Passive Wireless Programmable FSS for Adaptive Electromagnetic Shielding of Implanted Medical Devices

Francesco Lestini, *Member, IEEE*, Gaetano Marrocco, *Senior Member, IEEE*, and Cecilia Occhiuzzi, *Member, IEEE*

***Abstract*—Implantable Medical Devices (IMDs) such as pacemakers and defibrillators increasingly rely on wireless connectivity for remote monitoring and programming. However, this wireless access introduces significant cybersecurity and physical vulnerabilities, making IMDs susceptible to unauthorized access and electromagnetic interference (EMI). This paper proposes a wirelessly programmable smart shield based on a reconfigurable Frequency Selective Surface (P-FSS) as a novel defense mechanism for IMD security. The shield dynamically transitions between shielding and transparency states, passively controlled by an RFID-powered circuit, ensuring protection from malicious attacks while enabling authorized medical communication. This study extends prior theoretical investigations by introducing a fully functional prototype, realized with a rigorous design methodology and leveraging low-power varactor-based switching to enhance efficiency and miniaturize the size. The system demonstrates over 40 dB of shielding effectiveness in the Medical Implant Communication Service (MICS) band (401–406 MHz) while allowing controlled transparency via a battery-less RFID interface with an activation distance of 0.6 m. Experimental validation confirms the practical feasibility of the proposed approach, making it a viable solution for enhancing the cyber-physical security of IMDs.**

***Index Terms*—Cyber security, epidermal antennas, physical security, reconfigurable FSS, RFID, wireless programmability.**

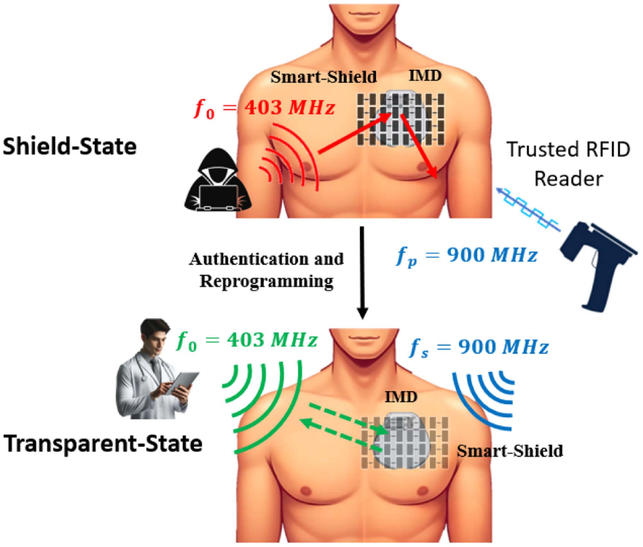


Fig. 1. Concept of reprogrammable smart shield for ICD protection. The FSS blocks all incoming fields at f_0 in the OFF state, while communication is allowed in the ON state. Surface reconfiguration is obtained through tunable components controlled via an RFID reader.

I. Introduction

ACTIVE Implantable Medical Devices (IMDs) are essential tools in modern healthcare, enabling diagnostic, therapeutic, and monitoring functions [1]. These devices, including pacemakers, defibrillators, and neurostimulators, increasingly rely on wireless communication for remote monitoring and programming [2]. Operating within the Medical Implant Communication Service (MICS) band (401–406 MHz) [3], IMDs use low-power RF signals to ensure safe and interference-minimized communication with dedicated external programmers. However, despite encryption and authentication mechanisms [4], wireless connectivity introduces significant cybersecurity and physical vulnerabilities [5] that can compromise patient safety, particularly given that most IMDs fall under high-risk Class III medical devices [6].

IMDs are increasingly exposed to cybersecurity threats such as unauthorized access, data breaches, and electromagnetic interference (EMI) attacks, which can severely affect device functionality [7], [8]. Attackers can exploit vulnerabilities to alter device operation, disrupt telemetry, or accelerate battery depletion through repeated authentication requests [9]. Existing security measures, such as magnet-based switches [10] and wake-up mechanisms [11], offer only partial protection, as they either introduce usability constraints or fail to prevent sophisticated cyber-physical attacks. Since IMDs remain vulnerable to both active cyber intrusions and physical electromagnetic threats [12], additional hardware-based protection strategies

Received 18 February 2025; revised 13 May 2025, 30 June 2025, and 31 July 2025; accepted 25 August 2025. This work was supported in part by Project ECS 0000024 Rome Technopole, under Grant CUP B83C22002820006, in part by NRP Mission 4 Component 2 Investment 1.5, funded by European Union–NextGenerationEU . Spoke: 2. Flagship Project 7, and in part by Project "SEcurity and RIghts In the CyberSpace – SERICS, SPOKE 9" under Grant PE00000014 - CUP B53C22003990006 through the National Recovery and Resilience Plan (NRRP) funded by the European Union – NextGenerationEU. *(Corresponding author: Francesco Lestini.)*

The authors are with the DICII - Tor Vergata University of Rome, 00133 Rome, Italy (e-mail: francesco.lestini@uniroma2.it).

Digital Object Identifier 10.1109/JERM.2025.3604080

have been investigated. Some approaches propose external jammers or cryptographic key exchange devices [13], but these solutions typically rely on active circuitry, increasing power consumption and potentially violating regulatory constraints, such as those set by the FDA [14].

An alternative approach to mitigate these risks is the use of a wirelessly reconfigurable electromagnetic shield that selectively blocks unauthorized signals while enabling secure medical communications. A radio-frequency identification (RFID)-based smart shield was initially introduced in [15], [16] as a passive, two-state programmable barrier for implantable cardiac devices (ICDs). The key principle is based on a programmable frequency selective surface (P-FSS) [17], [18], whose electromagnetic properties can be dynamically adjusted via RFID-controlled switching elements [19]. The shield, embedded within an epidermal patch, is designed to block electromagnetic fields in the MICS band (Fig. 1) and can be selectively reconfigured to enable communication when in a trusted medical environment.

Previous studies have demonstrated the theoretical feasibility of this wirelessly reconfigurable shielding system through numerical simulations but lacked experimental validation [16]. This work extends the concept by providing the first experimental realization of a fully functional, passive, and wirelessly programmable electromagnetic shield. The proposed system is developed through a rigorous designing methodology, addressing key challenges such as energy-efficient reconfiguration, robustness of the switching mechanism, and practical integration into an epidermal patch. The use of ultra-low-power varactor-based switching, combined with a compact and scalable layout, ensures that the shield can be effectively deployed in real clinical environments.

The remainder of the paper is organized as follows. Section II introduces the rationale behind the proposed shielding mechanism, explaining the operating principles of the programmable unit cell and the key parameters influencing its performance. Section III presents the optimized P-FSS design, while Section IV evaluates its simulated behavior under different polarization modes. Section V describes the physical implementation of the shield, including the biasing network for the tunable components and the integrated RFID antennas for wireless programmability. Section VI reports on the fabrication of prototypes and experimental validation, assessing both the shielding effectiveness and the wireless communication and programming capabilities. Finally, Section VII summarizes the findings and discusses future research directions.

II. Rationale

The proposed smart-shield dynamically modulates its electromagnetic properties to protect IMDs from unauthorized signals while permitting secure communication with trusted external programmers. Structured as a P-FSS, it consists of an array of $N = L \times M$ unit cells, each integrating $K = 4$ varactor diodes. By adjusting their impedance in response to the applied bias voltage, these diodes enable a tunable frequency-selective behavior.

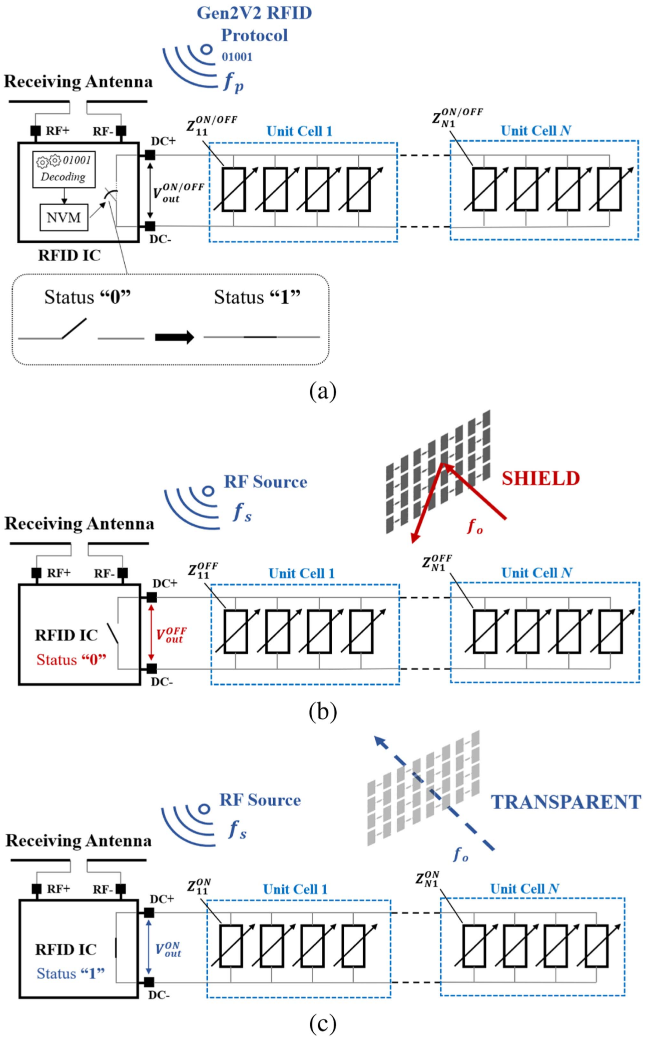


Fig. 2. Schematic illustration of the smart-shield reconfiguration and operation mechanisms. (a) The RFID IC harvests energy and receives digital commands through a dedicated antenna connected to the RF ports, thus applying the appropriate output voltage to the varactors via its DC terminals. (b) In the OFF state, with the internal memory set to 0 or in the absence of sufficient RF power, the output remains low, and the FSS blocks incoming waves at the target frequency f_o. (c) In the ON state, when the memory is set to 1 and the RF power exceeds the threshold p_o, a high output voltage is applied, switching the FSS to its transparent state and enabling authorized communication.

