# Wireless Reconfigurability of Electromagnetic Devices Through RFID Passive Technology

*Francesco Lestini, Gaetano Marrocco, and Cecilia Occhiuzzi*

*Abstract* – The growing demand for advanced wireless communication systems has underscored the urgent need for electromagnetic devices capable of adapting to diverse operational demands. In this scenario, reconfigurable objects, especially antennas and backscattering surfaces, have attracted considerable attention. In the case of electronic reconfigurability, the different electromagnetic features are selected by adequately adjusting the bias voltage across RF switches embedded in the device, generally by using costly external programmable controllers requiring power supplies and cables that are impractical in several contexts. Therefore, it is essential to explore alternative electronic tuning mechanisms to supply and reprogram electromagnetic elements in a wireless, efficient, and cost-effective way. This paper proposes RFID-based reconfigurable electromagnetic devices as a wireless, low-cost, and low-power alternative solution. The general framework of the system is provided, together with the possible architectures and their feasibility in real-world scenarios.

## 1. Introduction

The growing demand for advanced wireless communication systems and the rapid expansion of Internet of the Things applications have emphasized the urgent requirement for electromagnetic devices capable of adapting to a broad spectrum of operational needs. Indeed, the contemporary wireless communications landscape faces various challenges, including dynamic frequency allocations, diverse communication standards, and the necessity for optimized performance under unpredictable environmental conditions [1]. In response to these challenges, researchers are paying significant attention to reconfigurable objects, particularly antennas and backscattering surfaces, due to their ability to dynamically change operating frequency, radiation pattern, polarization behavior, or a combination of any of these properties [2]. Several types of reconfigurable devices have been studied over the years, from stand-alone elements [3, 4], antenna arrays [5, 6], and frequency selective surfaces (FSSs) [7], to the most recent reconfigurable intelligent surfaces [8, 9].

Reconfiguring electromagnetic devices involves inducing changes in their surface currents, thereby modifying their fundamental electromagnetic characteristics. However, integration with an external programmable platform (e.g., microcontrollers, field programmable gate arrays, or digital signal processors) is essential for such reconfigurability. These external platforms can alter the state of electronic tunable components integrated into the reconfigurable device (such as PIN diodes, varactor diodes, micro-electro-mechanical systems [MEMS] switches) by adjusting the bias voltage across them [10]. A significant challenge arises because external controllers necessitate wired connections, rendering the structure inflexible, costly, and power-intensive. These limitations pose obstacles, making reconfigurable electromagnetic devices impractical in environments where the use of external power supplies and cables is restricted, such as body-worn antennas or embedded radiating elements [11].

In this paper, we propose a solution that leverages UHF RFID technology. This choice is based on the technology's cost-effectiveness, low power consumption, and ability to offer wireless connectivity, sensing, and basic computational capabilities through simple and miniaturized devices [12]. Furthermore, the latest generation of RFID integrated circuits (ICs) [13, 14], can also serve as dc power sources for external devices. Indeed, they can be programmed to execute specific commands, such as supplying a dc voltage triggered by particular events [15], thus acting as *wireless controllers*. This functionality allows for the control of RF tunable components, facilitating modifications to the configuration of electromagnetic devices (see Figure 1). The idea of using RFID ICs as wireless controllers of an intelligent surface was previously introduced in [16], where authors demonstrated the possibility of assisting a source-destination link by forcing RFID tags to backscatter in carefully selected groups. In this paper, we propose a different approach that exploits RF switches and can be employed to reconfigure any electromagnetic device.

An early feasibility assessment was previously introduced by the authors in [17]. Here, a grid of two elements operating in the RFID UHF band, namely the *master tag* and the *slave tag*, was configured to selectively enable or disable communication with the external reader by properly setting the state of a PIN diode controlled by the *master* and integrated into the layout of the *slave*. Being the memory of the IC nonvolatile, the configuration was maintained even when the grid was not powered up and became effective every time the device received enough power from every compatible electromagnetic source (even if not modulated according to RFID protocol). The preliminary validation of the approach opened many challenges related to potential architectures, achievable performances, and limitations compared with traditional solutions. This paper aimed to

Manuscript received 7 January 2024.

