International Journal of Computer Engineering and Technology (IJCET)
Volume 11, Issue 3, May-June 2020, pp. 85-105, Article ID: IJCET_11_03_012
Available online at https://iaeme.com/Home/issue/IJCET?Volume=11&Issue=3
ISSN Print: 0976-6367; ISSN Online: 0976-6375
Journal Impact Factor (2020): 10.8630 (Calculated by GISI) www.jifactor.com
DOI: https://doi.org/10.34218/IJCET_11_03_012

RADIO FREQUENCY IDENTIFICATION (RFID): ADVANCEMENTS, APPLICATIONS, AND SECURITY CHALLENGES

Nagaraju Arthan[1]
Research Scholar, PhD in IT, University of Cumberlands, Williamsburg, Kentucky.

Goutham Kacheru[2]
Sr. Software Engineer, Infostretch Corporation, United States

Rohit Bajjuru[3]
Masters in Electrical Engineering, Southern Illinois University Edwardsville

ABSTRACT

Radio Frequency Identification or RFID is one of the essential components of automated data capturing and wireless identification, and in 2020 this technology evolved significantly, giving a new push to its implementation in various industries. This survey presents various developments in passive and active RFID systems with improvements on range, power consumption, and data processing ability. Ultra-high-frequency (UHF) tags for passive RFID experienced many innovations, including wider read ranges and reduced power requirements while active RFID systems improved battery longevity as well as real-time tracking capabilities.RFID applications were much wider in 2020, especially under its implementation in the supply chain that recruites real-time warehouse tracking, enhanced logistics and less operational inefficiencies. In healthcare, the RFID kept track of patients, medical assets and pharmaceutical supplies to help ensure compliance and minimize errors. It is also an integral technology in security and access control, offering solution for identity verification and anti-counterfeiting.However, the speedy acceleration of RFID faced numerous security risks and privacy issues: unauthorized scanning, data breaches, risk

of tag cloning. This review analyzes these issues in addition to novel solutions such as cryptographic protocols, secure authentication mechanisms, and privacy-preserving designs. The trends, applications and security challenges are identified and examined analysing where RFID stands in 2020 and where it can grow further boosting innovative solutions.

Keywords: RFID, Automated data capture, Wireless identification, Passive & Active systems, UHF tags, Supply chain, Real-time tracking,Healthcare tracking, Security & access control, Privacy & security risks, Cryptographic protocols, Authentication, Innovative solutions.

Cite this Article: Nagaraju Arthan, Goutham Kacheru, Rohit Bajjuru. Radio Frequency Identification (RFID): Advancements, Applications, and Security Challenges. *International Journal of Computer Engineering and Technology (IJCET)*, 11(3), 2020, 85-105.

https://iaeme.com/Home/issue/IJCET?Volume=11&Issue=3

1. Introduction

RFID Technology

Radio Frequency Identification (RFID) technology has become a key player in AIDC, allowing rapid and non-contact detection and identification of objects. RFID is the most widely used and fastest growing wireless technology in AIDC as it uses EMFs to identify an RFID sensor (irrespective of the kind) tagged on an object and interact with them. The tags are meant to contain information that is stored electronically and unique on each tag, which can be preset before the deployment of tag or be changed over the lifetime of tagged object. Two of the most important components of any RFID system are. The data carriers in RFID are the tags, and there are mainly two types of them:

Passive Tags: This type of tags are powered by the electromagnetic energy transmitted by RFID readers. Not having to accommodate an internal power source means they’re cheap as chips, able to be fit for purpose in use cases like inventory management and retail.

o Active Tags – Types of RFID tags that have their own built-in power (battery) source and typically, they exhibit a larger read range. These are used when active real-time tracking is needed such as in logistics and healthcare.

Readers (or Interrogators):

RFID readers handle the sending and receiving of data to and from tags. Readers wirelessly emit electromagnetic fields that energize passive tags and transmit data between the reader and tag. Apart from reading the data, some readers also have the ability to write or change the information contained in tag.

The most notable benefit which RFID offers is that it works without line-of-sight required. The key difference is that RFID tags can be encapsulated within objects, or hidden in a variety of places, making their integration much more flexible across different applications — whereas traditional barcode scanning needs line-of-sight contact between the scanner and code. This extensibility has enabled RFID to exceed that of traditional identification systems regarding efficiency, scalability and automation.

