Industrial RFID Sensing Networks for Critical Infrastructure Security

C. Occhiuzzi [1], S. Amendola [1,2], S. Manzari [1] and G. Marrocco [1,2]

[1]RADIO6ENSE,
[2]Pervasive Electromagnetics Lab,
University of Roma Tor Vergata, Via del Politecnico, 1, 00133, Roma, Italy

***Abstract*—The Radiofrequency Identification of the emerging Industrial Internet of Things is here applied to the low-level monitoring of critical infrastructures to detect early attempts of physical and cyber attacks. The proposed RFID sensor network, developed within the H2020 project SCISSORS, includes a new family of multi-purpose wireless boards, usable in both battery-less and battery-assisted modes, a multi-antenna reader unit and a multi-level command and control software capable to enforce a hierarchical monitoring of complex environments.**

I. Introduction

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 if recent critical events demonstrated how deep is the relationship between cyber and physical worlds [1]. The control of physical equipment or processes generally relies on traditional supervisory control and data acquisition (SCADA) systems which consists of several software and fixed hardware components dispersed across multiple networks within an organization. A simplified data flow of SCADA architecture starts from the sensors in the Remote Terminal Units (RTU) collecting measurements, and sending them to a supervisory system, which acquires and elaborates the data of the process and may additionally react with alarms and commands. An attack on such a system can produce physical effects/damages making a conventional SCADA system a particularly attracting target for attackers. Therefore, new paradigms for monitoring, detection and reaction must be envisaged and deployed, with innovative features such as the scalability, the pervasivity, the modularity and the flexibility.

Recent advantages in the area of Industrial Internet of Things offer several opportunities in redesigning SCADA systems, especially regarding the wireless sensors and the monitoring layer. 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 an holistic, multi-layered, security monitoring and mitigation framework, spanning all the issues related to a critical infrastructure deployment such as i) the control 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. Figure 1 provides a snapshot of the overall SCISSOR which comprises four layers, from the monitoring stage up to the human machine interface.

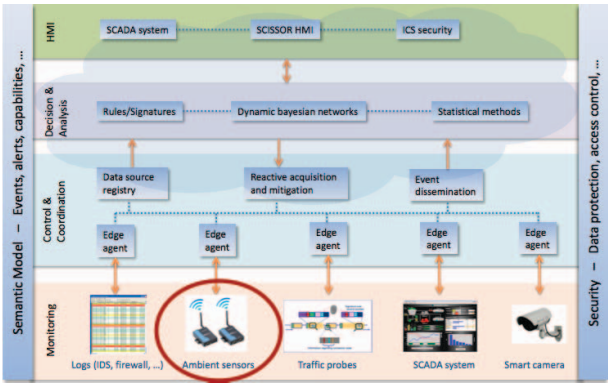

Fig. 1. SCISSOR's system layers and functionalities

The environmental sensing and monitoring layer of SCISSORS is demanded to an innovative class of passive wireless sensors networks, entirely based on the Radiofrequency Identification (RFID) technology. Such sensors can be quickly and massively integrated in the environment thanks to their flexible, pervasive, and ultra-low cost nature, thus sensibly empowering the monitoring capabilities of the network. Although many examples of RFID based sensors have been recently proposed by both Academia and Industry [2], 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 [3], [4], ranging and localization of people and objects [5], bus fleet monitoring and scheduling [6] and workplace safety management [7].

This contribution introduces for the first time the complete design and implementation of an *RFID industrial sensor network* starting from the definition of the architecture, the multi-purpose sensor boards, the development of the control software up to to the deployment and test of the network in a real environment.

II. RFID Sensor Network Architecture

The RFID Sensor Network (RFID-SN) for industrial ambient monitoring comprises a set of sensing RFID tags, with or without a local battery, that are placed over the machineries

to be monitored and in the nearby environment, and a limited number of reading nodes (readers) that scan the space according to either a fixed or a mobile network topology as well as by a combination of both. The network is suitable to perform some local data processing (filtering, thresholding) as well as to bidirectionally interact with the higher layers of the SCISSORS architecture e.g. to accept configurations and queries and to flush data. In particular, both synchronous and asynchronous interaction patterns can be used. In the first case a standard command-reply strategy is implemented, while in the second case the transmission of commands and the replies are completely independent.

The RFID-SN is conceived to complement existing wired diagnostic networks and to overlap them at the purpose to increase the pervasiveness and the robustness of the ambient monitoring level. In particular, the system is intended to detect abnormal power overloads (temperature spikes), to collect environmental parameters such as temperature, humidity and occasional flooding, as well as to reveal un-authorized access to critical areas and record the human interactions with the nearby equipments and possible tampering actions.

