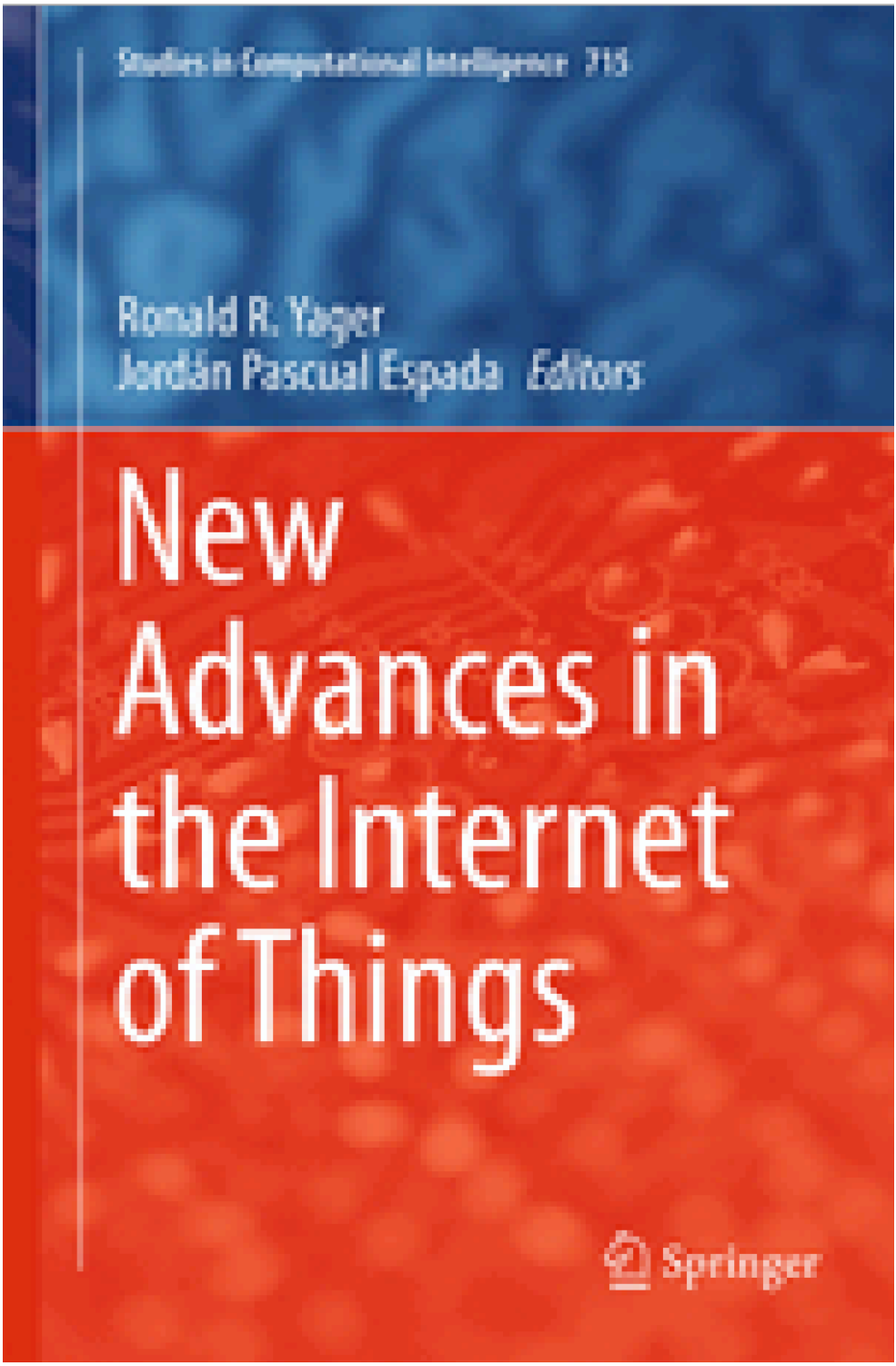
Studies in Computational Intelligence 713
Ronald R. Yager
Jordán Pascual Espada Editors
New Advances in the Internet of Things
Springer

RFID-Based Multi-level Sensing Network for Industrial Internet of Things

S. Amendola, C. Occhiuzzi, S. Manzari and G. Marrocco

Abstract A wireless sensor network fully based on battery-less radio frequency identification (RFID) devices is here proposed for application to the emerging Industrial Internet of Things. The hierarchical structure of the network enables a multi-level monitoring of complex spaces hosting industrial equipments. A multi-antenna configuration permits to select the zones of the space to be monitored while custom RFID boards, capable to host several kinds of sensors, permit to capture both environmental parameters (e.g., temperature, humidity, and light) and the human interaction with things. The system provides the real-time detection of a plethora of complex events ranging from critical environmental accidents, up to the (un)authorized access to a critical area and the tampering/overloading of equipments. The potential of the proposed sensor network is finally demonstrated through an application to the monitoring of a real electrical secondary substation cabin.

Keywords Wireless sensor networks · RFID · Multi-level sensing · Multi-level monitoring · Industrial Internet of Things · Real-time monitoring

1 Introduction

The current development of the Internet of Things (IoT), beside opening innovative scenarios in connectivity, gaming, leisure, and domotics, is also fostering changes in modern manufacturing, energy, agriculture, transportation, and in many others industrial branches where the possibility to improve the interactions between human and machines may generate unprecedented technical and economic opportunities [1]. Gathering information about environments and processes will increase the

S. Amendola · C. Occhiuzzi (✉) · S. Manzari · G. Marrocco
RADIO6ENSE S.r.l, Rome, Italy
e-mail: amendola@info.uniroma2.it

S. Amendola · G. Marrocco
Pervasive Electromagnetic Lab, University of Roma Tor Vergata, Rome, Italy

R.R. Yager and J. Pascual Espada (eds.), *New Advances in the Internet of Things*,
Studies in Computational Intelligence 715, DOI 10.1007/978-3-319-58190-3_1

capabilities to control complex systems and to predict events, thus optimizing the production, the security, and the overall efficiency. This particular implementation of the IoT, denoted as *Industrial IoT*, is hence referred to wireless sensor networks which are characterized by a high level of autonomy and reconfigurability and above all by a minimum impact on costs, energy, and procedures. Sensors will be added to existing machinery without compromising their integrity at the purpose to incrementally upgrade their functionalities up to achieve, over the long term, a fully automated, flexible, networked, and data-oriented industry [2].

Energy-autonomous wireless sensors for application to ambient monitoring, personal tracking, cold chain, and manufacturing control have been greatly improved in the latest years mostly thanks to the well-assessed radio frequency identification (RFID) standard EPC C1G2 which can now offer sensing functionalities [3] besides the basic identification capability. This kind of sensors demands for a rather limited maintenance in comparison with the more assessed wireless technologies such as ZigBee, Bluetooth, or Wi-fi [4]. The required energy is indeed provided by external interrogators, which can interact with a multiplicity of sensors, thus enabling a single- to multi-point link with a remarkable reduction of the overall wiring. Small batteries and energy harvesters like solar panels can be used as well to support the low-power sensing activity while the communication is based on electromagnetic backscattering and can hence be considered as passive. The convergence between IOT and RFID tech is a well-known driving force toward the real implementation of what the authors defined "the last meters of the Internet of things," i.e., the physical layer of IOT systems [5–8].

The RFID energy-autonomous sensors which are nowadays available on the market, or which are being experimented worldwide in research laboratories, can be classified into two sets: (*i*) low-cost and qualitative *analog tags* for item-level applications and (*ii*) medium-cost electronic-packed *digital tags* which permit an accurate and versatile sampling of physical parameters. The first class, mainly comprising traditional RFID passive tags, exploits the interactions between tag antenna and environment to indirectly gather sensing information and hence can be affected by many uncertainties sources [9]. The latter family can instead include real and even COTS sensors[10–14] and are suitable to produce accurate data. Moreover, their cost is currently decreasing so that they are becoming attractive also for massive applications.

