

UNIVERSIDAD DE CASTILLA - LA MANCHA

Departamento de Sistemas Informáticos



TESIS DOCTORAL

Análisis y eficiencia de comunicaciones y recursos
en sistemas de identificación por radiofrecuencia.

Autor: Jesús Blanco Rodríguez de Guzmán

Directores: José Manuel Pastor García y Andrés García Higuera

2020

A mi familia.

Agradecimientos.

Durante los últimos años han sido muchas las personas que directa o indirectamente han contribuido al desarrollo de esta tesis. A todas ellas, me gustaría expresarles mi más sincero agradecimiento por el apoyo incondicional y desinteresado que siempre me han brindado.

A mis directores de tesis, por la confianza depositada desde el primer momento y la ayuda, consejos, ideas y medios prestados a lo largo de todo este tiempo, sin los que no hubiera sido posible llevar a cabo el trabajo recogido en esta tesis.

A todos los que en un momento u otro han formado parte de la familia de AutoLog, tanto en Ciudad Real como en Cuenca, por los buenos momentos que hemos compartido y los logros que juntos hemos alcanzado. De una manera u otra, habéis contribuido a mi crecimiento y desarrollo personal y profesional.

A la Escuela Politécnica de Cuenca, lugar en el que inicié mi etapa universitaria, por permitirme la oportunidad de comenzar la labor como docente y hacerme sentir siempre como en casa.

Por último y no por ello menos importante, mi profundo y sincero agradecimiento a toda mi familia y amigos, por todo su apoyo incondicional mostrado a lo largo de estos años y a pesar de tener que soportar mis continuas ausencias.

Resumen.

En el actual marco de implantación del Internet de las Cosas (IoT), la tecnología de identificación por radiofrecuencia (RFID) es clave para identificar automáticamente de forma unívoca cada objeto que pueda participar en la red. En su sentido más amplio, la identificación por radiofrecuencia engloba a todas las tecnologías que empleen ondas de radio para identificar cosas. Por lo que en esta tesis se ha trabajado con diversas vertientes tecnológicas asociadas a la RFID, contribuyendo a su evolución, desarrollo y aplicación.

Algunas etiquetas incorporan sensores para obtener mayor información sobre los objetos que las portan, aparte de la identificación. Lo que ha derivado en la aparición de las redes inalámbricas de sensores (Wireless Sensor Network, WSN), que a su vez se han desarrollado en otras vertientes como las redes inalámbricas de sensores y actuadores (Wireless Sensor and Actuator Network, WSAN) o las redes inalámbricas de ámbito personal (Wireless Body Area Network, WBAN). En esta tesis se abordan varios estudios y desarrollos con estas tecnologías, prestando especial atención a cómo se producen las comunicaciones entre dispositivos, obteniéndose como resultados varios sistemas totalmente operativos y preparados para trabajar en el marco de la IoT.

La tecnología RFID pasiva es la más extendida e implantada, ya que un lector puede identificar multitud de etiquetas en un corto periodo de tiempo. Entre otros aspectos, presenta un amplio rango de cobertura, un reducido coste de las etiquetas y la posibilidad de funcionar en entornos con alta densidad de etiquetas. Todo ello la convierte en la tecnología más apropiada para emplear cuando sea necesario identificar grandes cantidades de cosas de manera rápida y eficiente.

Focalizando la atención en el estudio de las comunicaciones de los sistemas RFID pasivos, en un nivel físico, se ha abordado el diseño y desarrollo de un completo sistema de caracterización electromagnética de materiales de construcción y soluciones constructivas, que permite averiguar el comportamiento de las señales electromagnéticas cuando interactúan con las muestras bajo estudio. Este sistema puede ser aplicado en beneficio de la tecnología RFID, así como a otras tecnologías inalámbricas que utilicen radiofrecuencia.

Estudiando profundamente los protocolos y cómo se producen las comunicaciones entre lectores y etiquetas RFID, cabe destacar la relevancia del generador de números pseudoaleatorios que las etiquetas deben implementar, así como su influencia para que las comunicaciones se produzcan de manera adecuada. En este sentido, se propone un novedoso algoritmo ultraligero que cumple con la normativa vigente y supone una importante simplificación de la lógica de los chips que incorporan las etiquetas. Tras los resultados obtenidos al implementar el algoritmo en el emulador de etiquetas desarrollado y comparándolos con los generadores que incorporan las etiquetas, se propone utilizar la

propuesta para sustituir los mecanismos actualmente empleados. De tal manera que se reduciría la complejidad lógica de los chips de las etiquetas, dado que precisarían de menos energía para funcionar, lo que a su vez ampliaría el área de cobertura de los lectores.

Por otro lado, se ha realizado un estudio para caracterizar el comportamiento de la frecuencia de enlace por retrodispersión (Backscatter-Link Frequency, BLF), que es la subportadora con la que cada etiqueta transmite la información al lector. Los resultados arrojan un comportamiento bastante aleatorio de este parámetro, tanto en las variaciones que se producen respecto al valor esperado por el lector en la primera respuesta de la etiqueta, así como en el resto de los intercambios de información que se producen. Esto podría ser aprovechado como una característica diferenciadora de cada etiqueta y emplearse en los protocolos de comunicación.

Como consecuencia de todo ello, se propone la creación de dos clases de etiquetas pasivas: una clase ligera, en la que las etiquetas sean simplificadas empleando las propuestas que se realizan en esta tesis, manteniendo toda su funcionalidad y orientadas a labores de identificación masiva de objetos; y una clase robusta, con etiquetas más complejas que las actuales y que incluyan nuevas funcionalidades, estando más orientadas a aplicaciones específicas.

Los principales resultados obtenidos en los distintos trabajos llevados a cabo se han difundido mediante publicaciones en varias revistas científicas indexadas, la participación en distintos foros como congresos nacionales e internacionales y la obtención de una patente nacional.

Con todo ello, se ha pretendido contribuir al desarrollo de la RFID y todas las tecnologías asociadas, para facilitar su adopción masiva por todos los sectores a nivel mundial y como pieza clave sobre la que articular la implementación real del IoT.

Palabras clave: RFID, redes inalámbricas de sensores y actuadores, Internet de las Cosas, caracterización electromagnética, protocolos de comunicación, generación de números pseudoaleatorios, algoritmo ultraligero, emulador de etiquetas.

Summary.

In the current implementation framework of the Internet of Things (IoT), Radio Frequency Identification (RFID) is key for the automatic and univocal identification of every object that can be found in the network. In its broadest sense, radio frequency identification comprises all technologies in which radio waves are used to identify things. Therefore, different technological aspects associated with RFID have been worked with in this thesis, contributing to their evolution, development and application.

Apart from the identification, some tags incorporate sensors to collect more information about the objects that bring them. This has led to the emergence of Wireless Sensor Networks (WSN), which have been developed in other alternatives such as Wireless Sensor and Actuator Networks (WSAN) or Wireless Body Area Networks (WBAN). In this thesis, several studies and developments with these technologies have been faced, giving special attention in how communications between devices are carried out and obtaining several completely operative systems that are prepared to work in the IoT framework.

Passive is the most widespread and implemented RFID technology, because one reader can identify multitude of tags in a short period of time. Among other features, it presents long read range, reduced cost of tags and the possibility to operate in dense tag environments. Making it the most appropriate technology to use when huge quantities of things need to be quickly and efficiently identified.

Focusing on the study of passive RFID systems communications, in a physical level, the design and development of a complete system for electromagnetic characterization of construction materials and solutions have been carried out. The system allows to find out the behavior of electromagnetic signals when they interact with real samples of construction materials and solutions. Therefore, it can be applied to the benefit of RFID technology, as well as other wireless technologies that use radio frequency for their operation.

Deeply studying how communications between RFID readers and tags are carried out, it should be highlighted the relevance of the pseudorandom number generator that tags must implement and its influence for that the communications processes work properly. In this sense, a new ultra-lightweight algorithm is proposed that complies with current regulations and represents an important simplification in the logic of the chips. From the obtained results of the algorithm implementation in a developed tag emulator and their comparison with the generators that are implemented in tags, the use of the proposal to replace the currently used mechanisms is proposed. This would reduce the logical complexity of the tags chips because they would require less energy to operate, which in turn would increase the coverage area of the readers.

Also, a study to describe the behavior of the Backscatter Link Frequency (BLF), which is the subcarrier with which each tag transmits the information to the reader, has been carried out. The results show a sufficient random behavior of this parameter in the variations that appear with respect to the first expected value by the reader, in the first tag response, as well as in the remaining information exchanges. This could be handled as a distinguishing feature of each tag and applied in the communication protocols.

Consequently, the creation of two classes of passive tags is proposed: the light class, where tags are simplified using the proposals made in this thesis, preserving all the functionality and being oriented to massive identification tasks; and a robust class, with more complex tags that would include new features and where they would be oriented to specific applications.

The main results from the different executed works have been disseminated through publications in several indexed scientific journals and the participation in diverse forums such as international and national conferences, as well as the achievement of a national patent.

All these actions have been aimed to contribute to the development of RFID and all associated technologies, to accelerate their massive adoption by all sectors worldwide, as a key part over which to articulate the real implementation of the IoT.

Keywords: RFID, wireless sensor and actuator networks, Internet of Things, electromagnetic characterization, communication protocols, pseudorandom number generation, ultra-lightweight algorithm, tag emulator.

Índice.

Capítulo 1. Introducción.	13
1.1. Motivación	14
1.2. Objetivos	15
1.3. Estructura del documento.	16
Capítulo 2. La tecnología RFID en el contexto actual.	19
2.1. Orígenes y evolución	19
2.2. Sistemas de identificación por radiofrecuencia.	21
2.2.1. Tecnología RFID pasiva	22
2.2.2. Tecnología RFID activa.	24
2.3. Redes inalámbricas de sensores.	25
2.3.1. Evolución y aplicaciones.	25
2.3.2. Sistema de monitorización del consumo eléctrico real.	25
2.4. Redes inalámbricas de sensores y actuadores.	27
2.4.1. Evolución y aplicaciones.	27
2.4.2. Sistema de control inteligente para el uso eficiente de la energía.	28
2.5. Redes inalámbricas de ámbito personal.	31
2.5.1. Desarrollos para la mejora de la asistencia sanitaria y la salud	31
2.5.2. Sistema de seguridad activa para la monitorización de personas	32
2.6. Ahorro y eficiencia energética.	34
2.6.1. Hacia la sostenibilidad energética	35
2.6.2. Cosecha de energía	36
2.7. El papel de la RFID en el Internet de las Cosas.	38
2.7.1. Características y evolución	39
2.7.2. Sistema automático de monitorización y seguimiento de muestras.	40

Capítulo 3. Propuestas para la mejora de la eficiencia electromagnética en sistemas RFID.	45
3.1. Ondas electromagnéticas.	46
3.2. Propagación de señales en sistemas RFID.	48
3.3. Caracterización electromagnética de materiales.	50
3.3.1. Diseño y fabricación del equipo de medida.	50
3.3.2. Realización de medidas y resultados.	56
3.4. Discusión de resultados y aplicaciones.	59
Capítulo 4. Análisis y propuestas sobre protocolos de comunicación para RFID – UHF pasiva.	61
4.1. Protocolo de comunicación RFID – UHF.	62
4.1.1. Características físicas.	62
4.1.2. Consideraciones lógicas.	65
4.1.3. Identificación y gestión de etiquetas.	66
4.1.4. Mecanismos anticolisión.	69
4.2. Generación de números pseudoaleatorios en las comunicaciones RFID.	72
4.3. Algoritmo ultraligero para la generación de números pseudoaleatorios en etiquetas pasivas. .	73
4.3.1. Funcionamiento del algoritmo.	73
4.3.2. Adecuación a la especificación de EPC.	75
4.3.3. Validación de la propuesta.	77
4.4. Desarrollo de un emulador de etiquetas RFID pasivas.	83
4.4.1. Diseño y construcción del hardware.	86
4.4.2. Implementación del software.	90
4.4.3. Funcionamiento y pruebas realizadas.	92
4.4.4. Implementación física del algoritmo ultraligero propuesto.	96
4.5. Comportamiento de la BLF en etiquetas reales.	98
4.5.1. Frecuencia de enlace por retrodispersión.	98
4.5.2. Medida y caracterización de la BLF.	101
4.5.3. Análisis y aplicación de los resultados.	104
4.6. Discusión de resultados y sus aplicaciones.	108
Capítulo 5. Conclusiones.	111
5.1. Trabajos realizados y resultados obtenidos.	111
5.2. Aportaciones.	114
5.3. Propuestas de trabajos futuros.	117
Referencias.	119
Listado de tablas.	132
Listado de figuras.	133
Glosario.	135

Capítulo 1.

Introducción.

Según la RAE, identificación se define como acción y efecto de identificar o identificarse. Término que usamos y ponemos en práctica a diario, aunque en la mayoría de las ocasiones no seamos conscientes de ello. Estamos tan acostumbrados a realizarlo desde siempre, que lo tenemos totalmente interiorizado. Es algo prácticamente instintivo, que se ha convertido en un proceso que pasa totalmente desapercibido y al que no se le presta mayor atención, si bien no por ello conviene restarle la importancia que se merece. ¿Eres capaz de imaginar un mundo sin identificación?... El caos.

Inmediatamente posterior al nacimiento de una persona, una de las primeras tareas que se realizan es dotarla de una identidad, que también se define como el conjunto de rasgos propios de un individuo o una colectividad que los caracterizan frente a los demás. A partir de ese momento, siempre hay que identificarse antes de realizar cualquier tipo trámite y se obtiene un DNI (Documento Nacional de Identidad), con un número asociado a cada uno de nosotros y que nos diferencia del resto hasta el fin de los días.

Lo mismo sucede en el caso de los animales, sobre los que hoy en día se exige una exhaustiva trazabilidad a lo largo de toda su vida. Pero en este caso, el proceso de identificación es bastante más complejo que en el caso de los humanos. Probablemente debido al aumento en el número de ítems a identificar. Crecimiento que se convierte en exponencial si pensamos en la infinidad de objetos o cosas que nos rodean y que utilizamos a diario. A medida que aumentan los ítems, se complican más los mecanismos para diferenciar cada uno de ellos del resto de elementos.

Pero ahora, pensemos a lo grande. Un supermercado que tiene en sus estanterías miles de referencias, cada una con un precio y unas características determinadas. O una agencia de transportes, que tiene que gestionar millones de paquetes a la hora. En estos casos, identificar cada uno de los ítems puede convertirse en una auténtica pesadilla si no se dispone de las herramientas adecuadas.

Afortunadamente, el humano es un ser racional y con el paso de los tiempos ha ido empleando diversas técnicas para tener identificadas e inventariadas las cosas que le rodean. Pero cuando este tipo de tareas han de llevarse a cabo a gran escala, la identificación automática se convierte en una verdadera necesidad.

Precisamente para atajar esta situación surge la Identificación por Radiofrecuencia, o simplemente RFID, de sus siglas en inglés *Radio-Frequency IDentification*. Esta tecnología que se basa en el uso de cualquier dispositivo de radiofrecuencia cuya función principal es la identificación de un objeto, animal

o persona. No obstante, este concepto ha de entenderse en su más amplio sentido, dado que las características técnicas y distinciones entre los dispositivos de radiofrecuencia implicados se encuentran en constante cambio y evolución. Por lo que la RFID también puede entenderse como una tecnología para la identificación automática de objetos, animales o personas, en definitiva, de cualquier cosa.

El conjunto de dispositivos electrónicos encargados de convertir esta tecnología en una realidad y ponerla en práctica recibe el nombre de sistema RFID. Los hay de muy diversos tipos y características. Aunque un sistema RFID consta siempre de, al menos, dos componentes: una etiqueta, compuesta por una antena y un chip electrónico, que se encuentra en el objeto a identificar y es el dispositivo físico real en el que se encuentran los datos de identificación; y un lector, usualmente compuesto por una unidad de control, un módulo de radiofrecuencia (transceptor) y una antena, que es el encargado de la captura y/o escritura de los datos en la etiqueta y habitualmente dispone de interfaces adicionales para enviar los datos recibidos a otros sistemas, como ordenadores, sistemas de control, etc.

1.1. Motivación

Hoy en día, las personas ya usamos etiquetas RFID de forma rutinaria, aunque sin ser plenamente conscientes de lo que ello implica. Algunos ejemplos ilustrativos pueden ser el uso de las tarjetas de proximidad para el control de accesos, las etiquetas empleadas en los sistemas automatizados de pago de peaje, tarjetas para realizar los pagos mediante un simple gesto de aproximación, etc. Siendo todos ellos casos de la vida cotidiana que se basan en el uso de tecnología RFID.

Desde sus comienzos, la tecnología RFID ha experimentado una gran evolución, que se ha visto influenciada por la aparición de grandes avances que han emergido con fuerza para convertirse en tecnologías con entidad propia, como puede ser el caso de las redes inalámbricas de sensores. Llegando incluso en ocasiones a eclipsarla. Aunque conviene no confundir una cosa con la otra, ya que ambas tecnologías son complementarias.

Cabe mencionar que no es la única alternativa tecnológica para llevar a cabo labores de identificación automática. En cada aplicación específica se debe buscar la mejor solución de entre el conjunto de todas las tecnologías existentes para obtener los mejores resultados posibles. En este sentido, los sistemas RFID presentan un gran potencial por características como el manejo de cantidades considerables de datos, una velocidad de lectura muy rápida, distancias de lectura elevadas (del orden de metros) y sin necesidad de que exista visión directa entre los dispositivos, o la capacidad de funcionamiento en entornos muy poblados (con alta densidad de etiquetas) [1].

Por todo ello, la tecnología RFID, entendiéndose como la relacionada con los sistemas RFID, se erige como la sucesora del actual código de barras, ampliamente utilizado a nivel global, principalmente por dos motivos: identificación única, a diferencia del código de barras que indica el tipo de objeto en el que está impreso, la RFID va un paso más allá, proporcionando un número de serie único a cada objeto que lo distingue de entre el resto de muchos millones de objetos idénticos; y automatización, las etiquetas RFID pueden leerse sin contacto visual directo y de forma autónoma, pudiendo ser escaneadas cientos de ellas a grandes velocidades por un único lector, en contraposición a los códigos de barras, que necesitan ser escaneados ópticamente de manera individual mediante un contacto visual directo con los lectores y que en muchos casos requiere la intervención humana [2].

La identificación por radiofrecuencia (RFID) es una tecnología inalámbrica que puede ser utilizada para múltiples aplicaciones. En particular, la tecnología RFID que opera en la banda de UHF (Ultra High Frequency RFID) presenta, entre otras características, lectores con un largo alcance, baja inversión para

asociar etiquetas a cada objeto y la posibilidad de operar en entornos con alta densidad de etiquetas. Esto la convierte en la tecnología más apropiada para su uso en una amplia gama de sectores comerciales como la logística o la producción, en los que es necesario identificar grandes cantidades de artículos de forma rápida y eficiente [3]. En este sentido, la RFID puede ser vista como un medio de etiquetar explícitamente los objetos para facilitar su percepción por parte de los dispositivos y sistemas informáticos. Siendo estas, además, propiedades claves para el desarrollo del marco del Internet de las Cosas (Internet of Things, IoT) donde todos los objetos estarán en línea y conectados entre sí [4].

Desde la aparición de las primeras aplicaciones civiles, la tecnología RFID pasiva se ha ido perfeccionando. Gracias a los avances obtenidos durante años de investigación y que se han ido recogiendo en las versiones de los estándares, actualmente la convierten en una tecnología madura y que, a pesar de sus dificultades técnicas, presenta grandes resultados. Pero que precisa de revisión y cambio para adaptarse a las nuevas exigencias y demandas de los marcos de trabajo actuales, como es el caso del Internet de las Cosas (IoT) [5].

En lo que respecta a la identificación masiva de objetos, la tecnología RFID pasiva es la más extendida e implantada en la industria [6]. Ello es debido, en parte, al reducido coste de las etiquetas pasivas que se asocian a cada objeto que se desea identificar y a la relativa baja inversión que se ha de realizar para su implantación frente a otras alternativas de tecnología RFID.

Sin embargo, la tecnología RFID aún no ha experimentado el gran uso que se predecía. Probablemente debido, en parte, a algunos problemas de funcionamiento de la tecnología, como colisiones o identificaciones erróneas, que han sido objeto de una amplia variedad de trabajos de investigación y que a día de hoy están ampliamente subsanados y superados. No obstante, aún quedan aspectos que abordar y que se pueden mejorar de la tecnología, siendo este uno de los principales motivos por los que se aborda la presente tesis.

1.2. Objetivos.

Mediante la realización de esta tesis se pretenden llevar a cabo una serie de trabajos y estudios que ayuden a mejorar y optimizar el funcionamiento de los sistemas de identificación por radiofrecuencia, de tal forma que éstos se puedan aplicar más fácilmente y con mayor fiabilidad a multitud de aplicaciones actuales y futuras. Contribuyendo al impulso definitivo que necesita la tecnología para ser adoptada de forma masiva por todos los sectores de forma global, incentivada por la implantación del Internet de las Cosas.

Particularmente, se pretende contribuir a mejorar las comunicaciones y los dispositivos implicados de manera que éstos sean lo más eficientes posibles, contribuyendo así a un ahorro energético y probablemente de recursos en el uso de la tecnología. Los trabajos planteados giran en torno a la tecnología RFID tanto pasiva, puesto que es la más económica y extendida en el mercado; como activa, ya que dado su grado de desarrollo e implantación se trata de una tecnología más abierta y que permite mayor flexibilidad para la realización de trabajos de muy distinta naturaleza. Para lo que se fijan los siguientes objetivos:

- Realizar un análisis sobre el estado actual de la tecnología, detectando posibles problemas asociados con su uso e identificando ejemplos de aplicaciones en las que se emplee la tecnología.

- Contribuir a mejorar las instalaciones de RFID existentes, así como proporcionar herramientas que permitan un mejor entendimiento del funcionamiento de la tecnología, lo que repercutirá en su mejora y optimización.
- Trabajar con los protocolos de comunicación aérea para sistemas RFID pasivos de UHF, dado que es la tecnología más extendida, procurando detectar posibles problemas y proponiendo soluciones al respecto.
- Aportar nuevas ideas y propuestas que redunden en la mejora de la tecnología, facilitando su uso y aplicación.
- Desarrollar un dispositivo o plataforma que replique el comportamiento de las etiquetas pasivas para poder llevar a cabo pruebas reales de comunicación y cambios en los protocolos asociados.
- Trabajar con sistemas RFID tanto pasivos como activos, incluyendo redes inalámbricas de sensores y todas sus variantes, para contribuir en el desarrollo y aplicación de la tecnología en el marco del IoT.
- Utilizar la tecnología para contribuir en el uso eficiente de la energía y el ahorro de la misma, contribuyendo a afrontar el desafío energético existente en la actualidad.
- Publicar y difundir los principales resultados científicos que se obtengan en distintos foros y a través de diversos medios.

En definitiva, contribuir al desarrollo y evolución de las tecnologías asociadas a la RFID con todos los recursos humanos y materiales posibles.

1.3. Estructura del documento.

El resto del presente documento de tesis se estructura en varios capítulos en los que se agrupan y describen cada uno de los trabajos llevados a cabo, encontrándose todos ellos bajo el paraguas de la tecnología RFID.

En el capítulo 2 se analiza el estado actual de la tecnología RFID, realizando un recorrido desde los orígenes de la tecnología hasta su aplicación como base sobre la que implantar el Internet de las Cosas. Deteniéndose en los principales hitos que han cambiado su funcionamiento y la forma de trabajar con la tecnología. Poniendo especial énfasis en el caso de las redes inalámbricas de sensores, incluidas sus variantes, y describiendo algunos ejemplos de uso y desarrollos de equipos realizados.

Poniendo el foco en la tecnología RFID pasiva, a la que se le presta especial atención en esta tesis, el capítulo 3 se centra en los aspectos más físicos de la tecnología, como es la propagación de las ondas electromagnéticas de radiofrecuencia. Siendo el aire el medio por el que se realizan todas las comunicaciones e intercambian los datos. Además, se describe el diseño, la construcción y puesta en marcha de un equipo para la caracterización electromagnética de materiales de construcción y soluciones constructivas, especialmente diseñado para ser aplicado en la mejora del funcionamiento de los sistemas RFID en instalaciones reales.

El capítulo 4 se ha reservado para las comunicaciones aéreas entre lectores y etiquetas RFID pasivas, donde los protocolos de comunicación dictaminan cómo éstas han de llevarse a cabo. Tras un análisis sobre los trabajos de investigación desarrollados en este ámbito durante los últimos años, se detalla la propuesta de un algoritmo ultraligero que contribuye a la simplificación de las etiquetas pasivas,

reduciendo la complejidad de su lógica interna y mejorando su eficiencia energética. También, se describen algunas propuestas alternativas de mejora, como el estudio realizado para la caracterización de un posible elemento diferenciador de las etiquetas. En este capítulo también se recoge el diseño y desarrollo de un emulador de etiquetas pasivas que se comporta como si fuese una etiqueta pasiva real más y que permite la realización de pruebas reales de comunicación y funcionamiento en las que estén involucradas las etiquetas pasivas de RFID. Lo que ha permitido probar de forma práctica las propuestas realizadas en esta tesis

Finalmente, en el capítulo 5 se recogen las principales conclusiones que se alcanzan a partir de los resultados obtenidos tras la realización de todos los trabajos que han formado parte de esta tesis. Se destacan los hitos conseguidos, así como las principales aportaciones que han emanado del trabajo realizado. Por último, se plantean una serie de trabajos futuros que amplían y complementan los que se han desarrollado durante la tesis.

Capítulo 2.

La tecnología RFID en el contexto actual.

Los sistemas RFID generalmente se caracterizan por utilizar dispositivos simples en un extremo del enlace y dispositivos más complejos en el otro extremo. Los dispositivos simples, también llamados etiquetas, son pequeños y baratos, por lo que pueden desarrollarse a gran escala de forma rentable. Estos dispositivos se activan para enviar información al lector (dispositivo más complejo), mediante la modificación de la carga de la antena de la etiqueta de acuerdo con un código, o generando, modulando y transmitiendo señal de radio. Para ello se emplean una amplia variedad de técnicas de modulación y codificación para distintos valores de frecuencias de radio. Aparte de estos dispositivos, un software se encarga del tratamiento y la gestión de la información recogida de las etiquetas por el lector.

Pueden existir sistemas RFID de sólo lectura, en los que los datos son transmitidos en una única dirección, desde la etiqueta al lector; o de lectura y escritura, en los que la comunicación es bidireccional. Aunque para entender mejor su funcionamiento, conviene tener presente la evolución de esta tecnología, así como los fundamentos en los que se basa.

2.1. Orígenes y evolución.

La primera generación y transmisión controlada de una señal de radiofrecuencia, demostrada por Ernst F.W. Alexanderson en 1906, supuso toda una revolución y el comienzo de la era de las radiocomunicaciones modernas. A partir de este hito, en las primeras décadas del siglo XX, se comenzó a desarrollar la tecnología de radar, que consiste en la emisión de ondas de radio para detectar y localizar objetos mediante la reflexión de dichas ondas, pudiéndose determinar la posición y velocidad de un objeto. Y es que la RFID puede entenderse como una combinación entre las tecnologías de radiodifusión y el radar. Por lo que debido a la convergencia existente entre ambas disciplinas, la RFID se comenzó a vislumbrar justo después del desarrollo del radar [7]. Puede decirse que la tecnología RFID, tal y como se conoce en la actualidad, tiene sus inicios en la II Guerra Mundial, donde para las batallas aéreas se desarrolló el sistema Amigo-Enemigo (*Friend or Foe*). En este tipo de sistemas, se hacía rebotar en los aviones la señal de radar modulada, gracias a la que se podían identificar, por tanto, los aviones de uno u otro bando [8].

