WSN and RFID Integrated Solution for Advanced Safety Systems in Industrial Plants

C. Salvatore[†*], S. Bocchino[†*], M. Petracca[‡*], R. Pelliccia[†*], M. Ghibaudi[†*] and P. Pagano[‡*]

[†]Scuola Superiore Sant'Anna Research Unit, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Italy
[‡]National Laboratory of Photonic Networks, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Italy
[*]Real-Time Systems Laboratory, Scuola Superiore Sant'Anna, Italy
Email: [c.salvatore|s.bocchino|r.pelliccia|m.ghibaudi]@sssup.it, [matteo.petracca|paolo.pagano]@cnit.it

Abstract: **The Smart Factory concept has been enabled in the last few years thanks to both Wireless Sensor Networks (WSNs) and Radio-Frequency IDentification (RFID) technologies. Although the two technologies have been adopted in isolation in factory automation applications, their partial integration start to be considered in different research fields. In this work, we propose a fully integrated approach between RFID and WSN targeted to develop an advanced safety system in industrial plants. By integrating RFID tags and readers in WSN nodes the developed system extends sensing capabilities, efficiency and pervasiveness of the WSN solutions already installed in the factory plant, while allowing a safety access to dangerous areas under the requirement that safety equipments are adopted. The paper presents both hardware and software solutions developed as well as performance evaluation results, in terms of system response time and energy consumption reduction, in a real testbed.**

1. INTRODUCTION

The continuous miniaturization of embedded devices and the ceaseless reduction of their costs are fostering in recent years the development of intelligent houses, cities and factories. Academic and industrial research communities are making use of these novel components for enhancing the security, safety, efficiency and livability of a large number of human-related environments. In particular, several research activities are nowadays focused on proposing technological solutions aiming at realizing the so called "Smart Factories". Ideally, the Smart Factory goal is to assist people and machines in executing their tasks in a context-aware manner [1]. Although the implementation of a Smart Factory can be enabled by means of different key technologies, the solutions providing the best tradeoff between costs and performance are based on Wireless Sensor Networks (WSNs) [2] and Radio-Frequency IDentification (RFID) [3].

Wireless sensor networks are low-power embedded devices characterized by reduced computational capabilities that communicate among them to fulfill complex tasks. WSN technology is used in a Smart Factory context to perform real time environmental monitoring [4], industrial asset tracking [5], and localization of both people and equipments [6].

Radio-frequency identification, similarly to WSN, is an extremely low-cost and low-power technology implemented in several possible ways, each one of them characterized by different transmission bandwidth and communication ranges. Concerning the Smart Factory context, RFID is mainly adopted for simple object identification or, in case of advanced applications, for estimating goods positions and speed [7].

In this paper we propose an integrated WSN and RFID solution aiming at implementing an advanced safety system in industrial plants while requiring low-cost equipments and without affecting workers' comfort. The developed system has been specially designed for a Smart Factory scenario by adopting real-time software components able to reduce the system response time to effectively help workers to access to specific plant areas in respect of specific safety conditions determined a priori (e.g., wearing safety helmet, wearing safety boots).

The rest of the paper is organized as follows. In Section 2, we present the state-of-the-art in WSN and RFID integration describing several applications in other application domains due to the lack of integrated solutions in the Smart Factory scenario. In Section 3, the developed system is deeply described in its operating logic, hardware and software components. Performance result in terms of response time, as well as node power consumption considerations are presented in Section 4. Conclusion follows in Section 5.

2. WSN AND RFID TECHNOLOGIES INTEGRATION

In recent years, an increasing number of research activities started to propose integrated WSN and RFID systems for providing new or improved services.Thanks to this integrated design, the overall system can achieve the outstanding pervasiveness of RFIDs while preserving the advanced sensing and communication features of WSNs. The integration between WSNs and RFIDs can be reached, from a hardware equipment point of view, 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 capabilities 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 Internet of Things vision.