Although many examples of RFID-based sensors have been recently proposed by both academia and industry (refer to [3] for a review), the deployment of a fully autonomous wireless sensor network completely based on RFID technology is still in an embryonic stage. Some early successful examples are human activity monitoring [15, 16], ranging and localization of people and objects [17], bus fleet monitoring and scheduling [18], and workplace safety management [19].

To the best of our knowledge, this contribution introduces for the first time the complete design and implementation of an *RFID-based industrial sensor network* for application to critical infrastructures such as pipelines, smart grids, and power plants through the proper integration of the above two classes of analog and digital RFID sensors within the machineries and the nearby environment. The goal to be

achieved is an autonomous and easily reconfigurable wireless sensor network, suitable to be employed in an industrial scenario with a minimum impact on the existing infrastructures. The architectures of both entire network and sensors are conceived to be modular and scalable, such as to include several sensing devices which can be easily repositioned into the environment. The paper addresses the design of both hardware and software components, and it is organized as follows: The multi-level architecture of the network is introduced in Sect. 2. A new topology of multi-function RFID sensing board is then described in Sect. 3, while Sect. 4 resumes the implementation of the control and coordination software. The deployment of the network in a real environment and some examples of multi-parametric monitoring are finally described in Sect. 5.

2 Architecture of the RFID Sensor Network

The proposed RFID sensor network (hereafter RFID-SN) is organized as a multi-level hierarchical architecture (Fig. 1) suitable to achieve spatial selectivity and sensing selectivity. From a logical side, the *space* under observation is partitioned into *M zones*. Each zone includes N_m *things* of interest, and the *nm*-th *thing* has K_{nm} *attributes* to be monitored along with the time. Finally, the proper processing of the K_{nm} attributes (singularly or combined) defines an *event*, i.e., any occurrence that is relevant for the industrial infrastructure. This scheme is physically implemented by considering a multi-channel interrogation module, i.e. the RFID reader, connected via coaxial cables to transmitting/receiving antennas (A_m),

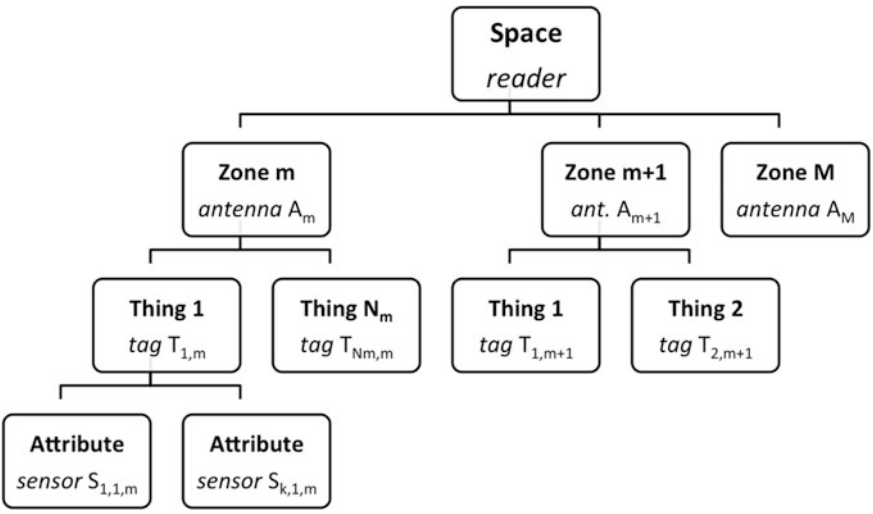

Fig. 1 Schematic multi-level architecture of the RFID sensor network

which interrogates the different RFID sensor tags (T_{nm}) properly dispersed into the environment. The electromagnetic coverage of each antenna within the space, which depends on the antenna gain, the radiated power, and the interaction of the electromagnetic field with the nearby environment [20], defines the extension of a zone. The RFID sensor tags, either analog or digital, identify the *things* to be monitored and may be integrated with one or more sensing mechanisms generating the measured data about the K_{nm} attributes of the thing itself. The number C of the independent channels (each channel being a sensor signal coming from a tag) produced by this architecture, e.g., the number of signals $\{S_{knm}\}$ collected by the reader node, is hence as follows:

$$C = \sum_{m=1}^{M} \sum_{n=1}^{N} K_{nm} \tag{1}$$

The reader node is managed by a control and command software living into the reader unit itself or into a remote system. Readers of different zones can be connected through Ethernet/Wi-fi links to a higher-level network whose description is, however, out of the scope of this paper.

This architecture offers a great freedom concerning the on-site physical reconfigurability (addition, repositioning, and dismantling of sensors) and, accordingly, in the space granularity of the surveillance. A remote dynamic handling of the power is moreover possible, i.e. the power emitted from the reader and even from the single interrogating antenna can be dynamically modified at the purpose to properly shape the extension of the zones and focus the available resources on the most critical areas where abnormal events have been detected.

The reader's antennas interact with all the kinds of tags by using the backscattering modulation principle: the energy needed by the sensors for data acquisition is directly scavenged from the electromagnetic field radiated by interrogation system, while no energy is wasted by the tag for the communication with the reader. The reader unit can interact with the sensors in time division according to a dynamic strategy allowing a periodic activation of all the beams to control the whole space volume, or, alternatively, trigger a reduced set of reader antennas at the purpose to control a subregion of the environment with a higher data rate.

2.1 Analog Signals

The analog tags (i.e. the conventional RFID tags) are displaced onto moving parts of the *space*, like cabinet windows or mobile equipments, as well as onto the access doors and on the wall of critical areas of the infrastructure to be monitored. The data produced by those tags is the level of the electromagnetic field (in the form of received signal strength indicator (RSSI)) they backscatter toward the A_m antenna of the reader during the interrogation. During an initial calibration, the system stores

the electromagnetic fingerprint of the environment, i.e. the values of the RSSI produced by the various sensors in stationary conditions (as in the case of an anti-theft system). Accordingly, any geometrical change of the environment such as somebody moving inside [8], the interaction with doors, cabinets, or with any other critical device will produce an *environmental modulation* of the backscattered fields, and it will be perceived by the system as a perturbation of the RSSI collected by the reader.

Due to the uncertainties related to such measurements [9], these analog RFID tags are preferably used as threshold sensors since they provide information about those events that are characterized by a strong contrast between normal and abnormal working conditions. The intelligence to retrieve the sensed data is hence mostly concentrated at the reader side, which could be equipped with detection and classification algorithms (not addressed here) which are applied to raw RSSI data to recognize specific events (refer to [15, 21] for some idea of RFID-based pattern recognition). Typical threshold events in an industrial environment would be flooding, open/closing of doors and cabinets, and shadowing/scattering caused by human presence. A particular case of this class of sensors are RFID badges [22] of workers which can be recognized and identified by the system in critical areas, as better discussed later on by means of a real-life example.

It is worth noticing that recalibration of the event detection algorithm could be required in case of a severe modification of the environment close to the specific tag, like the placement of a new big object or the repositioning of a cabinet which may substantially alter the ambient backscattering of some tags. Accordingly, the pre-defined RSSI thresholds used to identify anomalous events have to be retuned. Instead, minor geometrical changes like the placement/motion/addition of a small thing far from the specific tag are expected to produce only a negligible effect especially if threshold detection is applied. Anyway, these static artifacts could be fully removed by recollecting the signal baseline following a remote request, or by an automatic algorithm.

2.2 Digital Signals

The digital tags are instead provided with specific internal/external sensors that produce quantitative data about the specific physical parameters under observation (light, humidity, temperature, deformation, radioactivity, and others). A digital tag has to be considered as a real multi-channel sensor node, even if the local computation capability is rather modest and restricted to sensor handling and configuration. Each tag hence reproduces the global multi-level structure that is implemented for the general architecture of the RFID-SN since the logic unit of the board can selectively activate one or more sensors according to the request coming from the reader. Data produced by the digital tags is directly suitable for a remote interpretation.

As a whole, the RFID-SN is hence capable to detect discrete events as well as to collect continuous variation of physical parameters by using a unitary infrastructure and a single communication protocol.

3 The Configurable RFID Sensing Breadboard

The core of the RFID-SN is a proprietary digital tag, hereafter denoted as *Radio-board*, that enables multi-channel battery-less sampling and transmission of environmental parameters.