A possible arrangement (Fig. 2) of the RFID-SN inside an electrical cabin includes:

- a fixed reader unit connected to the communication network hub;
- one or more antennas connected to the reader and properly distributed to achieve a uniform radio coverage of the environment;
- perimetric RFID tags placed on the floor, close to the access point (door, windows) and in specific locations of the cabin subjected to flooding;
- one or more radiofrequency boards based on RFID technology (and described in the next paragraph) equipped with
  - a light sensor for placement in regions that are generally shadowed;
  - humidity and temperature sensors for placement in regions with controlled conditions (e.g. cabinet provided with cooling fans);
  - dedicated external high-temperature probes (thermoresistance or thermistor) for placement on cable harness for monitoring their surface temperature as an indirect indicator of power overload.

III. RFID Sensor Boards

The environmental RFID sensors, hereafter denoted as *Radio-boards*, are based on a new family of RFID transponders [8] that, beside the pure identification features, provide a native integrated electronics for sensing activities. 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 with a programmable dynamic range and resolution in the interval -40/150°C. This IC can be used in a fully passive mode, e.g. the energy required for activation and actions is scavenged from the electromagnetic waves

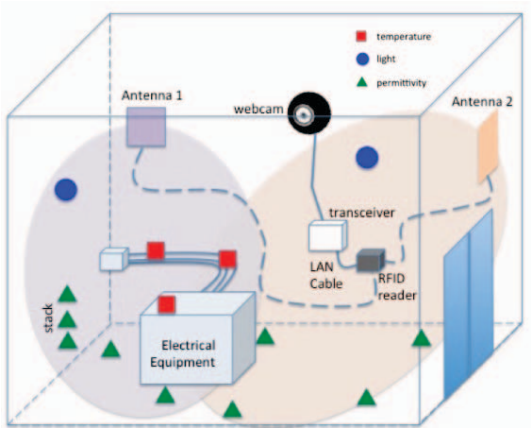

Fig. 2. Possible implementation of the RFID Sensor Network inside a distribution cabin of a smart grid with indication of the sensor types for i) access detection (triangles and circles) and for ii) flooding monitoring (triangles and stack of triangles) as well as for iii) possible power overload (squares) of the equipment and of their cable harness. Multiples reader antennas permit to achieve a uniform RF coverage (shadowed ellipses) of the cabinet.

emitted by the remote interrogator, or in battery-assisted mode, e.g. a local battery may provide additional energy for improved read range and, above all, to perform periodic measurement even in absence of the reader (data-logging mode).

The design of the Radio-board is oriented to pursue the maximum flexibility in measurement and installation in complex environments. The board will hence provide the following features:

a) low-profile and small-size: a credit-like card, at most;

b) compatible with placement over metals, plastics, concrete as well as close to liquids;

c) suitable to operate in both fully battery-less mode for instantaneous reading (synchronous) and in battery-assisted mode for data logging in absence of the reader (asynchronous mode);

d) capable to host a variable set of sensors for multi-parameter monitoring.

The Radio-board will be manufactured as a multi-layer printed-circuit board (PCB). The lower metallization (ground plane) provides a partial electromagnetic isolation from the object where the sensor will be attached on, thus permitting to use the same device in different applications. The upper metallization is properly shaped to achieve the desired radiation properties. This layer will moreover host the expansion slots for connecting external sensors and an optional battery for data-logging mode. Interconnection between the two layers, at the purpose of antenna miniaturization and frequency tuning in European or US band, are achieved by via-holes technology.

IV. Control & Command Software

The RFID-SN is governed by a software module written in C# (hereafter denoted as *RadioScan*) that enables the remote and multi-level control of the readers and the sensors, providing the SCISSOR system with the possibility of dynamically customizing the monitoring activity in terms of:

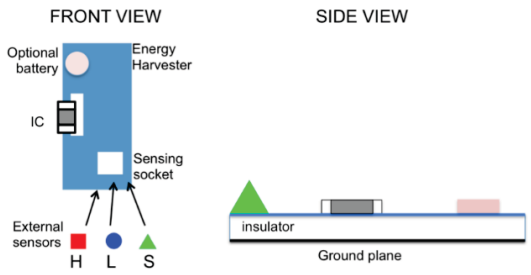

Fig. 3. Top) Schematic of the Radio-board architecture comprising a COTS integrated circuit for identification, modulation and analog to digital conversions, a set of external sensor and an optional battery for data-logging capability

- area (which is the part of the infrastructure to be deeply monitored?),
- mode of operation (which are the environmental parameters to be measured in that area?)
- operability (is it possible to increase/decrease the monitoring frequency or the power level ?),

The RadioScan is organized as a multi-level architecture suitable to comply with the hierarchical configuration of a typical smart grid (Figure 4) composed by a number of cabins located in different areas of the city/region. Each cabin consists of different monitoring zones, which are scanned by one of the antennas connected to the reader. Many Radio-boards equipped with various sensors can be deployed within each zone to create the most suitable sensing network. The RadioScan is able to dynamically modify the operative configuration of the sensor network and in particular to:

- select the cabin where it is necessary to focus the monitoring;
- select/enable/disable the cabin zones by switching on and off the related reader antenna;
- select/enable/disable the sensing boards and the connected sensors;
- modify the interrogation modalities in terms of sampling rate and power emitted by each reader antenna.