As illustrated in Fig. 2(a), the reconfiguration mechanism relies on a wireless, battery-less interface based on backscattering communication. Each unit cell is coupled to an RFID Integrated Circuit (IC), which operates in the Ultra-High-Frequency (UHF) band ($f_p = 860 - 960$ MHz). The IC harvests energy and receives digital commands wirelessly through a dedicated receiving antenna, connected to its RF ports (RF+ and RF-). Upon successful decoding of the command, the IC updates its internal Non-Volatile Memory (NVM) ($Status\,0 \leftrightarrow Status\,1$) and adjusts the output voltage accordingly $\left(V_{out}^{OFF} \leftrightarrow V_{out}^{ON}\right)$. This control voltage is delivered through the DC terminals (DC+ and DC-), which bias the K varactor diodes embedded in each unit cell, thereby modifying their impedance $\left(Z_{n,k}^{OFF} \leftrightarrow Z_{n,k}^{ON}, \forall \{n,k\}\right)$ and reconfiguring the electromagnetic response of the FSS with 1-bit reconfigurability.

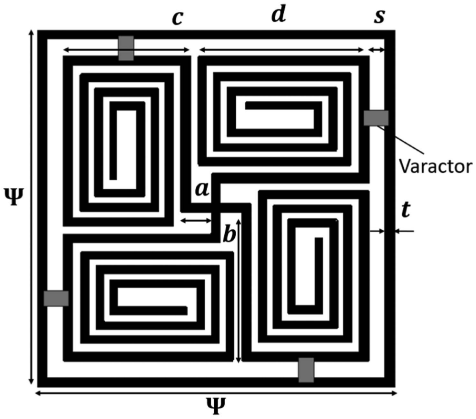


Fig. 3. Layout of the unit cell. Ψ is the periodicity.

During normal operation, the ICs are wirelessly powered by an external RF field at $f_s = 860 - 960$ MHz (*power-up frequency*), which can be generated by the same RFID reader or by any unmodulated RF source. Once powered, the IC reads its internal memory to retrieve the stored state and deliver the output voltage accordingly. If the stored status is 0 (Fig. 2(b)), the FSS is in the shielding (OFF) state, preventing malicious EMI and unauthorized access by blocking electromagnetic waves in the MICS band ($f_o = 401 - 406$ MHz). Conversely, if the status is set to 1 (Fig. 2(c)), the FSS enters the transparent (ON) state, thus restoring the communication at f_o by switching the impedance states of the K varactor diodes per unit cell $\left(Z_{n,k}^{OFF} \rightarrow Z_{n,k}^{ON}, \forall \{n,k\}\right)$.

It is worth noticing that the ON state is achieved only if two conditions are met: *i)* the IC is correctly programmed by the RFID reader, and *ii)* the received power at f_s exceeds the activation sensitivity threshold p_o [20]. Otherwise, the IC maintains V_{out}^{OFF}, keeping the shield in the OFF state. This architecture ensures that, in the absence of both a valid RFID command and sufficient RF power, the system reliably remains in its default shielding mode, providing robust, fail-safe protection. Moreover, this operational mechanism ensures robust and secure functionality even in RF-dense environments, such as clinical scenarios, where multiple sources may exist. Indeed, the shield can only be toggled via an intentional, authenticated interaction with a trusted RFID reader, for instance, through untraceable commands or cryptographic challenge-response protocols [21].

III. Unit Cell Layout

The layout of the unit cell is shown in Fig. 3. It consists of two resonators connected in parallel through four programmable varactors. The central conductive element is a meandered cross-shaped resonator surrounded by an inductive loop. The external arms of the meandered cross are folded into compact rectangular spirals, maximizing the use of available area and effectively reducing the overall size of the unit cell to make the footprint of the entire device compatible with the typical constraints of epidermal integration. The selected configuration stems from the design framework introduced in [22], where four varactor diodes are placed between an internal resonator and an external grid to allow for parallel DC biasing and polarization-insensitive frequency behaviour. In particular, the choice of four varactors respects the circular symmetry of the unit cell. This approach also permits using a single RF choke for RF/DC isolation, significantly simplifying the bias network. Additionally, this type of geometry inherently supports multiple resonances [23], enabling different frequency-selective behaviors depending on the state of the tunable elements. Finally, the layout offers a perfect circular symmetry, responding independently of the polarization of the incident wave.

According to [22], an FSS with this geometry can be approximated as a passive LC-resonant circuit functioning as a second-order bandpass filter. Consequently, the FSS transmission coefficient S_{21} exhibits two characteristic frequencies: the resonant frequency (f_r) and the anti-resonant frequency (f_{ar}). At f_r, the equivalent impedance of the structure approaches zero, resulting in strong induced surface currents and, consequently, in almost complete reflection of the incident wave. Conversely, at f_{ar}, the equivalent admittance of the structure is minimized, reducing the surface current density and enabling transmission of the incident wave with minimal attenuation [24]. The fundamental condition for designing a smart shield capable of completely reflecting or transmitting the incident field at $f_o = 403$ MHz is given by:

$$\begin{cases} f_r = f_o, & \text{if } V_{out} = V_{out}^{OFF} \rightarrow Z_{n,k}^{OFF}, \forall \{n,k\} \\ f_{ar} = f_o, & \text{if } V_{out} = V_{out}^{ON} \rightarrow Z_{n,k}^{ON}, \forall \{n,k\} \end{cases} \tag{1}$$

This dual-frequency condition imposes non-trivial constraints on the unit cell design, especially in the context of the proposed RFID-based programming approach, which can only toggle between two discrete varactor capacitance states. As a result, the geometry of the FSS must be carefully optimized to ensure that the structure meets both electromagnetic states, shielding and transparency, under strict tuning limitations. Specifically, the magnitude of the transmission coefficient S_{21} should be minimized in the OFF state ($S_{21,S}$) and maximized in the ON state ($S_{21,T}$) to closely match its value in the reference case (S_{21}^{ref}), i.e., when the P-FSS is absent.

A. Parametric Analysis

The impact of the unit cell geometric parameters on the resonant frequency in the OFF state and on the anti-resonant frequency in the ON state is here evaluated through a parametric analysis. The corresponding absolute value of the S_{21} is also considered. Simulations were carried out in CST Microwave Studio 2024 under the hypothesis of infinite periodic structure [17][1] (Fig. 4). The unit cell was laid on a biocompatible and flexible substrate (0.8 mm thick, $\varepsilon_r = 4.3$, $\tan\delta = 0.025$) placed above a three-layered human body phantom [26]. Two Floquet ports, illuminating the structure with a TE or TM polarized uniform plane wave, were considered to evaluate the shielding properties

[1] Periodic Boundary Conditions (PBCs) consisting of the repetition of electric and magnetic walls are imposed on the lateral boundaries of the unit cell to enforce periodicity [17], [25].