The *Radio-board* is based on a new family of RFID chip transponders [10] providing a native integrated electronics for sensing activities beside the pure identification features. In particular, the selected IC includes an analog-to-digital converter (ADC) capable to control up to two analog external sensors and an integrated temperature sensor with programmable dynamic range in the interval −40/150 °C. This IC can be used in a fully passive mode (synchronous modality), i.e. the energy required for activation and actions is entirely harvested from the electromagnetic waves emitted by the remote interrogator, or in battery-assisted mode, i.e. a local battery can provide additional energy to improve the IC sensitivity (from −5 dBmW down to −15 dBmW) for extended read range and, above all, to perform periodic measurements even in the absence of the reader (asynchronous/data logging mode). The possible additional sensors which can be connected to the chip are any resistive, capacitive, or optical device, provided that its power consumption is compliant with low-power applications.

In order to master the wide range of functionalities the IC is provided with, the transponder element was engineered to make it operating in several radiation and sensing modalities while making use of a same mother PCB layout, thus speeding up the prototyping and customization of new products.

The *Radio-board* (Fig. 2) is logically composed of three parts:

(i) a radiating element made of a meander line antenna (MLA);
(ii) a spiral impedance transformer connected to the IC and to a tuning inductor L_T;
(iii) additional expansion traces for battery and sensors interconnections.

Both the MLA and the spiral traces are partly interrupted in several points (trace gaps M in the MLA and N in the spiral). Two further gaps (SW1 and SW2) split the transformer section from the MLA. The device can be globally regarded as a multi-port antenna. By properly selecting the tuning inductor and the subset of connected trace gaps, the distribution of the surface current over the antenna and, accordingly, the impedance and the gain, can be shaped for a specific application and positioning. For instance, acting onto the MLA, the size of the antenna is modified and hence also its gain and impedance, while by connecting some gaps, the spiral could be enlarged or reduced as needed for the specific

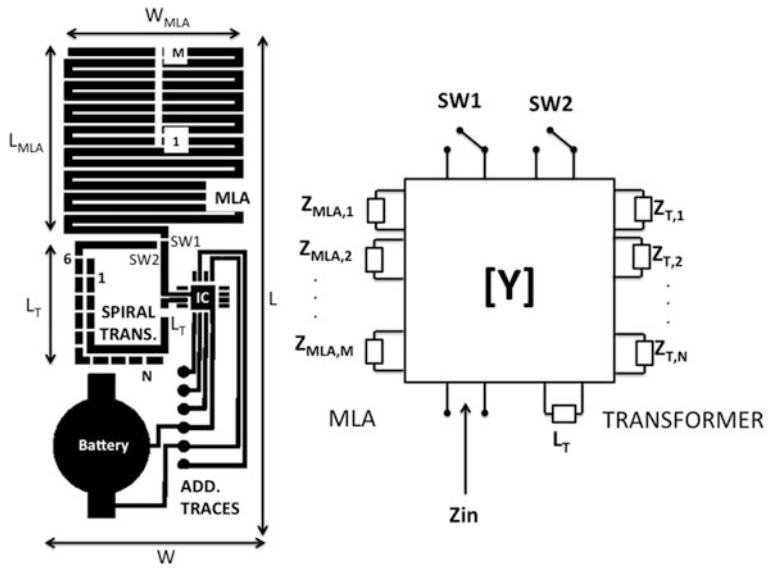

Fig. 2 (*Left*) Schematics of the customizable sensing breadboard architecture comprising the radiating meander line element (MLA), the spiral impedance transformer, and the expansion traces size in (mm): W = 28, L = 66, W_{MLA} = 24, L_{MLA} = 26, W_T = 12.5, L_T = 20 (mm); traces width: 1 mm (MLA and spiral) and 0.25 mm (sensor traces) (*Right*) A Multi-port model

microchip. Finally, depending on the status of the SW1/2 ports, the board can be used either as a tunable stand-alone RFID sensor board (SW1 closed and SW2 open) for application onto low permittivity and low losses materials, or as a basic module (SW1 open and SW2 closed) including the sensors, the chip, and the spiral transformer to be electromagnetically coupled to an external antenna, like a patch booster, for application over metals, or concrete walls.

Figure 3 shows a parametric exploration of the simulated realized gain [23] of the Radio-board in free space by acting either only on the trace gaps of the MLA or only on the spiral transformer ($Z_C = 31 - j330\ \Omega$). In the former case, replacing trace gaps with short circuits produces approximately a constant shift of about 10 MHz/gap. In the latter case, instead, the effect is less uniform but still suitable for a finer tuning of the impedance. By acting of the inductor it is finally possible to adjust the residual antenna reactance and hence to maximize the peak of the realized gain.

3.1 Application Examples and Performance

The potentiality of the proposed antenna architecture is here discussed by the help of two examples involving the full stand-alone breadboard radiating in air and the

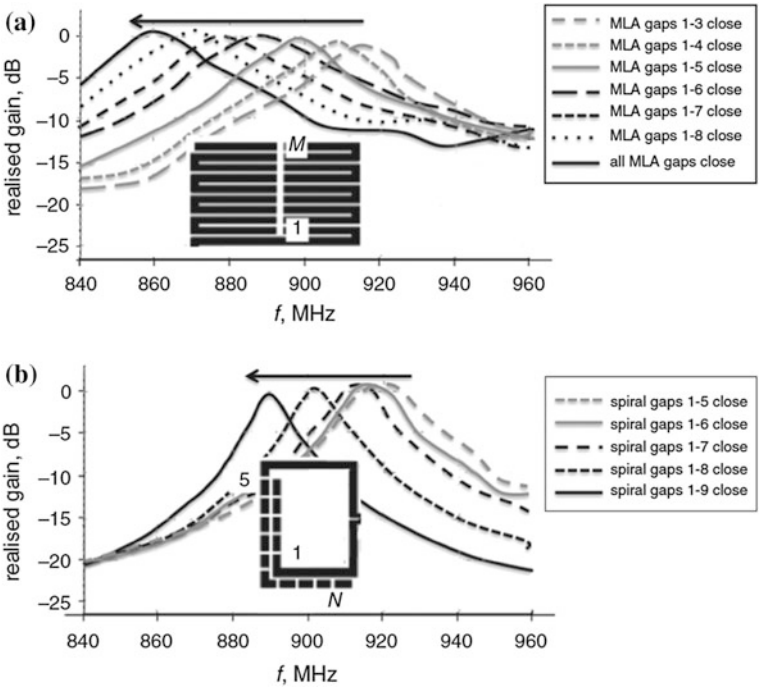

Fig. 3 Example of Radio-board tuning. Frequency shift of the broadside realized gain by connecting an increased number of the trace gaps of **a** the MLA and **b** of the spiral transformer length

same board placed onto an external patch booster for application over metals, or concrete walls.

The board prototype was fabricated by etching a 0.8-mm FR4 PCB. Flexible configurations on Kapton substrates can be manufactured as well.

In the first exercise, the SW1/2 gaps were configured so that the MLA is physically connected to the input section. Figure 4 shows the optimized realized gain close to 0 dB @ 868 MHz, having good agreement between measurements and simulations.

