Design and Integration of Low Power RFID Wake-Up Radio For the Activation Of Sensing Nodes In Industrial Plants

Alessio Mostaccio, *Graduate Student Member, IEEE,* Nicola D'Uva, Sara Amendola, Cecilia Occhiuzzi, *Senior Member, IEEE* and Gaetano Marrocco, *Senior Member, IEEE*

***Abstract*—Hybrid wireless sensing nodes, composed of different sampling/processing and communication interfaces are gaining increasing interest in industrial scenarios thanks to their capability to create sensing networks with limited impact on operational costs and architectures. In this paper, the authors present the design and characterization of a Radio Frequency IDentification (RFID) board for the on-demand activation of sensing nodes. The device resorts to the functionalities of the EM4325 RFID IC which can emit simple voltage transitions upon the reception of RF events to wake up an external device.**

The antenna, namely a coplanar F-antenna, fulfills the design constraints due to its application in a potentially explosive environment and achieves a realized gain of 4 dBi. The latter, combined with the extremely low power sensitivity of the IC configured in semi-active mode, grants a reading distance of approximately 10 m.

The potentialities of the IC are then investigated by comparing two configurations of the IC in terms of the duration of the wake-up signal and thus power consumption. The findings indicate that the most selective configuration is the most indicated choice in case of limited power sources.

***Index Terms*—RFID, Wake-up radio, Oil, Gas, UAV, Internet of Things (IoT)**

I. Introduction

Industrial plants are extensive and harsh operational scenarios where the monitoring and control of machinery, engines, and pipes are crucial for efficient and safe operations [1], [2]. Generally, monitoring is performed through wired networks and supervised by human operators. However, such configurations suffer limitations in terms of coverage area, especially in the case of large plants with unreachable zones, and undermine the safety of workers. Typical examples are Oil&Gas sites, which are characterized by restricted or even off-limits areas with relevant safety hazards due to chemical exposures, gas leakages, high pressure, vibration, and extreme temperatures so that the fatality rate is seven times higher than in general industry [3]. Accordingly, human surveillance is gradually being replaced by autonomous patrolling vehicles, both terrestrial (Unmanned ground vehicle - UGV) and aerial (Unmanned aerial vehicle - UAV) [4], [5].

Alessio Mostaccio, Cecilia Occhiuzzi, and Gaetano Marrocco are both with the Pervasive Electromagnetics Lab, University of Rome Tor Vergata, Via del Politecnico 1, Rome, Italy, and RADIO6ENSE srl, Via della Tenuta di Torrenova 142, Rome, Italy (e-mail: alessio.mostaccio@uniroma2.it, cecilia.occhiuzzi@uniroma2.it, gaetano.marrocco@uniroma2.it). Sara Amendola and Nicola D'Uva are with RADIO6ENSE srl (e-mail: amendola@radio6ense.com, duva@radio6ense.com).

The corresponding author is Alessio Mostaccio (e-mail: alessio.mostaccio@uniroma2.it).

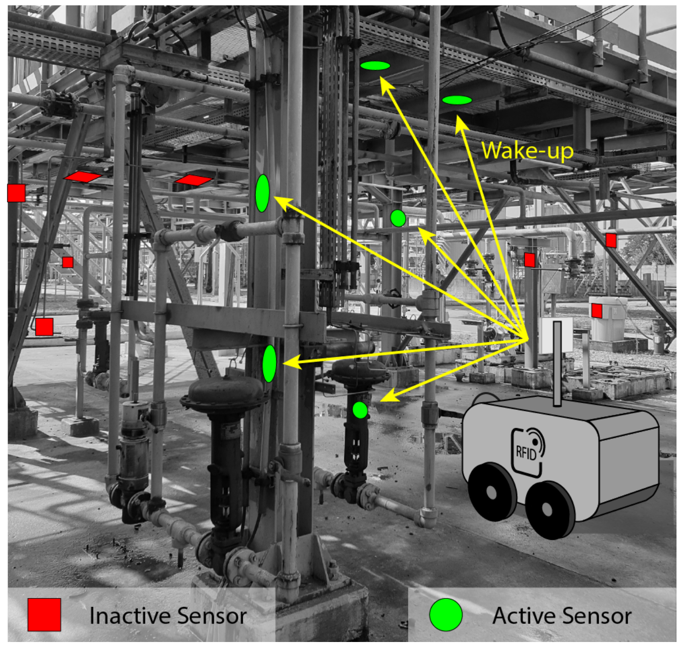


Fig. 1: Example of RFID-based wake-up architecture for the wireless monitoring of oil&gas plant through distributed gas sensors activated on demand by means of mobile RF scanners.

Recently, to improve and optimize the monitoring of the plants and hence gather information about environments and processes even in inaccessible areas, *Industrial Internet of Things* (I-IoT) [6] infrastructures have been progressively adopted. In this context, wireless sensor networks characterized by a high level of autonomy and reconfigurability and, above all, by a minimum impact on costs, energy, and procedures are added to existing machinery without compromising their integrity. Establishing robust and reliable wireless links in these contexts, however, is not trivial due to the presence of multiple and intricate metallic structures (e.g., pipe racks, pipelines, fuel tanks, vessels, and generators) which hinder the communication between distributed IoT sensing nodes and gateways, either fixed or mobile. Active devices, based on the most common communication protocols (Bluetooth, Bluetooth Low-energy, WiFi, LoRa, ZigBEE), are generally

TABLE I: WAKE-UP RADIO TECHNOLOGIES AND THEIR PERFORMANCES [13], [14]

Technology	Freq. [GHz]	Power $[\mu\text{W}]$	Type	Ref
Discrete	0.113	0.004	Active	[15]
	0.433	84	Active	[16]
	2.45	39	Active	[17]
	2.45	1620	Active	[18]
	2.45	24	Active	[19]
CMOS	2.45	395	Active	[20]
	2.45	2.4	Active	[21]
	2.45	95	Active	[22]
	0.045	37.5	Active	[23]
	60	9	Active	[24]
RFID	0.868	200	BAP	[25]
	0.868	200	BAP	**This work**

employed to extend the read range [7], [8]. However, the need for local power sources and the employment of timing procedures to establish communication with the interrogator constrain their applicability to the presence of the latter within the node's coverage region. In this scenario, autonomous patrolling missions could be successfully employed to *(i)* gather data from important spots throughout the plant that are inaccessible so far, *(ii)* rapidly span broad areas and thus avoid complex architectures to achieve adequate coverage of the sensors, and *(iii)* implement prediction models and custom flight missions based on real-time data always up-to-date [9]–[11].