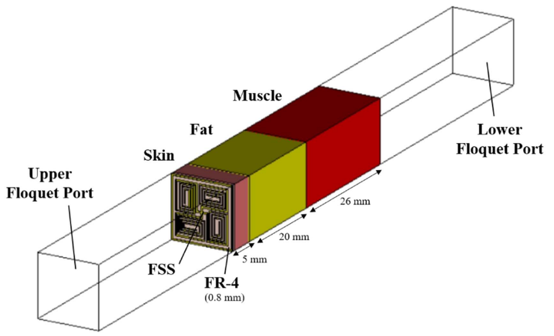


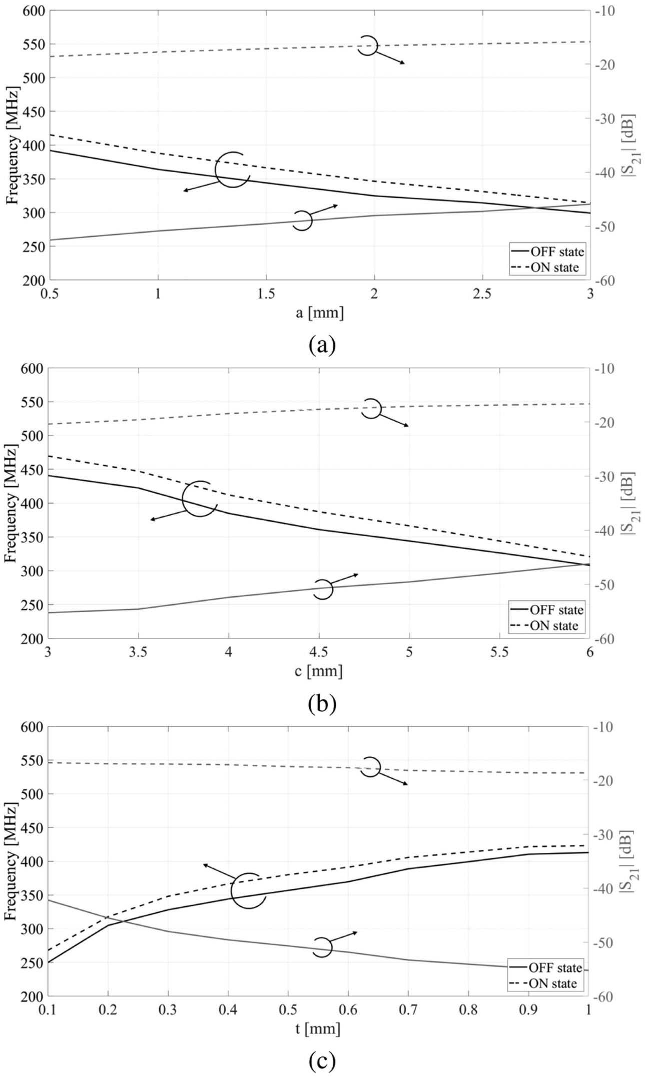
Fig. 4. Unit cell simulation setup under periodic boundary conditions. The numerical layered phantom consists of skin ($\varepsilon_r = 48.3$, $\sigma = 0.7$ S/m, $thickness = 5$ mm), fat ($\varepsilon_r = 5.57$, $\sigma = 0.04$ S/m, $thickness = 20$ mm), and muscle ($\varepsilon_r = 57$, $\sigma = 0.8$ S/m, $thickness = 26$ mm).

of the FSS [17], [25], [27]. Both ports were placed at a sufficient distance ($\geq \lambda/4$) from the structure to ensure that evanescent Floquet modes decay before reaching the ports [28]. The gap between the central conductive element and the surrounding loop is fixed at $s = 0.6$ mm to house the varactor, while the arms lengths $b = a + c - t/2$ and $d = \Psi/2 - s + a - 2t$ (being $\Psi = 2a + 2c + 3t + 2s$ the cell periodicity) are constrained to other design parameters to ensure symmetry with respect to the incident field. Due to the relationship between the geometrical parameters in Fig. 3, only a, c, and t were considered in this parametric study. The starting values were chosen as $a = 1.5\,\text{mm}$, $c = 5\,\text{mm}$, $t = 0.5\,\text{mm}$, as they allow for an overall periodicity of $\Psi = 16\,\text{mm} \approx \lambda_{eff}/10$, where $\lambda_{eff} = \lambda_0/\sqrt{\varepsilon_{eff}}$ is the free-space wavelength scaled by the square root of the effective permittivity ε_{eff} (calculated as in [29]). Finally, the varactors (SMV1213 [30]) were simulated through their SPICE model, incorporating a variable capacitance $C_j(V_{out})$ (with $C_j(V_{out}^{OFF}) = 28.9\,pF$ and $C_j(V_{out}^{ON}) = 10.74\,pF$) and parasitic effects characterized by an inductance $L_s = 0.14\,nH$, a capacitance $C_p = 2.2\,pF$, and a resistance $R_s = 1.4\,\Omega$ [31].

Results are presented in Fig. 5. The resonator arm lengths, a and c, exhibit a similar influence on both f_r and f_{ar}, causing a shift towards lower frequencies as their values increase. Likewise, the absolute values of $S_{21,S}$ and $S_{21,T}$ are directly proportional to the resonator arm lengths. Conversely, the trace width t is inversely proportional to the resonant and anti-resonant frequencies, while it directly affects the magnitude of the transmission coefficient in the OFF state with a minimal impact on $S_{21,T}$. These trends fully agree with the findings in [22].

B. Design

Starting from the parametric analysis, the final layout of the unit cell was retrieved by an optimization process aimed at achieving the smart shield condition (1) and tuning the values of $S_{21,S}$ and $S_{21,T}$. To account for the biasing circuitry, two orthogonally arranged traces were also included beneath the FSS in the unit cell model. The trace width is set to $t = 0.3$ mm to facilitate fabrication. Consequently, optimization is performed on the remaining parameters a and c, relying on the minimization of the following penalty function [32]:



(a)

(b)

(c)

Fig. 5. Parametric study of resonant/anti-resonant frequency and corresponding S_{21} magnitude as a function of geometrical parameters (a) a, (b) c, and (c) t. Specifically, continuous lines represent f_r and $|S_{21,S}|$ in the OFF(shielding)-state, while dashed lines denote f_{ar} and $|S_{21,T}|$ in the ON(transparent)-case.

$$U(\underline{\alpha}) = \sum_{i=1}^{2} \delta_i u_i(\underline{\alpha}), \tag{2}$$

where $\underline{\alpha} = \{\alpha_1,\ \alpha_2\} = \{a,\ c\}$, and δ_i are the weights that must be chosen so that $\sum_i \delta_i = 1$ [32]. $u_i(\underline{\alpha})$ are the sub-penalties to be minimized, defined as:

$$\begin{cases} u_1 = S_{21,T}^0 \cdot \frac{1}{S_{21,T}}\ , \\ \\ u_2 = S_{21,S} \cdot \frac{1}{S_{21,S}^0} \end{cases} \tag{3}$$

where u_1 maximizes the transmission coefficient in the ON state, and u_2, minimizes the transmission coefficient in the OFF state, both expressed in linear scale. The normalization parameters $S_{21,T}^0 = S_{21}^{ref}$ and $S_{21,S}^0 = \frac{S_{21}^{ref}}{1000}$ are such that each sub-penalty function is between 0 and 1 and of the same order of magnitude.

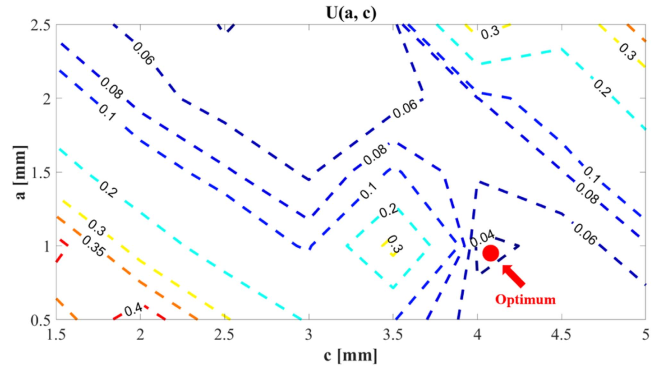


Fig. 6. Contour plots of the penalty function $U(a, c)$ (lower is better). The red dot indicates the optimum configuration: $a = 0.9\,\mathrm{mm}$, $b = 4.85\,\mathrm{mm}$, $c = 4.1\,\mathrm{mm}$, $d = 5.9\,\mathrm{mm}$, $\Psi = 12.4\,\mathrm{mm}$.

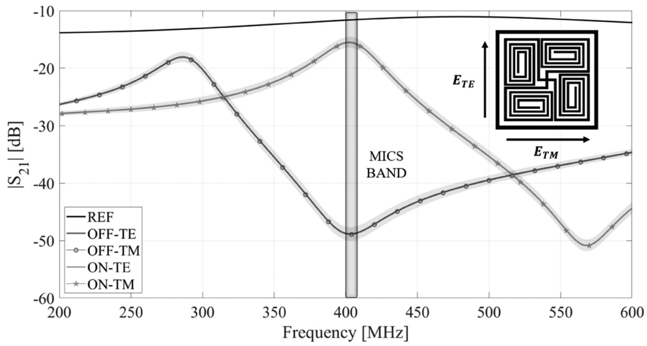


Fig. 7. Transmission coefficient under linearly polarized incident waves. “REF” indicates the cell’s response without the P-FSS. Shadowed area corresponds to the expected variation caused by human variability, here emulated through a ±20% variation of the dielectric properties listed in Fig. 4.