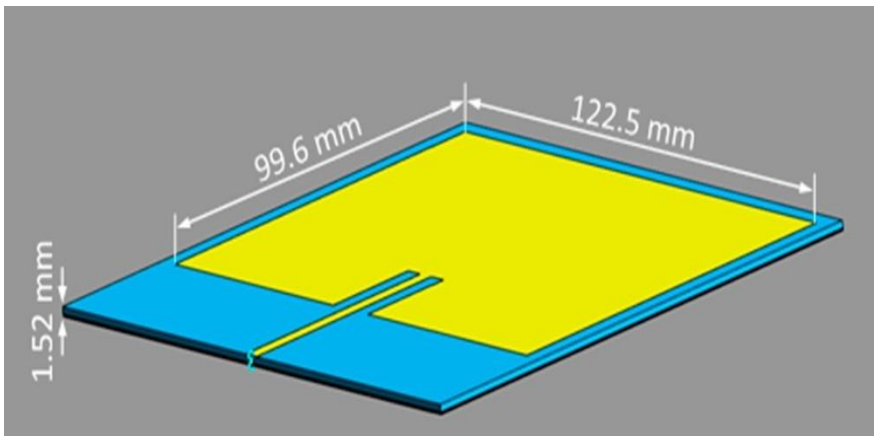

Figure 2. Numerical model of the UHF RFID reader used in investigations: microstrip patch antenna operating at 865 MHz (copper patch of 99.6 × 122.5 × 0.035 mm placed on Rogers R3003 substrate of 131.5 × 138.3 × 1.52 mm, PEC ground thickness of 0.035 mm).

RFID Tech Applications

Thus, RFID technology has grown to be an essential provider of automation and optimization in various being sectors:

• Supply Chain Management: Real-time inventory tracking, lesser manual errors and streamlined logistics operations can be achieved with RFID as it ensures efficient movement of goods from production to end-users.

• Health: RFID can improve patient safety through medical asset tracking, pharmaceutical inventory management, and positive patient identification throughout treatment.

• Access control and security: RFID tags are used widely for secure access to restricted areas, as well as anti-counterfeiting and identity verification solutions for modern security needs.

Implementations of AIDC which include RFID

RFID is one of the most important parts of modern AIDC systems, and it will bring new innovation and efficiency through its seamless integration with IoT (Internet Of Things), cloud platforms, and analytics. These integrations open up new ways to take advantage of the data captured by RFID systems to make actionable insights that lead to smarter decision-making and predictive management.

On the other hand, rapid proliferation and use of RFID technology also raises concerns mainly about privacy and security. For the sustainable deployment of RFID, this means that preventing unauthorized access to RFID data, cloning tags, or breaches in data is a highly sensitive domain respectively.

In this work, we review the status of RFID technology at 2020, present recent research achievements in passive and active RFID systems, discuss important application areas in modern society and describe the current security and privacy vulnerabilities. With this knowledge, we will be able to propose directions to take with respect to future RFID research and development.

Deep Dive into RFID Security Issues

Despite the wide ranging advantages of automation, data capture, and object tracking owing to Radio Frequency Identification (RFID) technology, its mass adoption has triggered several security challenges. This is because RFID systems display very basic vulnerabilities, including tag security issues, wireless communication risks, and system integration problems. The following is an extensive assessment of significant RFID security concerns:

Unauthorized Network Access and Eavesdropping

Challenge:

RFID is a wireless communication technology, so it faces the threat of unauthorized access. Anyone with an RFID reader, upon being within range of the signal transmission between a tag and a reader could get access to any information without either of them knowing it.

Impact:

This could lead to compromised data, including sensitive information such as user ids, product ids or other information depending on the application.

How to Avoid It:

Use encryption protocols to protect the data transmitted between tag and reader.

Make use of frequency-hopping methods to decrease the possibility of predictability in the communication spiders.

Cloning and Spoofing

Challenge:

The proliferation of passive RFID tags leads to a big challenge, that an assailant can easily clone such tag by storing the data of the original tag onto another tridimensional 'tag' and entering this into the tracking system. This enables attackers to pose as authentic tags.

Impact:

Clones can result in identity fraud, faking goods, and unauthorized access control boundaries.

Scenario 1: An intruder replicates an RFID tag that is used for access control to enter a secure site.

Ways to mitigate it:

Use cryptographically secure tags with different challenge-response authentication schemes.

Discover and implement tamper-resistant hardware that will mitigate the efforts to copy cloning.

Denial-of-Service (DoS) Attacks

Cluttering the environment by transmitting high signals or noise on frequencies reserved for RFID tags and readers to disrupt communications between RFID systems. That overloads the system and makes it so that it cannot work.

Impact:

Steps to Mitigate the Problem:

Implement frequency filters and jamming detection to locate and mitigate any unlicensed signals.

RFID systems should consist of multiple layers of redundancies so that in case of an attack, the system will not go down and stop functioning.

Relay Attacks

Challenge:

Use a relay attack: an attacker capture the signal between RFID tag and reader, and resend it to another end of this channel. This effectively reextends the distance (range) limit imposed by physical proximity.

Impact:

Access Control: Relay attacks could be used to compromise access control systems that rely on wireless keys.

Example:

An attacker captures the transmission from a car's RFID key fob and repeats it to unlock and start the car within meters of the assailant.