In the second example, the board was backed by a doubly folded patch [24], for improved operations over metal and lossy materials. In this case, the SW1-2 gaps were configured so that the MLA is physically disconnected from the input part. The spiral loop is hence inductively coupled with the radiating slot of the booster. The numerical multi-port characterization of the board over the patch included also an infinite ground plane where the tag is assumed to be attached on. As shown in Fig. 5, the device exhibits an appreciable realized gain (with/without battery) despite the close proximity of the ground plane. The presence of the battery yields worse performance in terms of realized gain, with respect to the battery-less

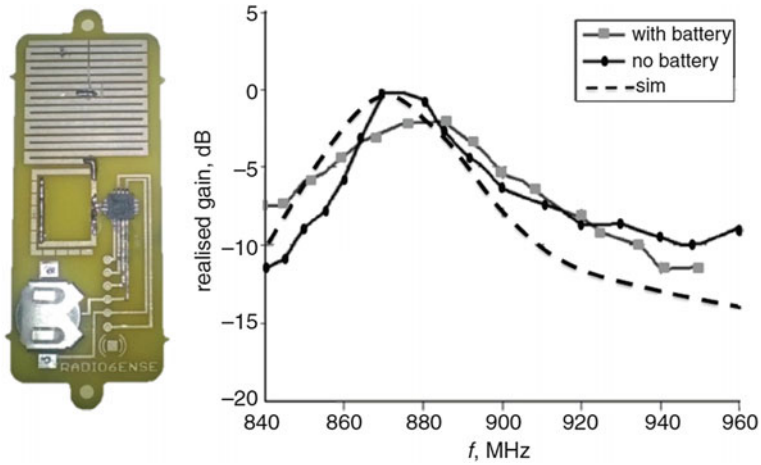

Fig. 4 Stand-alone RFID breadboard as optimized for working in air in UHF band. (*Left*) Prototype (optimized parameters $L_T = 47$ nH, $SW_1 =$ close, SW2 = open, $Z_{T1,10} = \infty$, $Z_{T11\text{-}15} = 0$, $Z_{MLA1} = 0$, $Z_{MLA2\text{-}6} = \infty$); (*Right*) Simulated and measured realized gain. (with/without battery)

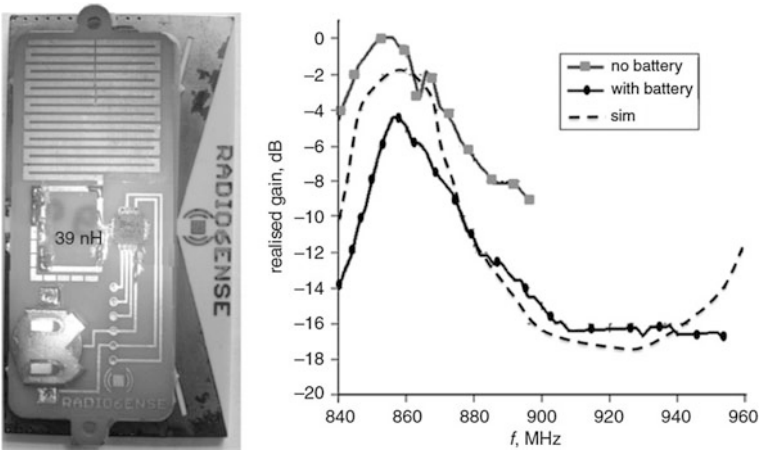

Fig. 5 Board backed by a patch booster (75 mm × 40 mm × 3 mm [24]) optimized for working on metal in UHF band. (*Left*) Prototype; (*Right*) Simulated and measured realized gain. (Optimized parameters $L_T = 39$ nH, $SW_1 =$ open, SW2 = close, $Z_{T1,3} = 0$, $Z_{T3,10} = \infty$, $Z_{T11,15} = 0$, $Z_{MLA1,6} = \infty$)

configuration probably due to parasitic currents, flowing into the IC through the battery traces, which are enhanced by the presence of surrounding metal layers.

The experimented read ranges of the board at 868 MHz, when the reader emits 3.2 W EIRP, are resumed in Table 1 for the two possible modes of operations.

Table 1 Read range of the Radio-board in various configurations

	In air (m)	On metal/concrete with patch booster (m)
Battery-less	2	2.3
Battery-assisted	6.5	7

The digital tag has to be considered as a real multi-channel sensor node, even if the local computation capability is rather modest and restricted to sensor handling and configuration. Each tag reproduces at the lowest level the concept of a modularity own to the architecture of the RFID-SN since the logic unit of the board can selectively activate one or more sensors according to the custom commands that are elaborated by the control software running on the central unit and sent to IC through the A_m reader antenna.

4 Control and Coordination Software

The RFID-SN is governed by a software module (hereafter denoted as *RadioScan*), written in C# .NET, which implements the remote control over the multi-level hierarchical architecture of the network in Fig. 1. The structure of network is declared by means of an XML file which is associated to *RadioScan*. This file can be modified at run-time for achieving a dynamic control over the system, for example, to switch from asynchronous to synchronous mode and to increase the sampling time within a specific zone if an anomalous event was suspected.

The Config file is conceived to implement the tree diagram in Fig. 1. *RadioScan* sets the operative configuration of the sensor network by (*i*) selecting the zones of the space to be controlled (by switching on and off the corresponding antenna of the reader); (*ii*) defining the specific interrogation modalities of the zones in terms of sampling rate, frequency, and power emitted by each reader antenna; (*iii*) selecting the things of each zone to be monitored and the relative attributes (by enabling/disabling tags and activating the embedded sensors). Figure 6 shows an example of Config file describing a network consisting of four reader antennas sourced at 868 MHz by 31 dBm power according to the sequential rotation {1, 2, 4, 3}. The spatial architecture is defined in the `<NetworkConfiguration>` section where each antenna of the reader is associated with the list of the tags to be interrogated within the corresponding zone of the space (`ZONE 1` "`name=`" `tag_list_A.1`). Those Radio-board that are equipped with multiple sensors ("`type`" = `Radio-Board`) require additional fields for the selection of the on-board sensors and the settings of the corresponding sensor front end, such as the type of the sensor, the voltage levels defining the dynamic range and the resolution of the sensors, and the parameters for data logging functionalities.

The output of the software are (*i*) a log file containing the current network configuration (active reader antennas and corresponding detected sensors) which is

```
<InterrogationSettings>
        <add key="FrequencyRegion" value="European" />
        <add key="Frequency(MHz)" value="868" />
        <add key="Power(dBm)" value="31" />
        <add key="ReaderAntennas" value="1243" />
        <add key="Mode" value="RealTime" />
        <add key="SamplingTime(sec)" value="1" />
        <add key ="TCP/IP_stream" value = "true"/>
</InterrogationSettings >

<NetworkConfiguration>

<ZONE1 name="tag_list_A.1">
   <tag name="T1" type="analog"></tag>
   <tag name="T2" type="RadioBoard

   Sensor Enabled ( RSSI="true" Temp="true"
                    Ext1="false" Ext2="true" Battery="false")

   Sensor Types    (Sensor1="-" Sensor2="Light" )

   Sensor Front-End Settings (V1="210" V2="310" ground="false"
                              Rref="8" current="31"....)

   DataLogger Settings (State="Start"  Interval="1"
                        Delay="6" Storage="normal"
                        Form="outoflimits"...)</tag>
   <tag name="T3" type="analog"></tag>
</ZONE1>
<ZONE2 name="tag_list_A.2">
   <tag name="T4" type="RadioBoard
   Sensor Enabled ( RSSI="true" Temp="true"
                    Ext1="false" Ext2="true" Battery="false")
</ZONE2>
```

Fig. 6 Example of Config file defining the configuration of the network

automatically saved at run-time when the software is started and (*ii*) a formatted string containing the time stamp and the (multi)sensor data of each tag at the current interrogation cycle. The string is both stored in a local text file and streamed over Ethernet port for remote processing.

In a possible complete architecture, these outputs could be accessed in real time by an upper decision layer (whose description is out of the scope of this paper) that implements detection algorithms [15] and, if needed, sends back the control software some input command to consequently update the network. Provided that each sensing node is reconfigurable via software (similarly to [25]), the RFID sensor

network as a whole is definitely provided with the capability of self-configuration, which is a key requirement for IOT platforms. Moreover, direct tag-to-tag communication could be in principle possible by means of a pure backscattering modality, as demonstrated in [26, 27], thus fostering in the future an autonomous data exchange among nodes like in the more complex M2M devices.

5 Application to the Physical Security in Electric Plants

A valuable application of the described RFID-SN is the protection of critical infrastructures against cyber and physical attacks. Security, in its meaning of defense against cyber-attacks and threats, has been traditionally considered not to be a prominent issue for critical infrastructures such as pipelines, smart grids, and power plants, even though recent critical events demonstrated how deep is the relationship between cyber and physical worlds [28].