Pseudo-asynchronous communication schemes [12], as in Fig. 1, can increase the power efficiency of these wireless sensor networks by remotely activating them only when needed (e.g., when the UAV/UGV enters the sensor's coverage area). As reported in Table I, several examples of wake-up radios (WuR) have been proposed through the years [13], [14], with the CMOS technology being appealing thanks to the minimal power consumption (i.e. few μW). However, the related fabrication efforts and costs fostered the development of WuRs based on discrete components. In this context, the ultra-high-frequency (UHF) radio frequency identification (RFID) technology, can be employed to empower these architectures by simply providing IoT nodes with configurable strategies for on-demand and selective activation through compact reader units integrated into patrolling unmanned vehicles.

The work of Smith *et al.* in the early 2000s first demonstrated the use of RFID transponders to power external devices with sensing capabilities. The outcome of their work was the creation of the well-known Wireless Identification and Sensing Platform (WISP) [26], [27]. More recently, De Donno *et al.* proposed and experimentally characterized a device triggering events upon a write operation to its memory banks with a power consumption of approximately 200 μW [25]. However, write operations are generally more energy-demanding in terms of transmitted power with an increase of chip sensitivity of about 5 dB. As a result, the achievable distance to wake up the node can be significantly reduced, especially in the case of fully passive operations.

A novel approach is presented here by resorting to more advanced functionalities of "modern" RFID ICs, which can generate output voltage signals when a target electromagnetic wave is detected and, thus, restrict the power consumption to the communication stage only [28].

This paper extends the preliminary work by the authors, in which the feasibility of a low-power RFID-based wake-up radio was demonstrated by resorting to Off-the-Shelf (COTS) components [5], [29]. Here, a system architecture suitable to be used in the monitoring of large areas of harsh industrial plants like oilfields is preliminarily presented. Then, the design of an ad-hoc RFID transponder, suitable to be integrated within the WSN node and compliant with ATEX regulations [30]–[32], together with the experimental characterization of the different wake-up configurations, is detailed.

The paper is hence organized as follows: Section II introduces the system architecture as well as the main design and operation constraints. The design of the RFID device is described in Section III, together with the prototype and the experiments. Finally, the wake-up mechanism provided by the IC and its experimental characterization are detailed in Section IV.

II. SYSTEM ARCHITECTURE

The proposed architecture consists of two main functional blocks, as schematized in Fig. 2.:

- the **wireless sensing node (WSN)**: distributed in numbers over the pipe-racks (e.g. vessels, valves, hose connections), consisting of *(a)* RFID transponders, namely *wakers*, implementing the wake-up function, and *(b)* IoT transceivers including ambient sensors and/or gas analyzers (e.g. methane sensors), a local power-source (e.g. solar panel) to supply the sensor unit and/or the RFID, an antenna for establishing a communication with the gateway, and finally an IC as a control unit.
- The **RF scanner**: a compact size and light-weight device suitable to be installed on the mobile platform (such as drones or rovers), comprising *(a)* the Micro Controller Unit (MCU), *(b)* the RFID-UHF reader, including the RF module and the interrogating antenna, for short-range communication with the WSN, and *(c)* an IoT gateway granting higher reading distances, from tens of meters up to km with fixed base stations, servers, or remote control units [33] [7].

The operation strategy can be described as follows. The MCU, acting as the main controller of the overall system, sends to the RFID reader the *start* command along with the instructions for the patrolling mission, e.g. the sampling rate and reading modality. The latter, indeed, can be *broadcast* when involving all the nodes present in the area or *targeted* in the case of a selective interrogation of target nodes included in a list. Once activated by the electromagnetic field emitted by the reader, the RFID transponder, energized over the *direct link* (reader to tag), generates a wake-up signal for the *IoT mote* and it is subsequently silenced to prevent multiple activations, thus saving power. The triggered mote starts performing local operations such as sensor sampling and pre-processing of measured data, and finally, transmits the packed data back to the IoT gateway which can be either installed on the mobile vehicle or placed in fixed positions throughout the plant.

The communication scheme includes the exchanges of control messages between the two blocks of the system. The first (*Ack 1*) is sent from the RFID board to the reader via *backward link* (tag to the reader), as a response to the reader's *Query*, regardless of the successful activation of the mote. The second acknowledgment (Ack 2) is sent to the MCU, through a different protocol, by the mote to confirm the completion of the entire communication loop. The hybrid architecture allows for extended read ranges thanks to the significantly lower sensitivity of active protocols w.r.t to RFID one while minimizing the power consumption by means of on-demand activation. Moreover, it improves the robustness of the system by separating the activation and communication tasks.

When the Ack2 is achieved with the RF scanner, i.e., the gateway is installed on board, the received data can be processed in real-time by the MCU to generate mission-related information (e.g. data-driven path planning). Alternatively, the data can be stored locally and downloaded at a later time for offline processing, in case significant computing resources are required. If the gateway is fixed, instead, the data are processed by the control center of the plant which then eventually transmits to the mobile platform updated instructions on the mission.

A. Design constraints

Due to the presence of explosive materials, the design, manufacturing, and deployment of electronic devices compliant with ATEX regulations [30]–[32] must attain some design constraints:

- the maximum transmitted RF power must be below 3.5 W. RFID technology, which is bounded in terms of the transmitted power to 3.2 W EIRP in the EU region [34], is hence compatible with the proposed architecture;
- the RFID transponder and its placement must be designed in order not to shadow the autonomous communication of the mote, whose layout must be minimally impacted by the presence of the waker to respect preexisting certifications;
- the RFID board must host on its surface a solar panel employed as the power source of the whole WSN;
- the use of dielectric materials for structural and coating purposes must be limited to prevent the accumulation of static charges. Depending on the gas under monitoring, the exposed dielectric surface varies with a limit of 2500 mm^2 in the most conservative case;
- the WSN must be wrapped around the pipe by means of flexible coating (the *Flange safety guard*) to deal with gas leakage detection tasks. As a matter of fact, the enclosure provides a closed environment in which the gas concentration rapidly increases in case of leakage, and thus eases its detection. To fulfill the constraint concerning the exposed dielectric area, the coating is loaded with conductive particles.