Francesco Lestini, Gaetano Marrocco, and Ceclilia Occhiuzzi are with DICII - University of Rome Tor Vergata, Via del Politecnico 1, Rome, 00133, Italy; e-mail: francesco.lestini@uniroma2.it, gaetano.marrocco@uniroma2.it, cecilia.occhiuzzi@uniroma2.it.

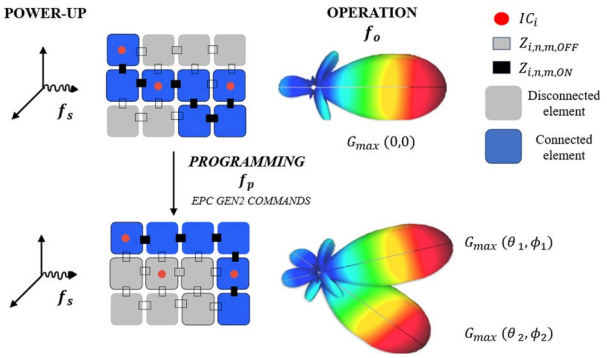


Figure 1. Concept of RFID-based wireless programmability of a grid of conductive elements.

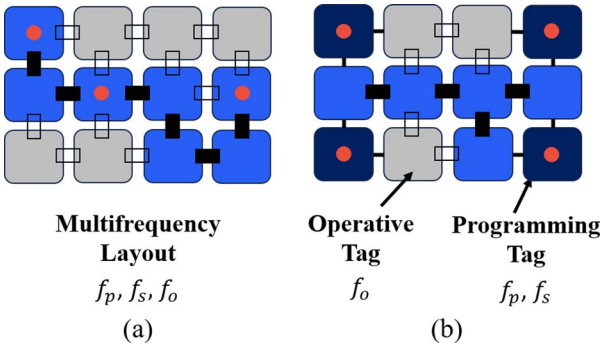


Figure 2. Possible architectures of the RFID-based reconfigurable electromagnetic object. (a) Fully integrated multifrequency layout. (b) Programming, power-up, and operative elements are physically distinguished.

give a perspective overview of the many open points and possible applications, such as to outline the main features of this new branch of research.

## 2. Rationale

Figure 1 sketches the working principle of the proposed reconfiguration method. Here, an electromagnetic object (EM-O) made up of a grid of $n \times m$ unit cells is considered, whose mutual connections are determined by the state of one or more RF switches ($Z_{i,n,m}^{ON,OFF}$) properly controlled by one or more RFID $IC_i$.

Programmability is achieved by activating or deactivating (*State 1 and State 0*) the IC dc output PIN through conventional EPC UHF Gen2 commands [18] sent by an RFID reader at the UHF frequency $f_p$, resulting in *1-bit reconfigurability*. Owing to the unique identification code, commands can be selectively transmitted and stored in the internal memory of each IC, which is writeable and nonvolatile [18], allowing the configuration settings to be permanently stored. The IC is activated when a compatible RF field at frequency $f_s$ and power $P_{harv}$ impinges upon the grid (Figure 1), provided that $P_{harv}$ is greater or equal to the power required to activate the circuitry ($p_c$). Subsequently, the RFID IC will drive or not the RF switch to which it is connected, depending on the command stored in its internal memory. This will result in modifying the currents flowing through the EM-O, thereby influencing its electromagnetic characteristics, such as its operative frequency $f_o$, bandwidth, radiation pattern, and polarization (Figure 1). Of note, the activation field can be either modulated or not, meaning that alternative ambient sources, such as Wifi, Bluetooth, cellular network signals, or even pure ad hoc sinusoidal fields, could be used [19]. Despite the source, the activation field must continuously illuminate the EM-O throughout its operation to benefit from the programmed configuration.

The following three working conditions of the system can be hence identified, each with its frequency and required/produced signals:

1. Programming: The desired RF switch status ($Z_{i,n,m}^{ON,OFF}$.) is stored in the $IC_i$ user memory. The RFID Gen2 protocol [18] must be used, and consequently, $f_p$ is fixed and corresponds to the UHF band.
2. Power-up: Depending on the imposed state, when a compatible RF source illuminates the ICi, it may or may not deliver a dc voltage to the connected RF component. In the most general case, the frequency of the source signal $f_s$, as well as its modulation, are not univocally defined, provided that the power harvested by the ICs exceeds its sensitivity.
3. Operation: While illuminated by the source, the EM-O performs actions according to the imposed configuration. Also, operations can be performed at different frequencies $f_o$.