In the framework of European Horizon 2020, the project *Security in trusted SCADA and smart-grids* (SCISSORS, www.scissor-project.com) addresses the design of a holistic, multi-layered, security monitoring and mitigation framework, spanning all the issues related to the deployment of a critical infrastructure such as the control (*i*) of the environment, (*ii*) of the network traffic, (*iii*) of the hardware and software system components, (*iv*) of the people accessing the infrastructure, and (*v*) the independent monitoring of the control process itself. The environmental sensing and monitoring layer of SCISSORS are demanded to the proposed RFID-SN.

A first version of the RFID-SN was deployed and preliminary tested within the electrical transformer secondary substation of the University of Rome Tor Vergata (Fig. 7a). Similarly to other smart grid substations, the bunker room is located in the basement of the building and it is a restricted access area. The room contains two working transformers, several control cabinets, a couple of electric generators, and many high-power cable bundles.

5.1 Events to Be Detected

The events to be detected were the authorized/un-authorized accesses to the cabin, possible tampering of the machineries, humidity changes and flooding of sensitive areas, and power overload of wire harnesses. At this purpose, the Radio-board were equipped with humidity and light sensors and with high-temperature external probes. Analog tags were used as well to detect intrusions and mechanical changes of the room. Each event has been detected through the processing of a single attribute of one thing inside the space or through a combination of them (Table 2).

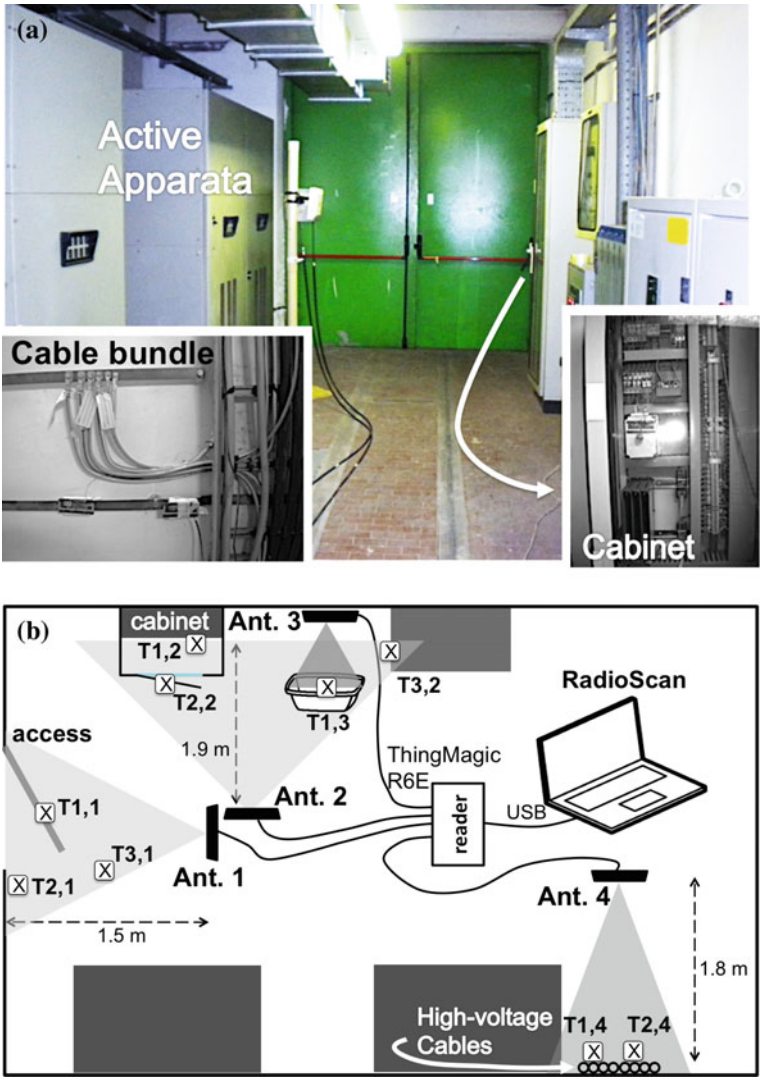

Fig. 7 **a** Electrical transformer secondary substation of the University of Rome "Tor Vergata." **b** Schematic representation of the deployed RFID-SN. The *gray* triangles highlight the read region (zone) of each antenna

5.2 *Network Configuration*

The configuration of the RFID-SN is sketched in Fig. 7b. A 1 W long-range RFID reader (ThingMagic M6E [29]) connected to four antennas (circularly and linearly polarized patches) was used to monitor four different zones ($M = 4$) in the cabin: access (A_1); cabinets and energy meters (A_2); flooding sensitive area (A_3);

Table 2 Events to be detected by the RFID-SN inside the electrical cabin and corresponding attributes to be measured

Event	Attributes
Authorized/un-authorized access	RSSI from tags installed onto the access door
	ID code from wearable tags
	Light on/off
Flooding	RSSI from tags placed over the floor
	Ambient humidity
Harness overload	Temperature variation of cables
	And bundles of cables
	(High and low range)
Manumission of cabinets	RSSI from tags placed onto the cabinet window
	Temperature variation inside the cabin

Table 3 Network configuration

Antennas (zones and events)	Tags	Sensor channel
A_1: Zone 1 (Authorized/un-authorized access)	$T_{1,1}$—W-tag	$S_{1,1,1}$: RSSI
	$T_{2,1}$—Radio-board	$S_{1,2,1}$: RSSI
		$S_{2,2,1}$: Light (S133-14 p.diode)
	$T_{3,1}$—W-tag	$S_{1,3,1}$: RSSI
A_2: Zone 2 (Manumission of cabinets and flooding)	$T_{1,2}$—Radio-board	$S_{1,1,2}$: Temp (internal sensor)
	$T_{2,2}$—W-tag	$S_{1,2,2}$: RSSI
	$T_{3,2}$—Radio-board	$S_{1,3,2}$: RH% (HCZ-D5 sensor)
A_3 : Zone 3 (Flooding)	$T_{1,3}$—W-tag	$S_{1,1,3}$: RSSI
A_4 : Zone 4 (Harness overload)	$T_{1,4}$—Radio-board	$S_{1,1,4}$: Temp (PT1000)
	$T_{2,4}$—Radio-board	$S_{1,2,4}$: Temp (internal sensor)

high-power cable bundles (A_4). The set of RFID tag (Table 3) comprised five Radio-board, embedding heterogeneous sensors, and four analog sensor tags [22], hereafter referred to as W-tags. The latter are platform-tolerant tag that can be used as wearable badge for automatic access identification of operators, as RSSI markers over doors and cabinet windows to detect a possible interaction with a persons and even deployed over the ground and wall for flooding control. The overall number of channels of the network was $C = 10$.

Measurements were carried out in both rest (stationary) and operative (dynamic) conditions. The critical events listed in Table 2 were emulated several times by the help of volunteers.

5.3 Flooding and Humidity

Flooding is a recurring event in smart grids, especially when the infrastructure comprises several underground cabins. In the case of partial flooding, the signals

backscattered by the W-tags placed on the critical regions of the floor are strongly perturbed. Eventually, when a tag is sensibly submerged by water, it becomes undetectable by the reader due to the abrupt change of the electromagnetic parameters of the surrounding medium which detunes the antenna. In addition to this threshold detection, the Radio-board with relative humidity sensors can be used to detect abnormal variation of the environmental relative humidity (%RH) which can be related to flooding.