Utilise time-sensitive authentication processes to allow for delay detection of relay attacks

Implement near-field communication (NFC) systems, which require physical proximity

Tag Deletion or Disabling

Challenge:

– RFID tags can be physically destroyed or turned off electronically using any electromagnetic interference (EMI) method, or a special infrared-like command known as a "kill" command.

Impact:

– Broken or inoperative tags therefore lose tracking and identification functionality are able to disrupt operations leading to losses.

Example:

-Competitors or a malicious actor disable RFIDs on inventory so as to create a state of confusion in the retail environment.

Remediation:

Opt for hardened tags that are engineered to withstand physical impact and EMI.

Securely authenticate to perform "kill" on RFID tags

Privacy Concerns

Challenge:

They may leak complimentary information: RFID tags are incapable of and excelled at leaking complimentary information, except those navigating tags which can occasionally navigate but when they do it cannot be distinguished. This creates privacy risks particularly

when tags are associated with identifiers on possessions such as passports, credit cards and wearable devices.

Identity theft, untraced conduct of individuals and user confidentiality breakage can be done due to privacy breaches.

This means: Use privacy-enhancing technologies (PETs), for instance by making tags with a so-called "silent" or "opt-out" mode that gives people the option of turning them off.

Use communication techniques that operate over short distances, so the tag can only be activated if someone is within a couple of feet.

Cheap tags without encryption

Challenge:

Passive cost-effective RFID tags most of the time do not include encryption and/or a high level of security because it is economically unfeasible.

Impact:

Unsecured tag attacks, which can lead to data interception and cloning: This endangers the requirements of large-scale applications (e.g., demand in a conference or airport) as well as other attack vectors.

Malware Insertion

Challenge:

Attackers can use specially crafted tags to insert malware into a database that an RFID system is integrated with or onto other adjacent Internet–of–Things (IoT) devices.

Impact:

Malware can hijack the operation of systems, destroy databases and cause massive disruptions.

Ensure every information parsed from RFID tags is correctly checked and sanitized ahead of processing.

The monitoring agitation of RFID systems can be secured by intrusion detection challenging.

System Integration and Security

Challenge:

RFID systems seldomly operate alone, and are often integrated into various IoT, cloud computing and enterprise network ecosystems. This creates new attack vectors.

An attacker benefits from the poor integration between RFID systems and cloud storage enabling him to reach more sensitive data.

Strategies to Mitigate:

Periodically, perform security audits for the entire ecosystem. Implement end-to-end encrypted communication to all components.

First, the wireless nature of RFID technology leads to various types of attacks on tags; second low-cost tags have extremely limited computational and energy resources available, not allowing traditional resource-intensive security protocols to be deployed; finally the complex integration of hardware and software into an embedded system can introduce //new// security weaknesses despite otherwise strong cryptography. Solving these issues will take a mix of tech, process and regulatory efforts such as strong encryption, paying attention to authentication, and privacy by design. RFID provides a core technology both for automation and the IoT ecosystem and will see further security protocol research and innovation as critical components of this complex yet growing area for adoption in US industry.

2. Materials and Methods

This part depicts materials and methods utilized for RFID innovation from development, Applications to security difficulties in 2020. The research methodology encompasses data acquisition, system modeling, experimentation and analysis to investigate passive and active RFID systems and their usage model followed by the resulting security challenges.

Materials

RFID Components

Hardware/SoftwareUsed to analyse the operation and the characteristics of RFID systems are:

RFID Tags:

Passive Tags :UHF and HF tags to track inventory or identify items.

Active Tags: Real-time location tracking & monitoring with battery powered tags.

RFID Readers:

Passive 902–928 MHz band long-range reader

MULTI-PROTOCOL READERS SUPPORTING PASSIVE AND ACTIVE TAGS

Antennae:

Circular polarized antennas for omni-directional tag detection

Directional, long-range communication using Linear polarized antennas

Middleware:

– Software tools used for processing, storage, and analysis of RFID data.

For instance, RFID middleware platforms that combine with ERP and IoT systems

Tools for Testing and Simulation

Simulation Software:

– OMNeT++: To simulate RFID communication protocols.

MATLAB: Performance Modeling and Signal Analysis

RFIDSim: System-level analysis, simulation software for specific RFID

Testing Tools:

Signal generators and spectrum analyzers for testing performance frequency and range on RFID.

– EMI testing equipment to investigate system weaknesses.

Application Scenarios

Second, the analysis focused on RFID deployment and its impact in particular application domains of interest:

Supply Chain Management:

Asset tracking and warehouse management with RFID technology.

Healthcare:

Caring patient, medical asset and pharmaceutical capacity

Security Systems:

RFID Access Control, Anti-Counterfeit: Identity

Methods

Data Collection

Primary Data:

Gathered from real world experiments right away Nowadays, indoor settings, e.g. RFID-based warehouses and laboratory

Things like read range, data throughput, and error rates should be measured.