La primera aplicación civil con tecnología RFID apareció en 1969 en EEUU y estaba destinada a la identificación de vehículos, pacientes y tarjetas de crédito. Aunque el uso y explotación industrial de la tecnología estaba poco extendido debido su elevado coste durante esos años. Por la misma época se desarrollaron los sistemas de vigilancia de artículos (Electronic Article Surveillance, EAS) [9], que básicamente emplean etiquetas pasivas de RFID de 1 bit. Se trata posiblemente del primer caso de uso de tecnología RFID más extendido a nivel mundial y que todavía sigue muy vivo a día de hoy [10].

Posteriormente, en la década de los 80, se comenzaron a implantar sistemas para el pago automatizado de peajes. En este caso, ya se trabajaba a 915 MHz, aunque la etiqueta sólo contenía una cantidad muy limitada de información. Paralelamente, otro campo de aplicación fue el seguimiento de ganado. Inicialmente para monitorizar vacas que estaban bajo tratamiento médico, pero su uso se expandió rápidamente [11], [12]. Para estas aplicaciones se empleaban frecuencias alrededor de 125 kHz, que proporcionan un menor tamaño de las etiquetas. En esta época, se lanzaron sistemas que todavía se comercializan hoy en día, como el caso de TIRIS de Texas Instruments®.

Pronto aparecieron desarrollos en tecnología de alta frecuencia (HF, alrededor de 13,56 MHz), lo que trajo consigo un mayor alcance de lectura y mayores velocidades de transferencia de datos [13]. En Europa, Mikron® (que más tarde pasó a ser parte de Philips®, actualmente NXP®), lanzó el legendario protocolo *MIFARE*, que, a día de hoy, junto con muchas variantes sirven como base para de la tecnología NFC y de las formas de pago más actuales, popularmente conocidas como *contactless* (Figura 2.1).



Figura 2.1. Ejemplos de etiquetas con tecnología NFC (CC).

A comienzos de los años 90, IBM® comenzó a realizar pruebas con la cadena estadounidense Walmart®. Pero es a finales de esta década cuando apareció el Auto-ID® Center, dentro del Instituto Tecnológico de Massachusetts (MIT®). Su gran aportación fue la de almacenar toda la información relevante en una gran base de datos, en vez de en la propia etiqueta. Lo que simplificó enormemente el funcionamiento de las etiquetas, orientándolas únicamente labores de identificación. En 2003, el Auto-ID® Center pasó el testigo de la investigación a los Auto-ID® Labs.

Al mismo tiempo, se estableció EPCglobal®, que es una organización creada para lograr la adopción y estandarización a nivel mundial de la tecnología de Código Electrónico de Producto (EPC, Electronic Product Code). Sus esfuerzos están enfocados en dos áreas principales: por un lado, crear estándares mundiales para el uso de la tecnología RFID, tanto a nivel de interfaces aéreas como del software que maneja la información; y, por otro lado, lograr la visibilidad global de todos los objetos, mediante EPCIS (EPC Information System) [14].

Todos estos pasos prepararon el camino para aumentar la compatibilidad, el rendimiento y la fiabilidad de los sistemas de RFID-UHF. En este sentido, surgieron estándares mundiales, como el *EPC Class 1 Gen2*, en 2004. Los cuales alentaron a las primeras organizaciones importantes que habían apostado por la tecnología, como Walmart®, Tesco® o el Departamento de Defensa de los EEUU, hasta el punto de que emitieron órdenes exigiendo a sus proveedores el uso de RFID en todos sus envíos.

Pero dada la inmadurez de los beneficios que aportaba la RFID a la cadena de suministro a finales de los años 2000. Posteriormente unida a la insalubre financiación de capitales, que derivó en una de las mayores crisis financieras a nivel mundial de los últimos años. A lo que también hay que sumar ciertas disputas sobre patentes y guerras comerciales. Generándose un clima desapropiado, que ha provocado algunos años de vacilación y retrasos en la adopción de la RFID a gran escala. Ya en la década de 2010, las principales compañías a nivel mundial han convertido a esta tecnología en indispensable, especialmente en aplicaciones industriales y minoristas.

Por lo que en la actualidad no hay nada que detenga el uso masivo de la tecnología RFID. De hecho, ya se ha convertido en parte de nuestra vida cotidiana en forma de etiquetas, tarjetas, controles de accesos, pagos, etc. Aunque en la mayoría de las ocasiones no somos conscientes de ello y empleamos RFID sin saber que en realidad la estamos usando. Además, la aparición de nuevas técnicas de identificación y seguimiento de productos y objetos, mediante etiquetas de radiofrecuencia (RFID), suponen un punto de inflexión para paliar los tradicionales problemas de integración en los sistemas altamente distribuidos [1].

En 2014, Smartrac®, Impinj®, Google® e Intel® se unieron para establecer una alianza con el objetivo de impulsar definitivamente la adopción global de la tecnología RFID-UHF. Esta alianza, bautizada como *RAIN RFID* [15], fue anunciada en abril de 2014 y a finales de año se habían unido unas 50 empresas de 4 continentes distintos. Sus principales funciones se centran en promover la concienciación, aumentar la formación y el apoyo universal a la tecnología RFID-UHF. Esta alianza la conforman fabricantes, distribuidores, vendedores e investigadores que trabajan con la especificación EPC Gen2 para RFID-UHF [16], incorporada a la norma ISO/IEC 18000-6 [17]. La alianza RAIN RFID forma parte de AIM Global [18], la autoridad mundial en materia de identificación automática, recolección de datos y establecimiento de redes en entornos móviles. Se dedica a acelerar el crecimiento y el uso de las tecnologías y servicios de identificación automática y movilidad en todo el mundo.

En definitiva, desde la aparición de la primera aplicación civil de RFID, la tecnología ha ido evolucionando e incorporando los avances tecnológicos que se han ido sucediendo, hasta llegar a los sistemas RFID que conocemos en la actualidad y que emplean tecnología microelectrónica vanguardista junto con las más avanzadas técnicas de comunicación por radiofrecuencia. Aunque en medio de esta evolución, han surgido variantes que se han distanciado de la RFID para convertirse en tecnologías con entidad propia y sobre las que merece la pena detenerse.

2.2. Sistemas de identificación por radiofrecuencia.

La identificación por radiofrecuencia es un concepto amplio, dado que puede aplicarse a cualquier tecnología en la que mediante ondas de radio se establezca una comunicación entre dispositivos y que durante esa comunicación se identifiquen emisor y/o receptor. De tal forma que quede asociada la información recibida y/o enviada con un determinado objeto físico, produciéndose el proceso de identificación. Pero con el paso de los años, el uso de estos términos se ha reservado casi en exclusiva para referirse a la tecnología RFID.

Todo sistema de RFID que se precie debe comprender, al menos, los siguientes elementos: una o varias etiquetas RFID asociadas a los objetos de los que se desea extraer información; un lector que recoja e interprete la información transmitida a través de las ondas electromagnéticas; y un software que gestione los datos para la aplicación en la que se esté usando el sistema y/o se conecte a una base de datos para su almacenamiento. Dado que la comunicación entre el lector y la etiqueta se produce por señales de radiofrecuencia, ambos deben estar equipados con antenas sintonizadas a la misma frecuencia de trabajo, haciendo posible el establecimiento del enlace y el funcionamiento de la interfaz de comunicación aérea.

Atendiendo al tipo de alimentación energética que posean las etiquetas, éstas pueden clasificarse en etiquetas activas, semiactivas o semipasivas y pasivas [19]. Y por tanto se habla de distintas variantes de la tecnología. Aunque, desde sus inicios, la tecnología RFID se basó en etiquetas pasivas, puesto que carecían de fuente de alimentación externa. Sin suministro de energía, la vida de una etiqueta pasiva es virtualmente ilimitada y no requiere mantenimiento. Siendo esta una de las características que hacen a esta tecnología idónea para implantarse a gran escala en infinidad de objetos y aplicaciones.

2.2.1. Tecnología RFID pasiva.

La tecnología RFID emplea las ondas electromagnéticas para transferir datos desde una etiqueta RFID, que se encuentra asociada a un objeto, y un lector RFID, que recoge esos datos y los entrega al software encargado de gestionarlos (Figura 2.2). Pero a diferencia de un sistema de comunicación al uso, en el caso de la RFID pasiva no es la etiqueta la que inicia la comunicación, sino que es el dispositivo con el rol de lector el que comienza el proceso mediante el envío de señales electromagnéticas que instan a las etiquetas que se encuentren dentro de su área de cobertura a responderle según el caso.

Las comunicaciones RFID constituyen un caso especial de las comúnmente denominadas como de radiofrecuencia (RF), dado que el emisor y el receptor trabajan de forma distinta. Los lectores RFID transmiten su señal utilizando determinadas técnicas de codificación y modulación, mientras que las etiquetas responden utilizando otras diferentes. Se debe tener en cuenta que ambos participan en el mismo proceso de comunicación y, por tanto, han de interpretar la información proporcionada por el otro extremo.

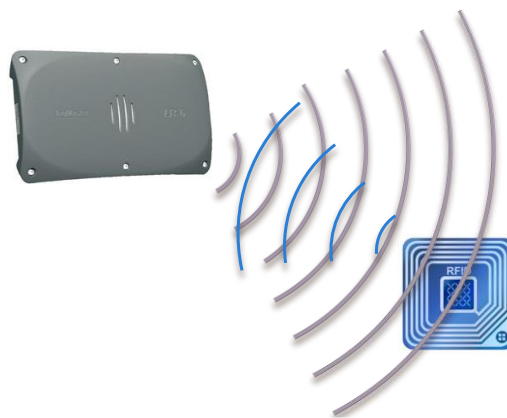


Figura 2.2. Lector y etiqueta RFID pasiva en funcionamiento.

En un sistema RFID pasivo, las etiquetas no disponen de una fuente de alimentación propia y han de obtener la energía que necesitan para funcionar de la onda electromagnética generada y transmitida por el lector. Para transferir información desde la etiqueta al lector se emplea el principio de la retrodispersión (*backscatter*). En este proceso, es el lector quien envía una señal sin modular (continua) a la frecuencia de trabajo hacia la etiqueta. Y con la energía que aporta esta señal, la etiqueta interpreta

los comandos recibidos, lee en su memoria interna los datos almacenados y cambia la carga de su antena según una determinada codificación, de acuerdo con los datos rescatados que desea transmitir. Dado que las etiquetas pasivas carecen de energía suficiente para emitir su propia señal, el circuito integrado de la etiqueta realiza la modulación de la portadora del lector modificando físicamente la impedancia de su antena. De tal forma que se refleja mayor o menor potencia según se desee en cada instante. Esquemáticamente, puede entenderse como un pequeño interruptor que conecta y desconecta la antena de la etiqueta, provocando que se refleje más o menos señal (Figura 2.3). Por tanto, la señal reflejada desde la etiqueta queda modulada con la información deseada previamente codificada. Finalmente, esta señal modulada de retorno, que es la propia portadora del lector con variaciones, es recibida por el lector, que es capaz de interpretarla y de extraer los datos útiles enviados por la etiqueta.

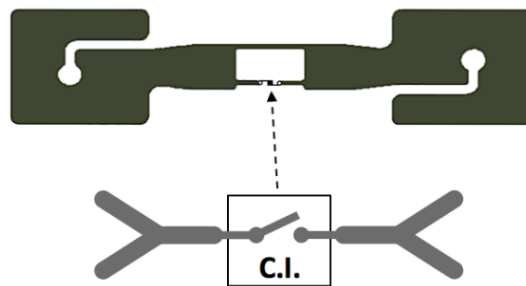


Figura 2.3. Etiqueta RFID pasiva y esquema de funcionamiento de su circuito integrado (CI).

Las etiquetas pasivas pueden operar en cualquiera de las bandas de frecuencias establecidas. Así se dispone de: las etiquetas de baja frecuencia (LF), que funcionan en el rango de 124-135 kHz y tienen rangos de lectura nominales de hasta medio metro; las etiquetas de alta frecuencia (HF), que funcionan en torno a los 13,56 MHz y presentan rangos de hasta un metro o más (aunque típicamente se reduce al orden de decenas de centímetros); y las etiquetas de ultra alta frecuencia (UHF), que operan en frecuencias de 860 a 960 MHz, e incluso a veces en los 2,45 GHz, poseen el mayor alcance de todas hasta las decenas de metros. Sin embargo, las etiquetas RFID pasivas de UHF están sujetas a más interferencias que las de frecuencias menores.

Debido a la falta de regulación coordinada del espectro radioeléctrico a nivel mundial, estatal y comarcal, desde sus comienzos, la tecnología ha contado con la limitación de no poder utilizar exactamente la misma frecuencia en todas las zonas geográficas del planeta. Por este motivo han de desarrollarse equipos específicos y adaptados a cada una de ellas. En el caso de las comunicaciones para RFID-UHF, han debido adaptarse a las bandas de frecuencia de libre uso y que no requieren licencia para el funcionamiento de los sistemas (Figura 2.4).

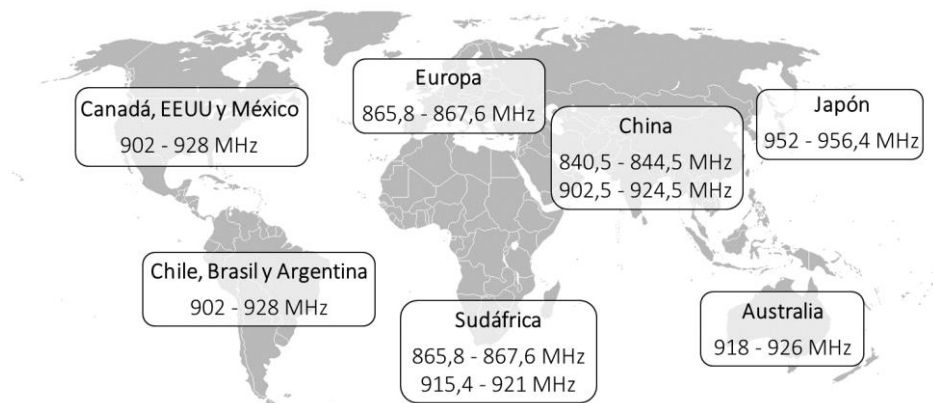


Figura 2.4. Rangos de frecuencias para el funcionamiento de la tecnología UHF-RFID en el mundo (CC).

Actualmente, el testigo de la tecnología RFID-UHF pasiva lo ha recogido RAIN RFID, que se entiende como una tecnología inalámbrica que conecta miles de millones de artículos de uso diario a Internet, permitiendo a las empresas y a los consumidores identificar, localizar, autenticar y prestar atención a cada artículo (Figura 2.5). Las etiquetas RAIN contienen un circuito integrado (chip) que es adherido o incrustado en artículos, cajas, palés, u otras cosas. Los lectores de RAIN envían una señal inalámbrica para identificar, localizar, autenticar y/o activar las etiquetas. Y pueden estar incrustados en dispositivos, sostenidos por una persona, o instalados en puertas o techos. Por su parte, el software RAIN se encarga de recoger los datos de la etiqueta y puede conectar esta información con redes o nubes para permitir la gestión de inventarios, el seguimiento de los activos y muchas otras aplicaciones. Lo que resulta fundamental para el desarrollo e implantación del Internet de las Cosas.

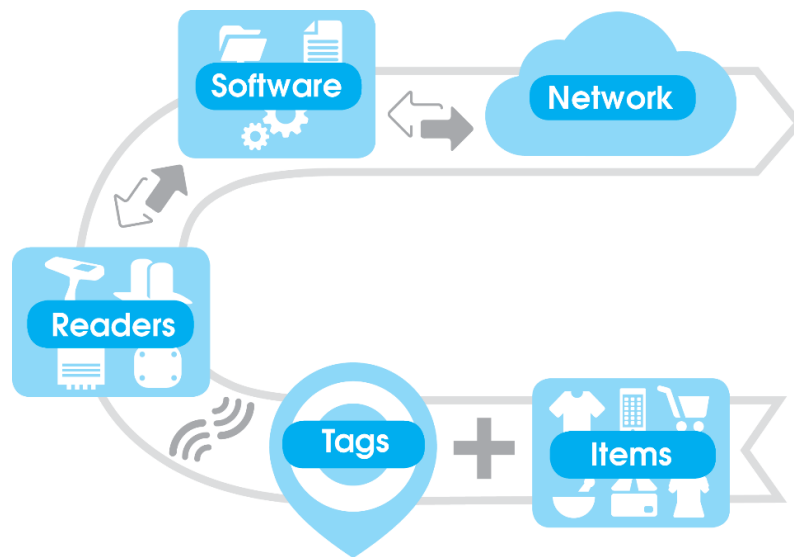


Figura 2.5. Partes de la tecnología RAIN RFID [15].

2.2.2. Tecnología RFID activa.

Dependiendo de la aplicación y para llevar a cabo un mejor seguimiento de los objetos a los que se encuentran asociados, algunas etiquetas RFID disponen de una batería asociada. Esta batería se utiliza para proporcionar energía a la etiqueta y/o a los sensores conectados a las etiquetas, denominándose como etiquetas semiactivas o semipasivas. Estas etiquetas siguen siendo pasivas, en el sentido de que emplean la retrodispersión de la señal del lector para comunicarse con él, por lo que también se las conoce como etiquetas pasivas asistidas por batería (BAP). Pueden recoger y almacenar los datos de los sensores conectados a ellas. Aunque también es cierto que la fuente de alimentación adicional provoca que suelen tener un mayor alcance, dado que no necesitan tanta potencia del lector para funcionar.

Las etiquetas activas se definen a menudo como etiquetas con una fuente de alimentación. Y aunque esto es cierto, lo que verdaderamente caracteriza a una etiqueta activa es que tiene un transmisor independiente. Este transmisor requiere para su funcionamiento de más energía de la que puede suministrar un lector, por lo que necesita una fuente de energía propia, normalmente una batería. Las etiquetas activas suelen tener un alcance muy largo (en ocasiones más de 100 metros) y, debido a la potencia extra, tienen menos problemas de interferencias en las comunicaciones como, por ejemplo, la proximidad de elementos metálicos. Tanto las etiquetas semiactivas como las activas necesitan de un mantenimiento y tienen una vida limitada.

Con la introducción de una batería externa que suministra a la etiqueta toda la energía que necesite, así como con la incorporación de sensores, las etiquetas comenzaron a tener cada vez más funciones y

fueron ampliando sus capacidades. Finalmente, esto vino a desembocar en la tecnología de Redes Inalámbricas de Sensores (Wireless Sensor Networks, WSN). En este tipo de redes quizás pase más desapercibida la función de identificación y se le preste especial atención a todos los datos que los distintos sensores son capaces de recolectar. Aunque la identificación del nodo desde el que se transmite la información resulta indispensable para el tratamiento de los datos y, por tanto, para el correcto funcionamiento de la aplicación en la que se utilice la red. Gracias a las características de este tipo de redes, aparece un gran abanico de aplicaciones en las que pueden emplearse las WSN.

2.3. Redes inalámbricas de sensores.

La popularidad de las Redes Inalámbricas de Sensores (WSN) ha ido aumentando en la última década. Su flexibilidad y su bajo coste de implantación las convierten en un sistema perfecto para capturar datos e interactuar con el entorno para múltiples aplicaciones [20]. Además, algunas investigaciones recientes sobre este tema apuntan a su creciente relevancia [21], [22].

2.3.1. Evolución y aplicaciones.

Hay trabajos enfocados en mejorar el consumo de energía de las WSN, por ejemplo: [23] se centra en la eficiencia energética en los protocolos de la capa MAC para WSN; en [24], se estudian las redes inalámbricas de sensores alimentadas mediante la cosecha de energía del ambiente; y en [25] se discute sobre distintas técnicas de codificación de red y sus beneficios en el ahorro de energía en las WSN. Pero este tipo de redes también es analizado desde el punto de vista interno de las comunicaciones, como el caso de los protocolos de enrutamiento para WSN empleados en [26], o cómo debe emplearse y desarrollarse el middleware específico para WSN [27].

El uso de las WSN se presenta como una solución óptima debido a su flexibilidad, lo que las hace fácilmente adaptables a casi cualquier entorno. En [28], se desarrolla una red inalámbrica de sensores para monitorizar la temperatura de un grupo de computadoras de alto rendimiento. Y es que estas redes son muy útiles y robustas, incluso en condiciones extremas, como se demuestra en [29], donde se emplea una WSN para la monitorización de personas en entornos peligrosos. O en [30], donde se implementa una WSN para el hostil entorno industrial de las arenas bituminosas. Por otro lado, las WSN también son adecuadas para monitorizar espacios cada vez más grandes como se puede ver en [31]. El trabajo presentado en [32] proporciona un estudio de las diferentes aplicaciones basadas en las WSN para su despliegue en la agricultura; como la monitorización de la humedad del suelo, de las instalaciones de riego automatizadas o del almacenamiento de productos agrícolas.

Si bien la mayoría de las primeras aplicaciones de las WSN se han centrado en escenarios exteriores como los que se citan anteriormente, el sector industrial también tiene como objetivo aprovechar la tecnología de las WSN para optimizar su rendimiento [33].

2.3.2. Sistema de monitorización del consumo eléctrico real.

En esta línea se ha colaborado en la implementación de una red inalámbrica de sensores, especialmente desarrollada para su uso en la medición dinámica del consumo de energía en una fábrica¹. El sistema

¹ Trabajo publicado en el *Congreso Internacional Smart SysTech 2013*, celebrado en Erlangen/Nuremberg (Alemania).

desarrollado se basa en la tecnología ZigBee® y permite la recogida de datos sobre energía y otras variables relacionadas de una planta industrial. Se trata de un sistema flexible y reconfigurable, de modo que se pueden añadir nuevos nodos para medir el consumo de energía en diferentes máquinas, además de la temperatura y la humedad en cualquier punto de la fábrica. Los datos recogidos por la red son analizados para su utilización con el propósito de reducir el desperdicio de energía y mejorar la eficiencia energética de la factoría.

El sistema ha sido inicialmente diseñado para que todos los nodos estén alimentados por la red eléctrica. Aunque también sería posible desplegar nodos adicionales alimentados por baterías para mejorar la captura de datos en puntos que no disponen de una toma de corriente accesible y se planteen como relevantes para el consumo de energía.

Los nodos alimentados por la red son dispositivos de funcionalidad completa (Full Function Devices, FFD), según la nomenclatura de IEEE 802.15.4 [34]. Es decir, son dispositivos con capacidad de interconexión que son capaces de gestionar el tráfico en la red y se denominan *ZigBee Routers*. Se ubican en el entorno de la maquinaria objeto de estudio o de su panel eléctrico de control. Además, mediante estos dispositivos es posible ampliar una red ya establecida, añadiendo redundancia a la arquitectura de la red o establecer una nueva red. En ese caso, uno de estos nodos debe asumir el papel de coordinador de la red o *ZigBee Coordinator*, adquiriendo la capacidad de crear la red.



Figura 2.6. Interior del prototipo del nodo sensor de la red.

Para esta aplicación específica, la arquitectura del sistema consta únicamente de dos elementos diferentes: nodos sensores y un nodo coordinador. Todos los nodos comparten un hardware común provisto de sensores que registrarán los datos para el middleware (Figura 2.6). La información es enviada por los nodos sensores al coordinador. El nodo coordinador recoge los datos del resto de los nodos de la red y envía la información al middleware, que reside en un ordenador y se encarga de enviar los datos al software encargado del análisis.

Se trata de un sistema no invasivo de fácil instalación para cualquier aplicación que se quiera monitorizar. Además, se presenta como una herramienta de bajo coste que recoge información para ayudar a las industrias a reducir su consumo energético. En este sentido, los usuarios de la red pueden aprovechar la información proporcionada por la red para elegir las políticas y acciones más apropiadas, así como para tomar nuevas decisiones estratégicas en aras de lograr un ahorro de energía a través de un consumo responsable.

2.4. Redes inalámbricas de sensores y actuadores.

Hace unos años, la mayor parte de los trabajos desarrollados en esta área se han centrado en las redes inalámbricas de sensores (WSN) en forma de redes centralizadas para la recogida de datos. Pero la inclusión de nodos actuadores ha impulsado su evolución hacia las redes inalámbricas de sensores y actuadores (Wireless Sensor and Actuator Networks, WSAN), abriendo la puerta a la creación de redes con capacidades inteligentes de toma de decisiones que operan de forma distribuida [35], [36].

La industria es la responsable de la utilización de una gran cantidad de los recursos energéticos globales. Y concienciada sobre la eficiencia, está impulsando acciones para optimizar el consumo de energía en los procesos industriales. Para optimizar este uso de la energía es necesario identificar los puntos específicos de actuación en las plantas industriales: es decir, es crucial conocer el rendimiento real de la maquinaria y de todos los demás consumidores de energía distribuidos dentro de las fábricas. Las WSAN presentan una gran flexibilidad que las hace especialmente apropiadas para aplicaciones que requieren la adquisición y gestión de datos distribuidos en casi cualquier ambiente [37].

2.4.1. Evolución y aplicaciones.

Recientes trabajos de investigación se han llevado a cabo abordando todos los niveles de la tecnología de las WSAN: desde la mejora de la organización interna de la red, como se muestra en [38] donde se analizan y clasifican diferentes soluciones para la gestión de los nodos y sus interacciones, o en [39] donde se propone un sistema basado en técnicas de aprendizaje automático (*Deep Q-Network*) para el control de nodos actuadores móviles en las WSAN; hasta la optimización de la colocación de los nodos como se propone en [40], o cómo llevar a cabo la asignación de tareas a los actuadores, que puede encontrarse en [41]. Todas estas ideas pueden complementarse con mejoras en las comunicaciones entre los nodos como las que se presentan en [42], donde se propone el uso de una red sobre una infraestructura IPv6. También con la utilización de nuevos algoritmos para mejorar la capacidad de reenvío del tráfico de los nodos, como se describe en [43]. Con propuestas para reducir la congestión y mejorar el rendimiento de la red [44]. Empleando métodos novedosos de salto de canal para el intercambio de paquetes de datos y que se presentan en [45]. O la propuesta presentada en [46] para mejorar la localización de las pérdidas de enlace. Pero la mayoría de estos trabajos están basados en simulaciones y se han obtenido pocos resultados reales de entornos empíricos, lo que puede limitar su aplicabilidad directa.

Algunos trabajos adicionales se centran en la reducción del consumo energético de las WSAN. Por ejemplo, en [47] algoritmos de control PID y de redes de neuronales difusas se aplican a los nodos para controlar la transferencia de datos, así como el consumo de esos nodos. En [48], se presenta un circuito de recolección de energía térmica para sensores autoalimentados. Y en [49] se proponen varios métodos para la elección del nodo actor correspondiente a la tarea requerida, encontrando la solución más eficiente.