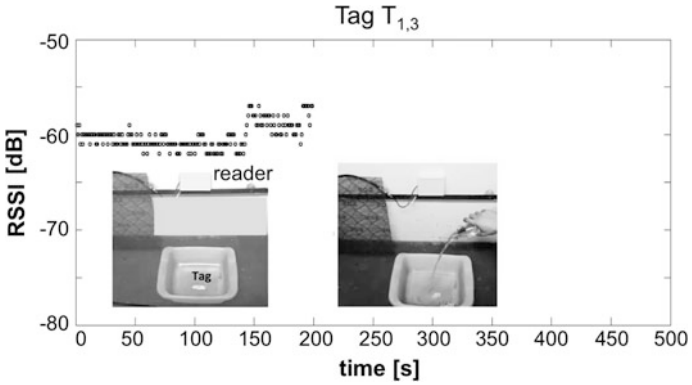

Fig. 8 Backscattered power from the analog tag $T_{1,3}$ during the simulation of a flooding event

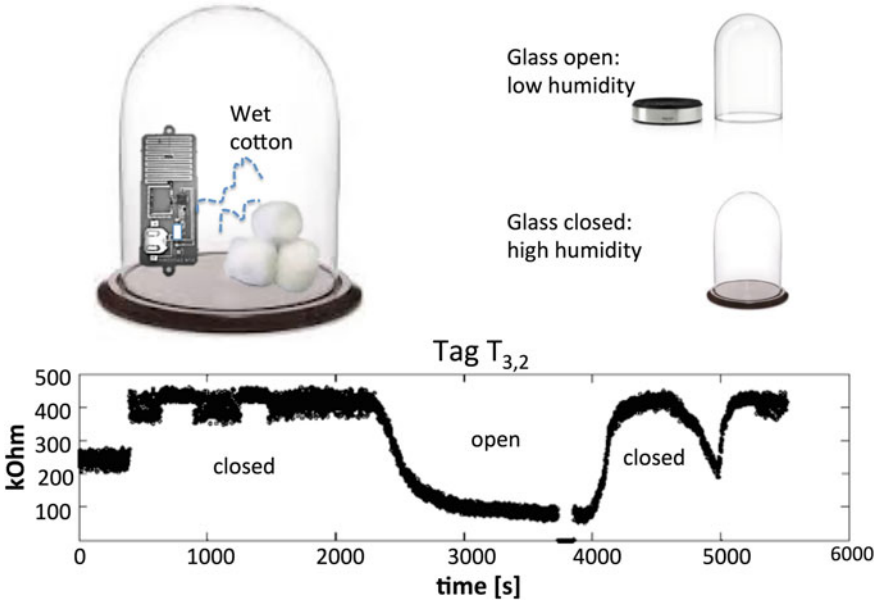

Fig. 9 Impedance of the humidity sensor connected to the Radio-board $T_{3,2}$ measured during cyclic humidity variations induced by opening/closing the glass bell

The flooding event was emulated (Fig. 8) by filling a plastic basin with water. A W-tag ($T_{1,3}$) was placed on the bottom of the basin. In normal conditions (absence of water), the tag was detected by the antenna A_3 with a stable level of RSSI ($S_{1,1,3}$). Then, as soon as it was covered by the liquid, it was severely mismatched and became unreadable by the antenna.

The humidity change was instead simulated by placing the Radio-board $T_{3,2}$ equipped with the humidity sensor into a glass bell together with a piece of wet cotton. When closing the glass, the internal relative humidity gradually increased up to saturation. Then, it rapidly came back to the initial ambient condition as soon as the top was removed. An example with some open/close cycles is reported in Fig. 9 showing the impedance of the sensor ($S_{3,2}$) which is inversely proportional to the humidity level detected by the antenna A_2.

5.4 Harness Overloading

An anomalous working load of the cabin transformer could produce high currents over the distribution cables. Radio-board including internal temperature sensors and/or connected to external high-temperature probes can be placed over the cable harness to monitor their surface temperature which is related to the currents flowing into the cables themselves. Those sensors can be also used to obtain indirect information about the aging of the dielectric insulators of the harness.

In the present experiment, some events of power overloading were reproduced by manually warming up two harnesses inside the cabin by using a heat gun. Figure 10 shows the temperatures ($S_{1,1,4}$ and $S_{1,2,4}$) detected by the two Radio-board ($T_{1,4}$ and $T_{2,4}$) attached over the two considered cables running along the perimeter wall of the cabin, the first one integrating a platinum thermo-resistance (PT1000) whose extremal sensitive part was at direct contact with electric cables and the second one detecting the temperature by its internal sensor.

5.5 Cabin Access and Manumission

In normal conditions, the door of the cabin is closed and the internal scenario is completely dark: Accordingly, a low-light signal can be collected by the light sensor of a Radio-board $T_{2,1}$ placed in proximity of the access doors. If somebody opens/tampers the door and gets inside the cabin, the system will detect an increase of the light (coming from outside or emitted by a torch or by any other light source), as well as a distortion of the RF fingerprint of the cabin due to the presence of moving people which perturbs the electromagnetic field produced by the reader antennas. Finally, if the subject is provided with an RFID badge, the passive

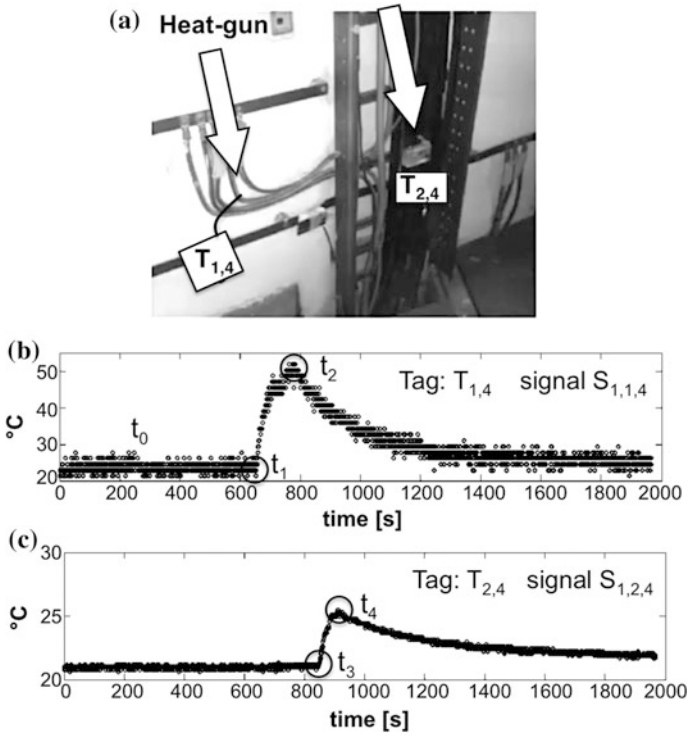

Fig. 10 Power overloading of two cables **a** equipped with Radio-board $T_{2,4}$ (internal temperature sensor) and $T_{1,4}$ (external PT1000 temperature sensor). **b** and **c** Temperature recording during an artificial warming by a heat gun in the time intervals (t_1, t_2) and (t_3, t_4) for the two cables, respectively

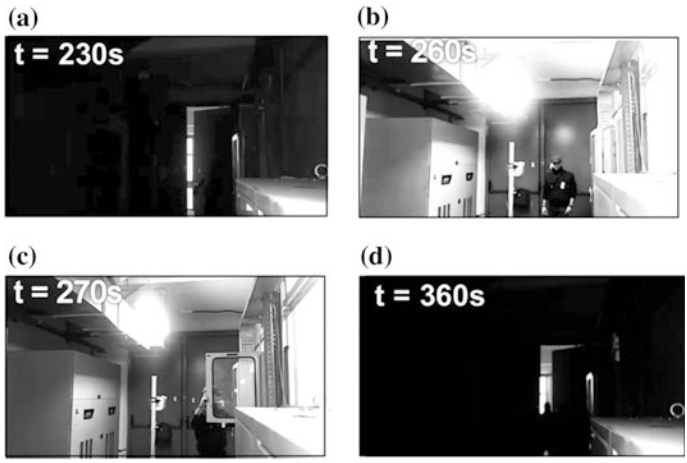

Fig. 11 Screenshots from the authorized access to the electric cabin and interaction with an equipment. **a** door opening; **b** light on and RF badge detection; **c** cabinet opening; **d** light off, badge recognized, door open and closed

network is able to verify his identity and his right to access the cabin, for instance, in case he is maintenance personnel.

5.5.1 Authorized Access

Figure 12 shows a subset of the signals recorded by the sensor network when an authorized technician came into the cabin for ordinary maintenance (screenshots in Fig. 11). In the initial reference condition, the light in the room was off ($S_{2,2,1}$ signal of Radio-board $T_{2,1}$) and the W-tags for the access control ($T_{1,1}$) and cabinet opening ($T_{2,2}$ returned stable RSSI values. No authorized people were detected inside the ambient (null signal from wearable tag $T_{3,1}$). The evident drop of the RSSI collected by sensor $T_{1,1}$ reveals the opening of access door.