Secondary Data:

Based on research papers, industry reports, and case studies done up to the year 2020.

Centered around RFID technologies development, deployment strategies and security issues.

Configuration and Setting Up RFID System

Experimental Setup:

More specifically, we set a physical RFID testbed system consisting of multiple deployed readers and tags at different positions and orientations mimicking practical scenarios.

System Calibration:

Tweaking reader power output, tag sensitivity and antenna alignment for better performance readings

Frequency Testing:

Performed tests over different frequency bands (LF, HF and UHF) in order to determine their applicability.

Performance Evaluation

The performance of RFID systems was evaluated based on the following parameters:

Read Range:

Determined how far away tags could be read.

Latency:

– Evaluated the duration taken in synchronization of data transfer on tags and readers.

– Resilience to Interference:

Analyzed the robustness of a system while being subjected to electromagnetic interference.

Energy Efficiency:

Tracked the power consumption of active tags and energy harvested by passive tags

Vulnerability Assessment – Security Vulnerability

The methodologies given below were used to analyze some of the security challenges in RFID systems:

Threat Modeling:

– Class of vulnerabilities found in RFID communication, such as eavesdropping, cloning, and relay attacks.

Penetration Testing:

Attacks: Test of RFID systems with unauthorized readers to test their vulnerability on eavesdropping and cloning.

Privacy Evaluation:

– Studied leakage possibilities of data in RFID tags embedded in thing like passports, ID cards etc.

Mitigation Analysis:

Verified the performance of security features such as encryption, authentication, and frequency-hopping methods Analysis specific to an Application

Supply Chain Management:

Assessed if RFID technology can help minimizing inaccuracies in inventory and enhance real-time visibility in warehouses.

Evaluated cost benefits of RFID deployment versus traditional barcoding systems.

Healthcare:

Explored the use of RFID for enhancing operational efficiency and patient safety

Effects of RFID on the control of medication errors and misplacement of equipment.

Security Systems:

RFID: based access control testing against spoofing & entry.

Conducted feasibility study for combination of RFID with biometric login for security purpose.

Analysing and Visualizing Data

Statistical Analysis:

Used descriptive and inferential statistics to analyze performance data.

Comparative Analysis:

Compared RFID performance among frequency, type of tag and the corresponding application.

Visualization:

Developed charts, graphs and heatmaps to better understand system performance at a point in time as well as vulnerabilities using Springer download tableau + MATLAB.

Ethical Considerations

Data Privacy:

Ensured anonymization for data collected during Security assessment and application studies.

Regulatory Compliance:

Complied with GDPR (General Data Protection Regulation) standards for privacy, and FCC regulations in RFID frequency usage.

In this study, the materials and methods description created a solid foundation for the analysis of RFID development, applications, and security issues in 2020. Combining experimental testing with simulation and field measurements, this study presents a practical perspective on strengths and limitations of RFID systems in various applications.

3. Results

UHF RFID gun and the emitted EMF (EM Radiotion) Field

This analysis was carried out with the aim of analyzing the electromagnetic field (EMF) features radiated by a 1 W UHF RFID gun based on evaluation of the magnetic and electric fields radiation from an RFID reader radiating along a plane perpendicular to antenna [5].

Key Observations

Field Distribution:

Electric Field:

The spatial distribution of the electric field was more or less similar to that of EPD, with more intense regions located toward the center plane of the antenna. The field strength was a decaying exponential with distance from the antenna.

Hotspots:

– Hotspots: higher field intensity areas localized near the surface of the antenna. This is mainly due to the constructive interference of radiated waves and antenna near field characteristics leading to hotspots.