Las WSAN son adecuadas para multitud de aplicaciones en diferentes escenarios, proporcionando soluciones a los retos medioambientales [50], como el ahorro de energía para la reducción de las emisiones de gases de efecto invernadero. Una de las aplicaciones más relevantes en este contexto es el uso de las WSAN para edificios inteligentes. Por ejemplo, en [51] una WSAN se utiliza para controlar el sistema de ventilación de un edificio. Y en [52], una WSAN autoalimentada mejoró la eficiencia energética del sistema de calefacción, mediante el uso de técnicas de cosecha de energía. Igual que sucede con las nuevas construcciones, estos sistemas también pueden mejorar el rendimiento de edificios antiguos, dado que son fácilmente adaptables y precisan de poca instalación invasiva. Este es

el caso de [53], donde se emplea una WSN para lograr ahorros en el consumo de energía del sistema de iluminación de un edificio. Pero la aplicación de las WSN no sólo es útil en grandes instalaciones, ya que también pueden ser directamente empleadas para monitorizar y controlar el gasto energético de los aparatos eléctricos [54]. O para proporcionar apoyo a técnicas de control más avanzadas como en [55], donde se aplican métodos de control difuso en un entorno industrial mediante WSN. Una aplicación sencilla es que estos sistemas ayudan a mejorar los sistemas de control y gestión del aire acondicionado en los edificios, como se describe en [56]. En definitiva, un amplio abanico de aplicaciones y posibilidades.

2.4.2. Sistema de control inteligente para el uso eficiente de la energía.

En este campo, se ha desarrollado una Red de Sensores y Actuadores Inalámbricos (Wireless Sensor and Actuator Network, WSN) que proporciona el apoyo necesario a un sistema avanzado de gestión de la energía eléctrica, aportándole datos actualizados y fiables, así como un medio para la transferencia de instrucciones. Esto se logra mediante el uso de una red de servicios, que incluye algunas características de las futuras plantas industriales inteligentes sin interacción humana propuestas en [57]. El sistema proporciona una óptima gestión de todas sus necesidades energéticas de manera exhaustiva, inteligente y automática.

La WSN desarrollada da soporte a un nuevo sistema inteligente de gestión y control de la energía² que decide cuándo los dispositivos deben conectarse dentro de un determinado rango de tiempo para optimizar los costes. Su funcionamiento se basa en el análisis y la toma de decisiones a partir de datos de generación y consumo de energía en tiempo real, según algunas condiciones preestablecidas. Se trata de un sistema exportable y adaptable a cualquier industria o tipo de actividad y puede desplegarse para muchas aplicaciones específicas.

El sistema propuesto se divide en dos partes: el hardware, que controla el suministro de energía y captura información sobre el consumo real de energía y la eficiencia energética de la maquinaria; y el software, que captura información sobre el funcionamiento de las redes eléctricas, analiza todos los datos recogidos y toma decisiones que son ejecutadas por el hardware.

El núcleo de la parte software del sistema se basa en un árbol de decisiones que es apoyado por otras partes. Algunas de las cuales le proporcionan las entradas de información necesarias para su funcionamiento: como los datos recogidos del mercado eléctrico; los datos de los sensores de la WSN con información sobre el consumo real de energía; y las especificaciones establecidas por los usuarios a través de un conjunto de reglas y restricciones que debe cumplir el sistema.

Se consideran todos los datos recopilados para tomar la mejor decisión que asegure el cumplimiento de las especificaciones establecidas por los usuarios. Es decir, como resultado de la toma de decisiones, el sistema gestiona los tiempos de funcionamiento de cada máquina bajo control y decide cuándo y cómo se consume la energía (Figura 2.7). De tal forma que se encuentra la mejor combinación para llevar a cabo todas las tareas, con el menor consumo de energía posible. El sistema funciona de forma continua y actualiza sus datos de entrada, de manera que cualquier cambio en cualquier instante puede causar variaciones en las decisiones arrojadas por el software. Persiguiendo en todo momento, si es posible, mejorar el escenario de consumo real.

² Trabajo publicado en *Sensors*, 18(6), 1892, junio de 2018. Edit. MDPI. e-ISSN: 1424-8220. JCR:3.031-T1 (Instruments & Instrumentation 15/61).

Por ejemplo, si se necesitan seis horas para cargar una carretilla eléctrica y hay doce horas disponibles para hacerlo, el sistema distribuirá el proceso de carga a lo largo de este tiempo, logrando el uso más eficiente posible de los recursos energéticos disponibles y reduciendo el coste del proceso. Por supuesto, siendo la principal restricción que el sistema asegure la carga completa de la carretilla en el tiempo especificado.

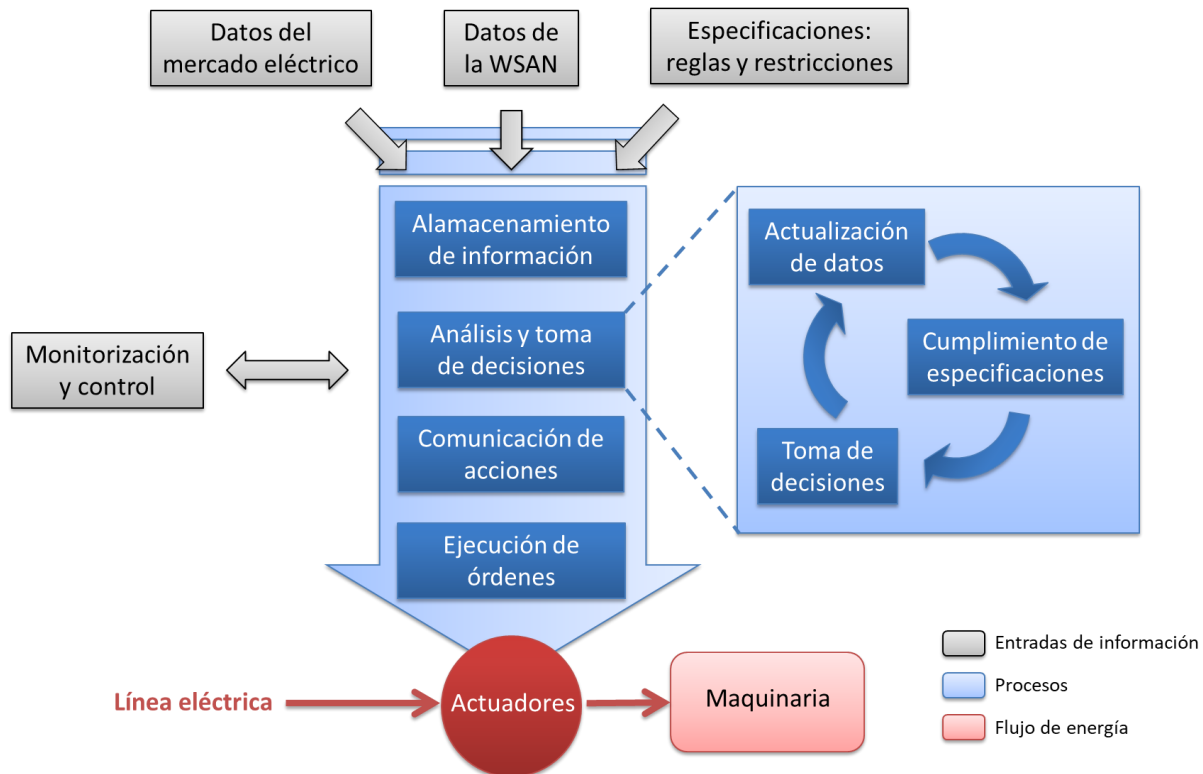


Figura 2.7. Lógica de funcionamiento del sistema desarrollado para el control del uso de la energía.

La parte hardware es un sistema de monitorización y control, basado en una WSN, que puede emplearse en cualquier aplicación. Además, estas redes permiten la conexión entre la maquinaria e Internet, de manera que todo el conjunto queda integrado en el marco de trabajo del IoT.

En este caso se ha empleado tecnología ZigBee®, mediante el desarrollo de una red de varios nodos trabajando como routers. Estos dispositivos disponen de capacidad de interconexión con otros nodos y son capaces de gestionar el tráfico de la red, permitiendo la expansión de una red preestablecida y/o añadiendo redundancia. Cada nodo crea un área de cobertura para establecer las comunicaciones con otros nodos. Uno de estos nodos adquiere el rol de coordinador de la red, cuyas principales funciones son el establecimiento de la red y su interconexión con el interfaz de la aplicación para la que se usa.

En la Figura 2.8 puede apreciarse el hardware de los dispositivos desarrollados. Han sido diseñados para alimentarse directamente de la red eléctrica (230 VAC), a una fuente de alimentación de 5 VDC, o a través de una batería. Constan de una etapa de alimentación que regula los posibles suministros de energía a una tensión de 3,3 V y una corriente máxima de 500 mA, suficiente para el adecuado funcionamiento del equipo. El núcleo del sistema lo forman un microcontrolador y un transceptor de radiofrecuencia, que conectado a una antena sintonizada a 2,4 GHz hacen posible las comunicaciones entre dispositivos. El dispositivo cuenta con los interfaces suficientes, tanto analógicos como digitales, para incorporar un amplio abanico de sensores. Y varios relés de estado sólido acoplados a las salidas digitales del microcontrolador, para que trabajen como actuadores capaces de encender y apagar la alimentación de la maquinaria.

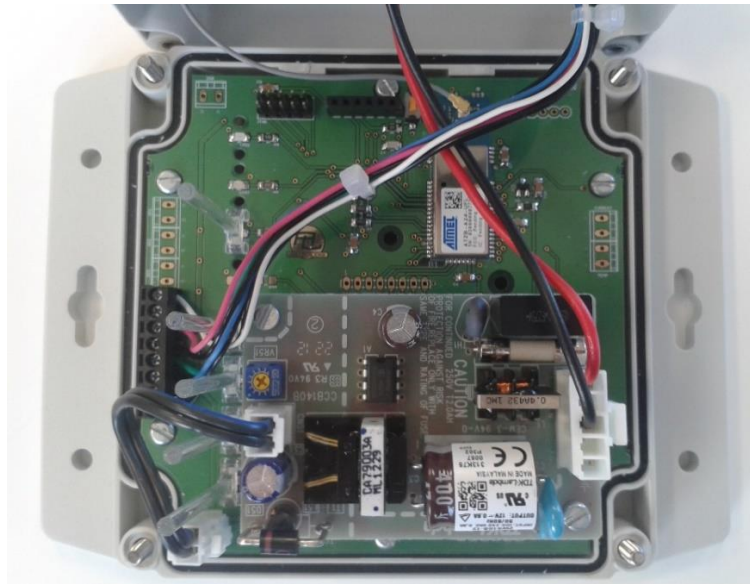


Figura 2.8. Interior del prototipo de router desarrollado para crear la WSN.

La WSN creada realiza una monitorización y control del consumo energético en tiempo real mediante el uso de los sensores y actuadores necesarios en los nodos (Figura 2.9). Por tanto, actúa como interfaz física entre la parte lógica del sistema de ahorro de energía y la maquinaria cuyo funcionamiento se está viendo optimizado.

Para la monitorización de la eficiencia energética, los dispositivos desarrollados toman periódicamente muestras de sus sensores. Estas lecturas son debidamente procesadas antes de ser transmitidas mediante el acondicionamiento de la señal que se requiera. De tal forma que se optimiza el rango de medición, asegurando la coherencia y la fiabilidad de los datos recogidos. Además, el hardware está siempre alerta para la recepción y ejecución de peticiones específicas que pueden venir de la parte de software del sistema y que permite llevar a cabo un control apropiado de la alimentación de la maquinaria asociada. Cuando todas las tareas se han ejecutado debidamente, todos subsistemas del dispositivo se vuelven inactivos y los nodos entran en modo de espera (*stand-by*) para reducir su consumo de energía. Esto es particularmente apropiado para la WSN, donde puede haber nodos alimentados por baterías de larga duración, gracias al empleo de técnicas de cosecha de energía.



Figura 2.9. Pruebas de laboratorio del sistema final antes de ser implantado.

En definitiva, la propuesta desarrollada consiste un sistema automático inteligente y flexible que puede fácilmente adaptarse a cualquier aplicación. Contribuye a poner en práctica el uso eficiente de la energía y permite la optimización de los recursos energéticos disponibles en cada momento, mediante la gestión del uso de la energía de dispositivos y maquinaria en los consumidores finales³. Además, al estar construido sobre una WSN diseñada para capturar datos y proporcionar capacidades de control de forma económica y no invasiva, el sistema global propuesto ha obtenido una gran ventaja competitiva por ser especialmente fácil de desplegar y utilizar, incluso en entornos complejos como el de las fábricas en funcionamiento.

2.5. Redes inalámbricas de ámbito personal.

Hoy en día, hay un incremento masivo de dispositivos que nos proporcionan un entorno móvil de vigilancia de la salud, lo que permite a los usuarios personalizar estos sistemas y su interacción con otros dispositivos. Como consecuencia está surgiendo una nueva generación de sistemas personalizados de vigilancia, que ofrecen grandes ventajas a los usuarios y pueden utilizarse para múltiples aplicaciones. Este tipo de equipamiento proporciona un aumento en la seguridad de las personas, evitando comportamientos inapropiados y ayudando a tener una mayor concienciación sobre el cuidado de la salud. En definitiva, proporcionan una mejor calidad de vida a la vez que contribuyen a reducir los costes del servicio de salud [58].

Acompasado a la aparición de estos nuevos dispositivos con capacidades de detección de variables fisiológicas mediante sensores, surge el concepto de redes de ámbito personal (Body Area Network, BAN). En este tipo de sistemas, los nodos que conforman la red están estratégicamente colocados en el cuerpo humano o en la ropa. Las BAN permiten la monitorización continua del estado de salud, la actividad física y las condiciones ambientales durante la realización de actividades diarias. Particularmente, las redes inalámbricas de ámbito personal (Wireless Body Area Networks, WBAN), basadas en tecnologías electrónicas para la salud (*e-health*), suponen un gran potencial para la monitorización ubicua de la salud en actividades de la vida cotidiana [58]. En este sentido, multitud de aplicaciones de esta o similar tecnología y empleadas en distintas áreas coexistirán en las futuras ciudades inteligentes, para proporcionar a la ciudadanía una serie de servicios que mejoren sustancialmente su calidad de vida [59].

2.5.1. Desarrollos para la mejora de la asistencia sanitaria y la salud.

A lo largo de los últimos años, se han desarrollado múltiples prototipos para aplicaciones médicas. Por ejemplo, en [60], [61] se presentan diferentes sistemas de monitorización empleados en cardiología. Y en [62] se describe un sistema de autoevaluación para pacientes bipolares. Si bien, todas estas propuestas están basadas en aplicaciones para teléfonos inteligentes (principalmente para Android), siendo una buena alternativa en muchos casos, dado su uso generalizado. Aunque algunos estudios concluyen que, los teléfonos inteligentes no siempre son la mejor opción para este tipo de tareas, porque no proporcionan todas las funcionalidades y características requeridas para un sistema de monitorización de la salud fiable [63]. Por ello, una solución combinada, como la presentada en [64], puede ser de utilidad. En esta propuesta se utiliza una red inalámbrica de sensores (WSN) para la captura de datos y la tecnología móvil para la transmisión de los datos recogidos sobre los pacientes. Pero esta

³ Ideas presentadas en el *Energy and Environment Knowledge Week International Congress*, celebrado en 2014 en Toledo (España).

solución no es genérica, ya que estos sistemas deberían incluir a todos los participantes involucrados en el cuidado de la salud. Para lo que resulta imprescindible la implementación de una infraestructura robusta que garantice el servicio, como se muestra en [65]. Además, los sistemas de prevención y de monitorización de la salud deben alimentarse continuamente con datos en tiempo real para llevar a cabo buenas labores de prevención y detección temprana de accidentes [66]. Para lo que resulta muy importante obtener información personal relacionada con la salud mientras la persona continúa con su vida cotidiana, incluyendo su puesto de trabajo. En este sentido, los sistemas convencionales de vigilancia de la salud utilizados actualmente en los hospitales e industrias no pueden proporcionar este servicio.

También, existen otras soluciones de asistencia sanitaria basadas en la monitorización por vídeo, como en [67], donde se presenta un sistema de monitorización mediante vídeo para personas con demencia senil. Pero esta solución no es válida para muchas aplicaciones porque no puede ser implementada en cualquier lugar, ya que la grabación de video probablemente viole algunos derechos de protección de datos personales. Por lo que es importante tener en cuenta la naturaleza de los datos que manejan estos sistemas para cumplir los requisitos legales de protección de datos personales. Por consiguiente, es necesario definir un marco común para proteger los flujos de datos en las aplicaciones de ciber-salud de las redes mundiales de telecomunicaciones [68]. Teniendo en cuenta estas consideraciones, el proyecto europeo *ANGEL* desarrolla una arquitectura de seguridad que tiene en cuenta los requisitos de despliegue y funcionamiento de las aplicaciones para el cuidado de la salud y los servicios asistencia domiciliaria [69]. Lo que proporciona un marco útil para el despliegue seguro y sencillo de futuras redes y aplicaciones que mejorarán la calidad y eficacia de este tipo de servicios, bajo el paraguas del IoT.

Las redes inalámbricas de sensores (WSN) se están convirtiendo rápidamente en la tecnología escogida para el desarrollo de muchas aplicaciones de *e-Health*. Características como su diseño no intrusivo, su bajo consumo de energía, su bajo precio y su flexibilidad para integrarse en entornos de atención sanitaria, hacen que las WSN sean perfectas para capturar datos necesarios e interactuar con el entorno en múltiples aplicaciones [21]. Aparte del entorno de la sanidad, esta tecnología se emplea en otras aplicaciones, dado que las WSN mantienen los requisitos de seguridad y fiabilidad para la recogida de datos sensibles. Y son adecuadas para aplicaciones de monitorización de personas en situaciones extremas, como en el subsuelo de una mina de carbón [70], o en subestaciones eléctricas [71]. Además, su aplicación puede ser bastante directa como en [72], donde se propone una WSN con fines de seguridad y monitorización de personas utilizando únicamente la información proporcionada por los enlaces inalámbricos entre nodos y sin necesidad de emplear ningún sensor específico.

2.5.2. Sistema de seguridad activa para la monitorización de personas.

Dada la importancia de controlar y supervisar la salud de las personas, especialmente en diversas situaciones peligrosas, se ha desarrollado un sistema portable para aumentar la seguridad en el ámbito personal⁴. El sistema ha sido diseñado para aplicaciones industriales, pero también puede utilizarse para otros fines o sectores. El sistema desarrollado es: pequeño, portátil y ligero, ya que los trabajadores deben llevarlo consigo mientras realizan sus tareas; robusto para soportar choques y condiciones adversas; y energéticamente autónomo para mantenerse activo, al menos, a lo largo de una jornada de trabajo. Como el sistema se adapta a muchas aplicaciones, es fácil de instalar, administrar y utilizar.

⁴ Trabajo publicado en el *Congreso Internacional Smart SysTech 2014*, celebrado en Dortmund (Alemania).

Específicamente, se ha desarrollado un dispositivo inteligente personal (Figura 2.10) basado en la tecnología de redes inalámbricas de ámbito personal (WBAN), para proporcionar seguridad adicional a los trabajadores en aquellas situaciones en las que es necesario y en respuesta a las solicitudes planteadas por importantes industrias multinacionales del sector aeroespacial. El módulo se encarga de monitorizar la actividad y el movimiento de las personas que lo portan, así como de detectar impactos y lanzar señales de socorro.

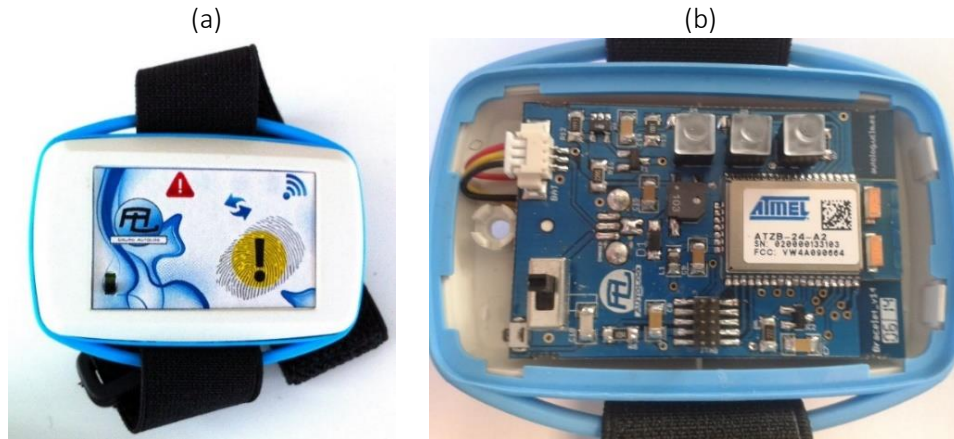


Figura 2.10. Exterior (a) e interior (b) de la pulsera Inteligente desarrollada.

El sistema está compuesto por varios dispositivos inalámbricos que están conectados mediante una red de seguridad activa (Figura 2.11). Esta red se basa en nodos de comunicación que se distribuyen en la planta industrial, creando la red de seguridad activa. A la cual se conectan dispositivos portátiles que consisten en pulseras inteligentes que son portadas por cada trabajador, para aumentar su seguridad dentro de la fábrica. Por último, una aplicación de software recoge la información recolectada por la red para su procesamiento.



Figura 2.11. Dispositivos fijos y móviles de la red desarrollada.

La red de seguridad activa, basada en WBAN, permite a los trabajadores generar una señal de alarma en caso necesario e interactuar con el personal de seguridad en tiempo real. Además, la red se encuentra continuamente chequeando que todo esté correcto, mediante el envío periódico de balizas. Cuando se detecta algún problema, el propio sistema genera una señal de alarma e informa sobre el foco donde se ha producido (Figura 2.12). Por lo que el sistema desarrollado contribuye a proporcionar una rápida respuesta ante las situaciones de emergencia que se puedan generar.

Se trata de una propuesta fácil de desplegar, al haber sido diseñada con características de "plug & play". La principal contribución del sistema es la reducción del tiempo de respuesta en las acciones de primeros auxilios ante una situación de emergencia. Presenta una mejora significativa para la seguridad en el trabajo cuando se compara con las medidas de seguridad habituales que se aplican en la mayoría de las empresas. Dependiendo de los periféricos y sensores empleados, el sistema puede tener nuevas características y funcionalidades, pudiéndose emplear para otras aplicaciones.

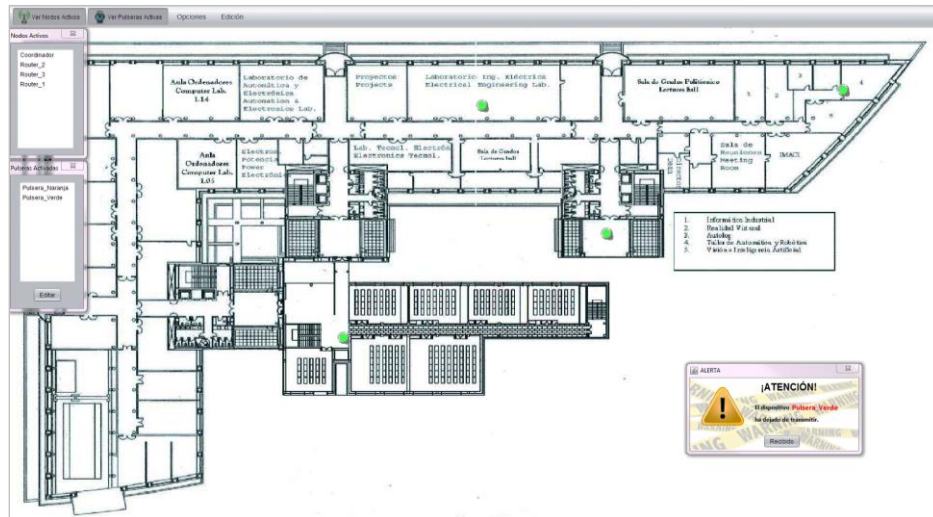


Figura 2.12. Pantalla del software de gestión y control de la red de seguridad activa.

Está demostrado que una atención médica eficaz durante los primeros minutos después de un accidente tiene un impacto decisivo en las posibilidades de recuperación de la persona que lo sufrió. Así que, especialmente en las grandes fábricas, una respuesta rápida es crucial y decisiva, ya que son vidas humanas las que están en juego.

2.6. Ahorro y eficiencia energética.

Intercalado con el desarrollo y evolución de los sistemas RFID y las redes de sensores, en todas sus variantes, han tomado especial relevancia temas como la eficiencia energética y el ahorro de energía (influyendo también en su desarrollo y evolución). Y es que el desafío energético es uno de los problemas más importantes para la sociedad actual. Por lo que los gobiernos en todo el mundo tienen que adoptar políticas estratégicas para afrontarlo satisfactoriamente. Estas acciones implican importantes consecuencias estructurales para la vida cotidiana y deben centrarse en resolver los problemas con los recursos disponibles, para lograr un futuro energético sostenible. La Unión Europea (UE) está exigiendo fuertes acciones de todos los países miembros [9] a este respecto. Los objetivos "20-20-20", dentro del paquete de medidas para el clima y la energía en 2020 (ratificado por el Acuerdo de París), preveían una reducción significativa de las emisiones de gases de efecto invernadero, un crecimiento sustancial del uso de la energía renovable y un importante incremento del ahorro de energía; y que todo ello que estuviera cumplido en el año 2020. Para 2030, se prevé que estas acciones tendrán que ser mejoradas aún más para alcanzar un aumento en una eficiencia energética del 27-30%. Los gobiernos europeos han establecido sus propios planes para cumplir estos objetivos; por ejemplo, el Gobierno español ha desarrollado el "Plan de Acción de Eficiencia Energética 2017-2020", en el que se dictan las medidas para lograr estos objetivos de la UE [10]. Y que definitivamente se ha visto ratificado con el Plan Nacional Integrado de Energía y Clima 2021-2030, en el que además se incide especialmente en la reducción de las emisiones de CO₂ [11].

2.6.1. Hacia la sostenibilidad energética.

La UE centra sus acciones en el transporte público y la industria, debido a su alto potencial de ahorro de energía. Sin embargo, también se aplican todos los esfuerzos en otros sectores, ya que pueden ayudar a alcanzar los objetivos especificados. Algunos ejemplos son las etiquetas de clasificación energética para los electrodomésticos, o los medidores inteligentes. Por lo tanto, todos los sectores y actividades económicas deben reducir el consumo de energía para realizar las tareas de manera más eficiente, optimizando todos los recursos energéticos disponibles.

Las energías renovables se encuentran fuertemente respaldadas en Europa, siendo el viento la más significativa de estas fuentes. La Asociación WindEurope afirma que, en 2030, el 31% de la energía generada será producida por el viento [12]. Durante 2016 el viento fue la principal fuente de energía renovable en España (47,3%), un país en el que el 40,8% de toda la electricidad es producida por fuentes renovables [13]. Dada su notable evolución, hay que tener en cuenta las peculiaridades de estas fuentes, porque serán clave para el futuro marco energético. Sin embargo, la energía eólica presenta un gran inconveniente ya que depende de la naturaleza intermitente del viento. Esto hace que esta fuente de energía sea propensa a producir picos de potencia que no son aprovechables y se convierten en un desperdicio de energía. Para lo que una buena gestión de la energía disponible en cada instante se vuelve especialmente relevante como un medio para abordar este problema. En este sentido, las Tecnologías de la Información y las Comunicaciones (TIC) se están convirtiendo en cruciales para mejorar la situación actual mediante la prestación de apoyo a la gestión eficiente de ambos extremos: demanda y producción de energía [14].