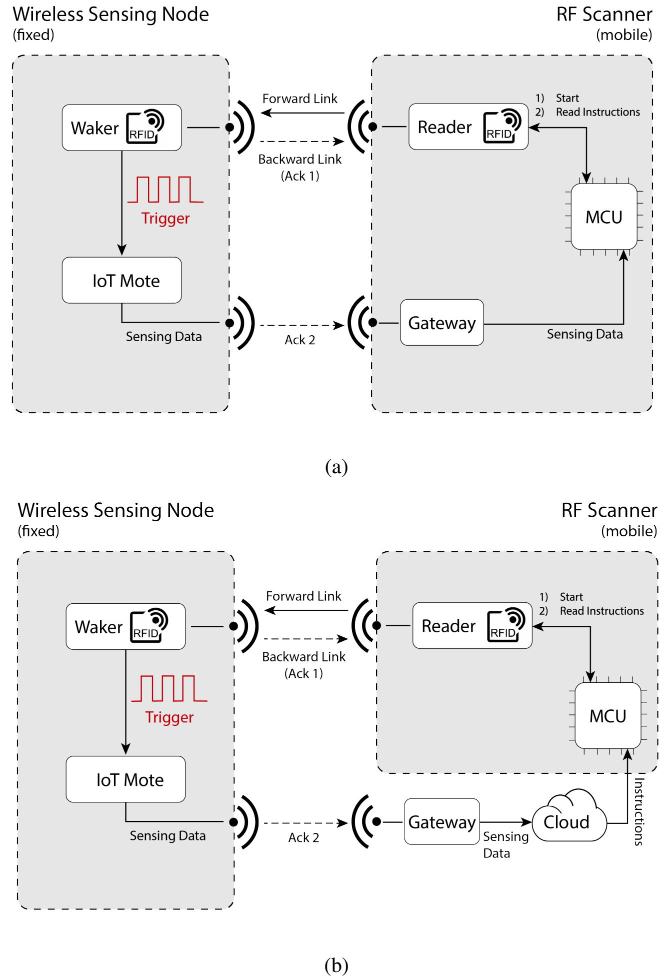


Fig. 2: System Architecture of a wireless monitoring system exploiting RFID-based wake-up mechanism. The mobile RF scanner can include the IoT gateway (a) to accomplish directly the acknowledgment (Ack2) with the WSN or (b) communicate with the cloud, connected to a fixed gateway.

III. RFID DEVICE LAYOUT

Within the previous constraints and without any loss of generality, here the IoT mote is equipped with a LoRa radio to achieve Ack 2, and we will only consider vertical stack alignments between the latter and the weaker. As a case study, the positioning of the IoT mote's antenna at its top left corner is considered. However, it is noteworthy that the following considerations remain applicable regardless of the antenna's positioning.

The RFID device layout is a double layer Coplanar Inverted F Antenna (C-IFA) which is a planar solution including a wide extent metallic area, serving as the ground plane, and a folded monopole responsible for the most of the radiation [35], [36] - Fig. 3. The dielectric is a low loss substrate, namely I-Tera MT40 ($\epsilon = 3.5$, $tan(\delta) = 0.0032$, $t = 0.9\ mm$) and the overall size of the transponder is $L = 77.4\ mm$, $W = 74.6\ mm$.

This configuration allows to

- optimize the overall footprint of the device, minimize modifications to the existing electronics, and facilitate the mounting of an additional wake-up transponder as an add-on layer;
- host a solar panel ($L_{sp} = 54\ mm$, $W_{sp} = 37\ mm$) with some degrees of freedom on the upper ground plane;
- fulfill the requirement on the maximum allowed exposed dielectric area (not ensured due to the size of the device), while preventing the shadowing of the IoT mote, by means of the partial metalization of both sides.

The RFID board was placed at a distance $\delta = 20$ mm from the mote to minimize the interference between the two components. Further, the IoT node, as big as the RFID transponder, was placed $d = 20$ mm far from a steel plate ($250 \times 250\ mm^2$) mimicking the presence of a pipeline. The connection lines between the two boards, supporting the power supply by the mote and the triggering signal to the latter respectively, were also included. Both lines are provided with RF chokes, namely ferrite beads, to prevent parasitic currents from entering the IC pins. The WSN coating is made of filled PTFE ($\epsilon = 2$, $\sigma = 3.1\ 10^{-4}\ S/m$) to prevent the accumulation of electrostatic charges on its surface. Finally, the waker integrates the EM 4325 RFID IC by EM Microelectronic [28] which can operate either in passive (chip sensitivity $P_{chip} = -8\ dBm$) or in battery-assisted (BAP) modes with a programmable sensitivity P_{chip} down to $-31\ dBm$ and input impedance $Z_{IC} = 7.4 - j122\ \Omega$. It also includes an internal temperature sensor ($-40°C$ to $+60°C$ range and $\pm 0.6°C$ accuracy). The local power source provided for the mote to empower LoRa transponder can be shared with the waker which can thus operate in BAP mode and extend the achievable read range by ten times w.r.t. to fully passive mode.

A. Numerical Simulations

The electromagnetic simulations were carried out by means of the Method-of-Moments (MoM) solver in the CST Microwave Studio 2023 implementation. The IoT node was modeled as a metallic surface accounting for the circuitry.

The matching of the antenna impedance to the IC is achieved by acting on the length of the horizontal trace (parameter d) and the vertical distance a; parameter b, instead, is fixed by the IC's width (6.6 mm). Furthermore, a capacitance C_{tune} was employed to fine-tune the antenna at the operating frequency and easily compensate manufacturing tolerance uncertainties on the material's properties, the effective layout of the mote rather than a metallic plane, and board positioning also after the PCB fabrication.