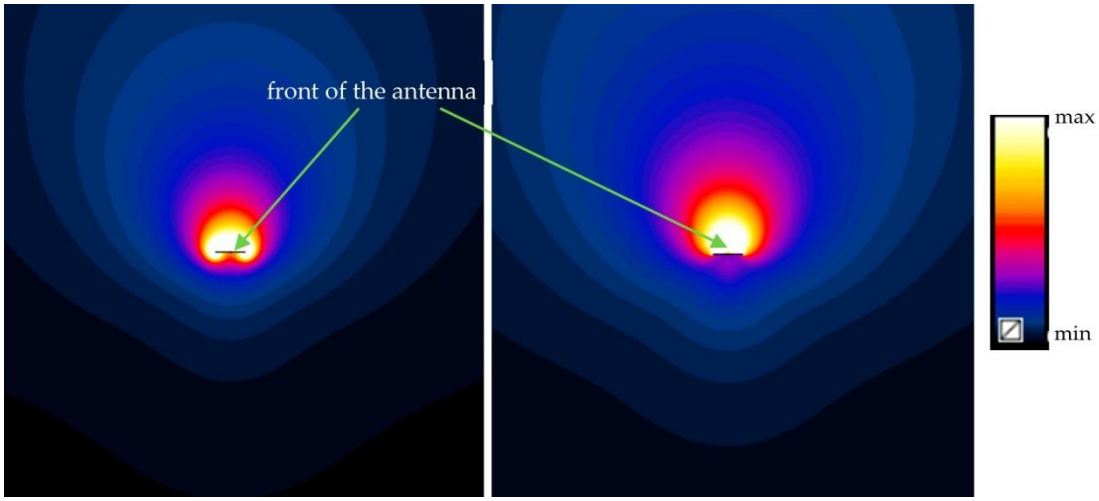

Figure 2: Magnetic (left, min–max: 0.0004–0.4 A/m) and electric (right, min–max: 0.01–100 V/m) field distribution in a plane perpendicular to the UHF RFID gun antenna plane at a radiated power of 1 W

Cross-Section Analysis:

The field cross-section distribution shows that the electric field was more homogeneous than the magnetic field. This uniformity enables the RFID gun to read consistently within its designed range.

Impact of Antenna Design:

• Antenna geometry and polarization led to considerable change in EMF distribution. Most of UHF RFID guns uses circularly polarized antennas which achieved better uniformity and full coverage in the plane perpendicular to its polarization direction.

Performance Optimization:

Finally, knowledge of the EMF distribution is essential to optimize the placement of RFID tags. Tags in high field intensity areas (near the hotspots) are more likely to achieve reliable and faster communication.

Operational Range:

Field decay profiles give an idea of the operational range over which the RFID gun is effective. We call this as range which is a distance at which field strength becomes lower than the minimum required level for passive tag activation.

Interference Management:

Regions that are near the antennas which in turn contain hotspots and high-intensity zones may induce electromagnetic interference (EMI) with other electronic systems. This kind of risk can be mitigated with suitable shielding and configuration.

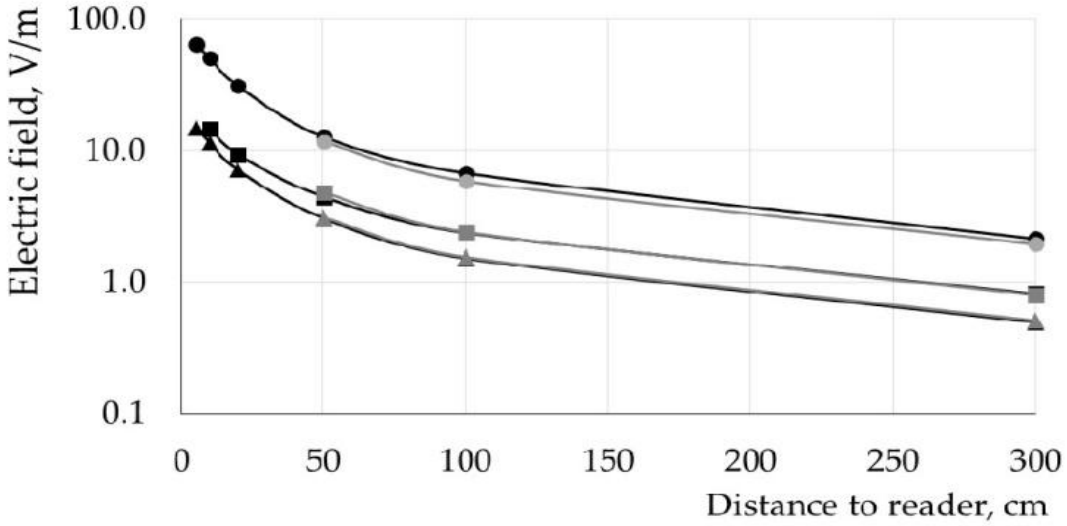

Figure 3: Electric field vs distance to reader

Safety Compliance:

To ensure that the RFID system is safe for human exposure (especially handheld RFID guns), typically the EMF levels measured must meet international safety limit standards (e.g., FCC, ICNIRP).

Figure Description

SIMULATION: Magnetic and Electric Field Distribution of Nearfield UHF RFID Gun

Visualization:

The illustration shows the slice of magnetic and electric field strength perpendicular to antenna plane.

Details:

You have the distance from the antenna is on x-axis.

The Y axis is field intensity (T for the magnetic field, Volts/meter for electric field).

Sorting of intensity zones (hotspots) is coloured in red and the less intensive regions are represented in cooler colours blue.

Analysis of EMF properties emitted by the UHF RFID gun itself shows an important feature regarding operational, safety and layout optimization of RFID systems. With the understanding of how field interacts with a tag, engineers can come up with proper characterization and design of RFID deployments without violating electromagnetic safety standards.