Para que verdaderamente se produzca un ahorro de energía, deben colaborar conjuntamente en él todos los actores implicados e involucrando a todas las partes interesadas. Por lo que los esfuerzos deben no sólo deben dirigirse a la generación eficiente de energía o a la obtención de una mayor cantidad de energía de fuentes renovables. La solución óptima únicamente se obtendría dirigiendo también la investigación hacia el transporte y consumo de energía [15]. Se han hecho algunos esfuerzos en las redes de distribución, como el que se muestra en [16], que presenta una nueva metodología para la medición inteligente, la monitorización y el análisis de la red, utilizando comunicaciones a través de la línea de energía (Power Line Communications, PLC), alimentadores a bajo voltaje e identificadores de fase para los medidores eléctricos inteligentes.

Para contribuir al aumento del cupo de las energías renovables en el global de la energía producida, en [17] se proponen nuevas técnicas para evitar la desestabilización de la red, proporcionando una respuesta rápida a posibles sobrecargas. Aunque, para un control adecuado de la red de suministro eléctrico, en estos casos, también es necesario actuar en el lado de la demanda energética [18]–[20] mediante desarrollos complementarios de redes inteligentes. Por ejemplo, soluciones que proporcionen una respuesta rápida que haga coincidir el consumo con los picos de suministro, o diferenciar el uso energético para ajustarlo a los períodos de consumo fuera de las horas punta. Tal y como hace el sistema propuesto en el apartado 2.4.2.

Proveedores de energía de todo el mundo están empezando a aplicar nuevas políticas e instrumentos de trabajo para contribuir al ahorro de energía a través de la eficiencia energética. Smart Meter Texas™ es una herramienta del Estado de Texas (EEUU), que permite a los usuarios ver su uso diario de electricidad, empleando esos datos para entender sus patrones de consumo. Proporciona a los usuarios la capacidad de gestionar el uso que hacen de la energía y la oportunidad de reducir su desembolso [21]. En España, un nuevo sistema activo de facturación se está implementando para los pequeños consumidores. Consiste en una variación de en el coste de la energía según el momento en que ésta se consume, gracias a la instalación de medidores inteligentes. Red Eléctrica de España, empresa

responsable del funcionamiento del sistema eléctrico español, proporciona datos sobre la generación de energía y consumo en tiempo real. En consecuencia, esta información permite la creación de nuevas herramientas de software que proporcionan a los usuarios nuevas formas de gestionar su consumo energético.

Las ciudades inteligentes son ejemplos emergentes que incluyen algunas de las herramientas mencionadas anteriormente [73], que mediante un nuevo modelo de gestión de la energía logran una reducción significativa de las emisiones de CO₂. En este caso, se fomenta el uso de sistemas de almacenamiento de energía con baterías, para que parte de la energía disponible pueda ser consumida después en el transporte eléctrico, el alumbrado público o el aire acondicionado de edificios. Además, este tipo de acciones globales también pueden comprender medidas complementarias, como por ejemplo: el modelo utilizado para mejorar la gestión de la respuesta a la demanda de los consumidores de electricidad residencial, presentado en [74]; el uso de modelos para mejorar la eficiencia energética y aplicación en edificios inteligentes, como se propone en [75], [76]; la aplicación para reducir el coste y aumentar el ahorro de energía con redes inteligentes en líneas ferroviarias, presentado en [77]; o la aparición de plataformas para el análisis y la gestión de datos de energía descrito en [78].

2.6.2. Cosecha de energía.

Todos estos nuevos desarrollos están destinados a causar un cambio en la sociedad, lo cual es clave para lograr un futuro energético sostenible. La energía se encuentra disponible en todas partes, en forma de energía mecánica, química, solar, etc. Aunque en algunos casos sólo es posible encontrarla frecuentemente en pequeñas cantidades y sin alcanzar demasiada potencia. De hecho, hasta hace relativamente poco, no había sido posible capturar y aprovechar la energía de algunas de estas fuentes para realizar un trabajo útil. Pero esta situación ha cambiado, gracias a la aparición de la cosecha de energía [79], que hace referencia a la obtención de energía útil del medio ambiente que rodea a los dispositivos.

La cosecha de energía se puede definir como el proceso de captura de cantidades minúsculas de energía, de una o varias fuentes ambientales, acumulándola y guardándola para su posterior uso. Por lo que se definen los cosechadores de energía como los dispositivos electrónicos encargados de capturar, acondicionar, acumular y administrar la energía obtenida de manera eficiente y efectiva. Normalmente, estos dispositivos suministran la energía en aplicaciones específicas de bajo consumo.

Emplear energías renovables para la generación de energía eléctrica no es ninguna novedad. Y grandes cantidades de megavatios son actualmente generadas en parques eólicos y campos solares. Sin embargo, este uso difiere mucho del concepto de cosecha de energía, donde los niveles de potencia son mucho menores, hasta llegar al orden de milivatios e incluso de microvatios. Y a diferencia de las grandes centrales, la energía se captura en el entorno de la aplicación y, por tanto, muy cerca de donde es usada [80].

Las aplicaciones de las técnicas de cosecha de energía son muy variadas, si bien se centran en el suministro de energía a dispositivos electrónicos y sistemas inalámbricos autónomos. Una de las aplicaciones fundamentales de los módulos cosechadores de energía es la de alimentar circuitos sensores y de control para aplicaciones de monitorización intermitente, como es el caso de las WSN. De forma que, aplicaciones que empleen tecnología de redes inalámbricas de sensores como la medicina, la domótica, el medioambiente, el transporte, los sectores militar y aeroespacial o la automatización industrial, pueden utilizar energía del ambiente donde se encuentran funcionando. Por ejemplo, la obtención de la energía procedente de las vibraciones inducidas por el tráfico de vehículos para alimentar los nodos sensores de una WSN encargada de monitorizar la salud estructural de un puente

[81]. O en el caso de las redes de sensores de ámbito corporal, también se puede obtener energía del movimiento de órganos tales como el corazón o los pulmones [82].

Por otro lado, la cosecha de energía también se emplea para la recarga de dispositivos electrónicos usados en la vida cotidiana como teléfonos móviles, pulseras inteligentes o gadgets. Lo que resulta toda una oportunidad para países en vías de desarrollo, en los que realizar la simple carga de una batería no es una situación trivial. Por otro lado, la cosecha de energía también puede ser empleada como fuente de energía alternativa para complementar la principal fuente de energía y mejorar la fiabilidad de todo el sistema en el que se instale, dotándolo de una herramienta alternativa con la que afrontar posibles interrupciones en la alimentación.

En este sentido, la cosecha de energía de fuentes ambientales puede resolver algunos problemas planteados en las WSN, donde un elevado número de nodos pueden precisar de batería y en algunos casos quedan inaccesibles tras su instalación. Los grandes avances realizados en la tecnología dedicada a la recarga de baterías también están siendo utilizados en los módulos cosechadores de energía. De manera que las baterías quedan relegadas a ser dispositivos de almacenamiento energético de los módulos cosechadores y no fuentes primarias de energía, reduciéndose su coste, peso y tamaño de forma significativa. Por lo que, empleando módulos cosechadores de energía se minimiza el mantenimiento y los costes de operación de este tipo de redes.

Además, los avances en la tecnología microelectrónica han aumentado la eficiencia energética de los microcontroladores actuales, reduciendo significativamente los requisitos de estos dispositivos en cuanto a consumo de energía. Y recientes desarrollos tecnológicos han incrementado la eficiencia de los dispositivos capaces de capturar cantidades muy pequeñas de energía del medio ambiente y transformarla en energía eléctrica. Todo ello, ha contribuido a despertar el interés del sector industrial para fomentar el uso de la cosecha de energía como solución de futuro [83].

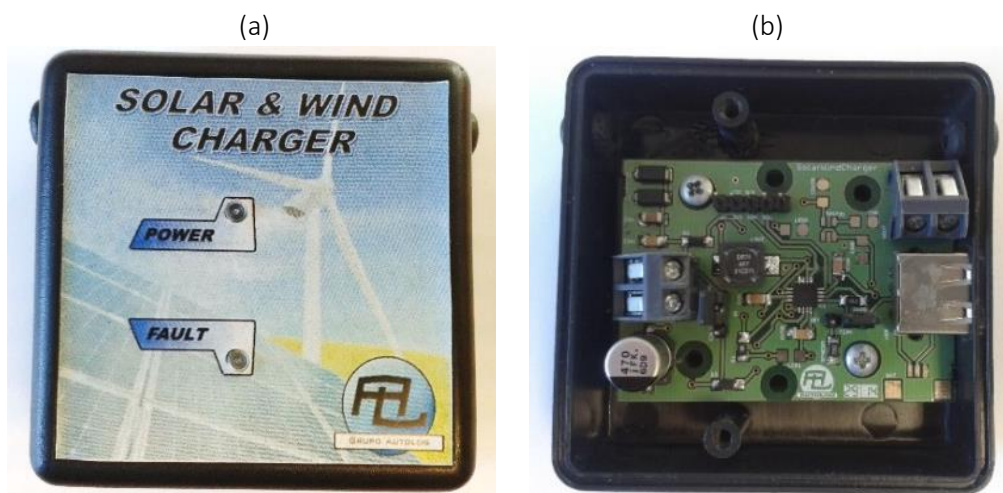


Figura 2.13. Exterior (a) e interior (b) del módulo cosechador de energía desarrollado.

En este campo, se ha contribuido a desarrollar un dispositivo cosechador de energía (Figura 2.13) para aplicarlo en las redes inalámbricas de sensores desarrolladas y descritas en puntos anteriores⁵. El dispositivo electrónico cuenta con dos transductores: una célula fotovoltaica para energía solar y una microturbina para energía eólica. Como tecnología de almacenamiento se han empleado baterías de

⁵ Parte del desarrollo definitivo de este dispositivo ha sido objeto del Proyecto Fin de Carrera de Roberto de Padua Espigares en la E.T.S. de Ingeniería Industrial de la UCLM (septiembre de 2016), bajo la continua supervisión del doctorando como codirector de este.

litio asociadas a los nodos de la red. Además de incluir todos los elementos electrónicos necesarios para controlar la carga de las baterías. Para ello, el dispositivo desarrollado permite dos montajes diferentes: uno como módulo cosechador de energía dentro de un nodo sensor de la WSN (Figura 2.14); y otro como cargador independiente de baterías, especialmente enfocado a los dispositivos móviles (pulseras).



Figura 2.14. Modulo cosechador de energía en el interior de un nodo.

El uso del módulo cosechador de energía, tanto como parte del hardware de los nodos fijos, como dispositivo independiente más orientado a los nodos móviles, implica disponer de un cargador de baterías que aumenta la autonomía de los equipos en los que se instale. Como consecuencia, estos equipos precisan de un menor mantenimiento, lo que los hace idóneos para ser instalados en localizaciones de difícil acceso por largos periodos de tiempo. Además, al obtener la energía del entorno se reduce la cantidad de energía externa que se ha de suministrar para el funcionamiento de los nodos. Por lo que también se contribuye a que la red de sensores necesite menos cantidad de energía para funcionar.

2.7. El papel de la RFID en el Internet de las Cosas.

La evolución que la tecnología RFID ha experimentado en los últimos años, junto con todas las tecnologías asociadas y que, además, se han ido reivindicando con entidad propia (como las redes inalámbricas de sensores y actuadores), ha allanado el camino para la implantación de lo que ha venido a denominarse Internet de las Cosas (Internet of Things, IoT). Gracias al desarrollo y evolución de todas estas tecnologías instrumentales, se ha alcanzado un nivel de madurez suficiente que permite la realización práctica de soluciones y servicios de IoT.

El Internet de las Cosas hace referencia a que todo el mundo esté interconectado, donde los objetos tienen integrados sensores, actuadores u otros dispositivos electrónicos, para que puedan conectarse en red con el fin de recopilar e intercambiar datos entre ellos [84]. Y es que un punto clave para el desarrollo del IoT es el uso de tecnología de identificación automática (auto-ID). Especialmente la RFID presenta un gran potencial para su aplicación en los objetos inteligentes, dado que sus características la convierten en la tecnología más apropiada para implantarse a gran escala.

Esta nueva forma de trabajar con los objetos trae consigo la aparición de un aumento exponencial del volumen de información, que debe ser adecuadamente gestionado por las redes, así como un

importante incremento de la operativa que deben ser capaces de realizar los dispositivos electrónicos asociados a los objetos físicos. Por lo que, por un lado, se requiere la creación de infraestructuras de red que soporten la tecnología que se implementará sobre ellas. Y por otro, se ha de reducir al mínimo posible la cantidad de operaciones que han de realizar los dispositivos, de manera que éstos sean lo más eficientes posibles.

Otro aspecto fundamental que debe tenerse en cuenta para evitar inconsistencias y errores de la red (como, por ejemplo, las duplicidades) y que en definitiva, los sistemas sean lo menos vulnerable posible, es que cada uno de los objetos que se encuentren en la red sean claramente identificados de forma unívoca [6]. En este sentido, los estándares impulsados en torno al Código Electrónico de Producto (Electronic Product Code, EPC), desarrollados por EPCglobal® y GS1®, están siendo ampliamente acogidos por la industria a nivel mundial. En estas especificaciones se incide específicamente en el uso de la tecnología RFID para hacer visibles cada uno de los objetos que participan en una red⁶.

2.7.1. Características y evolución.

El Internet de las Cosas (IoT), es un nuevo paradigma que rápidamente está ganando terreno en el ámbito de las telecomunicaciones inalámbricas modernas. La idea básica de este concepto es la presencia generalizada a nuestro alrededor de una variedad de cosas u objetos, como etiquetas de identificación por radiofrecuencia (RFID), sensores, actuadores, teléfonos móviles, etc. que son capaces de interactuar entre sí y cooperar con sus vecinos para alcanzar objetivos comunes [85]. Aunque incluso a día de hoy, existen varias visiones sobre cómo este paradigma debe ser e implementarse.

El uso de Internet ha cambiado drásticamente la forma en que vivimos y muchas de las interacciones entre las personas se han trasladado a un nivel virtual en varios contextos, desde la vida profesional hasta las relaciones sociales. Pero el IoT posee el potencial de añadir una nueva dimensión, permitiendo la comunicación con y entre objetos inteligentes. Lo que provoca que las comunicaciones se realicen en cualquier momento, en cualquier lugar, en cualquier medio y con cualquier cosa. En este sentido debe considerarse el IoT como parte del Internet general del futuro, que probablemente será muy diferente al Internet que utilizamos hoy en día. De hecho, es evidente que el paradigma actual de funcionamiento de Internet, construido en torno a las comunicaciones de punto a punto, se ha convertido ahora en un factor limitante para el uso que se requiere de Internet. En este nuevo paradigma, Internet se utiliza principalmente para la publicación y recuperación de información (independientemente de quién y dónde se publique o se recupere dicha información) y, por lo tanto, la información debe ser el centro de las soluciones de comunicación y del establecimiento de las redes. Lo que implica trabajar con redes centradas en datos, en las que los datos y las consultas asociadas a ellos se dirigen y encaminan automáticamente por la red.

Las comunicaciones del Internet de las cosas se consideran parte de la última generación de sistemas de comunicación inalámbrica [86]. Teniendo en cuenta que el IoT representa un concepto que implica el uso de varias técnicas de diseño para lograr diferentes objetivos de eficiencia y rendimiento. En este escenario, las estaciones base de comunicación deben disponer de una amplia cobertura para acoger un número masivo de nodos con baja tasa de transmisión de datos. También se exige que estos nodos sean dispositivos de bajo coste y estén diseñados con importantes restricciones en cuanto a la potencia total necesaria para su funcionamiento. Lo que motiva la implantación de dispositivos de bajo coste y eficientes desde el punto de vista energético, que funcionan con una potencia de transmisión mínima y

⁶ En consonancia con estas ideas y los trabajos realizados se presentó un trabajo en *RFID-Anwendertag 2016: AutoID – Basis für Industrie 4.0*, RFID-Anwenderzentrum München, celebrada en Garching, Múnich (Alemania).

emplean una pequeña cantidad de recursos para llevar a cabo las comunicaciones. Así como a aplicar novedosas técnicas en el análisis y el tratamiento de la información que se genere y se transmita por este tipo de redes [87], [88].

El Internet de las Cosas está aportando numerosos beneficios a la vida humana a través del entorno en el que se prestan servicios inteligentes para ser utilizados en cualquier actividad, en cualquier lugar y en cualquier momento [89]. Entre los principales campos de aplicación del Internet de las Cosas cabe destacar: la atención sanitaria y el cuidado de la salud; monitorización y cuidado medioambiental; ciudades inteligentes; aplicaciones comerciales; aplicaciones industriales; y aplicaciones de ámbito general que se pueden utilizar para solucionar problemas en varios ámbitos [90].

De forma casi paralela, surgió el término *Industria 4.0*, originariamente “Industrie 4.0” y que se conoció públicamente en 2011, cuando ese nombre fue tomado por una asociación de empresarios, académicos y políticos para apoyar la idea de mejorar la competitividad de industria manufacturera alemana [91]. La Industria 4.0 tiene como objetivo la creación de fábricas inteligentes, donde las tecnologías tradicionales sean actualizadas y transformadas mediante el Internet de las Cosas (IoT), la computación en la nube y los sistemas ciber-físicos (Cyber-Physical Systems, CPS) [92]. Y donde la tecnología RFID se convierte en una gran impulsora de la implantación de la Industria 4.0, actuando como ojos y oídos del resto de tecnologías de la información y sistemas involucrados [93].

En este sentido, las empresas tendrán que crear productos y servicios que satisfagan mejor las necesidades de los consumidores. De tal forma que desaparecerá la segmentación del mercado en su forma clásica. Para ello es imprescindible la información disponible de cada persona en el mundo moderno, que es grande y se encuentra accesible, a partir de la cual se diseñarán los productos y servicios del futuro [94].

Por tanto, el concepto de Internet de las Cosas se consolida como una prometedora oportunidad para construir potentes sistemas y aplicaciones industriales aprovechando la creciente ubicuidad de la identificación por radiofrecuencia (RFID) y los dispositivos inalámbricos y móviles con sensores y/o actuadores [4]. Se estima que en 2020, cerca de veintiún mil millones de dispositivos estarán interconectados y harán uso de la tecnología RFID [95].

Actualmente, nos encontramos a las puertas de la implantación masiva del Internet de las Cosas, en el que cualquier objeto es susceptible de estar online e interactuar con otros objetos presentes en la red. Y es que gracias a los avances tecnológicos, los objetos que comúnmente conocemos serán dotados de características operativas que hasta ahora nos resultarían inimaginables [57]. En los últimos años se ha desarrollado y desplegado una amplia gama de aplicaciones industriales de IoT [96]. En consecuencia, a partir de los ensayos y aplicaciones prácticas que se están llevando a cabo sobre el terreno, se ayudará a despejar las incertidumbres que aún impiden la adopción masiva del paradigma de la Internet de las Cosas.

2.7.2. Sistema automático de monitorización y seguimiento de muestras.

En este campo, se ha contribuido en el desarrollo de un sistema automático de monitorización y seguimiento de muestras⁷, que se ha desarrollado a modo de ejemplo de lo que sería una aplicación de

⁷ El sistema creado ha sido objeto de una patente de invención presentada por la UCLM en la Oficina Española de Patentes y Marcas el 14 de enero de 2013 con referencia ES201300070, número de solicitud P201300070, fecha de concesión el 18 de agosto de 2015 y número de publicación ES2518615.

IoT. El sistema se enmarca en la línea del seguimiento y trazabilidad de productos y está basado en el uso de tecnología RFID como fuente de identificación y generación de datos, que son complementados gracias al uso de otras tecnologías.

Aunque la propuesta es susceptible de ser empleada en un amplio abanico de aplicaciones, concretamente en este caso, el sistema se ha desarrollado e implantado para la recogida de muestras en la industria láctea. Lo que también ha provocado la participación de entidades reguladoras y empresas del sector para la realización de pruebas reales de implantación del sistema.

Tradicionalmente, para llevar a cabo la recolección de la leche de una zona ganadera, un camión cisterna visita cada granja para almacenarla en su interior. Al recoger la leche de cada productor, se adquiere una pequeña muestra, que se guarda para su posterior análisis. Cuando el camión termina su ruta y llega a la factoría, se analiza la leche contenida en su cisterna. En el caso de que el resultado no fuera satisfactorio, se analizan las muestras para intentar descubrir la procedencia de la leche en mal estado. El problema surge cuando el análisis revela la presencia de sustancias prohibidas a niveles superiores a los umbrales establecidos en la cisterna de leche, pero no en ninguna de las muestras. En este sentido, se ha demostrado que el calor y el tiempo influyen negativamente en la conservación de la leche [97]. Ya que las muestras tomadas han de viajar en el camión y son la única credencial que presentan los productores de leche para justificar la calidad de su materia prima, se ha de mantener el contenedor de muestras en el mejor estado posible, para asegurar que ninguna muestra ha sido degradada por agentes externos. Por lo que todas las muestras deben ser mantenidas en condiciones óptimas con una temperatura controlada durante el transporte para asegurar resultados fiables en el laboratorio.

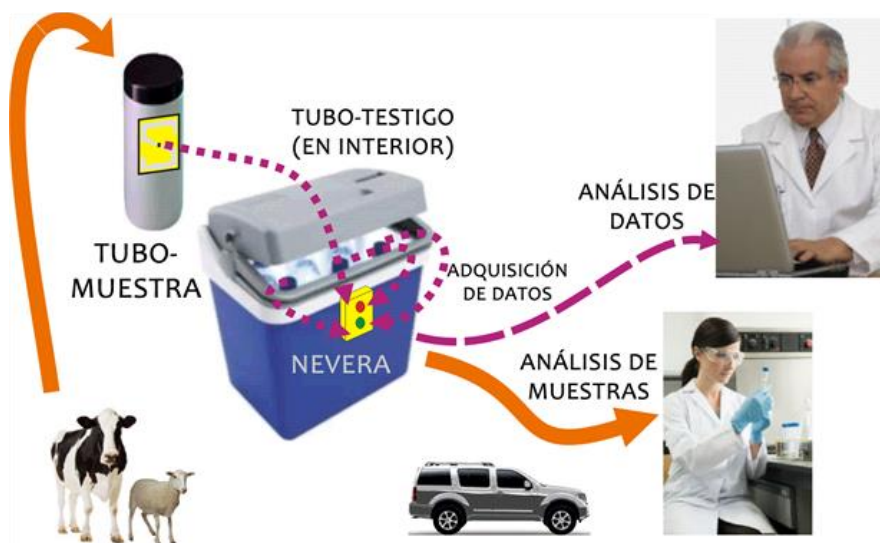


Figura 2.15. Sistema de trazabilidad para el proceso de recogida de muestras de leche.

El sistema propuesto para mejorar la calidad de las muestras de leche se divide en tres dispositivos principales: el tubo de muestra, el tubo de registro y almacenamiento de datos (tubo testigo) y la nevera de conservación (Figura 2.15). Se ha diseñado para que se adapte al proceso tradicional de recogida de muestras, que comienza con la toma de las muestras en la propia explotación ganadera.

El tubo de muestra es un recipiente de polietileno tereftalato (PET) que contendrá y portará la muestra de leche. En la parte exterior de su tapa se ubica una etiqueta RFID pasiva que identificará unívocamente cada una de ellas. Cada etiqueta enviará su ID al lector RFID para que pueda ser reconocido por el sistema. Acto seguido la nevera permitirá su apertura, dando acceso al tubo de muestra para que pueda ser colocado en la gradilla interior. En la Figura 2.16 pueden observarse varios tubos de muestras con sus correspondientes etiquetas RFID.

El tubo para el registro y almacenamiento de datos, o tubo testigo, es idéntico al tubo de muestra en material, dimensiones y forma, situándose en la gradilla junto al resto de muestras. Pero en su interior alberga un dispositivo electrónico, basado en microcontrolador, que incluye el hardware necesario para llevar a cabo sus funciones y comunicarse con el exterior de forma inalámbrica. Este dispositivo se encarga de captar y registrar la temperatura del interior de la nevera, así como de almacenar los datos de identificación, hora, fecha y lugar de recogida de cada muestra. Tanto la identificación de la muestra como las coordenadas de acceso se recibirán por radiofrecuencia a través de un transceptor. En la Figura 2.16 se puede observar el interior del tubo testigo (electrónico).

La nevera es el habitáculo encargado de transportar y conservar las muestras. Contiene el hardware y la lógica necesaria, basado en el uso de un microcontrolador, para el correcto funcionamiento del sistema. Además, incorpora la electrónica de interfaces necesaria para gestionar todas sus partes como: pantalla LCD, pulsadores, indicadores LED, etc. Dispone de un pequeño lector de RFID-HF (de 125 kHz) encargado de identificar los tubos de muestra y un cerrojo, controlado electrónicamente, que controla el acceso al interior de la nevera para que éstas puedan ser ubicadas en la gradilla correspondiente. La nevera también incluye un dispositivo GPS y un transceptor de radiofrecuencia. Además, se realiza un control sobre el propio funcionamiento de la nevera, consiguiendo que la temperatura en su interior se mantenga estable y dentro del intervalo estipulado. En la Figura 2.16 se muestra la nevera prototipo junto con la gradilla que contiene tanto los tubos de las muestras y el tubo testigo.



Figura 2.16. Sistema inalámbrico de trazabilidad para el proceso de recogida de muestras.

La muestra de leche se almacena en un tubo de muestra provisto de una etiqueta de radiofrecuencia (RFID), que la identifica de forma unívoca. Y posteriormente, se guardará en la nevera eléctrica, haciendo uso del lector de RFID, que solo se abrirá en presencia de una muestra válida. Además, la electrónica de la nevera se encargará de medir diversos parámetros de interés como la geolocalización (para lo que incluye un dispositivo GPS), el tiempo en el que la nevera ha permanecido abierta o el número de serie de las muestras en su interior. Pero la nevera no solo contiene los tubos con las muestras, también alberga el tubo testigo que mide constantemente la temperatura interior del compartimento en el que se encuentran las muestras y recibe los datos que le envíe la nevera de forma inalámbrica, almacenándose también en él toda la información generada. De tal forma que muestras y datos asociados siempre se encuentran físicamente juntos durante todo el proceso, desde la recogida

hasta el análisis. De este modo, se garantiza que las muestras se han mantenido en unas condiciones óptimas durante el trayecto.

Una vez realizada la recolección por todas las explotaciones y ya en el laboratorio, es posible obtener la trazabilidad de todo el proceso con datos de interés: temperatura, ruta seguida, tiempo empleado, etc. Para ello, se procede al volcado de la información almacenada durante la ruta, mediante un enlace inalámbrico por radiofrecuencia (Figura 2.17), desde el tubo testigo hasta un ordenador. En ese equipo residirá el software que permite el tratamiento, gestión y visualización de los datos, para su posterior análisis.



Figura 2.17. Dispositivo USB para el enlace de comunicación por radiofrecuencia.

Como resultado de la utilización del sistema se obtiene una serie de datos que permiten conocer, de manera objetiva, el estado de conservación de las muestras desde el origen hasta que son analizadas⁸. Y de entre los que cabe destacar: la curva de temperatura en las que se identifican cada una de las muestras recogidas (Figura 2.18); así como el mapa con la ruta de recolección realizada y el punto en el que se ha recogido cada una de las muestras (Figura 2.19).