Fig. 4 shows the power transfer coefficient (τ) of the antenna for different values of $\{a,\ d\}$; the optimal combination of them is around $\{10.1\ mm,\ 33.1\ mm\}$. In reference condition, $C_{tune} = 0$. The final antenna layout achieves a power transfer coefficient $\tau = 0.95$ and a realized gain $G_{\tau,tag} = 4.5$ dBi. The radiation pattern is instead visible in Fig. 5. The antenna radiates in the broadside direction.

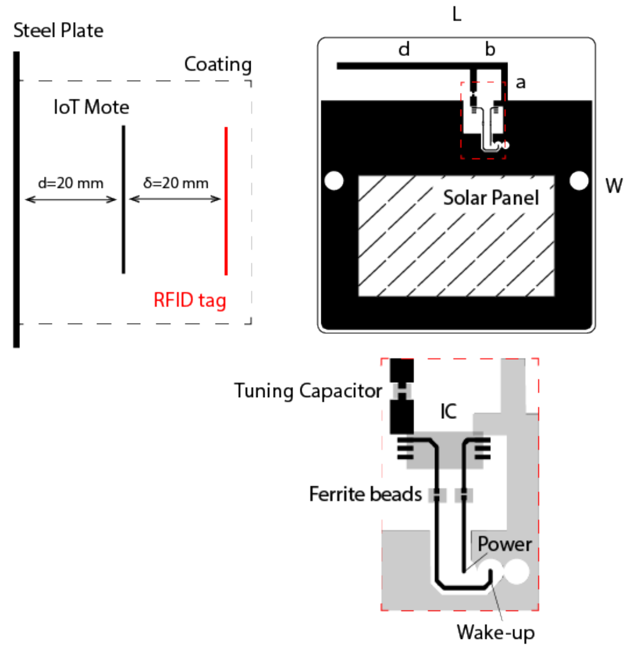


Fig. 3: Simplified model of the WSN including the filled PTFE coating, the solar panel, the metallic plate, the IoT mote, and the RFID board. Layout of the latter on the right and detail of the electrical connections on the bottom.

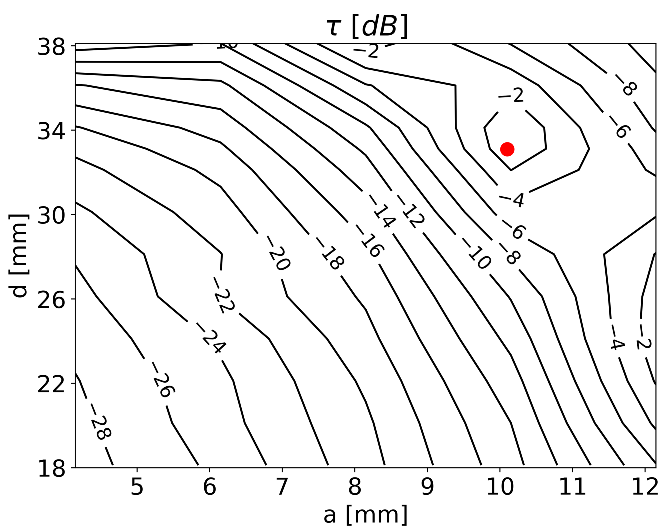


Fig. 4: Power transfer coefficient τ expressed in dB of the antenna at 868 MHz. The red dot indicates the optimal solution.

B. Prototype & Measurements

A prototype of the RFID antenna was manufactured on a 1 mm thick double layer copper clad I-Tera MT40 substrate (geometrical parameters and details in Fig. 6a and 6b). The IoT mote consists of a PCB board including a microcontroller to feed the RFID IC even when in sleep mode, a gas sensor, and a 900 MHz antenna and a UART interface for the communication (i.e. *Ack 2*) through LoRaWAN protocol and serial port respectively. The two boards are mounted in a vertically

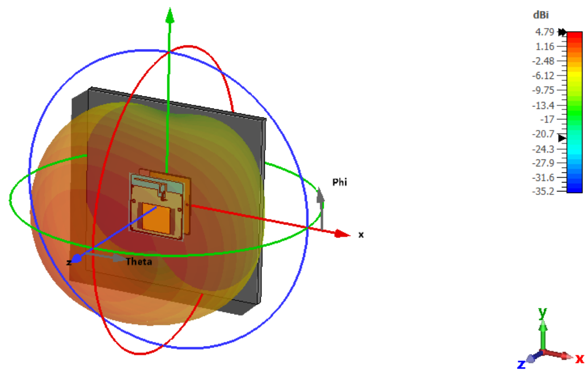
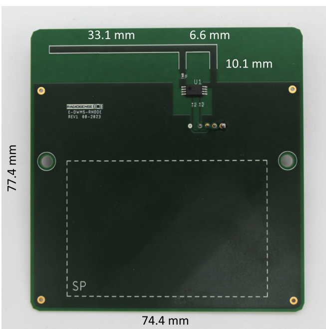
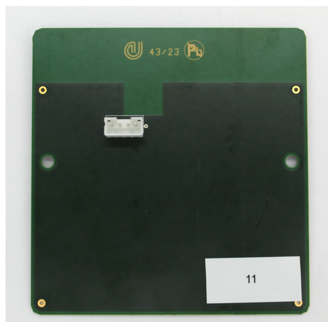


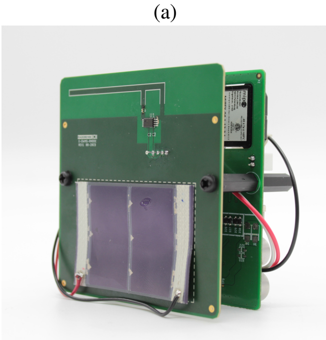
Fig. 5: Simulated radiation pattern of the WSN at 868 MHz.