The power-up and operation phases are dependent and synchronous. Programming can be performed, instead, off-line and repeated many times according to the particular application. Therefore, if power-up, operation, and programming rely on the same bandwidth/service, they can all be performed by the same antenna. For instance, if the system is conceived only for RFID applications, a single incident wave can perform programming, power-up, and operation (being $f_p = f_s = f_o$). On the other hand, if power-up and operation are executed at different frequencies ($f_s \neq f_o$), an ad hoc illuminator at $f_s$ is needed.

### 2.1 Architectures

Previous considerations make the EM-O an inherently multifrequency device. Two layouts can be envisioned as follows:

1. The ICs are embedded directly in the layout so that harvest, activation, and operation are seamlessly done by the same conductive elements (Figure 2a). This would allow for miniaturized and

more compact structures, but a trade-off between the performances at $f_p$, $f_s$, and $f_o$ is required.

2. Harvest, activation, and operation are demanded for specific portions of the layout, each of them tuned to a particular frequency $f_p$, $f_s$, $f_o$ (Figure 2b). From this perspective, it is possible to properly include in the device *Programming* and *Operating nodes* whose relationship can be assumed to be similar to that of the typical *master/slave*. Each portion can be optimized for its specific frequency, but the structure will be more complex and bulkier than the multifrequency layout.

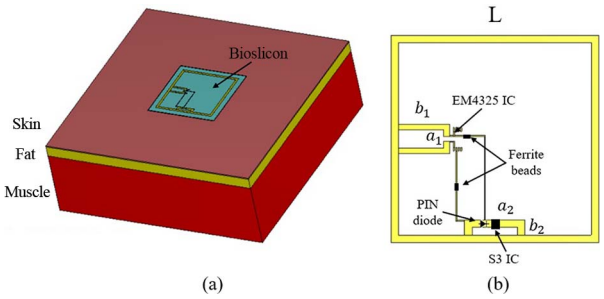


Figure 3. (a) Simulation model. Body tissues and substrate thicknesses and dielectric properties are as in [21]. (b) Dual-chip RFID antenna layout. $L = 55\ mm$, $a_1 = 4.8\ mm$, $b_1 = 12\ mm$, $a_2 = 16\ mm$, $b_2 = 4\ mm$.

### 2.2 Components

In addition to requirements related to the multifrequency behavior of the reconfigurable device, a key role is devoted to the power consumption of the ICs and the RF components. Indeed, from an operative point of view, the feasibility of the proposed architecture relies on the IC's ability to detect the presence of an RF field and harvest enough power to activate its circuitry and consequently drive the RF tunable element in a stable way and with adequate bias voltages.

To the best of our knowledge, there are only two commercially available ICs, the EM4325 ($p_c = -30\ dBm$) [13] and the EM4152 ($p_c = -18\ dBm$) [14], which provide the required feature of a controllable dc output port. The former operates in battery-assisted passive (BAP) mode, meaning that its waking up depends only on the availability of a compatible RF field while the battery supplies the external component. The latter, instead, is completely passive, which means that both the power-up and supply of the output port are based on the harvested EM field. Typically, such ICs are employed only in RFID applications (i.e., in the UHF band), but some experimental evidence [19] suggested that they can also operate in other frequency bands. However, the nominal features of both ICs (sensitivity $p_c$ and DC power output $V_{out}$) are available only in the UHF band. Hence, it is extremely important to characterize them when considering different frequency bands.

The available voltages/powers for controlling the tunable elements are extremely limited (3.3 V/30 mW for BAP IC and 1.8 V/420 $\mu$W for the pure passive one), so the choice of suitable elements is diriment. Among elements conventionally adopted for reconfigurable devices, PIN diodes have low thresholds (0.6–0.8 V) but require relatively high currents (0.1–1 mA), MEMS switches are low-power components (a few microwatts) that require high bias voltages starting from 2.6 V. In comparison, varactor diodes have a very low threshold (0.2 V), but their ON-state impedance strongly depends on the stability of the dc output voltage.