A first example of RFIDs and WSNs integration is presented by Chen in [8] where a wireless localization system for moni-

toring 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. In the same application scenario, we can cite the work presented by Xiong et al. in [9] in which an RFID tags grid is used to enhance the positioning accuracy reached by standard well-known RSSI based WSN localization algorithms. In this latter case the integration is reached again by installing RFID readers on WSN nodes. In the mentioned works, RFIDs are mainly used for implementing a coarse grain localization while trying to optimize the power consumption of each WSN unit. Extending this idea, Jurdak et al. proposed in [10] 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. The integration of RFID tags in WSN nodes is nowadays greatly considered by private companies that have started to sell commercial products [11] to promote the realization of new applications.

Concerning the integration classification reported above, the developed solution presented in this work belongs to both classes. In fact, both WSN nodes with integrated RFID tags and readers have been adopted, thus taking the maximum benefit from a WSN and RFID integration. Moreover, the major novelty of the presented work is the selected Smart Factory scenario in which a careful design of both hardware and software must be adopted to address real-time constraints.

3. SYSTEM DESIGN AND IMPLEMENTATION

As previously introduced, the presented work proposes an integrated WSN and RFID solution for advanced safety systems in industrial plants. The system mainly implements a two-level access control policy to monitor dangerous areas.

The first control level guarantees that the access to a given *Area Under Control* (AUC) is provided only to workers authorized to enter that plant area (e.g., only electricians can enter in power control rooms). This system feature is implemented by means of an RFID reader integrated with a WSN device (*WSN reader* in the following), installed on the access door of the area, and by a *smart node*, worn by the worker, that is a WSN node integrating a semi-passive RFID tag. The tag contains a unique worker identifier that can be used in conjunction with a workers database for retrieving worker's identity. The choice of storing an identifier on the smart node tag memory permits to manage cases in which more than one worker is waiting for entering the dangerous area. In this case, in fact, the access is granted or denied for each worker. Malicious cases in which unauthorized workers enter the dangerous area when the door has been opened by a successful authorization process have not been considered yet considering the good faith of the workers. In any case, the problem can be easily managed by installing several WSN readers in the area that could periodically check if the safety conditions are respected. The tag to be mounted on the smart node has been specially selected as semi-passive for a full integration in the WSN node and to provide advanced energy-aware policies allowing a significant extension of the node lifetime (i.e., the WSN node wakes up when the WSN reader gets tag information).

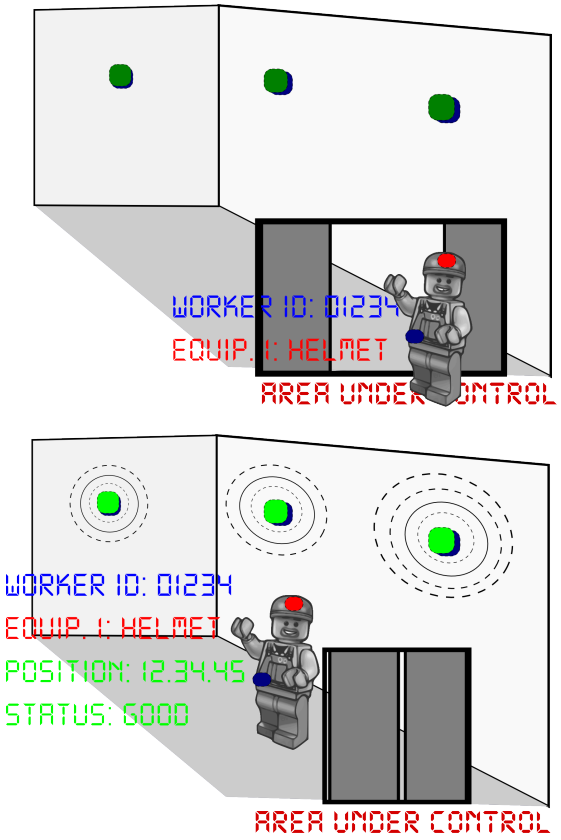

Figure 1: High level system overview with an intuitive example of the two-level access control policy implemented.