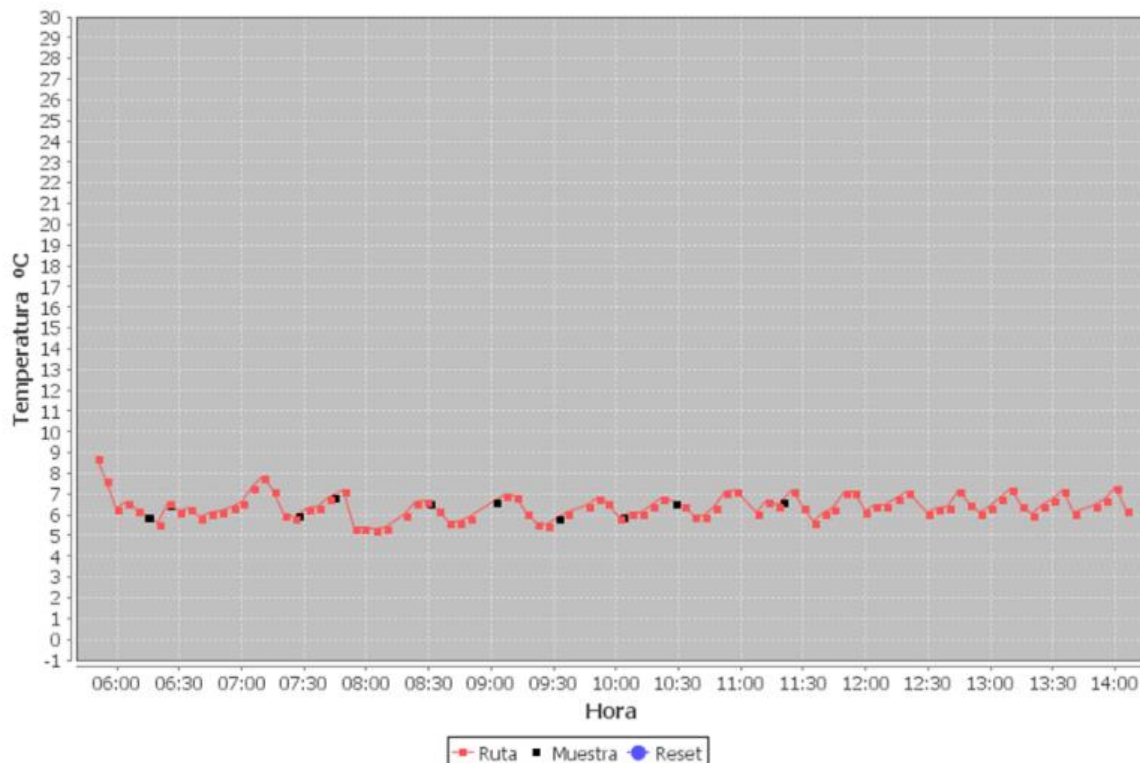


Figura 2.18. Evolución de la temperatura de las muestras en el interior de la nevera.

⁸ Resultados publicados en *Computers and Electronics in Agriculture*, Vol. 101, pp. 34-41, febrero de 2014. Edit. Elsevier. JCR:1.761-T1 (Agriculture, Multidisciplinary 6/56).

Con el desarrollo de este sistema se ha pretendido conseguir el establecimiento de una herramienta que facilite la trazabilidad y seguimiento de las muestras en todo momento, así como las condiciones de las mismas. Además, el adecuado funcionamiento del sistema ha quedado probado gracias a su uso práctico en condiciones reales⁹.

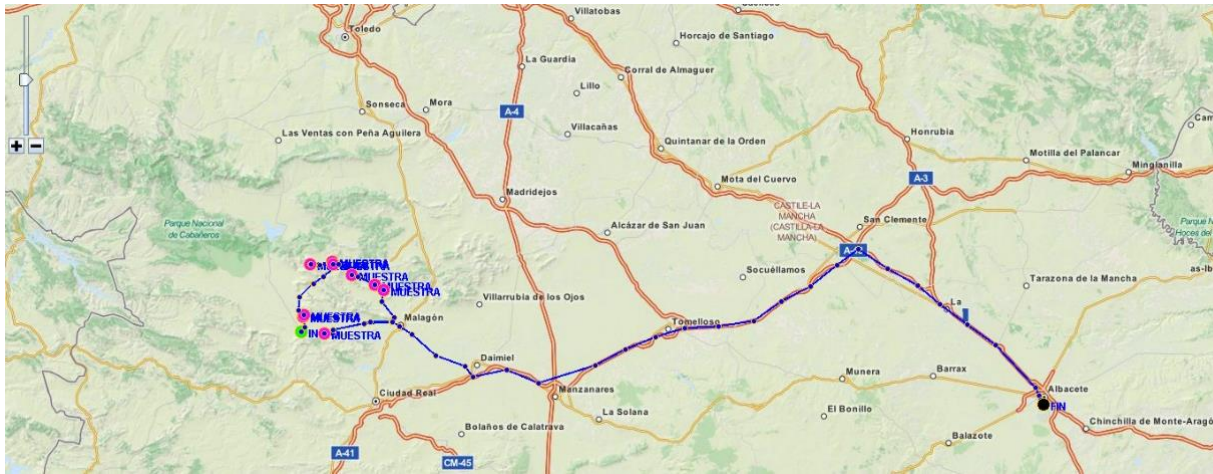


Figura 2.19. Ejemplo de ruta de recogida de muestras.

A la vista de los resultados obtenidos, se puede decir que el sistema desarrollado dota al proceso de recogida de muestras de leche de una calidad superior, pudiendo convertirse en un método de referencia en el sector. Además, la posibilidad de transportar muestras con alta calidad durante largos trayectos abre la posibilidad de exportar el sistema a una gran variedad de sectores. Los métodos de recogida, transporte y gestión de materiales, muestras y productos especialmente sensibles pueden tener aplicación en el sector agrario, médico y farmacéutico. Y la implementación de este tipo de tecnología es beneficiosa para todos los miembros de la cadena de producción y suministro.

⁹ Resultados publicados en el SEOC 2016 XLI Congreso Nacional y XVII Congreso Internacional de la Sociedad Española de Ovinotecnia y Caprinotecnia, celebrado en Talavera de la Reina (España).

Capítulo 3.

Propuestas para la mejora de la eficiencia electromagnética en sistemas RFID.

Bien de una forma o de otra, todas las variantes de la tecnología RFID se basan en el intercambio de información a través de ondas electromagnéticas de radiofrecuencia. Ante el amplio abanico de posibilidades, en esta tesis se ha decidido trabajar con la tecnología RFID pasiva (en adelante RFID) para la banda de UHF por varios motivos. Entre ellos cabe destacar el potencial de esta tecnología que queda aún por explotar y la escasez de trabajos de investigación desarrollados en esta área, especialmente si se compara con otras variantes de la tecnología RFID.

Un aspecto fundamental para el buen funcionamiento de cualquier tecnología inalámbrica es que las comunicaciones se produzcan de manera adecuada y exista un enlace de calidad entre emisores y receptores. En este sentido, también requiere prestar atención al medio físico sobre el que se intercambia la información.

En el caso de la tecnología RFID pasiva, el principal medio de transmisión es el aire. Se trata del medio más común, aunque en algunas ocasiones las ondas deben atravesar otros medios como materiales porosos o líquidos. En otros casos, la disposición del entorno en el que el sistema se encuentra implantado también puede acarrear la aparición de múltiples reflexiones y/o desviaciones de la señal. En definitiva, situaciones que pueden derivar en la distorsión de la señal original. Lo que se traduce en posibles fallos de funcionamiento de los sistemas RFID y la consiguiente caída del rendimiento y la eficiencia de estos sistemas. Por lo que el adecuado funcionamiento de un sistema RFID puede verse alterado por el medio y el entorno en el que esté implantado y opere [98]–[100].

Para tratar de solucionar estos problemas, en más ocasiones de las deseables, los instaladores de sistemas RFID optan por aumentar la potencia de la señal de RF, radiando en exceso la totalidad del área de cobertura de las antenas. Lo que acarrea como consecuencia la generación de muchas reflexiones más fuertes. Apareciendo, por tanto, más interferencias que provocan la distorsión y degradación de la señal de interés. El ruido aumentará exponencialmente y el sistema deberá operar en un entorno más hostil. Además, del consiguiente desperdicio energético que únicamente contribuye a que el sistema RFID funcione peor y sea menos eficiente.

A esto habría que sumar la probable existencia de más de un equipo de transmisión (lector), lo que implicaría la aparición de nuevas señales y, por consiguiente, interferencias en las comunicaciones del sistema. Aunque éstas últimas se procuran resolver en un nivel más alto, que se aborda en el capítulo 4 del presente documento.

3.1. Ondas electromagnéticas.

Analizando cómo se producen las comunicaciones en la tecnología RFID al más bajo nivel, es decir, en la capa física del modelo OSI [101], que comprende todos los medios necesarios para la transmisión de los bits (información), los sistemas de identificación por radiofrecuencia (RFID) se basan, desde un punto de vista puramente físico, en la transmisión, propagación y recepción de ondas electromagnéticas.

Las antenas son los elementos encargados de transmitir y recibir este tipo de señales [102]. Se trata de estructuras especialmente diseñadas para radiar y captar ondas electromagnéticas a la frecuencia de trabajo que adaptan la entrada/salida del receptor/transmisor al medio de propagación.

Cuando se propaga una onda electromagnética, pueden diferenciarse tres regiones (Figura 3.1) alrededor de la antena radiante en función del comportamiento de los campos. Aunque cabe destacar que no hay fronteras definidas, sino un paso gradual de una zona a otra. Considerando r como la distancia desde la fuente emisora, se define:

- Campo cercano reactivo o de inducción: se trata de la zona más próxima a la antena y en ella los campos dependen de forma cuasi-estacionaria de la distribución de cargas y corrientes de la antena en cada instante de tiempo. En esta región, el valor medio temporal del transporte de energía es nulo. Y como frontera suele aceptarse que:

$$r \leq r_1 = 0,62 \sqrt{\frac{D^3}{\lambda}} \quad (3.1)$$

Donde D es la máxima dimensión lineal de la antena emisora, λ es la longitud de onda correspondiente y r_1 es la frontera con la siguiente región.

- Campo cercano radiante o región de Fresnel: es una zona intermedia en la que predominan los campos de radiación y que sí transporta potencia media. La distribución angular de los campos (diagrama de radiación) varía en función de la distancia a la antena.

$$r_1 = 0,62 \sqrt{\frac{D^3}{\lambda}} \leq r \leq \frac{2D^2}{\lambda} = r_2 \quad (3.2)$$

Donde r_2 es la frontera con la siguiente región.

- Campo lejano de radiación o región de Fraunhofer: en esta zona los campos de radiación son una onda esférica elemental que también transporta potencia media. Y en esta zona el diagrama de radiación es independiente de la distancia a la antena. Como frontera para encontrarse en esta región debe cumplirse que:

$$r \geq r_2 = \frac{2D^2}{\lambda} \quad (3.3)$$

$$r \gg D \quad (3.4)$$

$$r \gg \lambda \quad (3.5)$$

En la tecnología RFID pasiva y teniendo en cuenta las distancias a las que pueden encontrarse los objetos a identificar (y por ello las etiquetas con las que interactúan), desde la antena del lector, resulta de especial interés el comportamiento de las ondas en el campo cercano para el caso de frecuencias de trabajo en HF, o del campo lejano o región de Fraunhofer para la banda de UHF [103].

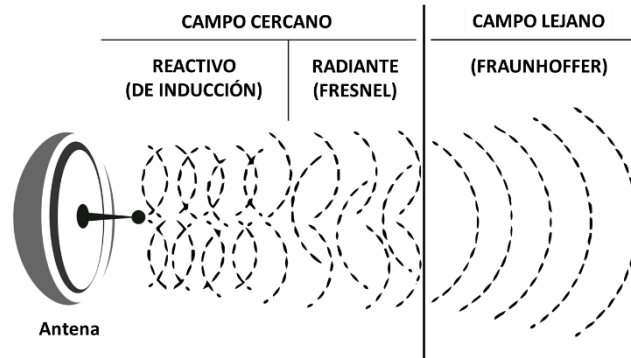


Figura 3.1. Diferencias entre campo cercano y campo lejano (CC).

Al igual que cualquier fenómeno electromagnético que se precie, el comportamiento en la propagación de estas ondas queda descrito por las ecuaciones de Maxwell [1]. Y teniendo en cuenta que se trabaja en campo lejano y con grandes distancias, la señal electromagnética puede aproximarse a una onda plana. De donde se deduce que el valor de los campos eléctrico (E) y magnético (H) depende de la posición y del tiempo. Y que en el dominio del tiempo pueden tomar las siguientes expresiones:

$$E_x = E_m e^{-\alpha z} \cos(\omega t + \beta z + \theta) \quad (3.6)$$

$$H_y = \frac{E_m}{\eta} e^{-\alpha z} \cos(\omega t + \beta z + \theta + \theta_\eta) \quad (3.7)$$

En campo lejano, la radiación electromagnética es una onda de tipo transversal (Figura 3.2), donde las magnitudes que definen la perturbación son los campos eléctrico y magnético. En este tipo de ondas, el campo eléctrico y el campo magnético son perpendiculares entre sí y se sitúan en un plano normal a la dirección de propagación de la onda. Como consecuencia y dependiendo del desfase (φ) existente entre los fasores que representan el campo eléctrico y el campo magnético, la magnitud física que se propaga no siempre se mantiene en la misma dirección y va describiendo unas figuras según se va propagando la onda. A este fenómeno se le denomina polarización. Y lo habitual es que el vector electromagnético resultante vaya describiendo una hélice de sección elíptica. Aunque cabe destacar unos casos particulares:

- Si el desfase es $\varphi = \pm n\pi$, el vector resultante se desplaza a lo largo de una recta y se define como polarización lineal.
- Si el desfase es $\varphi = \pm (2n + 1)\pi$, el vector resultante describe una circunferencia y se trata de polarización circular.

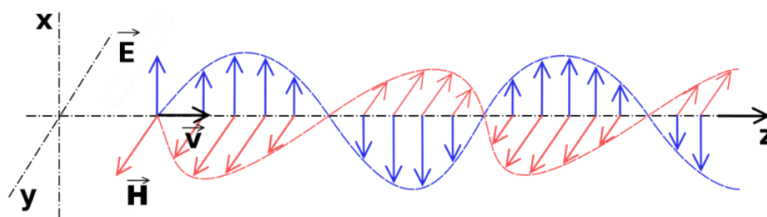


Figura 3.2. Ondas en un determinado instante para los campos eléctrico y magnético (CC).

De las ecuaciones (3.6) y (3.7) se puede deducir que la relación entre campo eléctrico y campo magnético es η , que se denomina impedancia intrínseca del medio. Este factor depende de las características propias del medio en el que se propagan las ondas, las cuales se ven afectadas y modificadas. Se calcula mediante la siguiente fórmula:

$$\eta = \sqrt{\frac{j\omega\mu}{\sigma + j\omega\epsilon}} \quad (3.8)$$

En la expresión (3.8), correspondiente a un medio con pérdidas, aparecen la conductividad (σ), la permitividad o constante dieléctrica (ϵ) y la permeabilidad o constante magnética (μ) del medio. Donde:

$$\mu = \mu_r \cdot \mu_0 \quad (3.9)$$

$$\epsilon = \epsilon_r \cdot \epsilon_0 \quad (3.10)$$

Cuando las ondas electromagnéticas se propagan en un medio material distinto del vacío, lo hacen a una velocidad de propagación distinta en cada medio. Además, en ellos tienen lugar otros fenómenos como dispersión, reflexión, refracción y absorción que también alteran la propagación de las ondas. La velocidad de propagación se calcula como:

$$v = \frac{1}{\sqrt{\epsilon \cdot \mu}} \quad (3.11)$$

Y para el caso de la propagación a través del aire se aproxima que $\epsilon_r \approx 1$. Por lo que se considera que la velocidad de propagación en el aire es la misma que la del vacío, $c = 3 \cdot 10^8$ m/s. Manteniéndose esta velocidad constante para todas las frecuencias, ya que siempre se cumple la ecuación (3.12), donde λ es la longitud de onda y f la frecuencia de la señal.

$$c = \lambda \cdot f \quad (3.12)$$

3.2. Propagación de señales en sistemas RFID.

Aplicando una hipótesis ideal, en la que el único medio por el que se propagan las ondas es el aire en condiciones de espacio libre, las comunicaciones se producirían sin ningún tipo de interferencia ni error. Pero este escenario dista mucho de los entornos y situaciones reales en los que se instalan los sistemas RFID, que normalmente no suelen facilitar la propagación de las ondas electromagnéticas. Aun así, la tecnología RFID es lo suficiente robusta como para funcionar siempre de manera adecuada, incluso cuando las condiciones son menos favorables.

Además, se ha de tener en cuenta que, en muchos casos, los sistemas RFID son empleados en espacios cerrados. Por lo que, para tener un buen conocimiento sobre el funcionamiento de la tecnología en esos entornos, resulta de gran utilidad el estudio de esos espacios, los elementos que se encuentran en su interior y los materiales que los forman. De esta manera es posible determinar el efecto de su interacción con las ondas electromagnéticas, dado que en algunas ocasiones las ondas se verán afectadas por la proximidad de éstos y en otras ocasiones las ondas deberán pasar a través de ellos [104].

Una vez que son emitidas, las ondas electromagnéticas interaccionan con la materia que hay a su alrededor mediante la transferencia de parte de la energía que transportan. Estando este hecho

directamente relacionado con la cantidad de señal que incide sobre cada una de las superficies. Lo que a su vez depende de la potencia de transmisión de los distintos dispositivos de radiofrecuencia.

Otro factor a tener en cuenta es el tiempo de exposición a dichas radiaciones: a mayor intervalo de exposición, mayor cantidad de energía pasa al medio expuesto. A mayores transferencias de energía, las señales de radiofrecuencia sufren mayores transformaciones.

Estos fenómenos pueden concretarse en si la onda electromagnética tiene la energía suficiente como para arrancar un electrón sobre el átomo en el que incide. Por debajo de un determinado nivel, no es posible arrancar ningún electrón y, por tanto, no modificar la estructura de la materia. En este sentido se puede diferenciar entre las radiaciones ionizantes, que tienen capacidad de alterar la estructura atómica del material; y las radiaciones no-ionizantes que, en principio, no tienen ningún efecto sobre la materia. Este comportamiento está fuertemente condicionado por la frecuencia a la que se producen estas ondas o radiaciones, ya que por debajo de una determinada frecuencia no es posible ionizar la materia.

Algunos ejemplos de radiaciones ionizantes pueden ser los rayos ultravioletas, los rayos X o ciertas radiaciones liberadas por materiales radiactivos. En todos los casos, las frecuencias de este tipo de ondas son millones de veces superiores a las frecuencias empleadas en los sistemas de radiocomunicación. En la Figura 3.3 se puede apreciar el uso que actualmente se realiza del espectro radioeléctrico, por lo que se puede afirmar que las ondas empleadas para la radiocomunicación no son ionizantes.

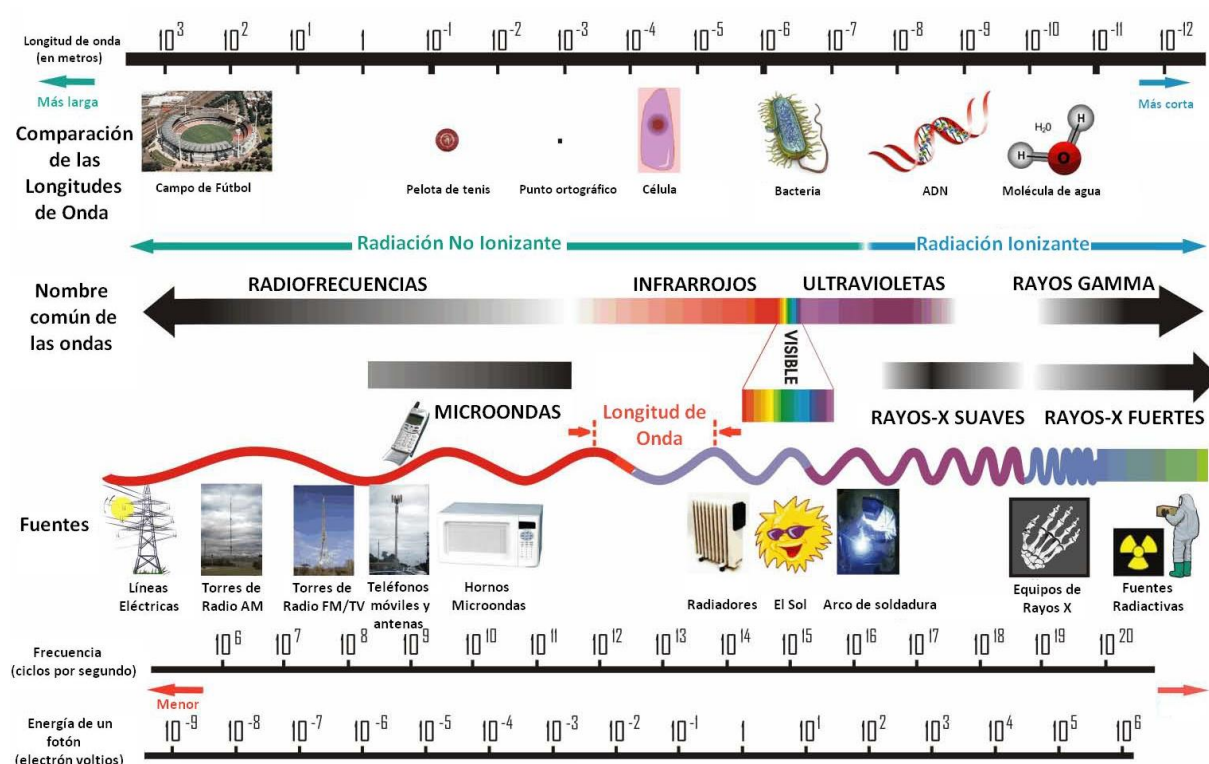


Figura 3.3. Espectro electromagnético y sus aplicaciones (Fuente: <http://www.electromagneticos.es>).

Por ejemplo, las microondas producen un incremento térmico sobre el material en el que inciden. En el caso del cuerpo humano, que tiene un alto porcentaje de agua, el efecto sería un posible calentamiento. Por lo que la potencia de los equipos de radiocomunicaciones debe estar limitada. Existe multitud de normativa vigente a lo largo de todo el mundo, tanto en ámbitos estatales como regionales, con el

objeto de regular la potencia de los dispositivos de radiofrecuencia, así como el uso adecuado y seguro del espectro radioeléctrico.

Para los humanos, las radiaciones electromagnéticas pueden resultar inofensivas o perjudiciales dependiendo del grado de exposición, es decir, de la intensidad de la señal y del tiempo de exposición. Pero dado que para el funcionamiento de la tecnología RFID no se precisa de una cantidad de señal excesiva, los niveles de exposición para las personas son muy bajos. Además, los sistemas RFID operan a frecuencias relativamente bajas (bandas de HF y UHF principalmente) y se consideran radiaciones no-ionizantes. Por todo ello, junto con los resultados de las investigaciones realizadas hasta el momento, se puede afirmar que no hay ninguna evidencia científica de que este tipo de señales tengan efectos adversos sobre la salud [105].

3.3. Caracterización electromagnética de materiales.

Para un mejor funcionamiento de la tecnología RFID y teniendo en cuenta los distintos fenómenos y comportamientos de las ondas electromagnéticas, resulta de especial interés el estudio y caracterización del entorno en el que funcionará el sistema [106]. De tal forma que, una vez conocido este, se podrá averiguar el comportamiento de las ondas electromagnéticas en el mismo. Lo que directamente podrá ser aplicable para realizar buenas instalaciones de sistemas RFID.

A la hora de plantear la instalación de un sistema RFID conviene estudiar pormenorizadamente los materiales que forman el entorno y que en definitiva serán el medio por el que se propaguen las ondas electromagnéticas. Para ello es necesario recurrir a los datos técnicos de cada material y obtener, por ejemplo, los valores de μ_r o ϵ_r . Pero lamentablemente, las características electromagnéticas de cualquier material no son una información que se pueda obtener de forma relativamente sencilla, sobre todo en los materiales de construcción más comunes. En este sentido, pocos fabricantes son los que realizan ensayos electromagnéticos en laboratorios especializados a los materiales que venden.

Desde el punto de vista de los sistemas RFID, resultaría útil poder conocer el efecto que un determinado material va a tener sobre las ondas electromagnéticas que emita y/o reciba, de tal forma que se pueda predecir este comportamiento e instalar y ajustar el sistema para obtener un funcionamiento óptimo.

Se puede encontrar una bibliografía extensa [66]–[80], relacionada con la preparación y caracterización electromagnética de materiales para aplicaciones de radiofrecuencia. La mayor parte de ellos se basan en simulación numérica, aunque existe un número considerable de trabajos que ponen el foco en la realización de medidas experimentales. Básicamente, los métodos para caracterizar el efecto de los materiales en las ondas electromagnéticas usados comúnmente son cuatro: el método de campo abierto o espacio libre; el método de caja blindada; el método de sala blindada; y el método de la línea de transmisión coaxial [122]. En este último método, empleado frecuentemente para la caracterización de materiales basados en cemento [123]–[128], las dimensiones de la cámara de medida limitan el espesor de la muestra de material a sólo unos pocos milímetros. Por lo que los resultados que aporta este método no son aplicables en materiales de construcción reales, o composiciones de materiales y estructuras mucho más gruesas y que, en muchas ocasiones, incorporan aditivos cuyo tamaño de sus partículas excede esas dimensiones.

3.3.1. Diseño y fabricación del equipo de medida.

Teniendo en cuenta las características, ventajas y desventajas de los distintos métodos de medida analizados, se detecta una falta de equipos y herramientas disponibles en el mercado para la

caracterización electromagnética de materiales a escala real, priorizando algunos aspectos relacionados con el tamaño de la muestra a medir. En este sentido se establece un tamaño máximo de la muestra de material para evitar problemas en su manipulación debidos al peso excesivo y grandes dimensiones. De tal forma que los resultados que se obtengan puedan ser aplicables a instalaciones reales y no sea necesario fabricar e integrar la solución constructiva en una sala blindada. Por lo que se decide diseñar y construir un equipo de medida que permita averiguar el comportamiento electromagnético real de materiales o conjuntos de ellos y que se encuentran habitualmente en las instalaciones de los sistemas de RFID. Gracias al cual se permitirá conocer el efecto que éstos tendrán sobre las ondas electromagnéticas o señales de RF que los puedan atravesar.

Para ello, se pueden plantear dos alternativas. Por un lado, obtener los parámetros característicos del material en cuestión, como son la conductividad, la permitividad o la permeabilidad. Y emplear dichos datos en cálculos teóricos que expliquen el comportamiento de la onda sobre ese material (más orientado al campo de la simulación). Y por otro lado, empleando la teoría de líneas de transmisión [129], se puede caracterizar un determinado medio haciendo incidir de manera experimental una onda electromagnética conocida y obteniendo los parámetros que definan el comportamiento de dicha onda al atravesar el medio material bajo estudio. Para este caso concreto se van a emplear los *parámetros-S* o parámetros de dispersión (*scattering*). En este contexto, la dispersión hace referencia a la forma en que las ondas electromagnéticas que se desplazan por una línea de transmisión se ven afectadas ante discontinuidades, como es el caso de que la onda electromagnética atraviese varios materiales con distintas impedancias (Z_0).

Los parámetros-S son unas propiedades empleadas en ingeniería y se utilizan para describir el comportamiento básico de las redes de transmisión (medios materiales en este caso), cuando se someten a estímulos de régimen permanente. Estos parámetros representan información de gran utilidad en el campo de la radiofrecuencia y varían en función de la frecuencia a la que se midan.

