Bocchino, M. Petracca, P. Pagano, M. Ghibaudi, and F. Lertora," Speed routing protocol in 6LoWPAN networks," in Proceedings of IEEE International Conference on Emerging Technologies and Factory Automation, Toulouse, France, September 2011, pp. 1–9.

[30] E.D. Gutierrez Mlot, S. Bocchino, A. Azzarà, M. Petracca, and P. Pagano, "Web services transactions in 6LoWPAN networks," in Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Lucca, Italy, June 2011,pp. 1–2.

[31] A. Azzarà, D. Alessandrelli, S. Bocchino, P. Pagano, and M. Petracca,“ Architecture, functional requirements, and early implementation of an instrumentation grid for the iot,” in Proceedings of International Conference on High Performance Computing and Communications, Liverpool, UK, June 2012, pp. 320–327.

Matteo Petracca received the M.S. degree in Telecommunication Engineering in 2003 and the Ph.D. degree in Information and System Engineering in 2007, both from the Politecnico di Torino, Turin, Italy. From March2007 to November 2009 he was a post-doc researcher at the Politecnico di Torino working on multimedia processing and transmission over wired and wireless packet networks. In 2009 he joined the Scuola Superiore Sant’Anna in Pisa, Italy and in the 2010 the CNIT(National Inter-University Consortium for Telecommunications)as research fellow. Dr. Petracca has been actively involved in many Italian and European research projects. He is co-author of more than 30 scientific papers published in international journals, peer-reviewed conference proceedings and book chapters.

Stefano Bocchino received the B.S. degree in Informatics and Automation Engineering and the M.S. degree in Informatics Engineering both from Università Politecnica delle Marche, Ancona, Italy. He is currently a Ph.D. student in Embedded System at Scuola Superiore Sant’Anna, Pisa, Italy. His research interests include wireless sensor networks, routing protocol for6LoWPAN networks and wireless based localization techniques.

Andrea Azzarà received the M.S. degree in Computer Engineering from the University of Pisa, Pisa, Italy. He is currently a Ph.D. student in Embedded System at Scuola Superiore Sant’Anna, Pisa, Italy and is currently involved in Italian and European research projects. His research interests include wireless sensor networks, network abstraction, and architectures for the Internet of Things.

Riccardo Pelliccia was born in 1983, he received his M.S. degree cum laude in Electronic Engineering at Università Politecnica delle Marche in February 2011. Since November 2011 he is a Ph.D. student in Innovation Technologies (curriculum Embedded System) at Scuola Superiore SantAnna, Pisa, Italy. His research interests include hardware design in wireless sensor networks and visible light communication targeted to vehicular environment.

Marco Ghibaudi is a Computer Science Engineer specialized in Control Systems. He has collaborated in various projects related to wireless sensor networks(IPERMOB), to smart vehicles (Salon de l’Auto de Geneve) and to field programmable gate arrays for telecommunications. He is actually a Ph.D. student at Scuola Superiore Sant’Anna and a Doctoral Student at CERN, where he is actively collaborating in the update of the ATLAS experiment.

Paolo Pagano received his M.S. degree in Physics in1999 from Trieste University (I). In 2003 he received his Ph.D. degree in High Energy Physics from Trieste University having worked for the COMPASS collaboration at CERN (CH). In 2004 he was hired by HISKP at Bonn University (D). In 2006 he received a Masterin Computer Science from Scuola Superiore Sant’Anna in Pisa (I). In the same year he joined the REal-Time System (RETIS) laboratory of the Scuola. From 2009 he is with the CNIT (National Inter-University Consortium for Telecommunications). He is leading the Networks of Embedded Systems team at Sant’Anna University in Pisa. His research activities have a specific focus on Wireless Sensor Networks applied to traffic monitoring. He is responsible of public and private research grants in the domain of Intelligent Transport Systems. He co-authored about 70 peer reviewed papers to international journals and conferences.