The second control level is enforced by using passive RFID tags installed on workers' equipments, thus guaranteeing the access in safety conditions. In this second case the control is performed again by using the WSN reader installed in the access point of the area under control. The list of all necessary equipments is stored in the smart node in order to keep the access data as much as closer to the worker for future extensions going in the direction of ad-hoc RFID networks in which the smart node could be aware at any time if a certain worker has its own safety equipments. The two control level policies just described are depicted graphically in Figure 1, where at the top both controls on worker identifier and equipments are reported. At the bottom of the picture another feature that can be reached by the system is reported. Thanks to the integrated solution provided by the WSN reader, old applications (e.g., localization services) can be triggered when strictly necessary.

Starting from the above introduced high-level description of the system its hardware and software building blocks are described in the following of this Section in respect of their capabilities and design strategies.

3.1 Hardware Components

The main hardware component of the full system is the *smart node*, which in our design is a custom WSN node equipped with a semi-passive RFID tag. The WSN device adopted is the SEED-EYE [12] board developed within the IPERMOB

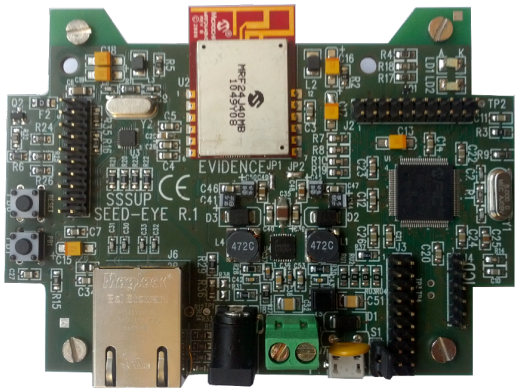

Figure 2: SEED-EYE board.

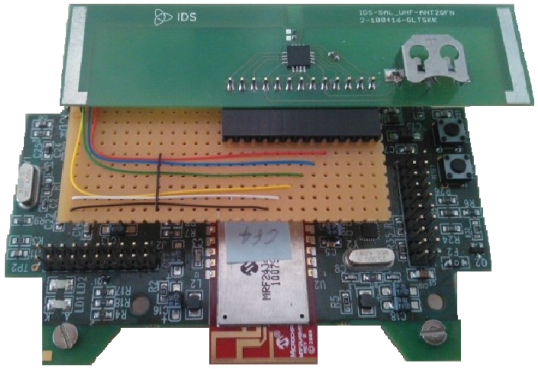

Figure 3: Smart node based on SEED-EYE.

project [13]. The board, depicted in Figure 2, is equipped with a 32-bit microcontroller, a IEEE802.15.4 transceiver, ethernet interface and various expansion connectors. The adopted microcontroller is the Microchip PIC32MX795F512L, a 80 MHz, 32 bit, MIPS processor that comes with 128 KB of internal RAM memory. PIC32MX795F512L power consumption can be extremely reduced bringing, via software, the unit into idle and sleep states. The exit from low-power states can be driven by external or internal interrupts. The transceiver, the MRF24J40MB, is a IEEE802.15.4 fully compliant device that, similarly to the MCU, can be brought into a low power state. Expansions connectors provide an access to the Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I2C) and UART peripherals of the MCU. SEED-EYE presents a small form factor (80 cm^2) and can be powered by batteries as well as by USB port. By using the SEED-EYE expansion connectors it is possible to connect a semi-passive RFID tag. This tag (20 cm^2), based on the IDS SL900A chip, communicates in the two UHF bands of 860-960 MHz and can be used either as passive or semi-passive RFID tag (battery powered). Thanks to an internal Real Time Calendar (RTC), the SL900A chip can be operated as data-logger by connecting external sensors to dedicated pins. Furthermore, a dedicated memory of the chip can be addressed through an SPI interface, allowing in particular the access to the EPC memory (containing the Electronic Product Code) and to a 1052 byte USER memory. Moreover, SL900A provides a status pin that is driven low when the tag receives a transmission. Thanks to this signal (connected to one of the external interrupt port of PIC32MX795F512L) the microcontroller can be informed of the RFID activity, fostering smart node activation based on wake-on-RFID. The smart node integrating the semi-passive RFID tag on top of the SEED-EYE is depicted in Figure 3. Thanks to the intelligent activation fostered by semi-passive tags a smart node can stay in a sleep-mode when outside AUC, and in an activate state only inside the AUC. Table 1 shows the current consumption at 3.3 V for the main components of the smart node, demonstrating the importance of the correct use of sleep features.