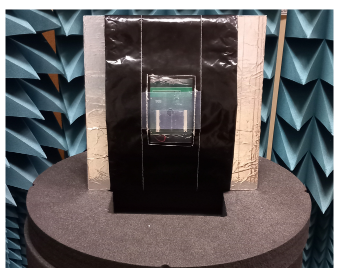
(a)



(b)



(c)



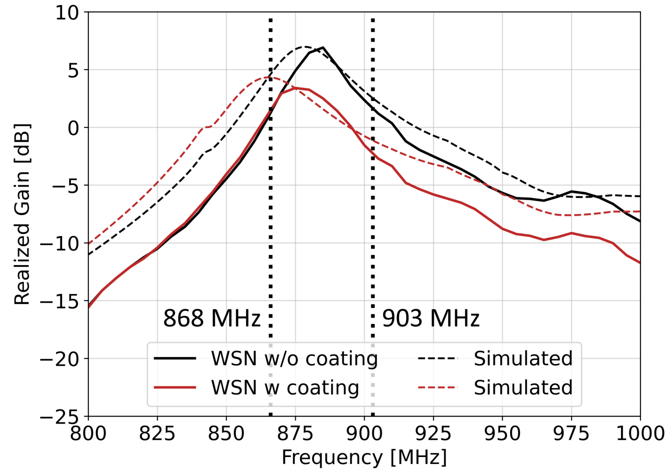
(d)

Fig. 6: (a) top and (b) and bottom view of the manufactured RFID board. (c) Stacked configuration of the RFID board with the IoT mote. (d) Assembly layout of the wireless sensing node.

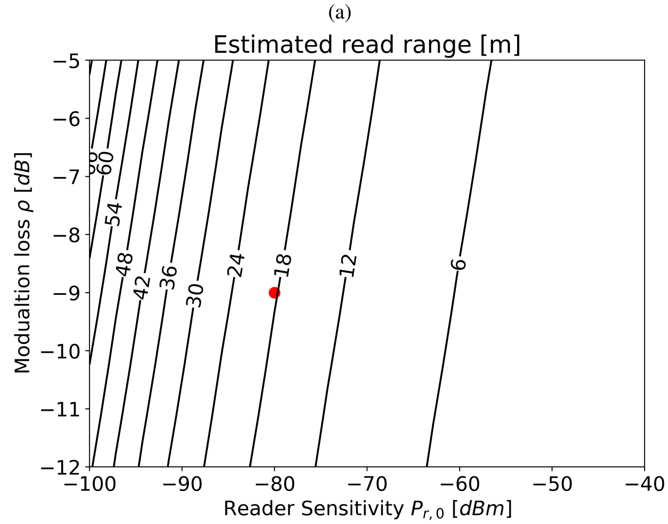
stacked configuration by means of 20 mm nylon spacers and connected through JST PH connectors (Fig. 6c). Finally, as a protective coating the SAFECAP® TFE-B-AS/SOLAR [37] is employed. The final assembly of the realized node is reported in Fig. 6d.

The electromagnetic performances of the RFID node were tested by means of the TagFormance Pro UHF station. The device was placed 50 cm far from a circularly polarized patch antenna (MT-242025/TRH/A from MTI Wireless Edge) and interrogated by means of the turn-on power method [38].

Fig. 7a reports the comparison between the measured and simulated realized gain, i.e. the gain of the antenna scaled by the mismatch with the IC impedance [36], in the case of



(a)



(b)

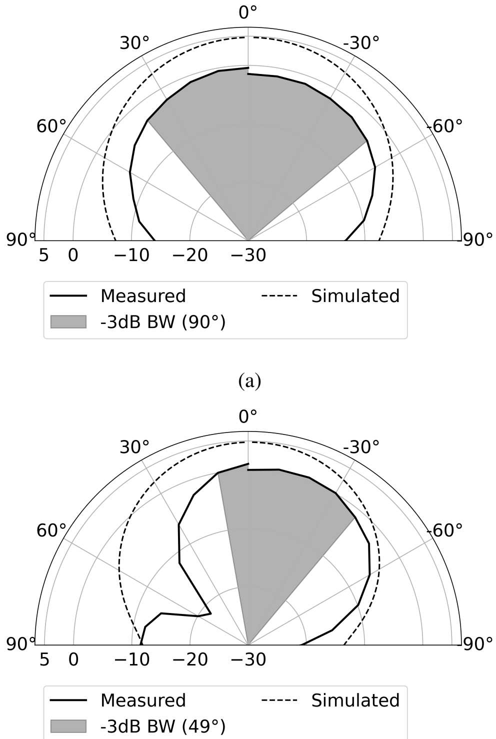
Fig. 7: (a) Comparison between the measured and simulated realized gain in the case of the WSN with (red) and without (black) protective coating. (b) Estimated read range (in meters) for the WSN from (1) by considering different values of the reader sensitivity and modulation loss factor. The red marker is the estimated reading distance for $\{P_{r,0},\ \rho\} = \{-80\ dBm,\ -9\ dB\}$.

the WSN with and without the protective coating respectively. The latter, indeed, can be removed when non-gas-related sensing tasks are required. In both the considered cases, by choosing $C_{tune} = 3.3pF$ to compensate for manufacturing and assembly uncertainties, there is a good agreement between measurements and simulations with a maximum realized gain of about 4 dBi when the coating is included.

The maximum reading distance D in free space can be accordingly estimated by considering the backward link Friis equation (1).

$$D = \frac{\lambda}{4\pi} \sqrt[4]{\frac{P_{tx} G^2_{\tau,tag} G^2_{\tau,r} \rho \eta_p^2}{P_{r,0}}} \tag{1}$$

Where P_{tx} is the input power emitted by the RFID reader and entering the reader's antenna, $G_{\tau,r}$ the gain of the latter, λ



(a)

(b)

Fig. 8: Measured radiation pattern at $868\ MHz$ of the RFID board along the E-plane (a) and H-plane (b). The filled areas indicate the half-power beamwidth.

the wavelength at 868 MHz in free space, η_p the polarization mismatch, ρ the modulation loss factor, and $P_{r,0}$ the minimum detectable power by the reader that for RFID semi-active transponders limits the read range [39], [40]. It is noteworthy that the additional losses introduced by the backscatter modulation are not constant but depend on the distance between the interrogator and the reader. The latter can vary from a couple of meters (i.e., $\rho = -12\ dB$) to approximately ten meters ($\rho = -6\ dB$). Fig. 7b, hence, shows the estimated reading distance from (1) by considering $G_{\tau,r} = 4\ dBi$ for the reader's patch antenna, $P_{tx} = 1\ W$ to fulfill EU RFID regulations, and different values of modulation loss factor and reader's sensitivity according to state of the art.