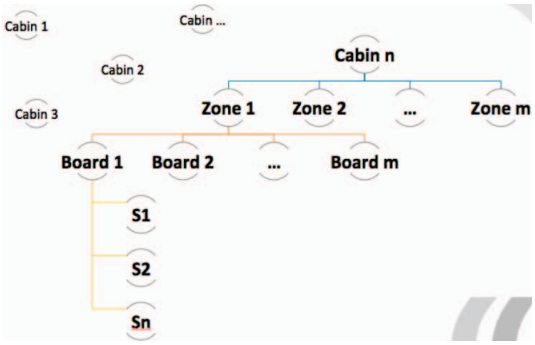

Fig. 4. Schematic multi-level representation of the physical monitoring of real world smart grid

V. A First Test-bed

An early version of the complete RFID-SN was deployed and tested within the Electrical transformer secondary substation of the University of Rome "Tor Vergata" (Fig.5 a). Similarly to other smart-grid substations, the bunker room is located in the basement of the building and has a restricted access. The room contains two working transformers, several control cabinets, a couple of electric generators and different cable harnesses.

The configuration of the RFID-SN is sketched in Fig.5 (b). A 3.2W long range RFID reader connected to four surveillance antennas was used to monitor four different zones in the cabin: Cabinets and meters (Antenna 1); Access (Antenna 2); Flooding sensitive area (Antenna 3); Cable harness (Antenna 4).

Ten Radio-boards with different sensors were properly dispersed into the environment. The following parameters were monitored:

- Received Signal Strength Indicator (RSSI) to be used to extract motion/position and flooding sensing parameter (boards F3, F8, A2, F1);
- Environmental temperature T by means of the semiconductor sensor embedded into the radio-board microchip (boards 22,44,110);
- Ambient light by means of an external photodiode with binary response (ON-OFF sensor, boards 66, 44)
- Environment relative humidity RH by means of an external sensor (boards 66)
- High temperatures by means of an external Platinum Thermo-resistance PT1000 for cable harness integrity (boards 33, 55);

Finally, a wearable RFID passive tag [10] was integrated in the badge of the operator for automatic access identification.

Measurements were carried out in both rest (stationary) and operative conditions. Critical events, such as the access of authorized/non-authorized persons, the local flooding and the increase of cable temperature were emulated several times by the help of volunteers at he purpose to produce a rich dataset useful for both system evaluation and for a first application of the SCISSOR classification and recognition algorithms.

Fig.6 shows a subset of the signals recorded by the sensors network when an authorized access to the cabin for ordinary maintenance occurred. In the initial reference condition, the light in the room is off (sensors 44) and the sensors for the access control (F1) and cabinet opening (F3) show stable RSSI values. No people are detected inside the ambient (null signal from F5). The evident drop in the value of the RSSI collected from sensor F1 reveals the opening of access door. Immediately after, the person entering the room is automatically recognized by the system as an authorized personnel through his badge identification (F5). The maintenance technician turns on the light (sensor 44 switches to ON state) and opens the electrical cabinet (sensor on the door F3 is no longer read in the open position) to perform ordinary operations. Finally, he approaches the exit door and turns-off the light; the system

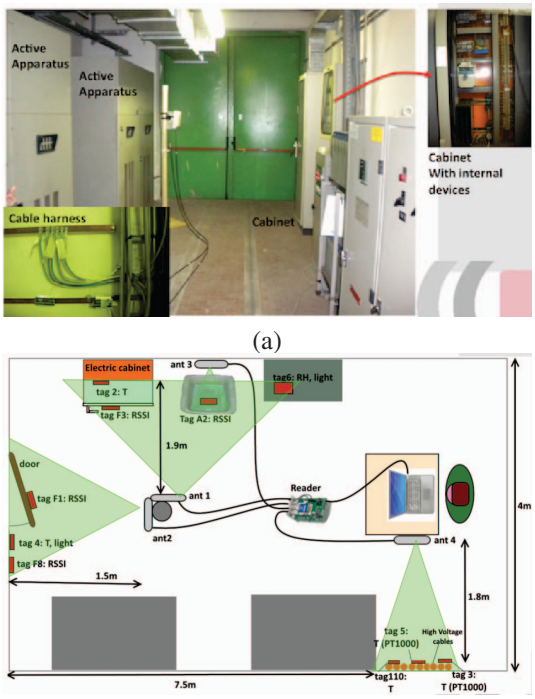

Fig. 5. a) Electrical transformer secondary substation of the University of Rome "Tor Vergata". b) Schematic representation of the RFID-SN.