Se consideran puertos cada uno de los terminales sobre los que se tiene el control de las señales de radiofrecuencia que los atraviesan y es posible averiguar físicamente sus características. Así, se define el puerto 1 o de entrada y el puerto 2 o de salida. La definición de los parámetros-S asociados a una red a caracterizar se realiza en función de ondas de potencia que representan las ondas electromagnéticas incidentes y reflejadas en cada puerto (Figura 3.4). Por lo que en cada puerto se define una onda incidente (i_n) y onda reflejada (r_n). A partir de una onda de potencia incidente en el puerto 1 (i_1) pueden resultar ondas existentes en el mismo puerto 1 (r_1) o en el puerto 2 (r_2). Las relaciones entre cada una de estas ondas de potencia pueden definirse en términos de una matriz de parámetros-S.

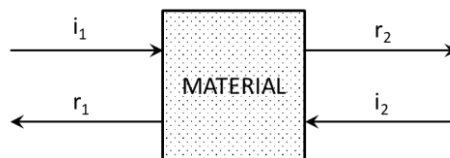


Figura 3.4. Red de dos puertos.

Aunque pueden emplearse tantos puertos como sean necesarios mediante una red multipuerto, para este caso basta con emplear una red de dos puertos. Se trata del tipo de la configuración más común y sirve como base para el desarrollo de matrices de órdenes superiores en redes más grandes. En este caso, la relación entre las ondas de potencia incidente y reflejada y la matriz de parámetros-S viene determinada por la siguiente ecuación:

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} \quad (3.13)$$

Y operando la ecuación (3.13), resulta:

$$r_1 = S_{11} \cdot i_1 + S_{12} \cdot i_2 \quad (3.14)$$

$$r_2 = S_{21} \cdot i_1 + S_{22} \cdot i_2 \quad (3.15)$$

En las ecuaciones (3.14) y (3.15) se obtiene la relación entre las ondas de potencia reflejada e incidente para cada uno de los puertos de la red, puertos 1 y 2, en función de los parámetros-S individuales y característicos de esa red: S_{11} , S_{12} , S_{21} y S_{22} . Cada uno de estos parámetros-S de la red de dos puertos bajo estudio se asocia con las siguientes descripciones:

- S_{11} es el coeficiente de reflexión de la onda electromagnética del puerto de entrada.
- S_{12} es la ganancia inversa de la onda electromagnética.
- S_{21} es la ganancia directa de la onda electromagnética.
- S_{22} es el coeficiente de reflexión de la onda electromagnética del puerto de salida.

Además, gracias a estos parámetros es posible determinar también si existen pérdidas de potencia dentro de la red. Es decir, si se disipa potencia al atravesar las ondas electromagnéticas la red. Lo que se traduce en que la suma de las potencias incidentes en todos los puertos es mayor que la suma de todas las potencias reflejadas en todos los puertos.

$$\sum |i_n|^2 > \sum |r_n|^2 \quad (3.16)$$

Gracias a los parámetros-S, es posible caracterizar y averiguar el comportamiento electromagnético de materiales o conjuntos de ellos frente a las ondas electromagnéticas de radiofrecuencia, sin necesidad de conocer su estructura interna, ni sus propiedades electromagnéticas concretas.

Se propone utilizar un analizador vectorial de redes para la medida de los parámetros-S de la muestra bajo estudio. A partir de los cuales, poder obtener datos que permitan describir y aportar información sobre el comportamiento electromagnético del material medido. Pero en este planteamiento el principal problema reside en el porta-muestras. Es decir, en el acoplamiento de la muestra al equipo de medida, cuyos terminales (puertos) normalmente tienen forma de conector-N. Para solventar este problema se decide construir una cámara anecoica electromagnética en la que introducirán dos antenas, conectadas a cada uno de los puertos del analizador, entre las que se colocará la muestra de material bajo estudio, evitando así que interferencias externas puedan adulterar la medida (Figura 3.5).

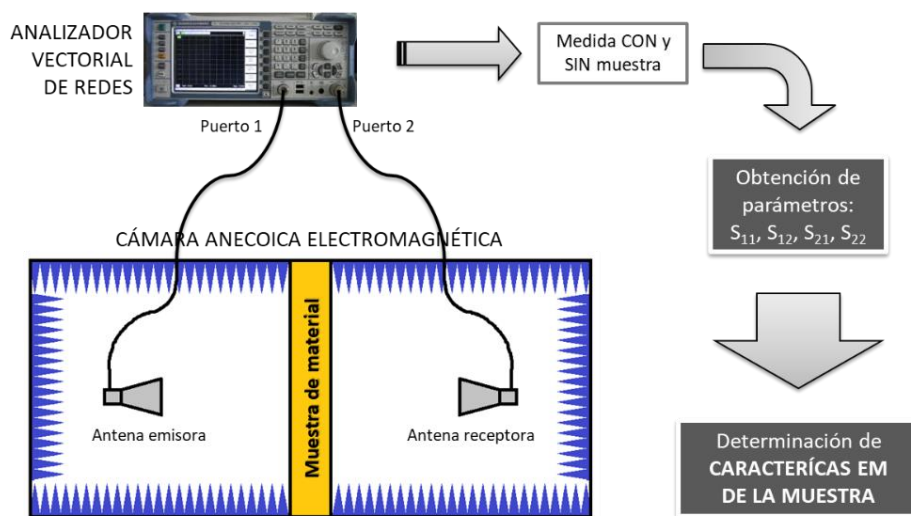


Figura 3.5. Diagrama del sistema de medida para la caracterización electromagnética de materiales.

En línea con los trabajos que se han llevado a cabo en esta tesis, se ha decidido seguir trabajando con la tecnología RFID en la banda de UHF. Es decir, poniendo el foco en la tecnología RFID pasiva, que es la que opera en este rango de frecuencias. Aunque en esta ocasión se ha contemplado también la posibilidad de que la caracterización se realice a frecuencias superiores.

3.3.1.a. Diseño de la cámara anecoica electromagnética.

Se diseña una cámara anecoica electromagnética de doble cavidad (Figura 3.6), consistente en dos cubos de 80 cm de lado. Dado que se quiere caracterizar el material, al menos, en la banda de UHF, estas dimensiones de las cavidades hacen posible que la onda electromagnética se encuentre en campo lejano (región de Fraunhofer) cuando incida sobre la muestra de material a analizar. Además, la cámara ha sido fabricada en acero inoxidable para aislar cualquier onda electromagnética que provenga del exterior (Figura 3.7).

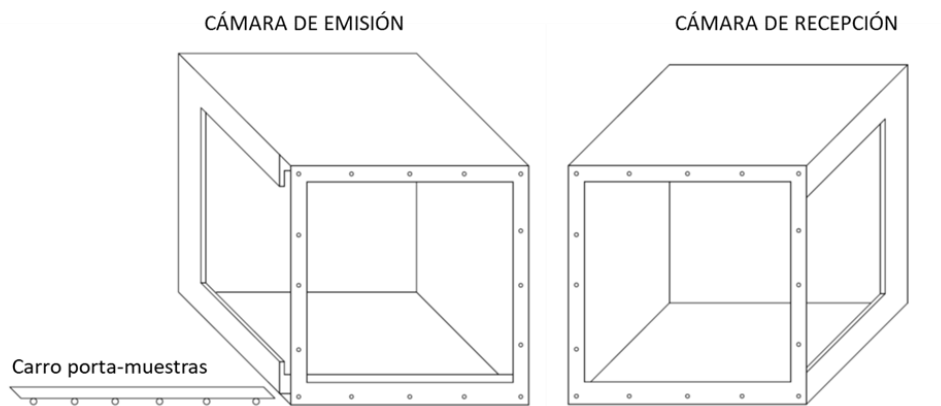


Figura 3.6. Cavidades que forman la cámara anecoica electromagnética.

Cada una de estas cavidades es independiente y dispone de una puerta propia para poder acceder a su interior. Se unen entre sí alojando la muestra entre ambas, siendo ésta la separación existente entre ambas cámaras. Y para sellar los bordes de la muestra, es decir, los encuentros entre la superficie de la muestra y las paredes de la cámara, se coloca un marco perimetral de acero inoxidable que evite la fuga de señal electromagnética. También se provee de dos tapas laterales, una para cada cavidad, por si se desea utilizar cada una de ellas como cámaras independientes para realizar otro tipo de ensayos.



Figura 3.7. Estructura metálica y acabado de la cámara diseñada y fabricada.

Todas las paredes interiores de las cámaras están forradas por material absorbente electromagnético para evitar que las reflexiones de las ondas en las superficies de la cámara tengan efecto sobre la medida (Figura 3.8). Concretamente en este caso se ha empleado material absorbente electromagnético piramidal de 4" de altura para todas las superficies. Excepto las paredes paralelas al plano de la muestra, que se recubren con material absorbente electromagnético piramidal de 12" de altura, con el objeto de reducir todas las posibles reflexiones de las ondas dentro de la cámara.

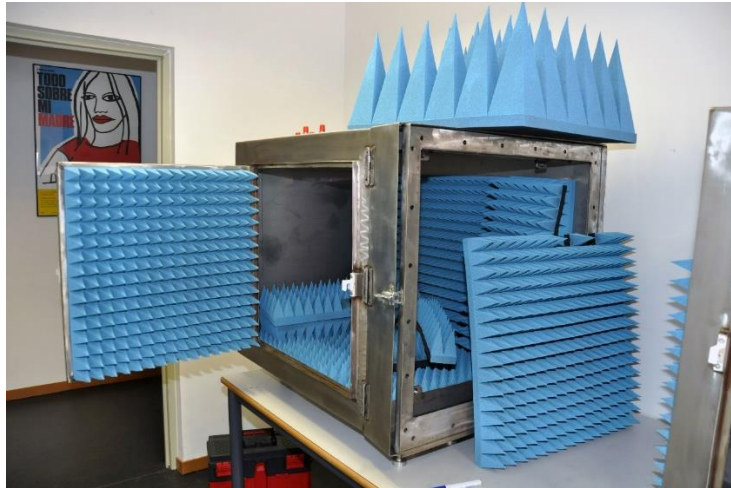


Figura 3.8. Material absorbente electromagnético que recubre las paredes interiores de la cámara.

En el interior de ambas cámaras se construyen unos soportes para la colocación de las antenas. Estos soportes descansan sobre dos barras, de 70 cm de longitud, que hacen que las antenas se puedan mover en planos paralelos a la muestra. De esta forma se puede modificar la distancia existente entre las antenas y la muestra en los ensayos (Figura 3.9). Tanto las barras, los soportes de las antenas y los elementos necesarios para la fijación de la muestra han sido contruidos en un material electromagnéticamente invisible para evitar que aparezcan superficies de reflexión indeseadas.

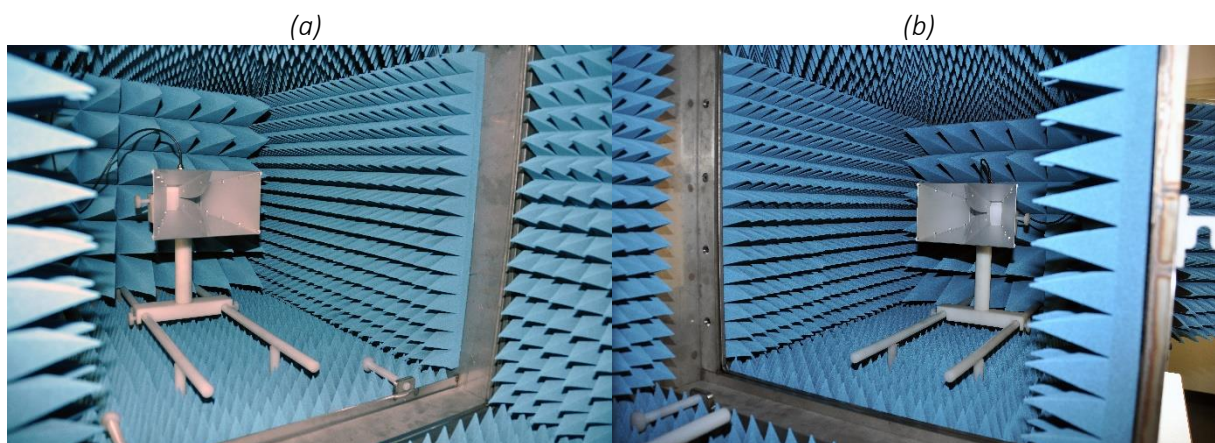


Figura 3.9. Interiores de las cámaras emisora (a) y receptora (b).

Dado que se desea caracterizar materiales que habitualmente se encuentran en los emplazamientos donde se instalan sistemas RFID, se diseña y construye también unos moldes para la fabricación de muestras de los materiales o conjuntos de materiales que se deseen caracterizar. Estas muestras tienen forma cuadrada y encajan perfectamente en la sección correspondiente entre ambas cámaras. Se contempla además que las muestras puedan tener distintos grosores hasta un máximo de 10 cm, que es la dimensión máxima de la cavidad para alojar las muestras. Concretamente, se han diseñado moldes para muestras de 1, 2'5, 5, 7'5 y 10 cm.

3.3.1.b. Montaje del equipo de medida.

La configuración completa del equipo de medida consta de varias partes (Figura 3.10). Los parámetros electromagnéticos han sido analizados con el analizador vectorial de redes Rohde & Schwarz® ZVL13, que proporciona resultados en un rango frecuencial desde los 9 kHz hasta los 13,6 GHz. El equipo consta de dos puertos cuya impedancia nominal son 50 Ω . Y a los que se conectan dos antenas de banda ancha Schwarzbeck® BBHA 9120 A, que son un modelo de antena de bocina de doble cresta con polarización lineal para el rango de frecuencias útiles desde los 800 MHz hasta los 10 GHz. El eje de estas antenas se sitúa perpendicularmente a la muestra de material que se quiera analizar dentro de la cámara anecoica descrita en el apartado 3.3.1.a. Debido a que las señales de RF que aporta el analizador no tienen demasiada potencia, es preciso intercalar un amplificador de radiofrecuencia. Concretamente el amplificador de microondas AR® 5S1G4 de 5 W de potencia continua en el rango de 0,8 a 4,2 GHz. De tal forma que la onda electromagnética generada en el puerto 1 del analizador (emisor), atraviese la muestra de material que se esté estudiando y llegue al puerto 2 (receptor). Todo ello se interconecta mediante cables de tipo coaxial y conexiones de tipo N con suficiente ancho de banda como para llevar a cabo los análisis.



Figura 3.10. Equipo de medida electromagnética de materiales completo.

El material absorbente electromagnético colocado en el interior de las cámaras se puede quitar fácilmente, convirtiendo ambas cavidades en dos cámaras reflectantes (dado que todas sus superficies son metálicas). Con ello se pretende que las cámaras sirvan también para realizar otros tipos de ensayos, como puede ser la prueba de un sistema de comunicaciones en entornos con mucho ruido e interferencias.

Todo el sistema se diseña con una impedancia característica de 50 Ω , de tal forma que el único elemento con una impedancia distinta será la muestra de material a caracterizar. De tal forma que el resto del sistema de medida afecte lo menos posible en la propagación de las ondas electromagnéticas.

Con este montaje de los equipos de medida se puede obtener de manera sencilla los parámetros-S, que caracterizan el comportamiento la muestra bajo estudio frente a las ondas electromagnéticas en función de la frecuencia.

3.3.2. Realización de medidas y resultados.

Para realizar la medida, el analizador vectorial de redes inyecta en el puerto 1 o puerto emisor una señal electromagnética a la frecuencia de trabajo que se esté analizando en cada caso, la cual es emitida por la antena transmisora (que se encuentra dentro de la cámara emisora), e incide con un ángulo de 90° sobre la superficie de la muestra de material. Parte de la energía de la onda electromagnética es absorbida por el material, otra parte se pierde por reflexión y la parte de energía que es capaz de atravesar la muestra es captada por la antena receptora (que se encuentra dentro de la cámara receptora), llegando ésta al puerto 2 o puerto receptor del analizador.



Figura 3.11. Disposición de las antenas en el interior de la cámara para la medida.

Además, para evitar la posible introducción de errores propios del sistema de medida y que los resultados de la medida sean lo más fidedignos posible, se han llevado a cabo varias acciones. Por un lado, se ha reducido al mínimo la influencia del campo electromagnético asociado con la configuración de antena transmisora en el interior de la cámara, gracias a la propia construcción de la cámara y teniendo en cuenta los valores transmitidos en ausencia de cualquier muestra. Por otro lado, tanto la antena emisora como receptora se colocan enfrentadas para asegurar la emisión centrada de la onda sobre la muestra y que la señal en la recepción provenga del centro de la misma, incluso para haces de cobertura estrechos (40° a 3 GHz). Lo que contribuye a evitar las posibles pérdidas por difracción que se producen en los bordes de la muestra, así como los efectos modales de la cámara (Figura 3.11). Por último, para minimizar también la influencia del campo magnético lejano y las reflexiones de fase o contrafase en el interior de la cámara, se han llevado a cabo cuatro medidas a diferentes distancias entre la antena transmisora y la muestra ($d_1 = 81$ cm, $d_2 = 71$ cm, $d_3 = 63$ cm y $d_4 = 55$ cm), para evitar interferencias.

Los resultados finales de los parámetros electromagnéticos se obtienen promediando los valores de las medidas realizadas en cada una de las cuatro posiciones (d_1 , d_2 , d_3 y d_4), y considerando siempre una desviación máxima de 3 dB entre los valores obtenidos para cada posición.

En vez de obtener las propiedades individuales de cada material como son la permitividad o permeabilidad, este procedimiento de medida permite obtener los parámetros-S que caracterizan el comportamiento de materiales o conjuntos de materiales reales, tal cual se colocan en realidad. Permitiendo cuantificar los efectos que tienen esos materiales sobre las ondas electromagnéticas con las que interactúan¹.

Para los sistemas RFID, resulta útil conocer qué cantidad de energía es reflejada por la superficie de un determinado material y qué cantidad de energía es capaz de atravesar ese material. Para ello, en las matrices de parámetros-S obtenidas en los resultados de las medidas, se presta especial atención a los parámetros S_{11} y S_{21} , asociados a estos dos conceptos. Es decir, por un lado, el valor de la reflectividad y por otro el de la atenuación o transmitancia (o más conocido como apantallamiento electromagnético, que es como se le denomina en la bibliografía) que sufre la onda electromagnética al pasar por ese material. Y con el fin de no condicionar los valores de los resultados con el sistema de medida, también se mide y caracteriza el sistema en vacío. Es decir, sin ninguna muestra de material en el interior de la cámara. De tal forma que a los valores medidos para cada material se les restarán los valores de referencia obtenidos con la cámara vacía (sin ninguna muestra). Obteniéndose, por tanto, los valores que describen el comportamiento electromagnético atribuible a la muestra de material bajo estudio.

En la Figura 3.12 se puede observar la respuesta del sistema de medida para los parámetros S_{11} y S_{21} , en las frecuencias de 950 MHz, 1,8 y 2,4 GHz. En este sentido se ha escogido un intervalo del espectro radioeléctrico que incluye las frecuencias comúnmente usadas por diferentes tecnologías de intercambio de información como Wi-Fi, WiMAX, RFID (Identificación por Radiofrecuencia), Bluetooth, GSM (Sistema Global para las comunicaciones Móviles), GPRS (Servicio General de Radiocomunicaciones por Paquetes), UMTS (Sistema Universal de Telecomunicaciones Móviles), LTE (Evolución a Largo Plazo), y las tecnologías emergentes y relacionadas con las comunicaciones móviles. Todas ellas muy necesarias para la implementación real del Internet de las Cosas (IoT, Internet of Things).

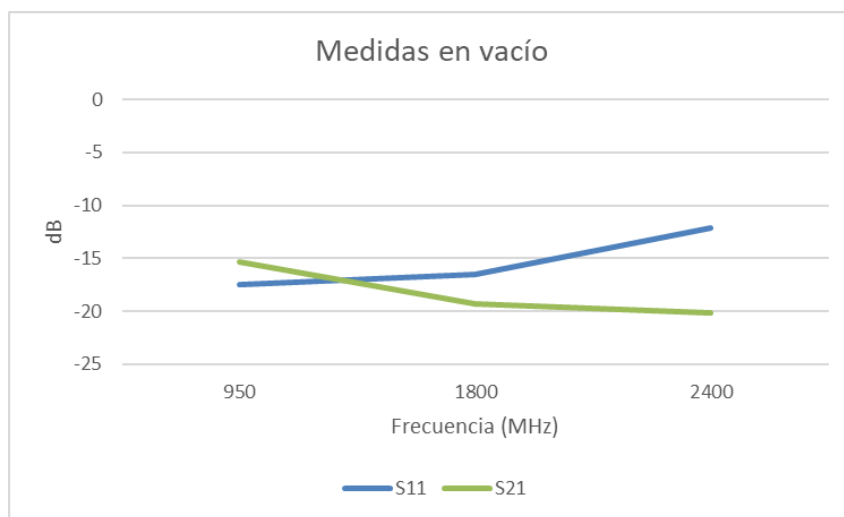


Figura 3.12. Resultados de las medidas en vacío, sin muestra de material, del equipo.

Se han llevado a cabo una serie de medidas con el objeto de poner en marcha el sistema y para poder visualizar y comprobar el tipo de resultados que se pueden obtener con el equipo de caracterización

¹ El sistema de medida propuesto ha sido empleado para la medida del apantallamiento electromagnético de materiales de construcción, cuyos resultados han sido publicados en la *Journal of Materials in Civil Engineering*, Vol. 30, Issue 8, agosto de 2018. Edit. ASCE. JCR: 5,768-T1 (Computer Science, Theory & Methods 8/104).

electromagnética de materiales diseñado y construido. Para ello, se han fabricado varias muestras representativas de algunos de los materiales de construcción empleados en la actualidad. Concretamente: una “muestra A” de hormigón con arena de cantera de 5 cm de espesor; otra “muestra B” de hormigón con arena de cantera y un 10% de fibras de acero para reforzar el hormigón de 5 cm de espesor; otra “muestra C” de yeso de 5 cm de espesor; y una última “muestra D” de un panel de yeso laminado para el aislamiento acústico de 1,5 cm de espesor. Los resultados obtenidos de reflectividad (Figura 3.13) y de apantallamiento electromagnético (Figura 3.14) que presentan las muestras analizadas se muestran a continuación. De ellos cabe destacar el efecto atenuante de la señal electromagnética que conlleva la incorporación de fibras metálicas en el hormigón (muestra B). Sobre todo, para la frecuencia de 1,8 GHz, donde el tamaño de las fibras metálicas coincide con $\lambda/4$.

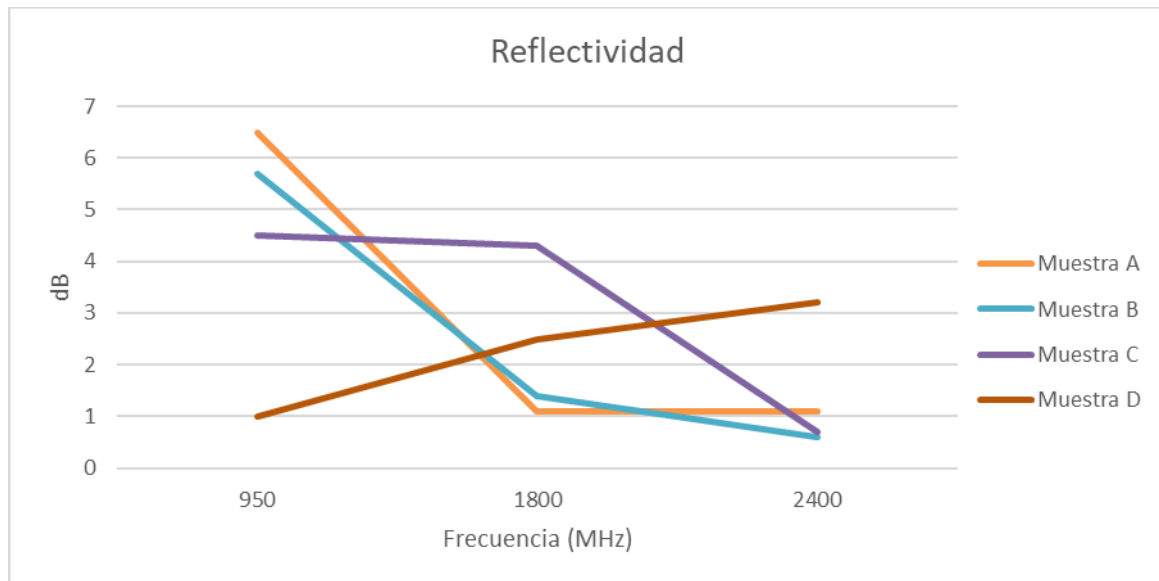


Figura 3.13. Energía reflejada en función de la frecuencia para las muestras analizadas.

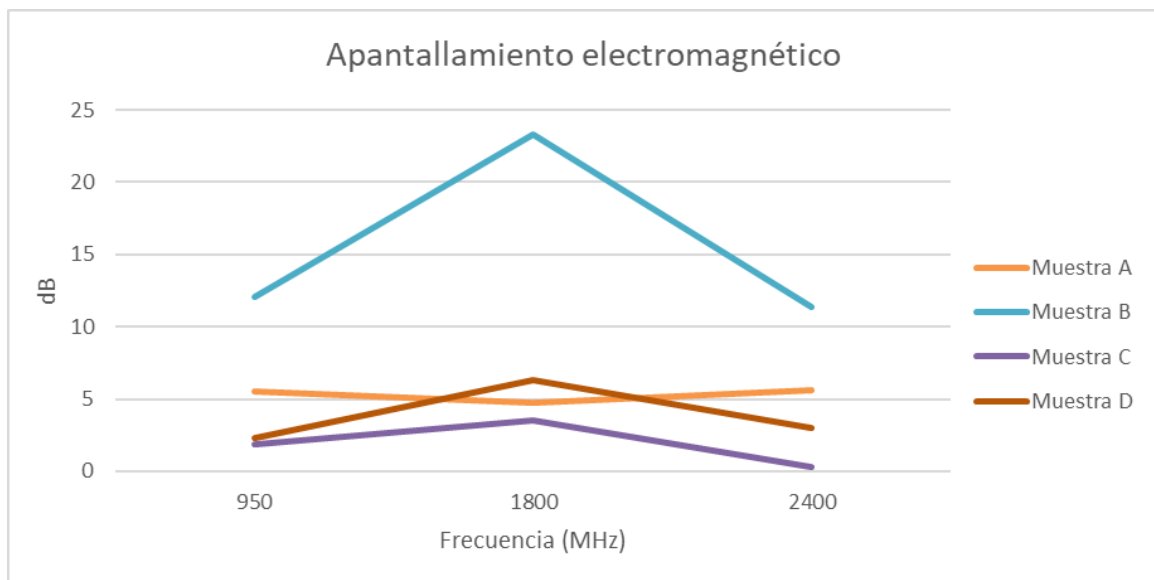


Figura 3.14. Energía absorbida en función de la frecuencia para las muestras analizadas.

Estos dos parámetros aportan información suficiente como para permitir la planificación y simulación de instalaciones y equipos de RFID, puesto que explican cómo se van a comportar las ondas electromagnéticas cuando incidan sobre ellos. Además, dadas las características de las muestras

analizadas en cuanto a tamaño y construcción, los resultados obtenidos son directamente aplicables a soluciones o instalaciones reales.