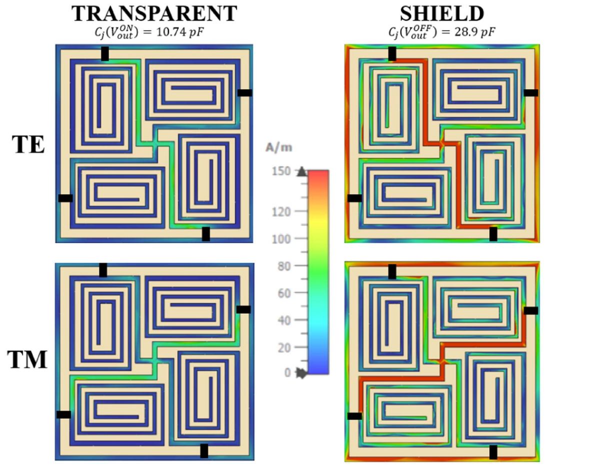

TRANSPARENT
$C_j(V_{out}^{ON}) = 10.74\ pF$
SHIELD
$C_j(V_{out}^{OFF}) = 28.9\ pF$
TE
TM
A/m
150
120
100
80
60
40
20
0

Fig. 8. Surface currents for both operational states (shielding-transparent) under TE and TM polarizations of the incident field.

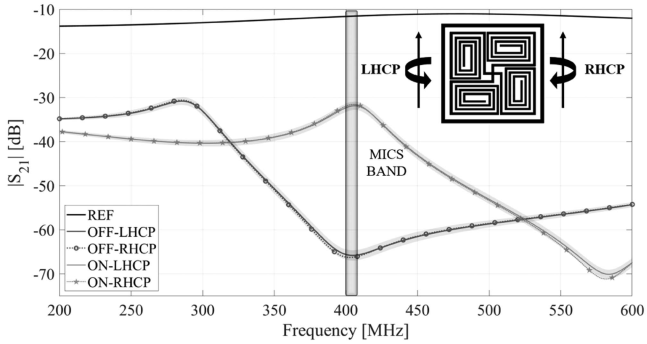


Fig. 9. Transmission coefficient under circularly polarized incident waves. “REF” indicates the cell’s response without the P-FSS. Shadowed area corresponds to the expected variation caused by human variability, as outlined in Fig. 7.

Result is shown in Fig. 6, highliting that the optimal geometrical configuration corresponds to $a = 0.9\,\mathrm{mm}$ and $c = 4.1\,\mathrm{mm}$, reflecting an overall cell dimension $\Psi = 12.4\,\mathrm{mm}$.

Fig. 7 shows the transmission coefficient S_{21} calculated for the optimum layout of the unit cell under a linearly Transverse Electric (TE) and Transverse Magnetic (TM) polarized incident wave. The FSS is shielding the impinging field in the MICS band with $S_{21,S} = -49\,dB$ when V_{out}^{OFF} is applied. On the other hand, when the applied voltage is V_{out}^{ON}, the anti-resonant frequency is shifted in the MICS band, achieving good transparency ($S_{21,T} = -16\,dB$). The contrast in the transmission coefficient between the two states is $\Delta S_{21}^{S,T} = 30\,dB$, while between the reference case (S_{21}^{ref}) and the transparent state is only $\Delta S_{21}^{ref,T} = 4\,dB$. Furthermore, due to the structural symmetry of the unit cell, the S_{21} remains unchanged for both TE and TM) polarizations (Fig. 7). This invariance is also highlighted in Fig. 8, which depicts the surface current distributions at the frequency of $f_o = 403\ MHz$ for both operational states under TE and TM polarizations, showing that the surface currents are significantly higher in the shield state for both the central conductive element and the surrounding loop.

The shielding properties of the proposed wireless reconfigurable FSS were also analyzed by considering left-handed and right-handed circularly polarized incident waves. Results for the transmission coefficient are visible in Fig. 9. The variation ΔS_{21} is equal to the case of a linear polarized impinging wave, but both resonance and anti-resonance exhibit a lower S_{21} in the MICS band (-65dB and -35dB, respectively). This is primarily attributed to the increased losses introduced by the human body, resulting from the higher current densities flowing through the metallic traces in both operational states (Fig. 10).

IV. Finite P-FSS Implementation

After defining the final layout of the unit cell, their $N = L \times M$ number was retrieved by balancing constraints related to the effectiveness of the operation of the FSS and the size of the final layout. Thus, $N = 6 \times 6 = 36$ unit cells were adopted to fit an overall dimension of 74.4 mm × 74.4 mm (Fig. 11(a)), which is compatible with commercial epidermal patches [33] and can adequately cover and protect the ICD (whose standard dimension is ≈45 mm × 43 mm). The structure consequently integrates $K = 144$ varactors in total, and the overall power consumption

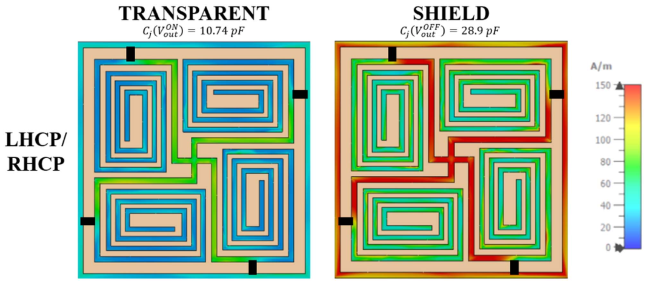

TRANSPARENT
$C_j(V_{out}^{ON}) = 10.74\ pF$
SHIELD
$C_j(V_{out}^{OFF}) = 28.9\ pF$
LHCP/
RHCP
A/m
150
120
100
80
60
40
20
0

Fig. 10. Surface currents for both operational states (shielding-transparent) under LHCP and RHCP polarization of the incident field.

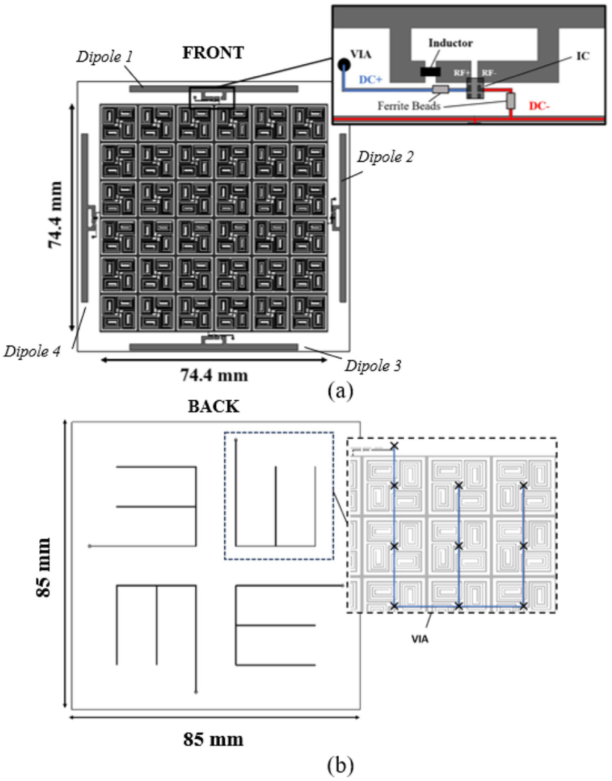


Fig. 11. (a) Front view of the final layout comprising 6 × 6 unit cells and 4 surrounding dipoles for wireless reconfiguration. (b) Back-side connections. The final size of the P-FSS comprising the RFID antennas is 85 × 85 mm.

is $P_{tot} = K \cdot P_{var} = 5.3\,\mu$W, where $P_{var} = 0.037\,\mu$W is the power consumed by one varactor with 1.8 V applied voltage.

Wireless programmability is achieved by integrating four RFID ICs in the final layout, such that each RFID IC is responsible for a sub-array of 9 unit cells, driving 36 varactors in total (Fig. 11) with a total required power $P_{out}^{IC} = 1.33\,\mu$W. The selected IC is the EM4152 [34] ($Z_{IC} = 17.6 - j271.9\ \Omega$ [34]), which is totally passive, with *power sensitivity* (i.e., the minimum required power to establish communication) $p_{chip} = -18$ dBm, with *programming sensitivity* (i.e., the minimum required power to program the IC) $p_w = -13.5$ dBm and *activation sensitivity* (i.e., the minimum power needed for DC voltage delivery) $p_o = -17\,dBm$ in case ultra-low power components such as varactors are connected to the output port. If the RF power reaching the IC exceeds p_o, the output voltage reaches its maximum value of $V_{out}^{\max} = 1.8$ V, while the maximum DC output power is $P_{out}^{\max} \approx 600\,\mu$W $\gg P_{out}^{IC}$ [20]. ICs were embedded in the final layout through four RFID antennas.

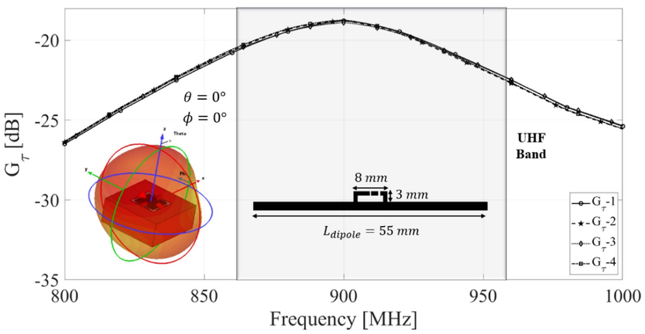


Fig. 12. Simulated realized gains in the broadside direction for the four dipoles surrounding the FSS, labeled as in Fig. 11.