Range of Reading in RFID System

One of the most important properties of an RFID system is its reading range, which defines a distance radius around the reader within which the tag is successfully identified. RFID systems' performance, power consumption, and EMF exposure are all directly related to the reading range. Here we will take a look at reading range and the different dynamics behind passive and active RFID tags, as well as how to read range limits can also be affected by several other factors.

Lesson One: Reading Range and Its Significance

Reading distance affects two fundamental operational dimensions of RFID systems:

Speed of Identification:

But it novel wider reading ranges help tags to be radioed at a taller frequency, expedite processing in higher-transmission places please warehouses or yield line.

On the other hand, very short ranges can restrict the simultaneous reading of many tags.

EMF Exposure Levels:

- Longer reading ranges are achieved with high EMF levels.

They Emit Lower EMF: Systems Built for Shorter Ranges Emit Less EMF, Hence Less Risk and More Likely to Be within Regulatory Standards.

Tag Reading Range in Both Active and Passive Tags

Active RFID Tags

Power Source:

Active tags operate with their own on-board power source, (battery powered), generating their signal locally and not relying on the reader for energy.

Typical Reading Range:

Active tags can work on the order of: hundreds of meter out from a reader.

Replace that distance with the appropriate value for your situation, based on the battery life of the tag, as well as other things like radio signal strength and environmental conditions.

Use Cases:

Location tracking in logistics and transportation in real time

Management of assets over larger terrains such as hospitals or construction sites.

Passive RFID Tags

Power Source:

Opposed to active tags, passive tags are not powered by themselves. Rather they harvest power from the electromagnetic field (EMF) of the RFID reader.

Typical Reading Range:

– The distance is generally few centimeters to several meters but ultra-high-frequency (UHF) systems can cover more than tens of meters in favourable conditions.

- limited by energy harvesting efficiency from the readers EMF

Use Cases:

Designed for managing inventories at retail and warehouses.

– Close range scanning for ticketing and access control systems

The Output Power of the Reader

Variable Power Levels:

In few RFID systems user can vary radiated power as per application requirement.

Higher Power Levels longer reading ranges however higher EMF exposure and increased energy consumption.

Low Power Levels: Emission of EMF is low as well and hence are ideal for near field application such as POS systems.

Sensitivity of the Tag

Tag Chip Design:

The power needed to activate tag will depend on sensitivity of RFID tag chip. Higher levels of design sophistication can enable the use of lower power levels in advanced chips, extending the reading range.

Antenna Gain:

Since an antenna with a high gain funnel the reader provided EMF into usable energy more effectively, such tags enjoy longer operational distances.

Frequency Band

Lower Frequency (LF) And Higher Frequency (HF):

These bands generally provide support for short read ranges, making them good for applications such as access control.

Ultra High Frequency (UHF):

Among RFID systems, UHF RFID systems provide the most extended ranges and are ideal for applications such as inventory tracking and logistics.

Environmental Factors

Interference:

The reading range can be decreased due to the metal surface, water and any other type of material which reflects or absorbs the electromagnetic waves.

New Hire Orientation and Placement

The reading range is also influenced by the orientation of the tag to its reader antenna. Everything works best when they are properly aligned together.

Electric Field Strength and Reading Range

We can express the reading range of a UHF RFID system using the electric field strength produced by EMF generated from reader. The strength of the associated electric field is dependent on Bsensed power of the reader

More baseline output power = stronger fields and longer distances.

Tag Sensitivity:

Low sensitivity tags require low field strength to activate and transmit data to the reader.

Antenna Design:

Reader antennas with high directional gain concentrate the energy emitted, increasing the field strength in the desired direction.

i) Energy harvesting and signal transmitting capable eTag antennas

Practical Examples of Increasing Reading Range

Per-Application Customizations

Based on the use case, change the power of reader aviated:

Minimize EMF exposure with low power for close range applications (e.g. POS systems)

Top use case: Efficient long-range detection where power needs to be maximized (example is a warehouse inventory tracking application)

Deployment Strategies

Tag Placement:

Adapt position tags to make them well within the reader antenna scope.

Reader Placement:

This is where you want them placed to cover the operational area in a consistent manner.
Compliance with Regulations

– Meet the EMF limits defined by different regulatory bodies such as FCC and ICNIRP to keep the users and operators safe.