Finally, in Fig. 8, the antenna's realized gain at 868 MHz (both measured and simulated) on the E-plane (i.e., parallel to the horizontal radiating element) and H-plane (i.e., orthogonal to the horizontal radiating element) are reported. In the latter case, a beam tilting is present due to metallic components of the IoT mote underneath (considered as a homogeneous metallic plane in the simulations). By considering the half-power beamwidth (BW_{-3dB}), instead, the antenna is more directive on the H-plane $BW_{-3dB,H} = 49°$ while the other direction $BW_{-3dB,E} = 90°$ ensure wider coverage and thus a more robust link. The difference between the two curves is due to the frequency shift of the measured profile w.r.t. the simulated one.

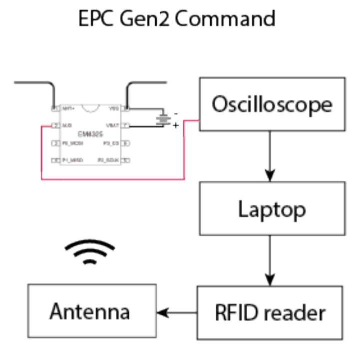


Fig. 9: Block diagram of the test setup employed for the experimental characterization of RFID tags.

IV. Wake-up Function

A. RFID IC with Wake-up Mechanism

The considered IC EM4325 offers two possible configurations for performing the wake-up of the IoT mote, depending on the port adopted for the connection and the activation signal required by the RFID reader: More particularly, the mote can be connected through:

- the 4-pin Serial Peripheral Interface (SPI) and activated by means of memory read/write operations to generate complex output signals;
- the 2-pin DC port (comprising a $100\ k\Omega$ pull-down resistor) and activated by means of a read-only operation to generate a simple signal voltage transition.

In this work, the latter option was selected as it significantly simplifies the interface towards the mote. Furthermore, the IC can be configured to produce the signal as soon as one of the following radio-frequency (RF) events is verified:

(i) an RF field in the ISM band is present in the environment and the waker collects enough power to power up its logic and emit a signal;
(ii) the RFID board receives a broadcast Gen2 *Query* request;
(iii) the waker receives an EPC targeted Gen2 *Query* request. In this case, the RFID board state is Open, Acknowledged, or Secured, meaning that the acknowledgment between the reader and the transponder has been achieved by means of a 16-digit random number (RN16) backscattered by the waker and checked by the reader.

Configurations *(i)* can generate the wake-up signal even in the case of RF noise; hence, it is not suitable for the proposed architecture where on-demand activation is needed. Configurations *(ii)* and *(iii)*, instead, robustly prevent unwanted activation and thus they will be further investigated.

B. Experimental characterization

The aim of the measurement campaign is to define and test the most suitable IC settings for the use case of interest, i.e., that in Fig. 2. Accordingly, the reception of the *Ack 2* was verified but not reported since it is outside the scope of this paper.

The experimental setup schematized in Fig. 9 considers an RFID reader (M6e from Jadak) sending specific EPC Gen2 commands to the waker and a digital oscilloscope (PicoScope 2000 Series) connected to the AUX pins of the EM4325 IC to measure the wake-up signal. To comprehensively assess the configuration modalities of the IC and without any loss of generality, two RFID boards were configured to detect different RF events, namely events *(ii)* and *(iii)*, as previously described. For the sake of simplicity, tags were powered by means of a 3.3 V coin battery since in the final integrated WSN the power supply will be provided by the solar panel through the mote's IC. When in BAP mode, the output signal is proportional to the supply voltage down to 1 V [29] with a power consumption of approximately 200 μW.

By means of the RFID reader, 3 different EPC Gen2 commands were repeatedly emitted:

A. *broadcast* inventory round in which all the wakers present in the environment that collect enough power are expected to reply;
B. *selective* inventory with a filter on the EPC to target wakers configured with spec. *(iii)*
C. *selective* inventory with a filter on the EPC to exclude wakers configured with spec. *(iii)*;

During interrogation, the duty cycle of the trigger signal (Eq. 2) is evaluated for each configuration as:

$$DC_{wup} = \frac{T_{wake-up}}{T} \tag{2}$$

where T, namely the period, is the time between two subsequent activations (raise front) and it is common to all the configurations under test, while $T_{wake-up}$ is the time during which the trigger is on, that is expected to be dependent on the IC settings. Accordingly, the overall energy consumption E can be computed as

$$E = T_{wake-up} \cdot P \tag{3}$$

C. Results

Fig. 10 reports the generated trigger signal for each configuration tested (by rows) as a consequence of a different RF event (by columns). It is worth noting that the trigger signals are temporarily shifted since they correspond to different moments of communication between a reader and an RFID device through the EPC Gen2 Protocol.

Both configurations can selectively wake up external devices through simple RFID commands. Options *(ii)* enables the triggers as soon as a Query request is received by those tags participating in the current inventory round. Event *(iii)*, instead, enables the trigger only during the acknowledgment phase between the reader and the tag which backscatters a 16-bit random number (RN16), then validated and transmitted back by the interrogator as acknowledgment.

Concerning the duty cycle, the results are summarized in Table II. The shortest DC_{wup} is achieved by condition *(iii)* since the acknowledgment phase only involves the reader and one waker per time. Configuration *(ii)*, instead, enables the trigger for a longer period of time, i.e., approximately 5 times

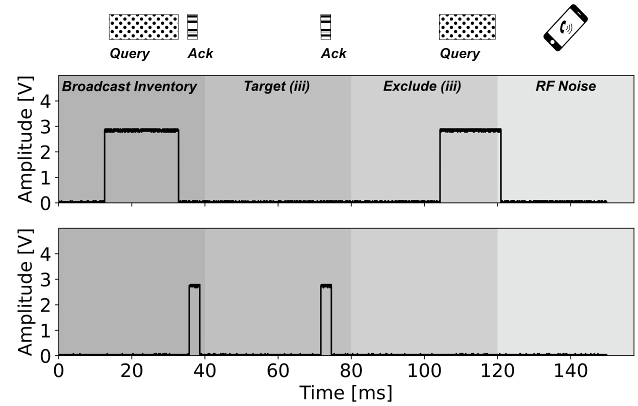


Fig. 10: Example of emitted triggered signal for IC configurations *(ii)* and *(iii)* - first and second row respectively - in case of different RF events (by column): *broadcast* inventory round, and *selective* inventory round with filter on the EPC (either for selecting or excluding specific nodes), and finally noise. The patterned rectangles indicate different stages of the communication through the Gen2 Protocol.