Table 1: Smart node power consumption.

Component	Wake status	Sleep Status
MCU	120 mA	40 μ A
Transceiver (Tx) Max Power (+20 dBm)	130 mA	5 μA
Transceiver (Tx) Avg Power (0 dBm)	23 mA	5 μA
Transceiver (Rx)	25 mA	5 μA

Other key component of the system is the *WSN reader*, an RFID reader interconnected with the SEED-EYE board, depicted in Figure 4. The adopted reader is the module Sensor ID Discovery UHF OEM which has been connected to the WSN device by means of a simple serial interface while developing a set of software functions able to abstract the device as a common interface. The reader is able to support the EPC standard for reading data from tag memories and is able to reach a transmission power of 500 mW (27 dBm). The final distance in reading tag memories is close to 5 m with an omni-directional antenna. Regarding the passive tags to be used on safety equipments we selected the ALN-9654 G, produced by Alien, due to its extreme low-cost and compliance with the EPC standard.

3.2 Software Components

Concerning the software components and the operating system to be used in the system nodes, the choice has been based on the following assumptions:

- smart nodes can perform memory consuming operations, such as vital parameter acquisition and transmission;
- smart nodes and WSN reader nodes can perform time critical operations, for example, they can alert a central system

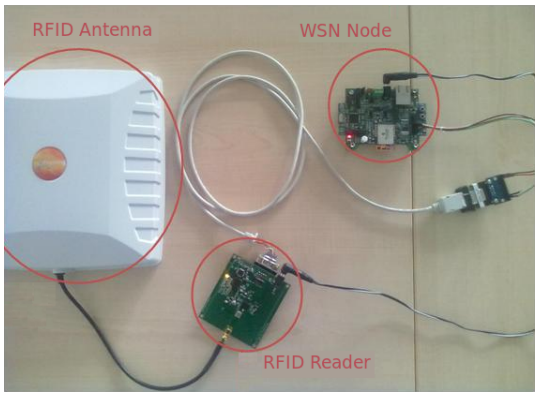

Figure 4: WSN reader node with integrated RFID component.

when the worker is injured;
- system nodes must adopt an effective power-aware policy.

Given these constraints we decided to adopt a Real Time Operating System designed for low-power, low-memory microcontrollers, Erika Enterprise OS [14]. Erika is characterized by an extremely reduced ROM footprint although it can provide advanced scheduling policies (Fixed priority, Earliest Deadline First) for organizing tasks execution, as well as resources and semaphores for implementing preemption policies. Furthermore, Erika comes with a fully compliant, light weight IEEE802.15.4 software stack, *uWireless* that can be configured for performing time accurate, periodic and aperiodic packet transmissions. Moreover, Erika permits to easily implement energy-aware scheduling policies by leveraging low-power features of microcontroller and transceiver.

The applications developed on top of the Erika operating system provide the following features:

- Communication with the tag reader. The WSN component of the WSN reader communicates with the Sensor ID Discovery UHF OEM through dedicated serial channel.
- RFID tags memory access. The internal memory of the RFID integrated in the smart node can be written and read through the SPI protocol, thus providing an access to the internal EPC and USER memories;
- User identification. Each user can be identified by a unique ID, that can be the EPC value contained in the semi-passive tag memory, or a value stored in the tag USER memory;
- Smart activation. An interrupt driven software routine is used for providing an extremely fast wake up of microcontroller and transceiver, fostering power-aware policies;
- Integration with WSN functionality. Smart nodes can perform intelligent activation and deactivation of the system as depicted in Figure 1, where once the worker has obtained the access to the AUC a WSN based service is performed.

Regarding the system logic able to guarantee a safety access to the AUC, a conservative choice has been made. More in particular, until the necessary equipments are not recognized the WSN reader keeps on trying to detect the objects. This choice permits to have a certain percentage of false access rejection, while no false access acceptances are allowed. In case of several workers try to access to the area simultaneously the number of missed objects is detected for each one of them thanks to a complete list stored in the memory of the smart node tag, thus allowing the access only to the right worker. As previously reported, at this stage the scenario in which a worker maliciously either tries to enter when the access has been guaranteed to another one or fakes his identity has not been considered.