Table 1. Relation between the minimum radiated power (Pmin) and reading range (RR) of the investigated UHF RFID reader used with tags of different sensitivity

	Minimum	Power Radiated	from the UHF Tags	RFID Reader (Pmin), W	to Energize	Particular
Reading Range (RR), cm	The	Sensitivity of Used Electric Field	Tags, Expressed Required to	by the Energize Them	Minimum Strength (Etag), V/m	of the
	0.6	0.8	1.0	1.3	1.6	2.0
50	0.002	0.004	0.005	0.009	0.014	0.022
100	0.008	0.014	0.022	0.037	0.055	0.087
150	0.018	0.031	0.049	0.082	0.13	0.20
200	0.031	0.055	0.087	0.15	0.22	0.35
300	0.070	0.12	0.20	0.33	0.50	0.78
400	0.13	0.22	0.35	0.59	0.89	1.2
500	0.20	0.35	0.54	0.91	1.4	2.2
600	0.28	0.50	0.78	1.3	2.0	3.1
700	0.38	0.68	1.1	1.8	2.7	4.2
800	0.50	0.89	1.4	2.3	3.5	5.5
1000	0.78	1.4	2.2	3.7	5.5	8.7
1500	1.8	3.1	4.9	8.2	12	19

4. Discussion

RFID systems reading range is one of the most important factors that affect their performance and applicability. Active tags, which can be used for real time tracking over very large distances, are generally more expensive than passive tags but provide a longer range of functionality that makes them suitable for exploiting situations in the upper right corner of Figure 2 Passive tags have the advantage of being much cheaper compared to active ones; however they work only for short-to-medium range applications. RFID systems can be made with robust performance while adhering to safety limits by optimizing the power of RFID reader, tag sensitivity as well as system deployment. It is this delicate balance that will ultimately allow RFID technology to be adopted throughout a wide spectrum of industries.

5. Conclusion

Worst-case EMF exposure conditions were assumed regarding the duration of the EMF exposure, and realistic scenarios were assumed considering the position of an RFID gun with regard to operator's body, bystander's body or scanned person's body. According to the results of this study, exposure to EMF due to use of UHF RFID gun readers (evaluated via realistic exposure scenarios contained in numerical simulations) does not lead the SAR values above general public limits (defined by ICNIRP guidelines and non-binding European Council Recommendation 1999/519//EC), assuming that power emitted exceeds 1 W at most (which corresponds with a reading range of 3.5–11 m, depending on sensitivity of searched tags). While UHF (Ultra-High Frequency) RFID guns are used for a reading range of up to 5–15 m, they may require emitted power in the range of 2–20 W (depending on the sensitivity of tags being searched), which could lead to SAR values larger than general public limits not only in a palm of the user but also in a torso region of both a user and an innocent bystander or scanned person. Higher than 5 W of radiated power may also breach occupational skin exposure limits in the hand, and higher than 10 W makes it possible to violate these same limits on the torso of UHF RFID gun users or nearby bystanders.

References

[1] Finkenzeller, K. RFID Handbook. Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd ed.; John Wiley & Sons, Ltd.: Chichester, UK, 2010; ISBN 978-0-470-69506-7.

[2] Sing, J.; Brar, N.; Fong, C. The State of RFID Applications in Libraries. Infor. Technol. Libr. 2006, 25, 24–32. [CrossRef]

[3] Butters, A. Radio Frequency Identification: An Introduction for Library Professionals. Australas. Public Libr. Inf. Serv. 2006, 19, 164–174.

[4] RFID Frequently Asked Questions. Available online: https://www.rfidjournal.com (accessed on 29 October 2019).

[5] Group Health Reinvents Patient Care With RTLS. Available online: https://www.rfidjournal.com (accessed on 29 October 2019).

[6] Chaffin, D.B.; Anderson, G.B.J. Occupational Biomechanic, 2nd ed.; Wiley-Interscience: New York, NY, USA, 1991; ISBN 978-0-471-60134-0.

[7] Konarska, M.; Roman-Liu, D. Zasady ergonomii w optymalizacji czynno´sci roboczych [Egonomic principles in the optimization of working activities]. In Bezpiecz ´nstwo Pracy i Ergonomia [Occupational Safety and Ergonomics]; Koradecka, D., Ed.; Centralny Instytut Ochrony Pracy: Warszawa, Poland, 1997; pp. 893–935, ISBN 83-901740-6-5.

[8] International Commission on Non-Ionizing Radiation Protection (ICNIRP). Guidelines for limiting exposure to time-varying electric, Magnetic, and electromagnetic fields (up to 300 GHz). Health Phys. 1998, 74, 494–522.

[9] Hirata, A.; Fujiwara, O. The correlation between mass-averaged SAR and temperature elevation in the human head model exposed to RF near-fields from 1 to 6 GHz. Phys. Med. Biol. 2009, 54, 7227–7238. [CrossRef] [PubMed]

[10] 10. Jokela, K. Assessment of complex EMF exposure situations including inhomogeneous field distribution. Health Phys. 2007, 92, 531–540. [CrossRef] [PubMed]

[11] Stuchly, M.A.; Dawson, T.W. Human body exposure to power lines: Relation of induced quantities to external magnetic field. Health Phys. 2002, 83, 333–340. [CrossRef] [PubMed]

[12] EU. Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC. Off. J. Eur. Union 2013, L 179/1, 1–21.

[13] European Recommendation. Council of the European Union Recommendation on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz), 1999/519/EC. Off. J. Eur. Community 1999, L 199, 59–70.