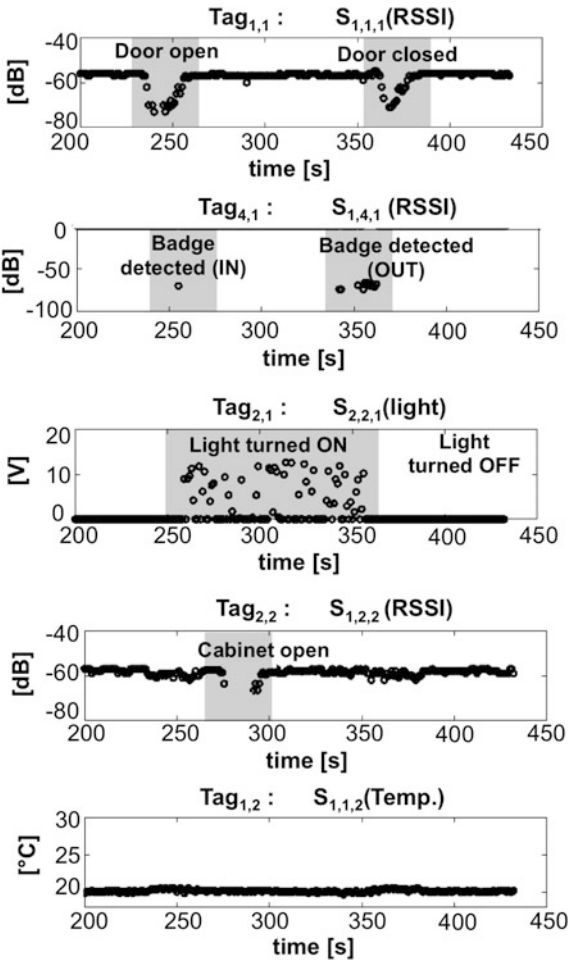

Fig. 12 Subset of signals collected by the RFID-SN in case of authorized access to the electric cabinet as sketched in Fig. 11

Immediately after, the person entering the room was automatically recognized by the system and classified as "authorized person" through his badge identification ($S_{1,3,1} \neq 0$). The maintenance technician turned on the light ($S_{2,2,1}$ switches to ON state) and opened the electrical cabinet (sensor on the door cabinet $T_{2,2}$ was no longer read in the open position) to perform ordinary operations, with no modification of the equipment temperature. Finally, the technician approached the exit door and turned off the light; the system detected again his badge and recorded the exit (Fig. 12).

5.5.2 Un-authorized Access and Attack

In a second experiment, the person entering the room was an intruder, i.e. he did not wear any RF badge, and he walked in the dark by using a torch, opened the windows of the cabinet, and artificially increased the temperature of an internal equipment to emulate a tampering event (Fig. 13). The multi-parameter recording by the RFID-SN is shown in Fig. 14 and could be interpreted, a posteriori, as follows: when the person came inside, the system recognized the door opening through a perturbation of the RSSI from the tag $T_{1,1}$. Since no pre-registered ID

Fig. 13 Screenshots from the un-authorized access to the electric cabin with tampering. **a** door open; **b** torch pointing toward the light sensor; **c** cabinet opening and tampering; **d** attacker going outside

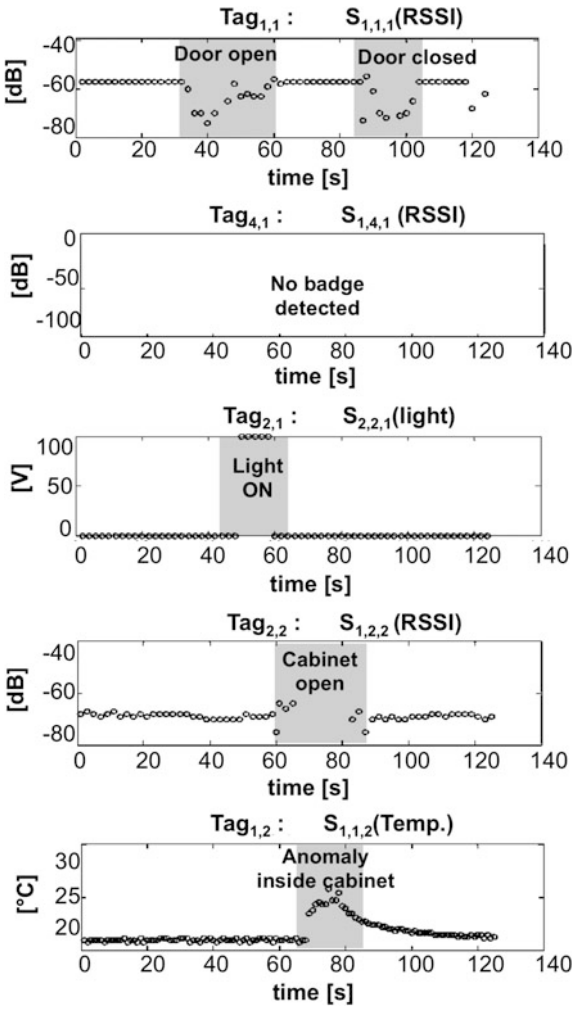

Fig. 14 RFID-SN measurements in case of an un-authorized access to the electric cabinet producing a thermal anomaly

code was detected, the person could be classified as an intruder. Then, a variation in the light level was revealed by the sensor $T_{2,1}$ for a short period suggesting that the intruder turned on the light just for a few seconds or used a torch. The sensor $T_{2,2}$ detected an interaction with the cabinet, and during this time interval, the internal temperature of the cabinet abnormally increased (sensor $S_{1,1,2}$ of $T_{1,2}$). This event could be considered as a warning of a potential power overload of some internal circuitry produced by a possible manumission. The sensor $T_{1,1}$ at the main door detected again an interaction when the attacker came out the cabin.

6 Summary and Conclusion

The proposed monitoring platform exploits the combined processing of analog and digital signals to detect anomalous event.

The hierarchical architecture enables a flexible and easily reconfigurable monitoring of a complex space as well as it permits to capture the user's interaction with specific nearby objects.

A custom transponder supporting multi-purpose sensing and radiation modes was specifically designed to provide the same layout with post-fabrication configurability by manually soldering tuning elements and wirelessly programming the IC logical unit.

An important issue is how the system complexity scales with respect to the size of the space under observation. The number of interrogating antennas, and hence of the cables, increases only linearly with the volume of the space to monitor, while it is independent of the number of things in each zone. Most of industrial-oriented RFID readers are provided with multiple antenna ports (up to four, as in the given example), and an even larger number of antennas could be addressed by using an electronic-controlled switch so that large spaces could be monitored with a unique centralized node.

The deployment of the network in the experiment required a try and error effort to identify the best position of the reader antennas so that all the tags were correctly read by the network. This procedure could, however, be driven by electromagnetic modeling, which includes the scattering of the nearby environment, and by evolutive optimization algorithms as in [30] for automatic antenna placement.

The proposed solution could find successful application to the empowering of SCADA (supervisory control and data acquisition) and video surveillance systems which are currently used in industrial infrastructures, thus producing both complementary and backup data.

In the framework of the SCISSOR project, a realistic test bed is currently running in an operational smart grid in Favignana Island (Italy) where the whole RFID-SN was successfully and permanently installed in September 2016. Figure 15 shows a snapshot of the dashboard that is remotely accessible from anywhere for the real-time visualization of the acquired data (see https://www.youtube.com/channel/UCkJHWrnq9bBJhUyQrJfwBlA for demo video (Fig. 15).

Furthermore, unlike the more conventional wired/wireless equipments for environmental monitoring and access control that sensibly suffer from the lack of a unique infrastructure [31], the proposed sensor network relays onto a well widespread and standardized protocol and on a growing set of COTS devices with clear benefits for the interoperability among services and the integration with existing industrial infrastructures. The system is hence suitable to be easily tailored and customized for combined access control, environmental as well as thing-level monitoring with minimal installation, maintenance, and dismantling times and costs (see Table 4 for a qualitative comparison).