Gracias a esta información será posible la instalación de sistemas RFID con un mayor control sobre el campo electromagnético que generan, optimizando la energía que consumen. O incluso empleando materiales para conseguir determinados comportamientos específicos de los sistemas RFID o mejorar sus prestaciones. De forma que se consigan implantar sistemas RFID más eficientes.

3.4. Discusión de resultados y aplicaciones.

Tras los trabajos desarrollados en este campo, se dispone de una herramienta totalmente operativa que permite la caracterización electromagnética de materiales y soluciones constructivas a escala real. El equipo desarrollado proporciona información sobre cómo se van a comportar las ondas electromagnéticas cuando interactúan con un material. O, dicho de otro modo, qué efectos va a tener un determinado material o conjunto de ellos sobre unas ondas electromagnéticas que lo atraviesen.

La puesta en marcha del sistema de medida permite la caracterización electromagnética masiva de materiales de construcción y conjuntos o composiciones de ellos. De este proceso se obtienen datos tanto del apantallamiento electromagnético como de la cantidad de señal que se refleja sobre la superficie en la que incide la onda, tanto de forma gráfica como numérica. Los resultados que se obtienen para cada parámetro varían en función de la frecuencia, ya que las distintas longitudes de onda de las señales electromagnéticas que interactúan con la propia estructura interna de los materiales provocan este comportamiento.

En este tipo de sistemas de medida, la fabricación y preparación de la muestra a analizar es quizás uno de los puntos más críticos de toda la cadena y que mayor influencia tiene en los datos que se obtengan como resultados. Los cuales dependerán en gran medida de la estructura y características de la muestra bajo estudio. Ya que, por ejemplo, una grieta en medio de una muestra de hormigón provocaría que la mayor parte de la radiación electromagnética se colase por ella, falseando en este caso la medida y sus correspondientes resultados.

En un principio, el sistema de medida se ha configurado para analizar las bandas frecuenciales de radiofrecuencia en las que operan las tecnologías a las que se les pueden aplicar los resultados en mayor medida, como son la RFID, Wi-Fi o la telefonía móvil. Sin embargo, el sistema de medida permite ajustar el intervalo de frecuencias a analizar, ampliándolo o reduciéndolo según sea necesario. Existiendo también la posibilidad de obtener una mayor cantidad de resultados para distintas frecuencias en una determinada banda. Es decir, aumentar la resolución frecuencial de las medidas que se deseen realizar. Aunque siempre se han de tener en cuenta las propias limitaciones del sistema de medida construido. Las dimensiones físicas de la de la cámara anecoica electromagnética construida y el rango de trabajo del analizador vectorial de redes empleado en las medidas, limitan las frecuencias mínima y máxima de trabajo del sistema.

Los resultados que proporciona el sistema de medida construido se pueden incorporar a las características de cada material o solución constructiva como información referente a su comportamiento electromagnético, al igual que sucede habitualmente en otros campos como el aislamiento térmico o acústico. Además, cabe destacar que estos parámetros han sido obtenidos mediante un procedimiento práctico, por lo que su aplicación es directa. Esta información se podría proporcionar a los fabricantes de los materiales que se analicen en forma de ficha técnica con información gráfica y numérica sobre el comportamiento electromagnético de sus materiales. Como

consecuencia, se dispondría de un amplio catálogo de materiales y soluciones constructivas clasificado en función de su comportamiento ante las señales electromagnéticas de radiofrecuencia. De tal forma que los usuarios puedan tener accesible esta información y puedan comparar y seleccionar el material que mejor se ajuste a sus necesidades.

Este tipo de prácticas están comenzando a tomar sentido, puesto que nos encontramos en un mundo en el que las comunicaciones inalámbricas son cada vez más utilizadas y en más ámbitos. Además, se prevé que su uso aumente aún más con la implantación del IoT. Por este motivo resulta primordial tener un control exhaustivo sobre cómo y por donde se propagan las ondas electromagnéticas que se emplean para cada aplicación. De tal forma, que se haga un uso eficiente de las señales de radiofrecuencia de cada tecnología y se contribuya, en la medida de lo posible, a ahorrar energía.

Además, los resultados de caracterización electromagnética de materiales se pueden aplicar a otras tecnologías aparte de la RFID, dado que el sistema permite trabajar y obtener resultados para frecuencias superiores. Por lo que se presenta la oportunidad de conocer con exactitud cómo se comportan las ondas de Wi-Fi de una determinada instalación o cómo le afecta un determinado revestimiento a la señal que recibe un teléfono móvil en el interior de un recinto. Lo que en última instancia abriría la puerta a, por ejemplo, construir aulas docentes en las que no penetre señal de redes móviles; o aislar una determinada señal inalámbrica privada en el interior de un recinto. En este sentido, cabe destacar la necesidad de construir edificios que mantengan a las personas protegidas de la exposición dañina a la radiación, mientras que al mismo tiempo se facilita el uso de todo tipo de dispositivos electrónicos en los edificios en los que nos encontramos habitualmente, cada vez más sensorizados y automatizados.

Capítulo 4.

Análisis y propuestas sobre protocolos de comunicación para RFID – UHF pasiva.

Resulta evidente que para llevar a cabo una comunicación se precisa de: un emisor, que transmita la información; un receptor, que la reciba; ambos dos unidos por un canal, que es el medio físico por el que se transmite la información, se propaga y finalmente se capta por el receptor; el mensaje, que es la propia información que se desea comunicar; un código, que es el lenguaje o conjunto de reglas en el que se transforma el mensaje para viajar por el medio y que comparten tanto emisor como receptor; y un contexto, que hace referencia a todas las circunstancias temporales, espaciales y socioculturales, que son externas a la propia comunicación pero pueden incidir sobre ella. Pero en el caso de la tecnología RFID pasiva, este esquema básico se complica dado que las comunicaciones no son simétricas. Es decir, se utilizan códigos distintos dependiendo de si los mensajes se transmiten del lector a la etiqueta o de la etiqueta al lector. Aunque en RFID pasiva, tanto emisor como receptor comparten canal, en este caso el aire, éste puede verse alterado e influenciado por el contexto. Y es que es habitual el uso de este tipo de sistemas en entornos ruidosos, desde el punto de vista de las comunicaciones, y donde el canal se comparte con otras tecnologías. Además, físicamente los espacios en los que comúnmente se lleva a cabo el intercambio de mensajes en los sistemas RFID está plagado de obstáculos (en muchas ocasiones metálicos), que dificultan e inciden negativamente en el éxito de las comunicaciones.

En este capítulo se recogen los trabajos desarrollados en torno a los protocolos de comunicación en la tecnología RFID pasiva para la banda de UHF, así como los resultados de investigación más relevantes que se han obtenido.

Se ha estudiado en detalle cómo suceden las comunicaciones entre lector y etiqueta pasiva en ambas direcciones. Y se han realizado varias propuestas relativas a los protocolos de comunicación para contribuir al mejor funcionamiento de la tecnología. Paralelamente a estos trabajos, se ha desarrollado una plataforma física para emular el comportamiento de una etiqueta pasiva, de manera que se disponga de una herramienta física real para la evaluación de nuevos algoritmos o cambios introducidos

en los protocolos de comunicación de manera rápida y flexible, sin necesidad de fabricar nuevas etiquetas.

4.1. Protocolo de comunicación RFID – UHF.

Para que un intercambio de información pueda llevarse a cabo, han de establecerse previamente una serie de parámetros y reglas que tanto emisor como receptor deben conocer y acatar. El canal de comunicación, la velocidad de transmisión y recepción o qué tipo de codificación de datos se va a emplear son algunos ejemplos.

Al igual que sucede en otras tecnologías, todos los parámetros, comandos y reglas que dictaminan cómo han de producirse los procesos de comunicación existentes entre el lector de RFID y la etiqueta pasiva, se encuentran recogidos en diversos estándares y especificaciones. De entre todo el conjunto de especificaciones y normas, en esta tesis se ha trabajado con el “EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Standard” [16] (en adelante EPC Gen2), especificación del protocolo de interfaz aérea para comunicaciones de RFID en la banda de 860 MHz – 960 MHz. Desde su primera edición en el año 2004, la especificación lanzada por el GS1 [130] se ha convertido en el estándar de facto a nivel mundial en lo que se refiere a comunicaciones entre lectores y etiquetas en la tecnología RFID pasiva para la banda de UHF. Tanto es así que ISO (International Organization for Standardization), reconoció esta especificación, dándole cabida en las últimas modificaciones de su estándar ISO 18000-6:2013 [17]. Y que finalmente, a partir del año 2014, se ha impulsado y establecido con la aparición de RAIN RFID [131], cuyo principal objetivo es el establecimiento universal de la tecnología RFID-UHF usando el protocolo EPC Gen2.

El protocolo EPC Gen2 se encarga de especificar cómo han de ser y producirse las interacciones físicas entre lectores y etiquetas, así como los procedimientos lógicos y comandos que intercambian entre ellos. A partir de estas especificaciones, los fabricantes tienen cierta libertad para desarrollar sus dispositivos, siempre y cuando implementen todos los requisitos de conformidad con el protocolo.

4.1.1. Características físicas.

Normalmente, en los procesos comunes de comunicación por RF, tanto el emisor como el receptor siguen los mismos esquemas de transmisión y recepción de la información a todos los niveles. Sin embargo, esto no sucede en el caso de la comunicación entre dispositivos de RFID. Se trata de un caso especial de comunicación por RF y se caracteriza principalmente porque las transmisiones y recepciones de información entre dispositivos no siguen los mismos esquemas ni características. Pero, además, todos tienen que entenderse adecuadamente. Esto es debido a que las etiquetas pasivas carecen de alimentación, lo que se traduce en que todos los dispositivos RFID poseen diferentes mecanismos para transmitir y recibir la información. La comunicación entre lector y etiqueta es half-duplex o semidúplex, es decir, bidireccional y no simultánea.

Para una correcta transmisión y recepción de la información, tanto lectores como etiquetas, deben cumplir con todas las normas y restricciones de las diferentes técnicas de comunicación empleadas. Las secuencias de transmisión para todas las comunicaciones comenzarán siempre con el bit más significativo (Most Significant Bit, MSB). Es decir, para cada mensaje se comenzará a transmitir la palabra más significativa y para cada palabra el bit más significativo (MSB) en primer lugar. Además, todas las transmisiones deben incluir un código CRC (Cyclic-Redundancy Check), para asegurar la correcta recepción de la información.

Para que la comunicación se lleve a cabo de manera adecuada, todos los dispositivos RFID deben respetar los esquemas temporales de los procesos de comunicación y acatar los requisitos temporales marcados por el protocolo [16]. Los lectores deben emplear unos parámetros fijos para cada ronda de inventariado (*inventory round*), en las que las etiquetas pueden responder enviando tres tipos de respuestas: *immediate*, *delayed* o *in-process*; y que dependerán del tipo de operación que se esté llevando a cabo entre lector y etiqueta.

Las técnicas de modulación y codificación utilizadas para las comunicaciones RFID deben ser de baja complejidad, con el fin de evitar circuitos complejos que puedan tener consecuencias negativas. En el lado del lector, en principio, no habría problemas. Pero las limitaciones de las etiquetas pasivas imponen el uso de esquemas sencillos. Por un lado, porque el uso técnicas complejas requiere que los circuitos de demodulación precisen de una mayor área en la etiqueta, lo que aumenta linealmente el coste de cada una de ellas. Y, por otro lado, porque los circuitos de demodulación avanzados tienen un consumo de energía más alto. La Figura 4.1 muestra un ejemplo de cómo se transmite la información mediante modulación en amplitud (ASK) y que puede utilizarse en ambos enlaces de transmisión de la información.

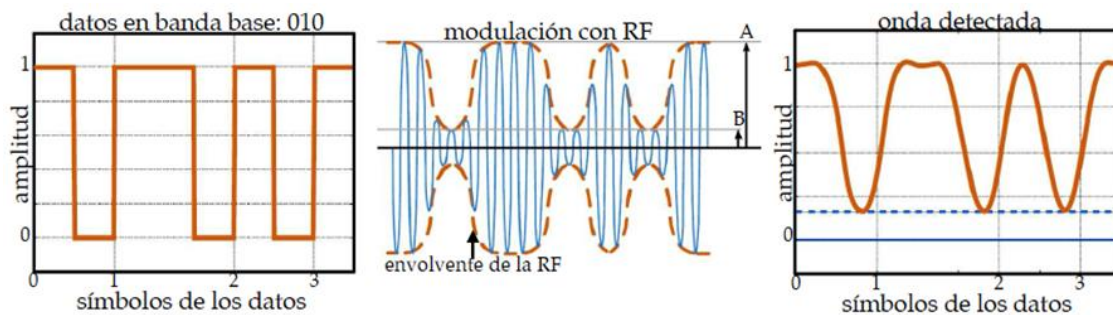


Figura 4.1. Información a través del enlace de comunicación con modulación ASK [16].

4.1.1.a. Enlace lector – etiqueta.

Para enviar la información, el lector RFID emplea un intervalo de tiempo, denominado T_{ari} , y que se encuentra entre $6,25\mu s$ y $25\mu s$. Este intervalo se emplea como referencia para codificar la información mediante el sistema PIE (Pulse-Interval Encoding), o codificación por ancho entre pulsos (Figura 4.2). En este sistema, el “dato 0” equivale a un periodo de señal de duración igual al T_{ari} en el que se inserta un pulso cuadrado a bajo nivel y de una anchura determinada (Pulse Width, PW). Y un “dato 1” equivale a un periodo cuya duración se encuentra entre $1,5$ ó $2 T_{ari}$, en el que también se inserta el mismo pulso anterior (PW). Este tipo de codificación maximiza la cantidad de energía que se envía a la etiqueta mediante la portadora de RF, ya que ésta, al ser pasiva, sólo dispondrá de la señal emitida por el lector como única fuente de energía para su funcionamiento.

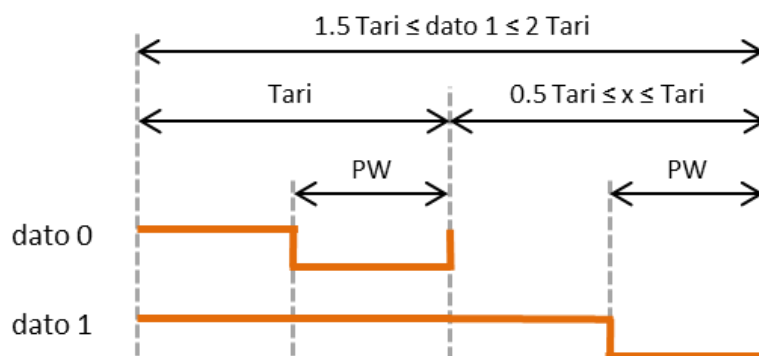


Figura 4.2. Codificación por ancho de pulso (PIE) [16].

Una vez codificada la información (señal moduladora), la portadora de RF se modula mediante DSB-ASK, SSB-ASK o PR-ASK para su transmisión. Todos los paquetes transmitidos comienzan bien con una secuencia *preámbulo* o con una secuencia *frame-sync*, cuya finalidad es proporcionar a las etiquetas la información necesaria para la decodificación del mensaje, así como los parámetros del enlace para el retorno. Además, de contribuir a la sincronización del proceso de comunicación. El *preámbulo* únicamente precede al primer comando, el resto comienzan por la secuencia *frame-sync*.

Cabe destacar que tanto los datos "0" y "1", como todos los símbolos especiales de limitación de trama, son unas composiciones de múltiples períodos de *Tari*. Como consecuencia las secuencias de bits, con el mismo número de datos, pueden tener diferente longitud una vez codificadas. Por otro lado, la anchura del *Tari* también es importante porque define la anchura mínima (frecuencia máxima) de la señal modulada. En otras palabras, el *Tari* es responsable del ancho de banda de la señal RF resultante: a menor valor de *Tari*, mayor es el ancho espectral necesario para transmitir la señal.

4.1.1.b. Enlace etiqueta – lector.

La información binaria que la etiqueta debe responder al lector se codifica mediante la modulación FM0 en banda base o mediante la modulación Miller de una subportadora, denominada *BLF* (Backscatter Link Frequency) y que se corresponde con la velocidad de transmisión de los datos en la respuesta al lector.

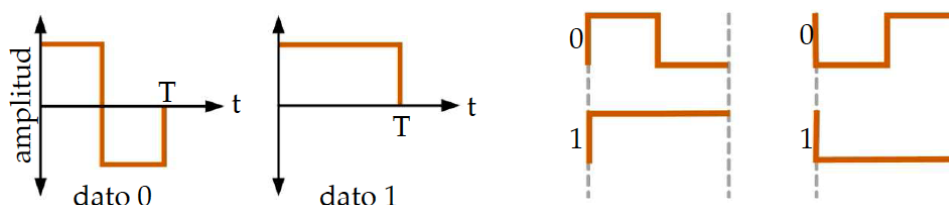


Figura 4.3. Codificación FM0 de los datos para enviarlos al lector [16].

Para la codificación FM0, la señal cambia en mitad del intervalo correspondiente a un "dato 0" y se mantiene constante durante un "dato 1" (Figura 4.3). Y al contrario para el caso de la codificación Miller. En ambos esquemas, se introduce una nueva inversión entre dos símbolos iguales consecutivos ("dato 0" o "dato 1"), tal y como se puede apreciar en la Figura 4.4.

Las etiquetas transmiten la información al lector empleando la modulación por retrodispersión (*backscattering modulation*), que consiste en que la electrónica interna de la etiqueta modifica la adaptación de su antena, realizando una variación temporal entre dos estados y de acuerdo con la señal binaria que se ha de transmitir. Por tanto, se puede decir que la etiqueta modifica el coeficiente de reflexión de su antena para lograr dos estados, correspondientes con dato "1" y dato "0". Dado que la etiqueta carece de un sistema de alimentación que le permita emitir su propia portadora, se emplea este sistema para aprovechar la reflexión de la portadora que llega del lector y hacerle llegar así la información, empleando para ello un esquema de modulación ASK o PSK.

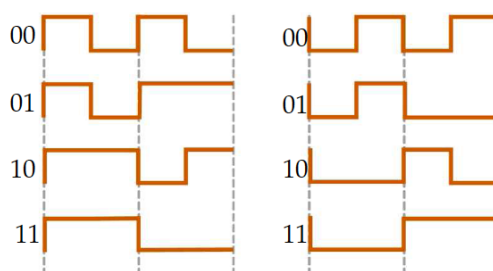


Figura 4.4. Secuencias de datos FM0 [16].

4.1.2. Consideraciones lógicas.

Aparte de las consideraciones físicas, una serie de esquemas lógicos son necesarios para la implementación de las comunicaciones entre lectores y etiquetas. En este punto no ha de perderse de vista el objetivo fundamental de un sistema RFID: identificar unívocamente todos los objetos (etiquetas) que se encuentren dentro del área de cobertura del lector. Para entender adecuadamente el funcionamiento de la tecnología RFID han de tenerse en cuenta algunas consideraciones y características de las etiquetas pasivas, que son descritas en los siguientes subapartados.

4.1.2.a. Memoria de la etiqueta.

La memoria de una etiqueta comercial está estructurada en cuatro bancos de memoria independientes: la memoria reservada, que incluye las contraseñas de acceso y/o para deshabilitar la etiqueta; la memoria EPC, que incluye el EPC, las palabras opcionales XPC en caso de que el *Extended Protocol Control (XPC)* esté implementado y los parámetros *StoredCRC* y *StoredPC*; la memoria TID (Tag Identification), que contiene información relacionada con la etiqueta y su fabricante, como identificador de clase, autoridad de registro o el número de serie de la etiqueta; y la memoria de usuario, que contiene espacio libre para el almacenamiento de datos de usuario y puede ser configurada como uno o varios ficheros.

4.1.2.b. Sesiones. Flags de inventariado y selección.

Desde un punto de vista organizativo y para gestionar las posibles poblaciones de etiquetas, los lectores y etiquetas pueden participar arbitrariamente en cuatro sesiones de lectura diferentes, denominadas S0, S1, S2 y S3. Pero una vez iniciado el proceso, las etiquetas únicamente pueden participar en una y solo en una sesión durante una ronda de inventariado.

Para ello, las etiquetas deben implementar un flag de inventariado (*inventoried flag*) independiente para cada una de estas cuatro sesiones, que puede contener dos valores: A o B. Se trata de los únicos recursos que posee la etiqueta separados e independientes para cada sesión. El resto de los recursos de la etiqueta son compartidos para todas las sesiones, como el flag de selección (*selected flag*), que los lectores también emplean para interactuar con unas etiquetas u otras.

4.1.2.c. Estados de la etiqueta y contador de slot.

Las etiquetas implementan diferentes estados lógicos en los que organizan su funcionamiento, condicionando el comportamiento de la etiqueta y la respuesta a los diferentes comandos del lector en cada momento. Aunque la implementación real de un tag puede tener más estados lógicos, la especificación EPC Gen2 considera los siguientes estados: listo (ready), de servicio (arbitrate), de respuesta (reply), reconocido (acknowledged), abierto (open), seguro (secured) y muerto¹ (killed).

Además, las etiquetas deben implementar un contador de slot (ranura) de 15 bits que es necesario para determinar cuándo va a contestar cada etiqueta al lector. Dicho contador de slot es precargado con un valor entre 0 y $2^Q - 1$, siendo Q un parámetro del comando *Query*, comando encargado de iniciar la ronda de identificación o inventariado. El valor del contador es decrementado en una unidad cada vez que la etiqueta recibe el comando correspondiente (*QueryRep*) del lector. Y cuando este contador de slot alcanza el valor 0 (0x0000), la etiqueta lanza su respuesta al lector. Si la etiqueta no recibe la confirmación del lector, el valor en el contador cambia a 0x7FFF y comienza de nuevo la cuenta atrás.

¹ Etiqueta deshabilitada. Fuera de uso.

4.1.2.d. Generador de números aleatorios o pseudoaleatorios de la etiqueta.

Las etiquetas deben implementar un generador de números aleatorios o pseudoaleatorios (en adelante PRNG, Pseudo-Random Number Generator), que es necesario para algunas operaciones, como generar el número para precargar el contador de slot o para generar el primer mensaje de respuesta que la etiqueta manda al lector: un número aleatorio de 16 bits, llamado *RN16*. Posteriormente, este generador también es empleado en algoritmos y operaciones más complejas. Por lo que el generador de números pseudoaleatorios (PRNG) es una parte crítica y fundamental de la lógica interna de las etiquetas pasivas.

4.1.3. Identificación y gestión de etiquetas.

Los lectores gestionan el conjunto de etiquetas que puedan encontrarse dentro de su área de cobertura mediante tres etapas básicas, cada una de las cuales engloba múltiples tipos de comandos y operaciones:

- **Select:** en esta etapa el lector selecciona o prepara un conjunto de etiquetas para operaciones posteriores. Incluye los comandos *Select* y *Challenge*.
- **Inventory:** es la etapa en la que el lector identifica unívocamente cada etiqueta. El lector comienza una ronda de inventariado (inventory round) con un comando *Query* para una de las cuatro sesiones, dado que una ronda de inventariado sólo puede llevarse a cabo en una y solo una sesión al mismo tiempo. A este comando pueden responder una o varias etiquetas y el lector debe ser capaz de detectar cada una de ellas. Para cada una de las respuestas únicas recibidas correctamente, el lector se encarga de recoger el parámetro *StoredPC*, las palabras opcionales *XPC*, *EPC* y el código *CRC* de cada etiqueta. Toda la etapa de Inventory incluye una gran variedad de comandos.
- **Access:** en esta etapa el lector interactúa individualmente con cada una de las etiquetas previamente identificadas. Durante este proceso, el lector puede realizar operaciones importantes como leer y/o escribir en la memoria de la etiqueta, bloquear o matar² la etiqueta, operaciones relacionadas con la seguridad como la autenticación de la etiqueta, u operaciones relacionadas con archivos que se encuentren en la memoria de usuario de la etiqueta. Para llevar a cabo todas las operaciones de la etapa de Access también existe una amplia gama de comandos.

Estas tres etapas engloban todas las posibles funciones e intercambios de información que un lector puede realizar con una etiqueta UHF pasiva. Pero de entre todo este conglomerado de procesos, comandos e intercambios de información, el momento más crítico, sin duda, es cuando el lector tiene que ser capaz de identificar unívocamente a todas y cada una de las etiquetas que se encuentren dentro su área de cobertura. Cabe destacar que este proceso se produce sin que el lector tenga un conocimiento previo del número de etiquetas a identificar, ni de sus características.

En la especificación EPC Gen2 se describe cómo deben de producirse las comunicaciones entre lectores y etiquetas pasivas; delimitando los tiempos y estableciendo los requisitos que tanto lectores como etiquetas deben cumplir. Cabe destacar en este punto que, en la tecnología RFID pasiva, las etiquetas carecen de una fuente independiente de energía. Por lo que, dado que la energía disponible en las etiquetas es limitada, las operaciones que éstas deban realizar han de ser simples y rápidas. En la Figura 4.5 se muestra la secuencia de comandos que suelen producirse entre el lector y la etiqueta en un

² Proceso irreversible por el que se inhabilita definitivamente una etiqueta y deja de estar operativa.

proceso de identificación. Destacando el hecho de que el lector nunca deja de emitir la señal portadora (rotulada como CW, Continuous Wave), puesto que las etiquetas pasivas precisan de esta energía para funcionar.

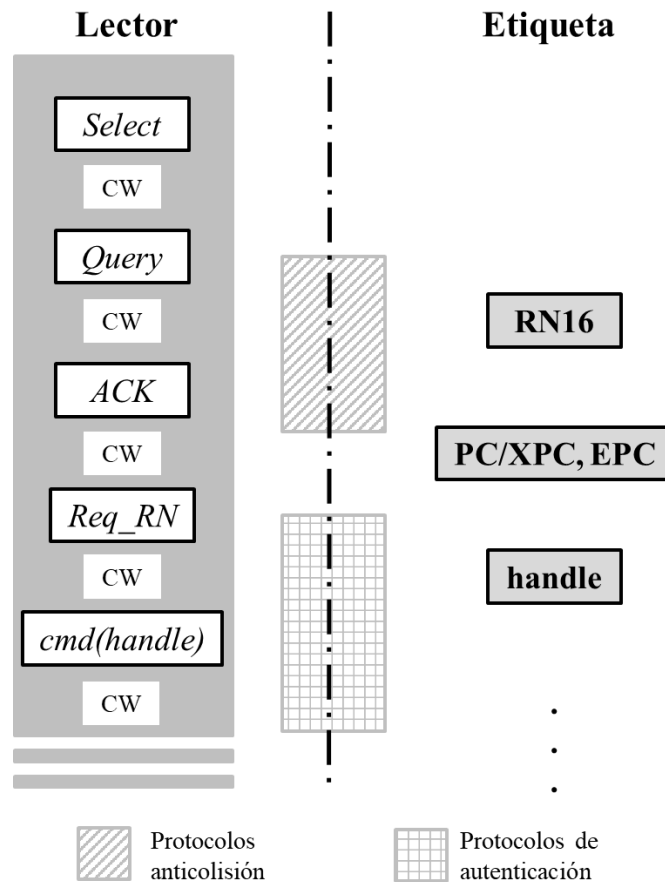


Figura 4.5. Secuencia de comandos entre lector y etiqueta.