For the sake of symmetry, four dipoles surrounding the FSS following an orthogonal arrangement (Fig. 11(a)) were chosen. Each dipole is matched to the IC impedance Z_{IC} through a T-match [35] and a tuning inductor. Moreover, ferrite beads were also embedded for DC decoupling purposes (Fig. 11(a)). The negative pin of each IC is connected to the surrounding grid of the FSS, thus representing the common ground. On the other hand, the positive pins are connected to the center of the cross-shaped resonator of each unit cell through back-side connections (Fig. 11(b)). Geometrical parameters of the dipoles and tuning inductors were defined by considering the maximization of the *realized gain* G_τ, i.e., the gain G of the antenna scaled by the *power transfer coefficient* τ, which accounts for the impedance mismatch between the antenna and the IC [35]:

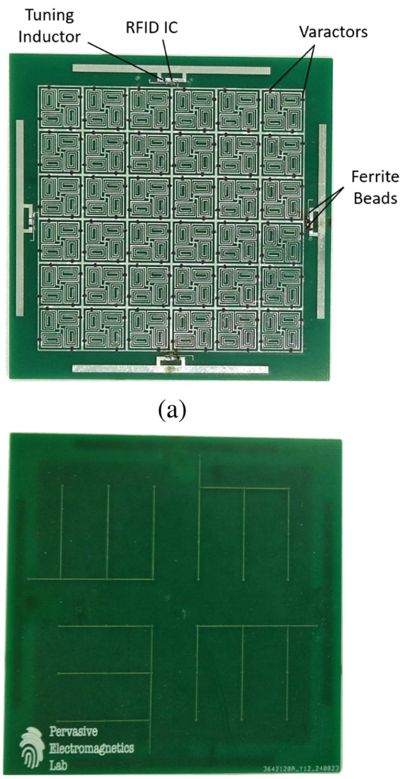
$$\tau = \frac{4R_{IC} \cdot R_A^{in}}{|Z_{IC} + Z_A^{in}|^2}\,. \tag{4}$$

In (4), the term $Z_A^{in} = R_A^{in} + jX_A^{in}$ is the impedance of the antenna, while $Z_{IC}^{in} = R_{IC}^{in} + jX_{IC}^{in}$ is the IC complex impedance. The simulated results are shown in Fig. 12. The maximum gain is $G_\tau^{\max}(\theta_b, \phi_b) = -18\,dB$ at $f = 900$ MHz in the broadside direction $\theta_b = \phi_b = 0°$ and is the same for all the dipoles, confirming no coupling between them, thanks to the orthogonal arrangements and the presence of the human body [27]. Moreover, the achieved G_τ is consistent with the typical performances of on-skin antennas [36].

The maximum distance for both reprogramming and activation can be computed through the following [35]:

$$d_{w,o}^{\max} = \frac{\lambda_0}{4\pi} \cdot \sqrt{\frac{\mathrm{EIRP}_R \cdot G_\tau(\theta_b, \phi_b) \cdot \eta_p}{p_{w,o}}}\,, \tag{5}$$

where λ_0 is the free-space wavelength, $\mathrm{EIRP}_R = 3.2\,W$ is the effective power transmitted by the RFID reader, and η_p is the polarization loss factor, which is equal to 0.5 since the incident field must be circularly polarized to energize all the ICs simultaneously. Thus, the theoretical maximum programming distance is $d_w^{\max} = 0.6$ m, while the maximum activation distance is $d_o^{\max} = 0.8$ m.



(a)

(b)

Fig. 13. Fabricated prototype of the smart-shield. (a) Front view. (b) Back view.

V. Prototype and Measurements

For the sake of prototyping, the smart-shield was realized by etching copper from a 0.8 mm-thick FR-4 Printed Circuit Board (PCB). The electronic components (ICs, varactors, inductances, and ferrite beads) were soldered with the help of a bench soldering iron. The resulting prototype is shown in Fig. 13. Two sets of measurements were carried out to evaluate the proposed system's communication link (@900 MHz) and shielding properties (@400 MHz). Reconfigurability in terms of maximum activation distance was also evaluated. In all the measurements, the shield lies on a gelatinous (20 cm × 20 cm × 5 cm) phantom (by AET [37]), resembling the human muscle, which is placed on a cardboard frame to maintain an upright position.

A. Communication Link @900 MHz

1) Setup: The communication link was evaluated through a circularly polarized antenna (patch with broadside gain $G_R = 7.5\ dBic$) placed at a fixed distance $d = 30$ cm from the FSS in the broadside direction. The reader antenna was connected to the Voyantic TagFormance UHF Pro station to measure the realized gains, which were retrieved through the turn-on power method [38].

2) Results: Fig. 14 compares the measured realized gains G_τ^{meas} of each of the four dipoles surrounding the FSS with the simulated realized gain $\overline{G_\tau^{sim}}$, which is calculated as the average of the simulated gains of these dipoles, all in the broadside direction. The plot highlights a good agreement between measurement and simulation. In particular, the maximum measured realized gain is approximately $G_\tau^{meas,max} = -20$ dB for all dipoles, only 2dB lower than the simulated one. Therefore, the measured maximum programming distance is $d_w^{\max} = 0.5$ m.

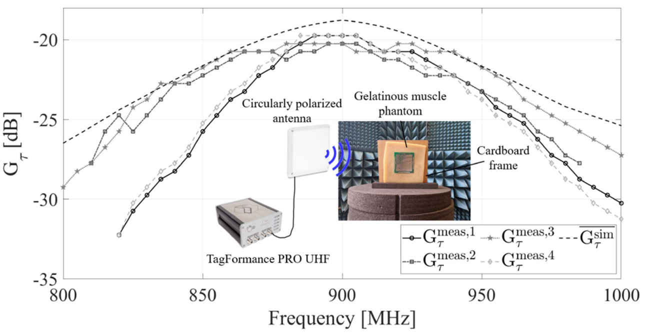


Fig. 14. Measured realized gains for the four dipoles surrounding the FSS, labeled as in Fig. 11. In the inset, the measurement setup.

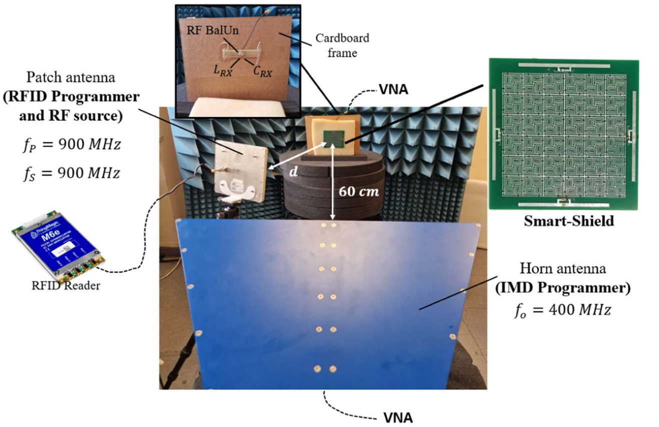


Fig. 15. Measurement setup for evaluating the shielding properties of the FSS in the MICS band.

B. Shielding Properties @400 MHz

1) Setup: The transmitting antenna, emulating the ICD programmer, is a broadband dual-ridge horn (SH-400 [39]). The receiving antenna, simulating the ICD, instead, is a dipole ($L_{dipole} = 55$ mm) adapted to $f = 400$ MHz through an LC-network ($L_{RX} = 75$ nH, $C_{RX} = 10$ pF) and electrically balanced through an RF BalUn [40] (Fig. 15). The SH-400 was placed 60 cm away from the FSS. The receiving dipole was placed behind the muscle phantom, attached to the cardboard frame (Fig. 15). The transmitting and receiving antennas were connected to the Pico108 Vector Network Analyzer (VNA) [41] to evaluate the scattering parameters between them. Since the horn and the dipole are both linearly polarized, three polarizations were considered for the incident field: horizontal, vertical, and oblique (45°). For each polarization, the horn and the dipole were rotated accordingly to be aligned, as the rotation axis coincided with the propagation direction of the field. Finally, wireless

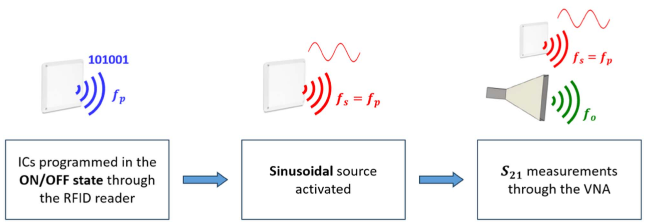

101001
f_p
$f_s = f_p$
$f_s = f_p$
f_o
ICs programmed in the ON/OFF state through the RFID reader
Sinusoidal source activated
S_{21} measurements through the VNA

Fig. 16. Measurement protocol @400 MHz.