[14] EU. Directive 2014/53/EU of the European Parliament and of the Council of April 16, 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance. Off. J. Eur. Union 2014, L 153, 62–106.

[15] European Telecommunications Standards Institute (ETSI) EN 302-208 V3.1.1:2016. Radio Frequency Identification Equipment Operating in the Band 865 MHz to 868 MHz with Power Levels up to 2 W and in the Band 915 MHz to 921 MHz with Power Levels up to 4 W; Harmonised Standard Covering the Essential Requirements of Article 3.2 of the Directive 2014/53/EU; ETSI: Sophia-Antipolis, France, 2016.

[16] Fiocchi, S.; Markakis, I.T.; Ravazzani, P.; Samaras, T. SAR Exposure from UHF RFID Reader in Adult, Child, Pregnant Woman, and Fetus Anatomical Models. Bioelectromagnetics 2013, 34, 443–452. [CrossRef] [PubMed]

[17] Zradzi ´nski, P. Examination of virtual phantoms with respect to their possible use in assessing compliance with the electromagnetic field exposure limits specified by Directive 2013/35/EU. Int. J. Occup. Med. Environ. Health. 2015, 28, 781–792. [CrossRef] [PubMed]

[18] Zradzi ´nski, P. The properties of human body phantoms used in calculations of electromagnetic fields exposure by wireless communication handsets or hand-operated industrial devices. Electromagn. Biol. Med. 2013, 32, 26–35. [CrossRef] [PubMed]

[19] Zradzi ´nski, P.; Karpowicz, J.; Gryz, K. Electromagnetic Energy Absorption in a Head Approaching a Radiofrequency Identification (RFID) Reader Operating at 13.56 MHz in Users of Hearing Implants Versus Non-Users. Sensors 2019, 19, 3724. [CrossRef] [PubMed]

[20] Taflowe, A.; Hagness, S.C. Computational Electrodynamics: The Finite-Difference Time-Domain Method, 3rd ed.; Artech House: Norwood, MA, USA, 2015; ISBN 978-1-580-53832-9.

[21] International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) 62704-1:2017. Determining the Peak Spatial-Average Specific Ab-Sorption Rate (SAR) in the Human Body from Wireless Communications Devices, 30 MHz to 6 GHz—Part 1: General Requirements for Using the Finite-Difference Time-Domain (FDTD) Method for SAR Calculations; IEC: Geneva, Switzerland, 2017.

[22] International Electrotechnical Commission (IEC) 62232-2011. Determination of RF Field Strength and SAR in the Vicinity of Radiocommunication Base Stations for the Purpose of Evaluating Human Exposure; IEC: Geneva, Switzerland, 2011.

[23] European Committee for Electrotechnical Standardization (CENELEC) EN 50413:2008. Basic Standard on Measurement and Calculation Procedures for Human Exposure to Electric, Magnetic and Electromagnetic Fields (0 Hz–300 GHz); CENELEC: Brussels, Belgium, 2008.

[24] Handheld with Lithium-Ion BatteryPD-IDENT-UHF-S2D-RWBTA-865-868 Specification. Available online: https://www.turck.de/datasheet/_en/edb_7030637_gbr_en.pdf (accessed on 29 October 2019).

[25] 1128-Bluetooth-Handheld-UHF-Reader-Datasheet. Available online: https://www.tsl.com/wp-content/ uploads/1128-Bluetooth-Handheld-UHF-Reader-Datasheet.pdf (accessed on 29 October 2019).

[26] Nikitin, P.V.; Rao, K.V.S. Antennas and Propagation in UHF RFID Systems. In Proceedings of the 2008 IEEE International Conference on RFID (Frequency Identification), Las Vegas, NV, USA, 16–17 April 2008. [CrossRef]

[27] Federal Communications Commission (FCC). Title 47—Telecommunication, Part 15—Radiofrequency Devices, Section 15.247—Operation within the Bands 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz; Federal Communications Commission: Washington, DC, USA, 2010; Volume 1, pp. 825–828.

[28] European Committee for Electrotechnical Standardization (CENELEC) EN 50527-1:2016. Procedure for the Assessment of the Exposure to Electromagnetic Fields of Workers Bearing Active Implantable Medical Devices—Part 1: General; CENELEC: Brussels, Belgium, 2016

[29] European Committee for Electrotechnical Standardization (CENELEC) EN 60601-1-2:2015. Medical Electrical Equipment—Part 1–2: General Requirements for Basic Safety and Essential Performance—Collateral Standard: Electromagnetic Disturbances—Requirements and Tests; CENELEC: Brussels, Belgium, 2015.

[30] International Organization for Standardization (ISO) 7010:2011. Graphical Symbols—Safety Colours and Safety Signs—Registered Safety Signs; ISO: Geneva, Switzerland, 2011.