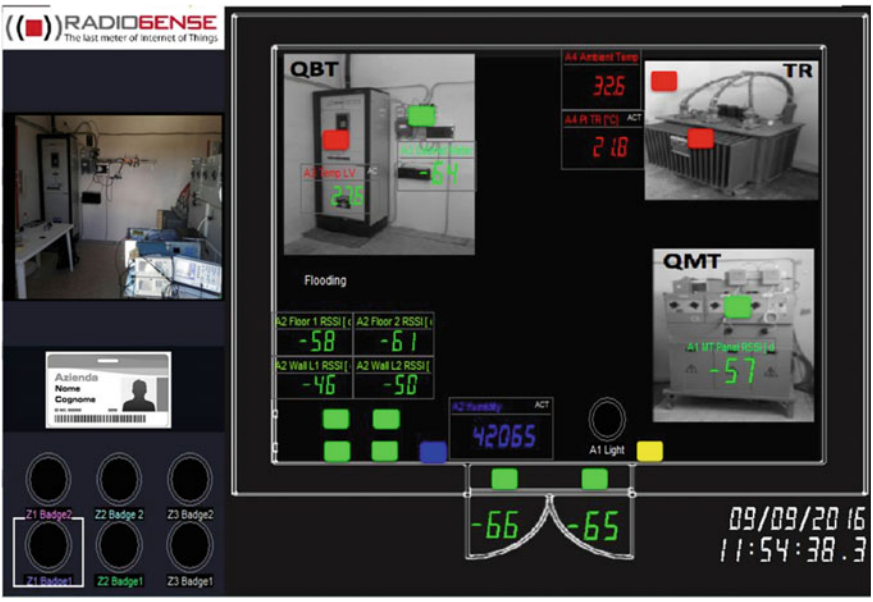

Fig. 15 Dashboard for the remote control of the RFID-SN installed within a smart grid in Favignana Island

Table 4 Industrial IoT Technologies

		RFID	Wired	Wireless
		Sensors	Sensors	Sensors
Costs	Installation	LOW	HIGH	LOW
	Maintenance	LOW	LOW	HIGH
	Power	LOW	LOW	HIGH
	Hardware	LOW	HIGH	HIGH
Benefits	Security	HIGH	HIGH	MEDIUM
	Scalability	HIGH	LOW	HIGH
	Reconfigurability			
	Interoperability	HIGH	LOW	LOW
	Sensor accuracy	MEDIUM	HIGH	HIGH

Finally, thanks to their local poor or even null computational capabilities, the RFID sensor nodes are expected not to be exposed to external cyber-attacks so that the whole security care could be entirely devoted to the reader node only.

Acknowledgements The work was supported by SCISSOR ICT project no. 644425, funded by the European Commissions Information and Communication Technology H2020 Framework Program.

References

1. Industrial internet of things: Unleashing the potential of connected products and services. World Econ. Forum Tech. Rep. (2015)
2. E. Brynjolfsson, A. McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies (W.W. Norton and Company, 2014)
3. C. Occhiuzzi, S. Caizzone, G. Marrocco, Passive uhf rfid antennas for sensing applications: Principles, methods, and classifications. Antennas Propag. Mag. IEEE **55**(6), 14–34 (2013)
4. W. Dargie, C. Poellabauer, Fundamentals of wireless sensor networks: theory and practice (Wiley, 2010)
5. G. Marrocco. et al., Rfid iot: a synergic pair. IEEE RFID Virtual J. **8** (2015)
6. M.A. Razzaque, M. Milojevic-Jevric, A. Palade, S. Clarke, Middleware for internet of things: a survey. IEEE Internet Things J. **3**(1), 70–95 (2016)
7. L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L. Tarricone, An iot-aware architecture for smart healthcare systems. IEEE Internet Things J. **2** (6), 515–526 (2015)
8. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, Rfid technology for iot-based personal healthcare in smart spaces. IEEE Internet Things J. **1**(2), 144–152 (2014)
9. C. Occhiuzzi, G. Marrocco, Precision and accuracy in uhf-rfid power measurements for passive sensing. IEEE Sens. J. (99), 1–1 (2016)
10. SL900A, http://ams.com/eng/Products/UHFRFID/UHF-Interface-and-Sensor-Tag/SL900A
11. L. Catarinucci, R. Colella, L. Tarricone, A cost-effective uhf rfid tag for transmission of generic sensor data in wireless sensor networks. IEEE Trans. Microw. Theory Tech. **57**(5), 1291–1296 (2009)
12. A. Sample, D. Yeager, P. Powledge, J. Smith, Design of a passively-powered, programmable sensing platform for uhf rfid systems, in IEEE International Conference on RFID, Mar 2007, pp. 149–156
13. EM 4325, www.emmicroelectronic.com
14. http://www.farsens.com
15. C. Occhiuzzi, C. Vallese, S. Amendola, S. Manzari, G. Marrocco, Night-care: A passive rfid system for remote monitoring and control of overnight living environment. Procedia Comput. Sci. **32**, 190–197 (2014)
16. M. Buettner, R. Prasad, M. Philipose, D. Wetherall, Recognizing daily activities with rfid-based sensors, in Proceedings of the 11th International Conference on Ubiquitous Computing, ser. UbiComp '09. (ACM, New York, NY, USA, 2009), pp. 51–60. doi:10.1145/1620545.1620553
17. A. Costanzo, D. Masotti, T. Ussmueller, R. Weigel, Tag, you're it: Ranging and finding via rfid technology. IEEE Microw. Mag. **14**(5), 36–46 (2013)
18. W. Sriborrirux, P. Danklang, N. Indra-Payoong, The design of rfid sensor network for bus fleet monitoring, in 8th International Conference on ITS Telecommunications, 2008. ITST 2008, Oct. 2008, pp. 103–107
19. M. Sole, C. Musu, F. Boi, D. Giusto, V. Popescu, Rfid sensor network for workplace safety management, in 2013 IEEE 18th Conference on Emerging Technologies Factory Automation (ETFA), Sept 2013, pp. 1–4
20. G. Marrocco, E. Di Giampaolo, R. Aliberti, Estimation of uhf rfid reading regions in real environments. Antennas Propag. Mag. IEEE **51**(6), 44–57 (2009)
21. S. Amendola, L. Bianchi, G. Marrocco, Movement detection of human body segments: passive radio-frequency identification and machine-learning technologies. IEEE Antennas Propag. Mag. **57**(3), 23–37 (2015)
22. S. Manzari, S. Pettinari, G. Marrocco, Miniaturized wearable uhf rfid tag with tuning capability. Electron. Lett. **48**(21), 1325–1326 (2012)

23. F. Amato, G. Marrocco, *Self-Sensing Passive RFID: from Theory to Tag Design—an Experimentation* (European Microwave Conference, Roma, Italy, 2009)
24. S. Manzari, G. Marrocco, Modeling and applications of a chemical-loaded UHF RFID sensing antenna with tuning capability. IEEE Trans. Antennas Propag. **62**(1), 94–101 (2014)
25. M.S. Khan, M.S. Islam, H. Deng, Design of a reconfigurable rfid sensing tag as a generic sensing platform toward the future internet of things. IEEE Internet Things J. **1**(4), 300–310 (2014)
26. G. Marrocco, S. Caizzone, Electromagnetic models for passive tag-to-tag communications. IEEE Trans. Antennas Propag. **60**(11), 5381–5389 (2012)
27. P.V. Nikitin, S. Ramamurthy, R. Martinez, K.V.S. Rao, Passive tag-to-tag communication, in 2012 IEEE International Conference on RFID (RFID), Apr 2012, pp. 177–184
28. M.B. Kelley, The stuxnet attack on iran's nuclear plant was 'far more dangerous' than previously thought, Businessinsider.com. Tech. Rep. (2013)
29. http://www.thingmagic.com/index.php/fixed-rfidreaders/mercury6
30. E.D. Giampaolo, F. Fornì, G. Marrocco, RFid-network planning by particle swarm optimization. Aces J. **25**(3), pp. 263–272 (2010)
31. O. Monnier, E. Zigman, A. Hammer, Understanding wireless connectivity in the industrial iot, Texas Instruments, Tech. Rep. (2015)