TABLE II: DUTY CYCLE AND DURATION OF THE WAKE-UP SIGNAL FOR EACH IC CONFIGURATION

Event	$\mathbf{DC_{wup}}$ [%]	$\mathbf{T_{wake-up}}$ [ms]
ii	25.6 ± 1.6	11.4 ± 0.4
iii	5.9 ± 0.5	2.9 ± 0.3

that of spec. *(iii)*. It is worth noticing that short pulses are preferable to trigger events while higher duty cycles ease the rectification of the signal thus enabling also functionalities of power supplying. Overall, both configurations ensure an energy consumption lower than 3 μJ for each activation which is thus negligible compared to the daily energy consumption of the mote by considering one transmission per hour (i.e., 1.5 J).

Finally, to verify the effective impossibility of unwanted activation, a generic RF source operating in the UHF band, which is likened to ambient noise (e.g. a smartphone during a call), was considered instead of the RFID reader. As expected, both tags are insensitive to RF noise since no trigger event is generated upon the reception of a signal in the UHF band, even if the received power is enough to activate the tags.

V. CONCLUSION

Having in mind wireless sensor networks aimed at covering extended harsh industrial scenarios, this paper introduced a hybrid architecture exploiting UHF RFID devices to implement a low-power wake-up strategy. The latter resorts to the auxiliary function of the EM4325 RFID IC.

The RFID waker was designed and experimentally characterized with a measured realized gain of about 4 dBi, thus ensuring a reading distance of almost 10 meters by considering a reader emitting 3.2 W EIRP.

Then, two configurations of the IC, compatible with the proposed architecture, have been comprehensively tested and compared in terms of robustness of the trigger signal w.r.t. unwanted activations and duty cycle. "*Selective activation*" has been identified as the most suitable one since the lower duration of the wake signal ensures a lower power consumption.

Future works will focus on the assessment of the possible cyber-security vulnerabilities of RFID-based wake-up function as an essential step to enable the adoption of this solution in critical industrial infrastructure like the oil&gas industry [41].

REFERENCES

[1] Z. Ge, "Review on data-driven modeling and monitoring for plant-wide industrial processes," *Chemometrics and Intelligent Laboratory Systems*, vol. 171, pp. 16–25, 2017.

[2] N. F. Thornhill, J. W. Cox, and M. A. Paulonis, "Diagnosis of plant-wide oscillation through data-driven analysis and process understanding," *Control Engineering Practice*, vol. 11, no. 12, pp. 1481–1490, 2003.

[3] R. Z. Witter, L. Tenney, S. Clark, and L. S. Newman, "Occupational exposures in the oil and gas extraction industry: State of the science and research recommendations," *American journal of industrial medicine*, vol. 57, no. 7, pp. 847–856, 2014.

[4] A. Buffi, A. Motroni, P. Nepa, B. Tellini, and R. Cioni, "A sar-based measurement method for passive-tag positioning with a flying uhf-rfid reader," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 3, pp. 845–853, 2019.

[5] A. Mostaccio, S. Amendola, N. D'Uva, G. Marrocco, and C. Occhiuzzi, "Distributed wireless monitoring in oil&gas plants through mobile uav-ugv rfid platforms," in *2023 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT)*. IEEE, 2023, pp. 1–6, to be published.

[6] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," *Computers in industry*, vol. 101, pp. 1–12, 2018.

[7] M. Y. Aalsalem, W. Z. Khan, W. Gharibi, M. K. Khan, and Q. Arshad, "Wireless sensor networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges," *Journal of network and computer applications*, vol. 113, pp. 87–97, 2018.

[8] S. Ali, A. Ashraf, S. B. Qaisar, M. K. Afridi, H. Saeed, S. Rashid, E. A. Felemban, and A. A. Sheikh, "Simplimote: A wireless sensor network monitoring platform for oil and gas pipelines," *IEEE Systems Journal*, vol. 12, no. 1, pp. 778–789, 2016.

[9] Q. Jiang, X. Yan, and B. Huang, "Review and perspectives of data-driven distributed monitoring for industrial plant-wide processes," *Industrial & Engineering Chemistry Research*, vol. 58, no. 29, pp. 12 899–12 912, 2019.

[10] Z. Ge and J. Chen, "Plant-wide industrial process monitoring: A distributed modeling framework," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 310–321, 2015.

[11] A. DiCarlofelice, E. DiGiampaolo, and P. Tognolatti, "mm-wave chipless rfid tag for healthcare applications," in *2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science*. IEEE, 2020, pp. 1–3.

[12] E.-Y. A. Lin, J. M. Rabaey, and A. Wolisz, "Power-efficient rendezvous schemes for dense wireless sensor networks," in *IEEE International Conference on Communications*. Citeseer, 2009, pp. 20–24.

[13] R. Piyare, A. L. Murphy, C. Kiraly, P. Tosato, and D. Brunelli, "Ultra low power wake-up radios: A hardware and networking survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2117–2157, 2017.

[14] H. Bello, Z. Xiaoping, R. Nordin, and J. Xin, "Advances and opportunities in passive wake-up radios with wireless energy harvesting for the internet of things applications," *Sensors*, vol. 19, no. 14, p. 3078, 2019.

[15] P.-H. P. Wang, H. Jiang, L. Gao, P. Sen, Y.-H. Kim, G. M. Rebeiz, P. P. Mercier, and D. A. Hall, "A near-zero-power wake-up receiver achieving- 69-dbm sensitivity," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 6, pp. 1640–1652, 2018.

[16] L. Gu and J. A. Stankovic, "Radio-triggered wake-up for wireless sensor networks," *Real-Time Systems*, vol. 29, pp. 157–182, 2005.