TABLE I
COMPARISON BETWEEN SIMULATED AND MEASURED TRANSMISSION COEFFICIENTS IN BOTH SHIELDING AND TRANSPARENT STATES

	$S_{21,S}$ [dB]	$S_{21,T}$ [dB]
Simulated	-49	-16
Measured *(horizontal)*	-44.4	-14.6
Measured *(vertical)*	-44	-14
Measured *(oblique)*	-44.5	-15.6

programmability and power activation were achieved through the same patch antenna used to evaluate the communication link connected to the Thing-Magic M6E RFID reader.

The measurement protocol is shown in Fig. 16. Before starting the measurement of the transmission coefficient S_{21} between the horn and the receiving dipole, each RFID IC was programmed in the ON/OFF state by means of the RFID reader antenna sending a modulated signal at f_w. Then, the same antenna was used as a sinusoidal source at $f_s = f_p$ for activating the ICs, and S_{21} measurements were performed at f_0.

2) Results: Fig. 17 shows the measured transmission coefficients for different polarizations. To ensure a meaningful comparison between simulations and measurements, the measured transmission coefficients were normalized to the simulated ones by compensating for systematic discrepancies. Specifically, the reference S_{21}^{ref} was first measured and compared with its simulated counterpart, determining an offset $|\Delta S_{21}| = S_{21}^{meas,ref} - S_{21}^{sim,ref}$ in the MICS band. This correction was then applied to all measured data to align the transmission characteristics with those obtained in simulations.

Results are summarized in Table I, highlighting a good agreement at least in the MICS band, where, regardless of the polarization of the incident wave, a difference of about 30 dB is measured between the ON and OFF states. The higher differences outside the MICS band, visible in both the reference and P-FSS measurements, can be attributed to the physical limitations of the transmitting antenna (whose lower band frequency is ∼300 MHz) and the receiving dipole (which has a narrow bandwidth centered at 400 MHz) as well as to possible truncation effects related to the finite size of the FSS. The same considerations apply to the measured shielding effectiveness $SE_{dB} = S_{21}^{ref} - S_{21}^{shield}$ [42] (Fig. 18), which highlights the reconfigurability of the smart shield within the MICS band and its shielding properties regardless of the polarization of the incident field.

The maximum reconfigurability distance was determined by analyzing the variation of the transmission coefficient S_{21} as a

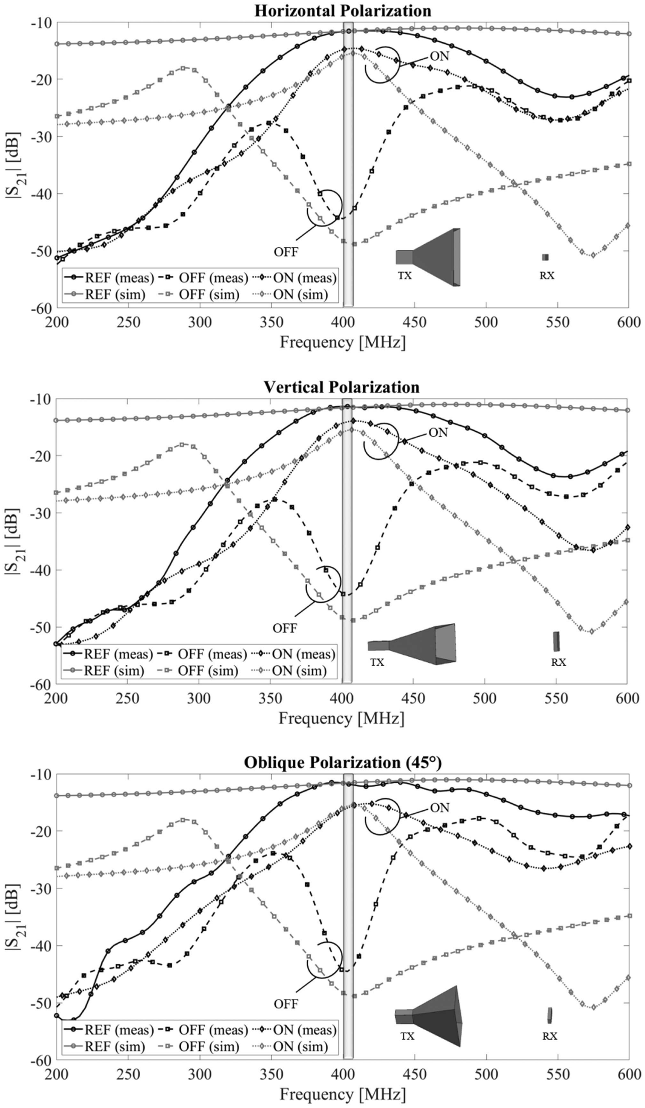


Fig. 17. Measured transmission coefficient S_{21} for the shielding and transparent states under different polarizations of the incoming field. Shadowed, the MICS band. “REF” indicates the FSS’s response without the P-FSS.

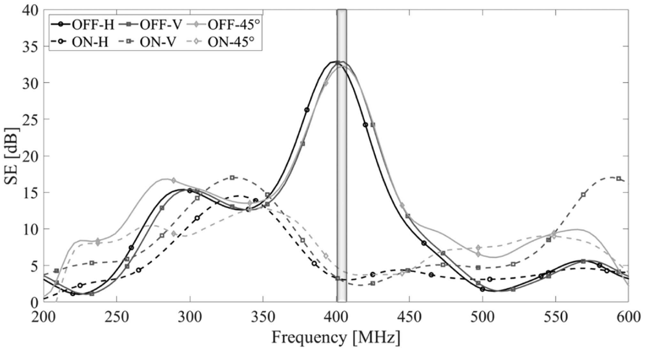


Fig. 18. Measured shielding effectiveness of the smart-shield. Shadowed, the MICS band.

TABLE II
COMPARATIVE OVERVIEW OF EXISTING SECURITY MECHANISMS FOR IMDS, INCLUDING PHYSICAL, CYBER, AND HYBRID APPROACHES

Approach	Protection Type	Interface	Remote Monitoring	Power Consumption	Advantages	Disadvantages
Cryptography	Cyber	Internal (software-based)	Yes	Moderate	Strong, standardized, no additional device required	Battery and memory consuming for the IMD, limited post-deployment flexibility
Magnetic Switching [10]	Cyber	External	No	N/A	Simple and passive solution, widely used in clinical pacemakers	No authentication required, remote monitoring not allowed, and vulnerable to physical attacks
RF Jammers (IMDShield [13])	Cyber/ Physical	External (wearable)	Yes	High	Effective against unauthorized RF reception, no equipment or software alterations	May interfere with other devices, violate regulatory restrictions, and require continuous supply
Authenticators (Cloaker, IMDGuard [47])	Cyber	External (wearable)	Yes	Moderate	User-controlled, support emergency override	Ineffective if lost or not worn, require continuous power supply, and are vulnerable to physical attacks
Smart Shield (this work)	**Cyber/ Physical**	**External (epidermal)**	**Yes**	**N/A**	**Passive solution, more comfortable, secure, and safe than other external devices, supports emergency override**	**Ineffective if lost or not worn, programming and activation may be affected by skin detachment or anatomical variability**

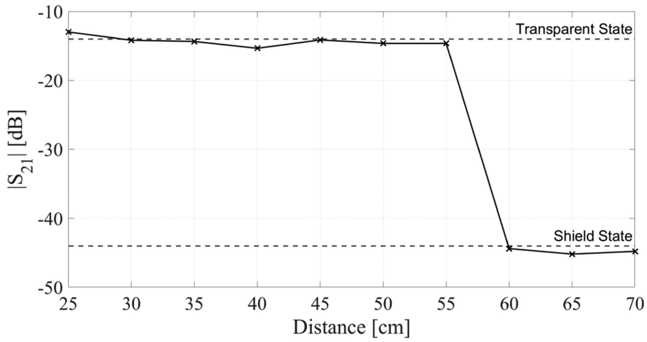


Fig. 19. Measured variation in the transmission coefficient S_{21} as a function of distance at a fixed output power (EIRP$_R = 3.2\,W$).

function of distance at a fixed output power (EIRP$_R = 3.2\,W$) between P-FSS and RF source. This approach identifies the critical threshold beyond which the RF-powered ICs can no longer supply sufficient energy to bias the varactors. Specifically, as long as S_{21} remains near $-16\,dB$, the ICs effectively harvest enough power to sustain the transparent state of the FSS. However, when S_{21} drops to $-44\,dB$, the power delivered to the ICs becomes insufficient to maintain the required DC voltage, causing the FSS to revert to its shielding state, even if previously programmed to be transparent. Experimental results indicate a measured maximum activation distance of $d_o^{\max} = 0.6\,m$ (Fig. 19), closely aligned with the theoretical prediction of $0.7\,m$ (computed assuming $G_\tau^{meas} = -20\,dB$). Therefore, the shield must remain within a safe operating distance of 0.5 m in the broadside direction to ensure reliable programming and activation. This constraint enhances the security of the smart shield, preventing unauthorized activation while effectively safeguarding the implanted device. Finally, this activation distance is fully compliant with international Specific Absorption Rate (SAR) regulations, even under worst-case exposure conditions, e.g., 3.2 W EIRP at 900 MHz [43], [44], and does not pose significant EMC risks to implantable devices [45], while precautions regarding nearby external equipment can be easily met in clinical settings [46].