## 3. Conclusion and Possible Applications

This paper introduced and discussed the idea of RFID-based wireless programmable antennas. The proposed architecture is considerably cheaper concerning state-of-the-art programming hardware and does not require any physical wire. Moreover, such a system is more sustainable and usable also in contexts where batteries or external power supplies are not allowed (e.g., embedded systems and sensors or on-body antennas). The topic can open many different research perspectives. First, it will be devoted to understanding the real feasibility of the platform by characterizing the ICs in different frequency bands, and then it will be aimed at evaluating the effective applicability in real-world scenarios.

Many different applications can be envisaged. In these contexts, we propose three possible future applications as follows:

1. Wireless security token: The *master/slave* architecture discussed in Section 2.1 can be exploited to realize a wireless security token, that is, a peripheral device that is used in addition to, or in place of, a password to gain access to another device [20]. In this scenario, the programmable node acts as the "authenticator" for the operating node. For example, we propose the same layout of the dual-chip epidermal antenna presented in [21]. The simulation setup is shown in Figure 3a. The programming node is the EM4325 IC ($Z_{chip} = 7.6 - j114\ \Omega$), while the operating node is the Magnus S3 IC ($Z_{chip} = 2.8 - j73.6\ \Omega$), acting as the temperature sensor. Both ICs were matched to the antenna impedance by a T-match [22], and ferrite beads were placed in dc connections for dc-decoupling purposes (Figure 3b). In this configuration, temperature data can be collected only if the EM4325 is programmed to forward bias the PIN diode embedded in the T-match of the S3 IC, which, otherwise, is mismatched. Indeed, the realized gain $G_T$ (i.e., the antenna gain scaled by the impedance mismatch with the IC) of the S3 IC drastically drops from $-16$ dB (diode ON) to $-32$ dB (diode OFF), as shown in Figure 4. The outcome is that communication with the operating node is possible only after reprogramming the programmable node through a trusted RFID

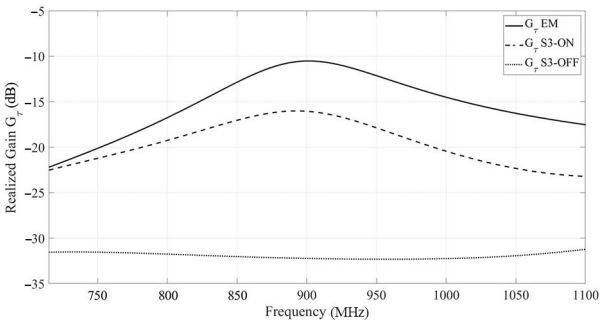


Figure 4. Realized gains for both ICs. When the diode is turned off, communications with the S3 IC is disabled.

reader. Therefore, attackers need to know the unique identification code (which can be hidden from untrusted RFID readers [18]) and the access password of the authenticator IC to retrieve temperature data.

2. Programmable lens for adaptive antenna focusing: Reconfigurability can be exploited to modify the radiation pattern of an antenna or an array, hence focusing the beam in specific directions. An application that could benefit from battery-less and lightweight configurations is related to body-centric communications, particularly to strategies for improving communication between implanted/wearable devices and external reading/powering units [23]. A particular case could be the optimization of hyperthermia treatments in which a target in-depth malignant tissue has to be reached by proper heating fields. In previous work, authors have introduced an RFID-based thermal monitoring sheet [24] for skin temperature monitoring during superficial hyperthermia treatment. The system works as an FSS and is a periodic structure with a dual-frequency response (434 MHz for hyperthermia, 900 MHz for RFID) in which each unit cell has embedded RFID ICs. In future works, the idea is to break the periodicity and exploit the architecture proposed in this paper to design a wireless programmable lens capable of adaptively routing the field coming from the hyperthermia applicator to the tumor region (Figure 5).