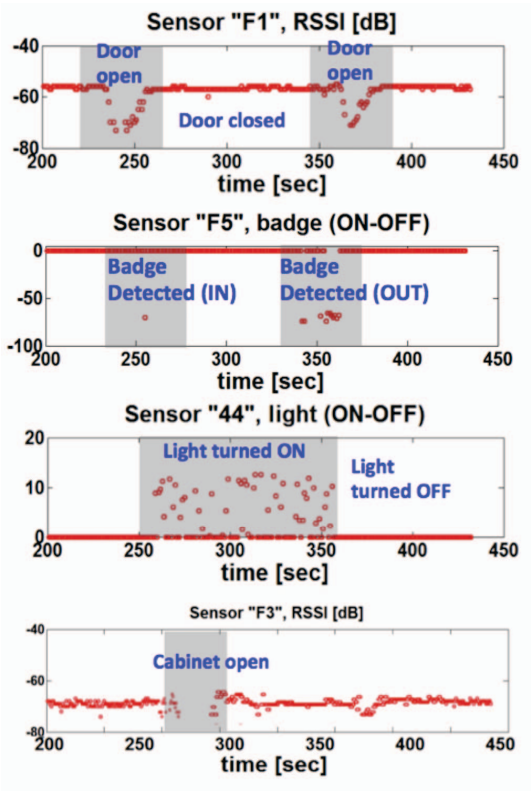

Fig. 6. RFID-SN measurements in case of authorized access to the electric cabinet.

detects again his badge and records the exit. The sequence of the events is here classified by means of a Human-based Semantic Analysis. In its final implementation, the Decision and Analysis Layer of the SCISSOR architecture will perform automatic event detection by on-line processing of the signal coming from the lower RFID-SN.

VI. Conclusion

Early considerations and tests seem to corroborate the feasibility of using RFID technology for multi-parameters monitoring of critical infrastructures and, more in general, of industrial plants. The proposed sensing network was successfully experimented in a real electric cabin and, as better shown at the symposium, it enabled the detection of a great variety of events by means of a unique and scalable infrastructure, borrowed from logistics. Anyway, the systems still deserves margins of improvements concerning the dynamic configurations of the nodes, the efficient handling of multitudes of sensors, the management of un-responding boards and the hybrid interaction with real-time and data-logger RFID-boards.

Acknowledgment

The work was supported by SCISSOR ICT project no. 644425, funded by the European Commissions Information & Communication Technology H2020 Framework Program. The authors would like to thank Stefano Milici for his valuable support to the experimental preparation and exploitation.

References

[1] Michael B Kelley. The stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. http://www.businessinsider.com/ stuxnet-was-far-more-dangerous-than-previous-thought-2013-11? IR=T.
[2] C. Occhiuzzi, S. Caizzone, and G. Marrocco, "Passive uhf rfid antennas for sensing applications: Principles, methods, and classifcations," Antennas and Propagation Magazine, IEEE, vol. 55, no. 6, pp. 14–34, Dec 2013.
[3] C. Occhiuzzi, C. Vallese, S. Amendola, S. Manzari, and G. Marrocco, "Night-care: A passive rfid system for remote monitoring and control of overnight living environment," Procedia Computer Science, vol. 32, pp. 190 – 197, 2014.
[4] M. Buettner, R. Prasad, M. Philipose, and D. Wetherall, "Recognizing daily activities with rfid-based sensors," in Proceedings of the 11th International Conference on Ubiquitous Computing, ser. UbiComp '09. New York, NY, USA: ACM, 2009, pp. 51–60.
[5] A. Costanzo, D. Masotti, T. Ussmueller, and R. Weigel, "Tag, you're it: Ranging and finding via rfid technology," IEEE Microwave Magazine, vol. 14, no. 5, pp. 36–46, July 2013.
[6] W. Sriborrirux, P. Danklang, and N. Indra-Payoong, "The design of rfid sensor network for bus fleet monitoring," in ITS Telecommunications, 2008. ITST 2008. 8th International Conference on, Oct 2008, pp. 103–107.
[7] M. Sole, C. Musu, F. Boi, D. Giusto, and V. Popescu, "Rfid sensor network for workplace safety management," in Emerging Technologies Factory Automation (ETFA), 2013 IEEE 18th Conference on, Sept 2013, pp. 1–4.
[8] AMS: SL900A www.ams.com
[9] ThingMagic M6E. http://www.thingmagic.com
[10] Manzari, S.; Pettinari, S.; Marrocco, G., "Miniaturized and tunable wearable RFID tag for body-centric applications", in RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on , vol., no., pp.239-243, 5-7 Nov. 2012