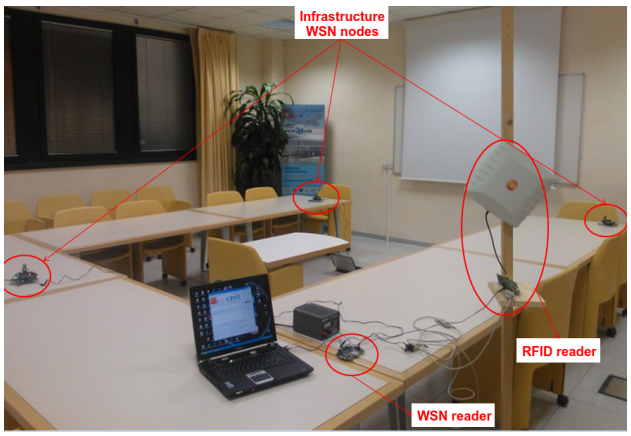

Figure 5: Testbed scenario with system nodes.

4. PERFORMANCE EVALUATION

The performance of the system has been evaluated by means of a real testbed developed at the TeCIP Institute of Scuola Superiore Sant'Anna in Pisa, Italy. A picture of the testbed, consisting in a room in which an AUC area has been simulated, is reported in Figure 5, where the positions of WSN nodes and the *WSN reader* are annotated. The *smart node* depicted in Figure 3 must be considered as the equipment worn by the worker, while the passive tags are installed on top of safety equipments.

The system performance has been evaluated in terms of response time as a function of the number of attempts necessary to recognize all the worn security equipments. Experiments have been conducted 500 times for guaranteeing a sufficient statistical relevance of the results. In the performed tests, the system has been able to provide a correct access authorization in several attempts with the percentages reported in Table 2. It must be pointed out that tags have been kept in the WSN reader transmission range (1 m of distance) in order to properly characterize system accuracy and response time.

Table 2: Correct accesses versus number of attempts.

Number of attempts	Correct access [%]
1	89.2
2	97.4
3	99.8
4	100.0

The missing acceptance rate at the first attempt is equal to 10.8% and significantly decreases after two attempts when the residual missing acceptance rate is 2.6%. No missing acceptances have been experienced after a number of attempts equal to 4. Regarding the final response time, the maximum experienced delay is shorter than 192 ms in case 4 attempts are performed, while it is lower than 67 ms in case the access is authorized after the first attempt. A delay time distribution for the first attempt case is reported in Figure 6. In the same graph

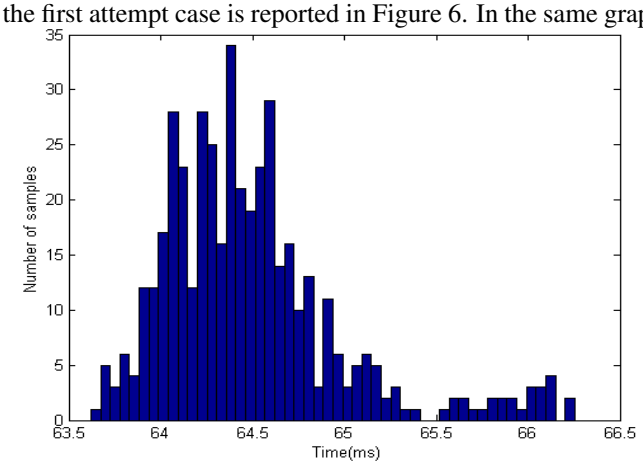

Figure 6: Delay time distribution for the first attempt case.

it is possible to see how in average the response time is close to 65 ms, while the full probability density function shows a Gaussian shape with a longer tail on the right side. In any case, the system response time in authorizing the entrance in the AUC is bounded and completely acceptable by the worker, mainly thanks to the software design choices and Erika OS.