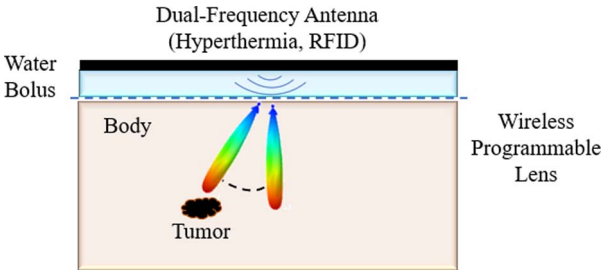


Figure 5. Concept of the programmable lens for adaptive hyperthermia focusing.

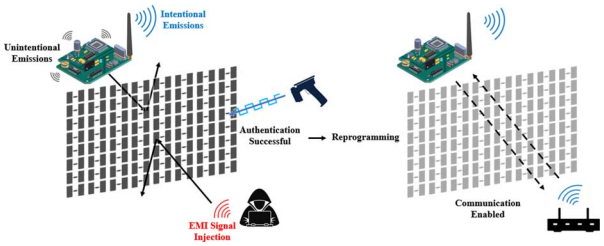


Figure 6. Concept of smart shielding for cyber/physical protection of electronic devices.

3. Smart shielding for cyber/physical security: Electronic devices are not only subject to cyber threats but also to physical threats by means of side-channel attacks [25]. Attackers can determine what the device is doing by intercepting unintended emissions from its electronic components or manipulating sensor readings without changing the underlying physical phenomena [26]. The best countermeasure for this type of attack is to shield the device so as to block both incoming and outgoing electromagnetic fields, but this can also alter the device's functionalities (e.g., block trusted communications). Therefore, the idea is to use wireless programmability to realize a wireless programmable FSS (smart shield) capable of being an electromagnetic shield or an invisible structure in the frequency band of interest, as needed. In other words, the FSS electromagnetically isolates the device until a successful authentication process with the wireless controllers (RFID ICs) allows the smart shield to be reprogrammed and become electromagnetically transparent (Figure 6).

## 4. References

1. C. G. Christodoulou, Y. Tawk, S. A. Lane, and S. R. Erwin, "Reconfigurable Antennas for Wireless and Space Applications," *Proceedings of the IEEE*, **100**, 7, July 2012, pp. 2250–2261.
2. J. Costantine, Y. Tawk, S. E. Barbin, and C. G. Christodoulou, "Reconfigurable Antennas: Design and Applications," *Proceedings of the IEEE*, **103**, 3, March 2015, pp. 424–437.
3. M. Li, Z. Zhang, M.-C. Tang, L. Zhu, and N.-W. Liu, "Bandwidth Enhancement and Size Reduction of a Low-Profile Polarization-Reconfigurable Antenna by Utilizing Multiple Resonances," *IEEE Transactions on Antennas and Propagation*, **70**, 2, February 2022, pp. 1517–1522.
4. U. Musa, S. M. Shah, H. A. Majid, Z. Z. Abidin, M. S. Yahya, et al., "Recent Advancement of Wearable Reconfigurable Antenna Technologies: A Review," *IEEE Access*, 10, November 2022, pp. 121831–121863.
5. D. Piazza, N. J. Kirsch, A. Forenza, R. W. Heath, and K. R. Dandekar, "Design and Evaluation of a Reconfigurable