VI. CONCLUSION

This work represents the first comprehensive experimental validation of an RFID-based wireless reconfigurable FSS, demonstrating the feasibility of the idea and its effectiveness in dynamically protecting Implantable Medical Devices from cyber/physical attacks. The experimental results confirmed the ability to seamlessly switch between two distinct operational states, enabling the structure to function as either a transparent medium or an electromagnetic shield (depending on the programmed state) with a measured shielding effectiveness exceeding 30 dB and a wireless activation distance of 0.6 m. Furthermore, the programmable FSS exhibited robust performance across various polarizations of the incident field, ensuring reliable operation in real-world scenarios. However, the reported activation range refers to optimal conditions (maximum EIRP and antenna alignment); thus, in realistic scenarios, the range may be reduced due to orientation and propagation effects. Similarly, human-induced variability, such as skin curvature, sweat, or partial patch detachment, is expected to impact the 900 MHz RFID link [48] more significantly than the 400 MHz shielding behavior, which should remain stable due to the system's bandwidth and tuning margin. Ongoing experiments are addressing these aspects under realistic conditions. Finally, a key strength of the proposed smart shield lies in its ultra-low power consumption, enabling fully passive and battery-less operation. This feature simplifies integration with epidermal patches and ensures that the solution is highly scalable, making it adaptable to a broad range of biomedical and security applications, thereby representing a viable alternative to existing protection techniques, as summarized in Table II. In this context, it should be highlighted that the shield remains in the OFF state under normal operating conditions and must be reprogrammed and actively powered only for short durations, typically during medical monitoring or device reconfiguration sessions.

Beyond IMD protection, the novel reconfiguration mechanism demonstrated in this work paves the way for future developments in adaptive electromagnetic shielding, programmable wireless security layers, and next-generation wireless systems. Future works will focus on improving the transmission response under circular polarization, on the implementation of programmable shielding at 2.45 GHz (enabling protection of emerging IMD platforms featuring BLE-based telemetry and wake-up signaling), on incorporating advanced authentication protocols, and on testing the shield in a real-world pacemaker-programmer communication scenario. Additionally, we will focus on adopting biocompatible and stretchable materials, such as PDMS (Polydimethylsiloxane) and Ecoflex [49], to enable conformal, skin-integrated, and even implantable implementations. Also, emerging materials such as Laser-Induced Graphene (LIG) on a polymeric precursor, e.g., polyimide films, are under consideration, as they allow the fabrication of stretchable and conductive patterns via direct laser writing, with excellent mechanical compliance and adhesion to the skin through biocompatible substrates like bio-compatible silicone [50].

References

[1] M. Jasim, A. J. A. Al-Gburi, M. Hanif, Z. A. Dayo, M. M. Ismail, and Z. Zakaria, "An extensive review on implantable antennas for biomedical applications: Health considerations, geometries, fabrication techniques, and challenges," *Alexandria Eng. J.*, vol. 112, pp. 110–139, 2025.

[2] E. Kwarteng and M. Cebe, "A survey on security issues in modern implantable devices: Solutions and future issues," *Smart Health*, vol. 25, 2022, Art. no. 100295.

[3] M. N. Islam and M. R. Yuce, "Review of medical implant communication system (MICS) band and network," *ICT Express*, vol. 2, no. 4, pp. 188–194, 2016.

[4] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices," in *Proc. IEEE 5th Int. Symp. Med. Inf. Commun. Technol.*, 2011, pp. 6–9.

[5] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, pp. 305–316, 2015.

[6] "Guidance on classification of medical devices," 2021. [Online]. Available: https://health.ec.europa.eu/system/files/2021-10/mdcg_2021-24_en_0.pdf

[7] D. F. Kune et al., "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Proc. IEEE Symp. Secur. Privacy*, 2013, pp. 145–159.

[8] "Hacking pacemakers, insulin pumps and patients' vital signs in real time," 2018. [Online]. Available: https://www.csoonline.com/article/566025/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html

[9] M. A. Siddiqi, W. A. Serdijn, and C. Strydis, "Zero-power defense done right: Shielding IMDs from battery-depletion attacks," *J. Signal Process. Syst.*, vol. 93, pp. 421–437, 2021.

[10] S. Jacob, S. S. Panaich, R. Maheshwari, J. W. Haddad, B. J. Padanilam, and S. K. John, "Clinical applications of magnets on cardiac rhythm management devices," *Europace*, vol. 13, no. 9, pp. 1222–1230, 2011.

[11] D. Panescu, "Emerging technologies [wireless communication systems for implantable medical devices]," *IEEE Eng. Med. Biol. Mag.*, vol. 27, no. 2, pp. 96–101, Mar./Apr. 2008.

[12] "Medtronic conexus radio frequency telemetry protocol vulnerability," Apr. 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-medical-advisories/icsma-19-080-01

[13] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM SIGCOMM Conf.*, 2011, pp. 2–13.

[14] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in *Proc. IEEE 13th Int. Wireless Commun. Mobile Comput. Conf.*, 2017, pp. 1495–1501.

[15] F. Lestini, A. Marino, G. Marrocco, and C. Occhiuzzi, "Design of an RFID-based wireless programmable smart-shield for implantable medical devices," in *Proc. 9th Int. Conf. Smart Sustain. Technol.*, 2024, pp. 1–4.

[16] F. Lestini, A. Marino, G. Marrocco, and C. Occhiuzzi, "Wireless programmable smart-shield for implantable medical devices physical protection," in *Proc. IEEE Int. Symp. Antennas Propag. INC/USNC-URSI Radio Sci. Meeting*, 2024, pp. 1553–1554.

[17] B. A. Munk, *Frequency Selective Surfaces: Theory and Design*. Hoboken, NJ, USA: Wiley, 2005.

[18] M. Abdollahvand et al., "Reconfigurable FSS based on PIN diodes for shared-aperture X/Ka-band antennas," in *Proc. 15th Eur. Conf. Antennas Propag.*, 2021, pp. 1–4.

[19] F. Lestini, G. Marrocco, and C. Occhiuzzi, "RFID-based reconfigurable electromagnetic devices," *IEEE J. Radio Freq. Identif.*, vol. 8, pp. 226–234, 2024.

[20] F. Lestini, A. DiCarlofelice, P. Tognolatti, G. Marrocco, and C. Occhiuzzi, "RFID integrated circuits as network controllers," in *Proc. 25th Riunione Nazionale di Elettromagnetismo*, 2024, pp. 1–4. [Online]. Available: https://art.torvergata.it/retrieve/c52780c0-dbfb-425d-97d6-21b2732f3672/RINEM2024___Selective_Activation.pdf

[21] "EPC radio-frequency identity protocols generation 2 UHF RFID Standard," 2024. [Online]. Available: https://ref.gs1.org/standards/gen2/

[22] A. Ebrahimi, Z. Shen, W. Withayachumnankul, S. F. Al-Sarawi, and D. Abbott, "Varactor-tunable second-order bandpass frequency-selective surface with embedded bias network," *IEEE Trans. Antennas Propag.*, vol. 64, no. 5, pp. 1672–1680, May 2016.

[23] F. Costa, A. Monorchio, and G. Manara, "An overview of equivalent circuit modeling techniques of frequency selective surfaces and metasurfaces," *Appl. Comput. Electromagnetics Soc. J.*, vol. 29, pp. 960–976, 2014.

[24] J. Bonache, I. Gil, J. Garcıa-Garcıa, and F. Martın, "Compact microstrip band-pass filters based on semi-lumped resonators," *IET Microw. Antennas Propag.*, vol. 1, no. 4, pp. 932–936, 2007.

[25] F. Capolino, *Theory and Phenomena of Metamaterials*, 1st ed. Boca Raton, FL, USA: CRC Press, 2009.

[26] "Modelling the frequency dependence of the dielectric properties to a 4 dispersions spectrum," Nov. 1997. [Online]. Available: http://niremf.ifac.cnr.it/docs/DIELECTRIC/AppendixC.html#FF

[27] F. Lestini, N. Panunzio, G. Marrocco, and C. Occhiuzzi, "Epidermal RFID-based thermal monitoring sheet (R-TMS) for microwave hyperthermia," *IEEE J. Electromagn. RF, Microw. Med. Biol.*, vol. 7, no. 4, pp. 365–374, Dec. 2023.

[28] "Ansys HFSS–Getting Started with Floquet Port Simulations," 2020. [Online]. Available: https://www.oldfriend.url.tw/Tutorials/Ansoft/hfss/HFSS%20Floquet%20Ports.pdf#::text=l%20The%20attenuation%20for%20both,in%20the%20Mode%20Table%20Cal%02culator

[29] F. Costa, "A simple effective permittivity model for metasurfaces within multilayer stratified media," *IEEE Trans. Antennas Propag.*, vol. 69, no. 8, pp. 5148–5153, Aug. 2021.