4.1 Power consumption analysis

As described in Section 3.1, *smart nodes*, thanks to the integration with the semi-passive tag, can minimize their power consumption when outside the AUC. Furthermore, as Table 1 shows, by limiting the transmission power of the transceiver from +20 dBm to +0 dBm, transceiver consumption when transmitting can be lowered of 82%. In a typical application scenario, workers will operate a maximum of 8 hours inside the AUC, meaning that for the remaining part of the day node can stay in low-power mode. Furthermore, during the active time, operators will probably be located sufficiently close to infrastructure WSN nodes thus making possible the reduction of the transmission power. The power consumption (mAh) for the node in active state can be approximated as:

$$C_a = \frac{(CPU_c * CPU_a + TRX_a(Tx_c + Rx_c))}{T/3600} \quad (1)$$

where CPU_c, Tx_c and Rx_c are the active consumption of MCU and transceiver in transmission and listening respectively. CPU active time, CPU_a, and transceiver active time, TRX_a, depends by the application but reasonable values can be respectively 1 and 0.05 seconds. Considering a IEEE802.15.4 communication period, T, equal to 60 seconds, when nodes operate at maximum transmission power C_a value becomes close to 585 mAh while when transmission gain lower value is adopted consumption is reduced to 264 mAh. For our considerations, sleep mode has a power consumption so negligible that can be approximated to zero. In the hypothetical scenario in which a node can be in sleep mode for the 12.5% of the working time (1 hour) and in the active mode with maximum and standard transmission powers for the remaining amount of time (7 hours), using a Li-Ion 2800 mAh battery smart nodes can increment their life from less than 5 hours to more than 12 hours.

5. CONCLUSION

In this work, an integration between WSN and RFID technologies is proposed for creating an advanced safety system for industrial plants. Both RFID tags and RFID readers have been integrated on WSN nodes in order to extend the sensing capabilities, the efficiency and the pervasiveness of the integrated devices, thus going towards the full accomplishment of the Internet of Things vision. In the paper, both developed hardware and software solutions are discussed, pointing out the attention on the real-time requirements of the system and on the high-level system logic that avoids false access by permitting false entrance rejections. The performance of the system has been evaluated in terms of response time, showing as in some cases more RFID tag reading attempts are necessary before guaranteeing the access to the worker. In any case the final experienced response time is always shorter than 192 ms, showing as a completely acceptable delay for the worker can improve his safety in factory environments. Concerning the power-aware policy proposed in the paper, the wake-on-RFID feature proved to be extremely useful for incrementing node lifetime and thus for enhancing system overall quality. A future extension of this work will allow the interoperability with the 6LoWPAN standard and will address existing security flaws. A full interoperability with 6LoWPAN will provide a full and easy access to the smart nodes information. Concerning the latter extension, our group is investigating low-complexity asymmetric signatures algorithms to be implemented on smart nodes for guaranteeing user privacy.

REFERENCES

[1] D. Lucke, C. Constantinescu, and E. Westkmper, "Smart factory - a step towards the next generation of manufacturing," in *Proc. of Conference on Manufacturing Systems*, May 2008, pp. 115–118.

[2] S.C. Lee, T.G. Jeon, H.S. Hwang, and C.S. Kim, "Design and Implementation of Wireless Sensor Based-Monitoring System for Smart Factory," in *Computational Science and Its Applications*, vol. 4706 of *Lecture Notes in Computer Science*, pp. 584–592. Springer, 2007.

[3] D. Zuehlke, "SmartFactory from Vision to Reality in Factory Technologies," in *Proc. of International Federation of Automatic Control World Congress*, July 2008, pp. 82–89.

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

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

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

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

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

[9] Z. Xiong, F. Sottile, M. Spirito, and R. Garello, "Hybrid Indoor Positioning Approaches Based on WSN and RFID," in *Proc. of International Conference on New Technologies, Mobility and Security*, February 2011.

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

[11] "Dual RFID-ZigBee sensors to enable NFC applications for the Internet of Things," www.libelium.com/rfid_nfc_zigbee_sensors, March 2012.

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

[13] A. Alessandrelli, A. Azzarà, M. Petracca, C. Nastasi, and P. Pagano, "ScanTraffic: Smart Camera Network for Traffic Information Collection," in *Proc. of European Conference on Wireless Sensor Networks*, February 2012, pp. 196–211.

[14] "The Erika Enterprise Real-time Operating System," erika.tuxfamily.org.