Antenna Array for MIMO Systems," *IEEE Transactions on Antennas and Propagation*, **56**, 3, March 2008, pp. 869–881.
6. Y. Wang, F. Xu, Y.-Q. Jin, and Z. Du, "Low-Cost Reconfigurable 1 bit Millimeter-Wave Array Antenna for Mobile Terminals," *IEEE Transactions on Antennas and Propagation*, **70**, 6, January 2022, pp. 4507–4517.
7. M. Abdollahvand, K. Forooraghi, Z. Atlasbaf, E. Martinez-de-Rioja, J. A. Encinar, et al., "Reconfigurable FSS Based on PIN Diodes for Shared-Aperture X/Ka-Band Antennas," 2021 15th European Conference on Antennas and Propagation (EuCAP), Dusseldorf, Germany, March 2021, pp. 1–4.
8. H. Zhang, B. Di, L. Song, and Z. Han, *Reconfigurable Intelligent Surface - Empowered 6G*, Springer, 2021.
9. Y. Liu, X. Liu, X. Mu, T. Hou, J Xu, et al., "Reconfigurable Intelligent Surfaces: Principles and Opportunities," *IEEE Communications Surveys & Tutorials*, **23**, 3, May 2021, pp. 1546–1577.
10. N. Ojaroudi Parchin, H. Jahanbakhsh Basherlou, Y. I. Al-Yasir, A.M. Abdulkhaleq, and R.A. Abd-Alhameed, "Reconfigurable Antennas: Switching Techniques-A Survey," *Electronics*, **9**, 2, February 2020, p. 336.
11. H. S. Munawar, "An Overview of Reconfigurable Antennas for Wireless Body Area Networks and Possible Future Prospects," *International Journal of Wireless and Microwave Technologies*, **10**, 2, April 2020, pp. 1–8.
12. D. Dobkin, *The RF in RFID: UHF RFID in Practice*, Oxford, UK, Newnes, 2012.
13. em microelelctronic, "EM4325 Datasheet," https://www.emmicroelectronic.com/sites/default/files/products/datasheets/4325-DS%20%28updated%20datasheet%20Feb%202023%29.pdf (Accessed 3 April 2023).
14. em microelelctronic, "Rain RFID Transponder IC with Capacitive Sensor Interface," https://www.emmicroelectronic.com/sites/default/files/products/datasheets/4152-DS%20v4.2.pdf (Accessed 3 April 2023).
15. A. Mostaccio, S. Amendola, N. D'Uva, C. Occhiuzzi, E. Martinelli and G. Marrocco, "Ultra-Low Power RFID-Based Wake-Up Architectures for Wireless Sensor Networks in Industrial Plants," 2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA), Aveiro, Portugal, September 2023, pp. 146–149.
16. I. Vardakis, G. Kotridis, S. Peppas, K. Skyvalakis, G. Vougioukas, et al., "Intelligently Wireless Batteryless RF-Powered Reconfigurable Surface: Theory, Implementation & Limitations," *IEEE Transactions on Wireless Communications*, **22**, 6, June 2023, pp. 3942–3954.
17. F. Lestini, G. Marrocco, and C. Occhiuzzi, "Feasibility of RFID-Based Control of Reconfigurable Intelligent Surfaces (RISs) for Wireless Communication Systems," 2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA), Aveiro, Portugal, September 2023, pp. 241–244.
18. GS1. "EPC Radio-Frequency Identity Protocols Generation 2 UHF RFID Standard," https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf (Accessed 2 January 2023).
19. A. Sample and J. R. Smith, "Experimental Results with Two Wireless Power Transfer Systems," 2009 IEEE Radio and Wireless Symposium, San Diego, CA, USA, January 2009, pp. 16–18.
20. M. Schink, A. Wagner, F. Unterstein, and J. Heyszl, "Security and Trust in Open Source Security Tokens", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, **2021**, 3, July 2021, pp. 176–201.
21. C. Occhiuzzi, S. Parrella, F. Camera, S. Nappi, and G. Marrocco," RFID-Based Dual-Chip Epidermal Sensing Platform for Human Skin Monitoring," *IEEE Sensors Journal*, **21**, 4, February 2021, pp. 5359–5367.
22. G. Marrocco, "The art of UHF RFID antenna design: impedance-matching and size-reduction techniques," *IEEE Antennas and Propagation Magazine*, **50**, 1, February 2008, pp. 66–79.
23. F. Amato, C. Occhiuzzi, and G. Marrocco," Epidermal Backscattering Antennas in the 5G Framework: Performance and Perspectives," *IEEE Journal of Radio Frequency Identification*, **4**, 3, September 2020, pp. 176–185.
24. F. Lestini, N. Panunzio, G. Marrocco, and C. Occhiuzzi," Epidermal RFID-Based Thermal Monitoring Sheet (R-TMS) for Microwave Hyperthermia," *IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology*, **7**, 4, August 2023, pp. 365–374.
25. Z. Martinasek, V. Zeman, and K. Trasy, "Simple electromagnetic analysis in cryptography," *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, **1**, 1, July 2012, pp. 13–19.
26. D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, et al.," Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, May 2013, pp. 145–159.