[17] H. Khodr, N. Kouzayha, M. Abdallah, J. Costantine, and Z. Dawy, "Energy efficient iot sensor with rf wake-up and addressing capability," *IEEE sensors letters*, vol. 1, no. 6, pp. 1–4, 2017.

[18] C. Petrioli, D. Spenza, P. Tommasino, and A. Trifiletti, "A novel wake-up receiver with addressing capability for wireless sensor nodes," in *2014 IEEE International Conference on Distributed Computing in Sensor Systems*. IEEE, 2014, pp. 18–25.

[19] J. Oller, E. Garcia, E. Lopez, I. Demirkol, J. Casademont, J. Paradells, U. Gamm, and L. Reindl, "Ieee 802.11-enabled wake-up radio system: design and performance evaluation," *Electronics Letters*, vol. 50, no. 20, pp. 1484–1486, 2014.

[20] R. Liu, A. B. KT, R. Dorrance, D. Dasalukunte, V. Kristem, M. A. S. Lopez, A. W. Min, S. Azizi, M. Park, and B. R. Carlton, "An 802.11 ba-based wake-up radio receiver with wi-fi transceiver integration," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 5, pp. 1151–1164, 2019.

[21] E. Nilsson and C. Svensson, "Ultra low power wake-up radio using envelope detector and transmission line voltage transformer," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 5–12, 2013.

[22] E. Alpman, A. Khairi, R. Dorrance, M. Park, V. S. Somayazulu, J. R. Foerster, A. Ravi, J. Paramesh, and S. Pellerano, "802.11 g/n compliant fully integrated wake-up receiver with- 72-dbm sensitivity in 14-nm finfet cmos," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 5, pp. 1411–1422, 2018.

[23] H. Cho, J. Bae, and H.-J. Yoo, "A 37.5/spl mu/w body channel communication wake-up receiver with injection-locking ring oscillator for wireless body area network," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 5, pp. 1200–1208, 2013.

[24] T. Wada, M. Ikebe, and E. Sano, "60-ghz, 9-μw wake-up receiver for short-range wireless communications," in *2013 Proceedings of the ESSCIRC (ESSCIRC)*. IEEE, 2013, pp. 383–386.

[25] D. De Donno, L. Catarinucci, and L. Tarricone, "Ultralong-range rfid-based wake-up radios for wireless sensor networks," *IEEE Sensors Journal*, vol. 14, no. 11, pp. 4016–4017, 2014.

[26] J. R. Smith, "History of the wisp program," *Wirelessly Powered Sensor Networks and Computational RFID*, pp. 13–29, 2013.

[27] H.-J. Chae, M. Salajegheh, D. J. Yeager, J. R. Smith, and K. Fu, "Maximalist cryptography and computation on the wisp uhf rfid tag," *Wirelessly Powered Sensor Networks and Computational RFID*, pp. 175–187, 2013.

[28] Em4325- epc and uhf ics. [Online]. Available: https://www.emmicroelectronic.com/product/epc-and-uhf-ics/em4325

[29] A. Mostaccio, S. Amendola, N. D. C. Occhiuzzi, E. Martinelli, and G. Marrocco, "Ultra-low power rfid-based wake-up architectures for wireless sensor networks in industrial plants," in *2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA)*. IEEE, 2023, pp. 146–149.

[30] T. Jespen *et al.*, "Atex—explosive atmospheres," *Springer Series in Reliability Engineering*, 2016.

[31] C. A. Boano, J. Brown, Z. He, U. Roedig, and T. Voigt, "Low-power radio communication in industrial outdoor deployments: The impact of weather conditions and atex-compliance," in *Sensor Applications, Experimentation, and Logistics: First International Conference, SENSAPPEAL 2009, Athens, Greece, September 25, 2009, Revised Selected Papers 1*. Springer, 2010, pp. 159–176.

[32] N. H. Versloot, A. Klein, and M. De Maaijer, "The atex directives: Explosion safety and regulation, the european approach," *Emerg. Plan. Prep. Prev. Response, Hoboken, NJ, USA: John Wiley & Sons, Inc*, pp. 389–404, 2010.

[33] G. M. Bianco, A. Mejia-Aguilar, and G. Marrocco, "Performance evaluation of lora lpwan technology for mountain search and rescue," in *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*. IEEE, 2020, pp. 1–4.

[34] M. Saelens, J. Hoebeke, A. Shahid, and E. D. Poorter, "Impact of eu duty cycle and transmission power limitations for sub-ghz lpwan srds: An overview and future challenges," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–32, 2019.

[35] T. Alam, M. T. Islam, M. A. Ullah, and M. Cho, "A solar panel-integrated modified planner inverted f antenna for low earth orbit remote sensing nanosatellite communication system," *Sensors*, vol. 18, no. 8, p. 2480, 2018.

[36] G. Marrocco, "The art of uhf rfid antenna design: Impedance-matching and size-reduction techniques," *IEEE antennas and propagation magazine*, vol. 50, no. 1, pp. 66–79, 2008.

[37] Copriflangia safecap® tfe-b-as per zone atex. [Online]. Available: https://copriflangedisicurezza.it/it/copriflange/copriflange-per-zone-atex/copriflangia-safecap-tfe-b-as-per-zone-atex/

[38] C. Occhiuzzi, F. Camera, M. D'Orazio, N. D'Uva, S. Amendola, G. M. Bianco, C. Miozzi, L. Garavaglia, E. Martinelli, and G. Marrocco, "Automatic monitoring of fruit ripening rooms by uhf rfid sensor network and machine learning," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 649–659, 2022.

[39] G. Li, M. Chen, F. Zhao, Z. Li, D. Inserra, and G. Wen, "A reflection-amplifier-based long-range semi-passive uhf rfid tag with standard compatibility," *IEEE Microwave and Wireless Technology Letters*, 2023.

[40] P. V. Nikitin and K. S. Rao, "Antennas and propagation in uhf rfid systems," in *2008 IEEE international conference on RFID*. IEEE, 2008, pp. 277–288.

[41] Cyber 4.0, cybersecurity compentec center. [Online]. Available: https://www.cyber40.it/