[30] Skyworks, "SMV121x series: Hyperabrupt junction tuning varactors," 2020. [Online]. Available: https://www.skyworksinc.com/-/media/SkyWorks/Documents/Products/101-200/SMV121x-Series_200057W.pdf

[31] *Skyworks*, "Varactor SPICE models for RF VCO applications," 2015. [Online]. Available: https://www.skyworksinc.com/-/media/SkyWorks/Documents/Products/1-100/Varactor_SPICE_Model_AN_200315C.pdf

[32] G. M. Bianco, S. Amendola, and G. Marrocco, "Near-field constrained design for self-tuning uhf-rfid antennas," *IEEE Trans. Antennas Propag.*, vol. 68, no. 10, pp. 6906–6911, Oct. 2020.

[33] J. Boateng and O. Catanzano, "Advanced therapeutic dressings for effective wound healing–A review," *J. Pharmaceut. Sci.*, vol. 104, no. 11, pp. 3653–3680, 2015.

[34] "Em4152 datasheet," 2021. [Online]. Available: https://www.emmicroelectronic.com/sites/default/files/products/datasheets/4152-DS%20v4.2.pdf

[35] G. Marrocco, "The art of UHF RFID antenna design: Impedance-matching and size-reduction techniques," *IEEE Antennas Propag. Mag.*, vol. 50, no. 1, pp. 66–79, Feb. 2008.

[36] S. Amendola and G. Marrocco, "Optimal performance of epidermal antennas for UHF radio frequency identification and sensing," *IEEE Trans. Antennas Propag.*, vol. 65, no. 2, pp. 473–481, Feb. 2017.

[37] AET Associates, Inc., “Human body equivalent phantom,” 2025. [Online]. Available: https://www.aetassociates.com/hardware.php?phantom

[38] P. V. Nikitin and K. V. S. Rao, “Theory and measurement of backscattering from RFID tags,” *IEEE Antennas Propag. Mag.*, vol. 48, no. 6, pp. 212–218, Dec. 2006.

[39] Microwave Vision Group, “SH-400 dual-ridge horn antenna,” 2024. [Online]. Available: https://www.mvg-world.com/media/2479/download/reference

[40] Mini Circuits, “ADTL1-12 RF BalUn,” 2025. [Online]. Available: https://www.minicircuits.com/pdfs/ADTL1-12.pdf

[41] “PicoVNA108 vector network analyzer,” 2025. [Online]. Available: https://www.picotech.com/vector-network-analyzer/picovna/picovna-series

[42] L. B. Wang, K. Y. See, J. W. Zhang, B. Salam, and A. C. W. Lu, “Ultra-thin and flexible screen-printed metasurfaces for EMI shielding applications,” *IEEE Trans. Electromagn. Compat.*, vol. 53, no. 3, pp. 700–705, Aug. 2011.

[43] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, “RFID technology for IoT-based personal healthcare in smart spaces,” *IEEE Internet Things J.*, vol. 1, no. 2, pp. 144–152, Apr. 2014.

[44] R. Lodato, V. Lopresto, R. Pinto, and G. Marrocco, “Numerical and experimental characterization of through-the-body UHF-RFID links for passive tags implanted into human limbs,” *IEEE Trans. Antennas Propag.*, vol. 62, no. 10, pp. 5298–5306, Oct. 2014.

[45] S. J. Seidman et al., “In vitro tests reveal sample radiofrequency identification readers inducing clinically significant electromagnetic interference to implantable pacemakers and implantable cardioverter-defibrillators,” *Heart Rhythm*, vol. 7, no. 1, pp. 99–107, 2010.

[46] S. J. Seidman and J. W. Guag, “Adhoc electromagnetic compatibility testing of non-implantable medical devices and radio frequency identification,” *Biomed. Eng. Online*, vol. 12, pp. 1–10, 2013.

[47] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, “IMDGuard: Securing implantable medical devices with the external wearable guardian,” in *Proc. IEEE INFOCOM*, 2011, pp. 1862–1870.

[48] C. Miozzi, S. Nappi, S. Amendola, C. Occhiuzzi, and G. Marrocco, “A general-purpose configurable RFID epidermal board with a two-way discrete impedance tuning,” *IEEE Antennas Wireless Propag. Lett.*, vol. 18, no. 4, pp. 684–687, Apr. 2019.

[49] J. A. Rogers, T. Someya, and Y. Huang, “Materials and mechanics for stretchable electronics,” *Science*, vol. 327, no. 5973, pp. 1603–1607, 2010.

[50] A. Mostaccio, F. Naccarata, F. M. C. Nanni, J. Filippi, E. Martinelli, and G. Marrocco, “Soft and flexible wireless epidermal plaster made by laser-induced graphene,” *IEEE Sens. Lett.*, vol. 8, no. 7, Jul. 2024, Art. no. 6007104.

Francesco Lestini (Member, IEEE) received the B.S. and M.S. (Hons.) degrees in medical engineering in 2019 and 2021, respectively, from the University of Rome Tor Vergata, Rome, Italy, where he is currently working toward the Ph.D. degree in computer science, control and geoinformation with Pervasive Electromagnetics Lab. Since 2023, he has been a part-time R&D RF Engineer with RADIO6ENSE Srl. Mr. Lestini is also part of Cyber4Health Observatory, which focuses on raising international awareness about the need for pre-market regulations related to medical devices’ Cyber and Physical security. His research focuses on the wireless reconfiguration of electromagnetic devices through RFID technology and on developing epidermal RFID grids for distributed skin temperature measurement. He won the Best Paper Award at the 7th edition of SpliTech Conference in 2022 on Smart and Sustainable Technologies, Gaetano Latmiral Award at the XXV Riunione Nazionale di Elettromagnetismo (RiNEm) in 2024, and Huawei Tech Arena Italy in 2024.

Gaetano Marrocco (Senior Member, IEEE) received the M.Sc. degree in electronic engineering, and the Ph.D. degree in applied electromagnetics from the University of L’Aquila, L’Aquila, Italy, in 1994 and 1998, respectively. He was a Researcher with the University of Rome Tor Vergata, Rome, Italy, from 1994 to 2014, Guest Professor with the University of Paris-Est Marne-la-Vallée in 2015, Associate Professor of electromagnetics from 2013 to 2017, and Full Professor with the University of Rome Tor Vergata since 2018. From 2018 to 2024, he was the Director with Medical Engineering School. Since 2003, he has been investigating sensor-oriented miniaturized antennas for Biomedical Engineering and Radiofrequency Identification (RFID), contributing to the move from the RF labelling of objects to the passive sensor networks in the Internet of Things era. He is currently the Deputy Director with the Department of Civil Engineering and Computer Science Engineering. The first phase of his research career was devoted to the modelling and designing of structural broadband and ultra-wideband antennas for Satellite (ESA, ASI), Avionic, and Naval (Leonardo) communications. He carried out pioneering research on bodycentric battery-less wireless sensors concerning textile RFID antennas, tattoo-like sensors (flexible and stretchable epidermal electronics), and radio-sensors embedded inside implantable prostheses. He was an Associate Editor for IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, IEEE JOURNAL OF RADIOFREQUENCY IDENTIFICATION, and member of IEEE Antennas and Propagation Society Awards committee. He is also an Associate Editor for IEEE JOURNAL OF FLEXIBLE ELECTRONICS. He is the Chair of Italian delegation URSI Commission D Electronics and Photonics. He was the Chair of the Local Committee of the V European Conference on Antennas and Propagation (EUCAP-2011), TPC Chair of the 2012 IEEE-RFID TA, Nice, France, TPC Track-Chair of 2016 IEEE Antennas and Propagation International Symposium, TPC Track-Chair of IEEE-RFID 2018 USA, and General Co-Chair of IEEE Flexible, Printable Sensors and Systems (FLEPS), Tampere, Finland, in 2024. Prof. Marrocco is the Director of Pervasive Electromagnetics Lab (pervasive.ing.uniroma2.it) and the co-founder and president of the University spin-off RADIO6ENSE (www.radio6ense.com), which is active in the short-range electromagnetic sensing for the Industrial Internet of Things, Smart Manufacturing, Automotive BioEngineering, and Pharma. He is listed in the PLOS ranking of Top 1.5% Scientists Worldwide (source Univ. Stanford, 2024) and in the first three places on ScholarGPs for worldwide RFID impact 2024.

Cecilia Occhiuzzi (Member, IEEE) received the M.Sc. degree in medical engineering, and the Ph.D. degree from the University of Rome “Tor Vergata,” Rome, Italy, in 2008 and 2011, respectively. She is currently an Associate Professor with the University of Rome “Tor Vergata,” where she teaches electromagnetic fields, biomedical interaction, and instrumentation and techniques for health monitoring and therapy. She is also the Co-Founder and CEO with RADIO6ENSE, a spin-off of the University of Tor Vergata active in RFID solutions for the industrial sector. She coauthored more than 80 papers in international journals and conferences and ten patents on RFID sensing systems. Her research interests include wireless health monitoring through wearable and implantable radio frequency/mm-wave identification techniques and pervasive sensing paradigms for the food sector and Industry 4.0. She is also listed in the PLOS 2023 ranking of the Top 2% Scientists Worldwide.