El lector es el responsable del establecimiento de la comunicación; desde que ésta comienza con el lanzamiento del comando *Select* hasta que se hayan realizado todas las operaciones necesarias. Mediante el comando *Select* es posible determinar qué etiquetas van a ser identificadas. Para ello, se emplean algunos parámetros de selección como la sesión de lectura o los flags de inventariado y selección en cada etiqueta. Resultando de esta operación que sólo un grupo de etiquetas, del total de la población existente en el área de cobertura del lector, serán identificadas. Por tanto, la primera acción que realiza el lector es tratar de dividir y organizar una población de etiquetas desconocida. Posteriormente, el lector envía el comando *Query*, que demanda la primera respuesta de cada una de las etiquetas seleccionadas. A continuación, estas etiquetas deben generar una respuesta, denominada *Unique Identifier (UID)* o *RN16*. Y que se trata de un número aleatorio o pseudoaleatorio de 16 bits que debe crearse únicamente con la energía recibida de la portadora del lector y que, además, debe ser suficiente para transmitir este número al lector mediante el proceso de retrodispersión (backscatter). Si una etiqueta recibe una señal de reconocimiento del lector (*acknowledgement, ACK*), que contenga su propio *RN16*, viene a indicar que el lector ya conoce la presencia de esa etiqueta y que el proceso de identificación se ha iniciado de manera correcta. A partir de ese momento, el lector puede acceder al banco de memoria de la etiqueta mediante operaciones de lectura y escritura, llevando a cabo las comunicaciones que se requieran en cada caso. En cambio, si el lector no recibe adecuadamente la respuesta de la etiqueta responderá un ACK erróneo, por lo que el proceso de identificación no continuará.

Una vez la etiqueta ha sido contabilizada por el lector, se pueden suceder una serie de operaciones que implican un mayor intercambio de información entre el lector y la etiqueta, como pueden ser el acceso a diferentes partes de la memoria, escritura de datos, comprobaciones, etc. Para ello, se emplean protocolos que incluyen técnicas de autenticación y mecanismos de seguridad. Estos procesos requieren una mayor capacidad de cómputo y por tanto, una mayor cantidad de energía disponible para poder ejecutar las operaciones necesarias [132]. Siendo ésta, otra de las principales limitaciones de las etiquetas RFID pasivas, puesto que únicamente se alimentan de la energía procedente de la señal de RF, emitida por el lector, y que incide sobre ellas.

Si varias etiquetas contestan al mismo tiempo sucede una colisión, dado que el canal es ocupado por varios mensajes en el mismo instante de tiempo. Dependiendo del tipo de colisión, el lector puede ser capaz de detectarla y resolverla. Pero si se produce una colisión durante el establecimiento de la primera comunicación, algunas etiquetas pueden pasar desapercibidas y no ser identificadas. Lo que supone errores y fallos en el funcionamiento de la tecnología RFID como sistema fiable de identificación. Para minimizar este fenómeno se han creado los protocolos anticolisión. En el caso del protocolo DFSA (Dynamic Frame Slotted Aloha), mecanismo anticolisión sugerido en la especificación EPC Gen2, antes de lanzar la primera respuesta, la etiqueta debe cargar en su contador de ranuras (*slot counter*) un número aleatorio o pseudoaleatorio entre 0 y $2^Q - 1$, donde Q es un entero del intervalo $[0, 15]$ determinado por el lector y enviado a la etiqueta como parámetro del comando *Query*, y que a su vez, puede ser modificado por el comando *QueryAdjust*. El *slot counter* de la etiqueta decrementa su valor cada vez que ésta recibe un comando *QueryRep*. Y cuando el *slot counter* alcanza el valor de 0x0000, la etiqueta emite su *RN16* como respuesta mediante backscatter. De manera que disminuye considerablemente la probabilidad de que dos etiquetas emitan su respuesta al mismo tiempo.

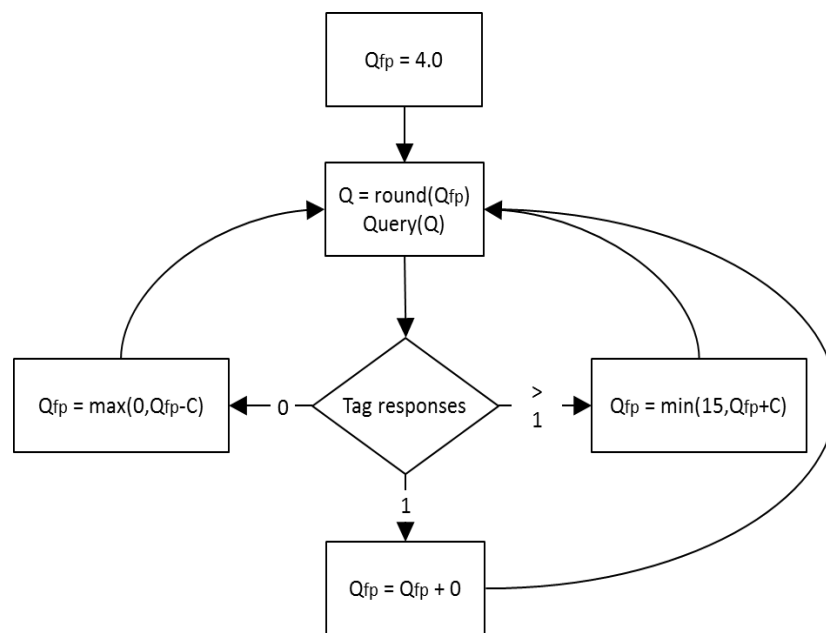


Figura 4.6. Algoritmo para la obtención del parámetro Q propuesto en EPC Gen2 [16].

Además, para minimizar aún más la posibilidad de respuestas simultáneas de varias etiquetas, la especificación EPC Gen2 propone un algoritmo para establecer el tamaño de la ventana temporal (*frame size*) en el que las etiquetas pueden responder. Efecto que se refuerza más concretamente para este caso, en el que la ventana (*frame*) está dividida en ranuras (*slots*). El número de ranuras en cada ventana (y, por tanto, su tamaño), viene determinado por la ecuación (4.1). Donde el valor de Q es dinámico y se establece a partir de los resultados obtenidos tras analizar lo que ha ocurrido en la ventana anterior.

El algoritmo propone actualizar el parámetro Q_{fp} (Figura 4.6), que es la representación en coma flotante (*floating-point*) del parámetro Q , basado en el número de transmisiones exitosas que se han producido en las distintas ranuras. Si una ranura está vacía, se decrementa el valor de Q_{fp} . Mientras que este valor se incrementa en el caso de ranuras que contengan colisiones. No variando el valor de Q_{fp} en tanto en cuanto todas las ranuras sean exitosas. El tamaño de cada uno de estos incrementos o decrementos depende de una constante C . Y cuyos valores recomendados están entre 0,1 y 0,5, empleando valores bajos cuando Q es grande y valores altos cuando Q es pequeño.

$$K = 2^Q \quad (4.1)$$

Varios son los trabajos que han sido presentados [133]–[136], en los que se proponen algoritmos eficientes para el cálculo del tamaño de cada marco temporal en el que pueden responder las etiquetas y para distintas condiciones en las que se produce la comunicación. En todos ellos se persigue un objetivo común: mejorar la eficiencia y efectividad del proceso de identificación de etiquetas.

Precisamente, dado que la etapa más crítica de todo el proceso de identificación es hasta el instante en que el lector tiene conocimiento de todas las etiquetas presentes en su área de cobertura. Y a pesar de la existencia de mecanismos anticollisión. En ocasiones, algunas etiquetas pueden verse enmascaradas por otras etiquetas con el mismo UID y que reciban o reflejen más nivel de señal que las adyacentes, predominando una señal sobre el resto. Lo cual implica que para el lector existe una única etiqueta con ese identificador, cuando en realidad pueden ser dos o más las etiquetas involucradas en el proceso y que quedarían invisibles para el lector. Resultando que el lector contesta como si únicamente una etiqueta hubiera respondido. Dado que el ACK esperado es el mismo en todos esos casos, todas las etiquetas se consideran identificadas, cuando en realidad el lector únicamente ha reconocido a una de ellas. Por lo que algunas etiquetas y, por consiguiente, algunos ítems quedarían sin identificar. Este fenómeno se conoce como Efecto Captura (*Capture Effect*) y en los últimos años se han realizado varias propuestas para tratar de solucionarlo [137]. Como en [138], donde se propone la utilización de protocolos específicos para resolver el efecto captura. O en [139], donde se presenta un algoritmo de estimación para minimizar el efecto captura en identificaciones masivas.

Una vez superada la etapa de identificación de las etiquetas, teniendo ahora el lector constancia de la existencia de cada una de ellas, la comunicación entre lector y etiqueta continúa dando paso a la transferencia de datos de identificación (EPC), de proveedor, de trazabilidad, etc. En definitiva, datos del banco de memoria interno de cada etiqueta y cuya información es más sensible, desde el punto de vista de la seguridad. Por lo que otros trabajos de investigación se centran en el campo de la seguridad de las comunicaciones, en los cuales se proponen nuevos protocolos de autenticación o modificaciones de los ya existentes. Estos trabajos abarcan desde aspectos más puramente físicos hasta cómo ha de producirse la encriptación de los datos que se transmiten vía aérea. En [140], esta clase de protocolos son clasificados en cuatro clases atendiendo principalmente a su complejidad. La clase más pesada (*weight*), en la que se incluyen los mecanismos criptográficos convencionales, se denomina “full-fledged”. Mientras que los generadores de números aleatorios y las funciones de empaquetado y compresión (*hashing*) de una sola dirección se encuentran en la clase “simple” (simple). La clase “lightweight” (ligera), incorpora protocolos basados en el uso de números aleatorios o funciones simples como las de paridad o sumas de comprobación (*checksums*). Y la clase “ultra-lightweight” (ultraligera), que incluye protocolos que impliquen operaciones simples a nivel de bit.

4.1.4. Mecanismos anticollisión.

Son varios los aspectos o partes de la RFID pasiva que podrían beneficiarse de un análisis detallado y susceptibles de aportar nuevas posibilidades para mejorar el rendimiento general de la tecnología. Una

de estas partes es la correspondiente a los protocolos de comunicación, donde se han realizado nuevas revisiones y desarrollos en los últimos años [6]. Estas propuestas versan sobre el proceso de comunicación entre lectores y etiquetas, donde la mayor parte de las contribuciones están basadas en la mejora de los protocolos de la capa MAC (*Media Access Control*).

Al contrario que sucede en las comunicaciones NFC (Near Field Communications), que utilizan frecuencias más bajas y permiten menores alcances, las que se llevan a cabo en el rango UHF han de contemplar la posible presencia simultánea de multitud de etiquetas en el área del lector. Lo que implica la necesidad de implementar protocolos anticolidión. Específicamente, los problemas de colisiones entre etiquetas son profundamente analizados en todos estos trabajos, dado que se trata de uno de los principales problemas que deben resolverse para garantizar fiabilidad y precisión en su funcionamiento [141]. El principal requisito que se le presupone a este tipo de sistemas es que todas las etiquetas deben ser siempre identificadas adecuadamente por los lectores; y siendo esto independiente de cómo, cuándo y dónde se lleven a cabo las lecturas.

En este punto, cabe volver a remarcar que los lectores nunca tienen conocimiento previo de cuántas etiquetas tienen que leer cuando se lleva a cabo el proceso de identificación. Por lo que resulta necesario emplear protocolos robustos que aseguren que todas las etiquetas presentes en el área de cobertura del lector van a ser leídas y proporcionen a los lectores los mecanismos necesarios para resolver cualquier problema que pueda suceder durante el proceso.

La identificación de cada una de las etiquetas es el paso más crítico de todo el proceso de lectura, dado que es el momento en el que más colisiones pueden suceder. Es por ello por lo que en esta tesis se le ha prestado especial atención. En ese instante, cada etiqueta se identifica al lector mediante el envío de un número aleatorio de 16 bits, denominado *Unique Identifier (UID)*, o *RN16*. Este número UID se emplea para asegurar la comunicación unívoca entre el lector y cada una de las etiquetas. Cuando se produce una identificación exitosa de una etiqueta, el lector envía el mismo UID de vuelta a la etiqueta, como una señal de reconocimiento (*ACK*), confirmando el establecimiento del enlace de comunicación. Una vez que el lector ha reconocido a la etiqueta, el protocolo de comunicación asegura que ninguna otra etiqueta interferirá en el intercambio de información entre el lector y la etiqueta identificada. Sin embargo, en el caso más común de tener varias etiquetas esperando a ser identificadas al mismo tiempo, durante el proceso de identificación pueden ocurrir problemas de colisiones entre los mensajes lanzados por las etiquetas, los cuales son abordados de dos maneras distintas.

Por un lado, se encuentran los protocolos basados en los árboles de búsqueda que son capaces de detectar todas las etiquetas, pero que requieren de mucho tiempo para llevarse a cabo [142]. Mediante el método de árbol binario de búsqueda (*Binary Searching Tree scheme, BST*), las etiquetas envían al lector una secuencia binaria de longitud fija, que es única para cada etiqueta. El lector busca diferencias entre las secuencias recibidas y marca éstas como colisiones si no se ha encontrado ninguna. En este caso, el lector solicita una nueva secuencia a las etiquetas involucradas, que se generará de acuerdo con la colisión detectada. Este proceso se repite hasta que todas las etiquetas son reconocidas [143]. Una alternativa es el método de árbol de consulta, (*Query Tree scheme, QT*), que divide a las etiquetas en subgrupos atendiendo al valor del bit más significativo del número identificativo de cada etiqueta. Es decir, un grupo de etiquetas se divide en dos subgrupos: las etiquetas cuyo bit más significativo es 0 forman un grupo, mientras que las etiquetas con un 1 pertenecen a otro. En cada ronda, se decrementa una posición el bit evaluado. Todos los grupos de etiquetas son divididos de esta forma hasta que todas las etiquetas son identificadas [144]. Y el mecanismo de árbol de rastreo de colisiones (*Collision Tracking Tree scheme, CTT*), es una mejora del método QT que reduce el intercambio de datos total durante su ejecución. En este caso, el lector compara los números de identificación de cada una de las etiquetas y únicamente les solicita nuevos números binarios para posiciones de bit que sean iguales o mayores que

el primer bit en el que se haya detectado una colisión [145]. Para reducir el flujo de datos, las etiquetas únicamente necesitan enviar las posiciones de bit no evaluadas de sus números de identificación. Empleando este mecanismo, también se reduce el tiempo necesario para la identificación de todas las etiquetas presentes [146]. Además, los métodos QT y CTT se pueden combinar para mejorar aún más la eficiencia del proceso [147], [148].

Por otro lado, se encuentran las soluciones probabilísticas que están basadas en variaciones sobre el protocolo de comunicación ALOHA. De hecho, en la especificación EPC Gen2 se recoge el uso del protocolo DFSA (*Dynamic Frame Slotted Aloha*), como mecanismo anticolisión. Siendo éste el más complejo de todas las variantes de ALOHA y cuyo funcionamiento se describe a continuación: el tiempo es dividido en ranuras (*slots*) en las cuales pueden transmitir las etiquetas y las ranuras se agrupan en marcos o ventanas temporales (*frames*); el lector envía tantos *frames* como necesite para la correcta identificación de todas las etiquetas; y en cada *frame*, son las etiquetas las que deciden, mediante un número aleatorio, en qué *slot* van a transmitir su número de identificación (UID). Además, en el protocolo DFSA, el número de ranuras por *frame* es variable en el tiempo (dinámico), ajustándose el tamaño de cada *frame* a las etiquetas pendientes de identificaren cada momento, realizándose el cálculo mediante un algoritmo y el parámetro Q (ver apartado 4.1.3). De forma que se maximiza la eficiencia del protocolo. Para lograr su rendimiento máximo, se necesita determinar el número de etiquetas presentes en el área de lectura para fijar el tamaño óptimo del *frame*. Aunque lo habitual, en prácticamente todos los casos, es que la cantidad de etiquetas presentes no se pueda conocer a priori [149]–[151].

Todos estos mecanismos para evitar o reducir los problemas de colisiones durante los procesos de identificación tienen un punto en común: el uso de un identificador de etiqueta (UID) para la comunicación. Basando su funcionamiento en este número de identificación único para cada etiqueta. En este sentido, para que estos mecanismos anticolisión trabajen adecuadamente (a nivel de capa MAC del protocolo de comunicación), todas las etiquetas deben tener un número de identificación independiente y único. En cualquier caso, si el número asociado a cada etiqueta fuese único y completamente diferente al de otras etiquetas, la eficiencia de estos mecanismos anticolisión mejoraría notablemente. Principalmente gracias a que los protocolos de identificación necesitarían menos iteraciones para alcanzar su objetivo.

Pero la generación del mencionado número único no es una tarea sencilla. De hecho, es por ello por lo que la especificación EPC Gen2 establece que las etiquetas deben implementar un generador de números pseudoaleatorios (PRNG), que se encargue de generar ese identificador único necesario para el proceso de comunicación e identificación con el lector. Por tanto, puede decirse que el éxito de las comunicaciones y del proceso de lectura, en general, viene fuertemente condicionado por la calidad del generador de números pseudoaleatorios implementado en las etiquetas. En cuyo caso contrario, los identificadores para cada etiqueta no presentarían las suficientes características de aleatoriedad provocando el fallo de los protocolos de comunicación debido a problemas en las comunicaciones como colisiones y/o interferencias.

Los algoritmos que se utilizan actualmente están adecuadamente diseñados y la probabilidad de que se produzcan errores en las lecturas es muy baja, al menos en teoría. Pero en la práctica, aparecen diversos problemas relacionados con el funcionamiento de estos mecanismos, especialmente los involucrados en la capa física y de naturaleza estocástica, pareciendo que ocurren más frecuentemente de lo deseable. Además, en escenarios de uso reales, los defectos e interferencias de la señal radioeléctrica o la posición relativa de los dispositivos RFID afecta al funcionamiento de algoritmos y protocolos. Provocando que los resultados teóricos difieran significativamente de los resultados empíricos [152].

4.2. Generación de números pseudoaleatorios en las comunicaciones RFID.

El método más fiable para la generación de números aleatorios consiste en la utilización de algoritmos deterministas con una base matemática sólida. Los cuales proporcionan secuencias de números que se asemejan fuertemente a series aleatorias, a pesar de que en realidad no lo son.

Se han venido proponiendo diversos métodos desde la década de 1940, cuando los matemáticos John von Neumann y Nicholas Metropolis presentaron el método del cuadrado medio (*Middle-Square Method*), que se basa en elevar al cuadrado un determinado valor. Hoy en día el mecanismo más extendido para la generación de números pseudoaleatorios consiste en la utilización de algoritmos de coherencia lineal. Su funcionamiento comienza con un valor inicial (denominado semilla), a partir del cual se va generando recursivamente la secuencia de números pseudoaleatorios de acuerdo con una determinada fórmula. Estos algoritmos pueden además combinarse entre sí para obtener mejores resultados. Este tipo de algoritmos es el método más empleado en implementaciones reales dado que, en la mayoría de los casos y con una configuración adecuada, pueden proporcionar resultados de una calidad comparable a la de los que se pueden obtener mediante otras alternativas más complejas.

El uso de generadores de números pseudoaleatorios (Pseudorandom Number Generators, PRNGs) en RFID se remonta a los inicios de esta tecnología. Y la implementación de PRNGs en etiquetas RFID se vio ratificada por los estándares EPCglobal e ISO. De acuerdo con estas especificaciones [16], [17], los generadores de números pseudoaleatorios deben satisfacer características de aleatoriedad especificadas mediante valores dados de: baja probabilidad de obtener cualquier número en particular, baja probabilidad de obtener secuencias idénticas, y baja probabilidad de poder predecir cualquier número generado.

Además, para poder realizar adecuadamente las operaciones descritas en el apartado 4.1.3 y de acuerdo a la especificación EPC Gen2, las etiquetas pasivas deben implementar un generador de números aleatorios o pseudoaleatorios, dado que es necesario para diversas operaciones (tal y como se ha mencionado anteriormente). Por ejemplo, para generar el número que deben cargar en el *slot-counter*, o para generar la respuesta *RN16* con la que la etiqueta debe responder al lector. Únicamente en estos primeros pasos del proceso de comunicación entre lector y etiqueta, el generador de números aleatorios o pseudoaleatorios es empleado varias veces. Posteriormente, también es usado en operaciones y algoritmos más complejos. Por lo que el generador de números aleatorios o pseudoaleatorios, que debe estar implementado en todas las etiquetas pasivas, es una parte crucial de su lógica interna e incide directamente en el adecuado funcionamiento de las comunicaciones entre lector y etiqueta

Por otro lado, es necesario tener en cuenta las limitaciones del hardware disponible en las etiquetas pasivas a la hora de implementar cualquier algoritmo complejo. Los circuitos integrados utilizados en etiquetas RFID de bajo coste tienen un número limitado de puertas lógicas (aproximadamente entre 5000 y 10000) y únicamente una parte de ellas pueden ser utilizadas para implementar el generador de números pseudoaleatorios [153]. Además, existen fuertes limitaciones en el tiempo disponible por la etiqueta para realizar estas operaciones, descritas en [16]. Algunos ejemplos de ello es el tiempo disponible para realizar la primera respuesta al lector, o el tiempo de respuesta establecido para cada comando del protocolo.

Evidentemente, la implementación de un determinado generador de números pseudoaleatorios u otro en las etiquetas, puede afectar de forma muy directa y significativa al coste de las mismas. La mayoría

de estas soluciones requieren de una gran capacidad de cálculo, para lo que resulta necesario emplear un hardware más complejo. Hasta la fecha se han propuesto diferentes métodos para generar secuencias de números pseudoaleatorios en aplicaciones RFID, en un intento de reducir los requisitos del hardware empleado y, por tanto, el precio de las etiquetas [154]. Pero esta reducción en la complejidad puede acarrear algunos efectos colaterales e incluso reducir algunas otras características de las etiquetas. Por ejemplo, una simplificación en la lógica de las etiquetas pasivas puede repercutir en que dejen de cumplirse algunos requisitos de seguridad. En realidad, la implementación de un PRNG robusto y seguro supone todo un reto en el caso de las etiquetas RFID de bajo costo [155]. Y dependiendo de la aplicación, ciertas simplificaciones pueden considerarse como una ventaja o una desventaja.

El uso de PRNGs es crucial para los procesos básicos de comunicación en RFID, tal y como se ha descrito en la sección 4.1.3. Pero también pueden ser empleados en protocolos de comunicación avanzados, como el presentado en [156], donde un PRNG es empleado para comunicación paralela en escenarios con múltiples lectores y múltiples grupos de etiquetas. Sin embargo, es en el campo de la seguridad y la autenticación donde los PRNGs son más empleados, dado que un PRNG es una de las partes fundamentales en procesos como el cifrado de información en las etiquetas [157].

El nivel de complejidad requerido a un PRNG puede apreciarse en el trabajo presentado en [158], donde se propone un nuevo generador de números pseudoaleatorios, denominado LAMED, que cumple con todas las especificaciones para las etiquetas RFID del tipo *EPC Class-1 Generation-2*. O en [159], donde se propone un PRNG más complejo y robusto para dispositivos inteligentes. En [160], se emplea un PRNG en combinación con una función CRC “en chip” para asegurar el anonimato y la autenticidad de las comunicaciones entre lector y etiqueta. Un PRNG también es empleado en [161], para garantizar el secreto en las comunicaciones RFID, previniendo de posibles ataques en las respuestas. Incluso cuando se desarrollan y emplean algoritmos livianos (como en la aplicación de IoT propuesta en [162]), donde el generador de números pseudoaleatorios juega un papel crítico y fundamental para su adecuado funcionamiento.

4.3. Algoritmo ultraligero para la generación de números pseudoaleatorios en etiquetas pasivas.

En este apartado se describe la propuesta de un nuevo y liviano algoritmo capaz de sustituir al generador de números pseudoaleatorios (PRNG) que debe implementarse actualmente en los chips de las etiquetas RFID pasivas³. Con el objeto de optimizar el uso de los recursos disponibles en este tipo de etiquetas, la propuesta consiste en el uso de un algoritmo ultraligero, basado en la utilización del EPC como punto de partida (semilla) del proceso de generación. De tal forma que el resultado obtenido satisface los requisitos establecidos en la especificación EPC Gen2 [16], que es la más extendida e implantada en la actualidad para todo lo relativo al funcionamiento de etiquetas RFID pasivas.

4.3.1. Funcionamiento del algoritmo.

Todas las etiquetas pasivas de RFID necesitan disponer de un generador de números pseudoaleatorios para cumplir con los protocolos de comunicación y pueda llevarse a cabo adecuadamente el

³ Resultados publicados en *Future Generation Computer Systems*, Vol. 99, pp 115-123, octubre de 2019. Edit: Elsevier. JCR: 5,768-T1 (Computer Science, Theory & Methods 8/104).

intercambio de mensajes entre lector y etiquetas. Por ejemplo, para obtener números de identificación únicos (UID) en cada etiqueta, indispensables para el establecimiento del canal de comunicación con el lector.

En este sentido, cabe recordar que el EPC (*Electronic Product Code*) es un conjunto de dígitos binarios (Figura 4.7), que representa la codificación unívoca del identificador único para cada objeto individual a nivel mundial y de acuerdo con el estándar EPCIS (*EPC Information System*) [14]. Todo el proceso de codificación se encuentra definido en el estándar EPC para los datos contenidos por las etiquetas (*EPC tag data Standard*) [163].

Por tanto, esta nueva propuesta se basa en sacar el máximo partido al EPC (parámetro único que ya se encuentra en el interior de cada etiqueta), empleándolo en el proceso de generación de números pseudoaleatorios. Y destacando que el EPC es un identificador único en el mundo y no un número o variable utilizada únicamente para determinadas operaciones a nivel local.

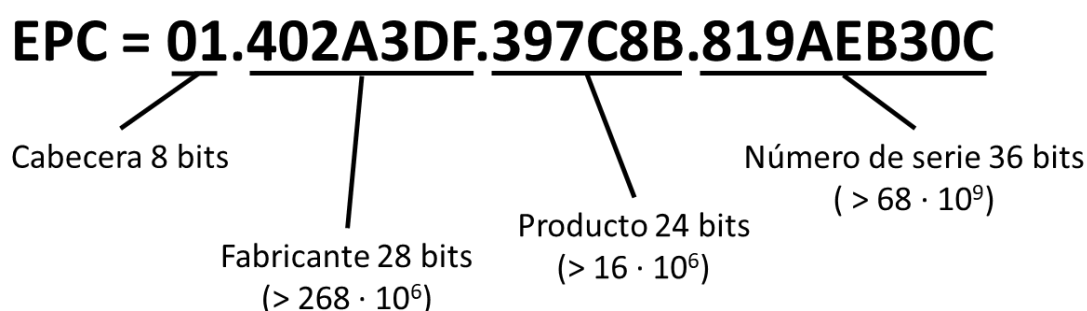


Figura 4.7. Ejemplo de EPC de 96 bits.

El núcleo del algoritmo propuesto⁴ lo constituye el uso de un registro de desplazamiento con realimentación lineal (LFSR: Linear Feedback Shift Register), inicializado por el valor del parámetro Q , enviado por el lector (según se comenta en la sección 4.1.3). Físicamente, el LFSR se implementa como una relación de grupos de puertas lógicas (Figura 4.8). Y dicha relación viene descrita por un polinomio primitivo, que debe ser elegido por los fabricantes de las etiquetas. El grado de este polinomio determina la longitud en bits del registro y, por tanto, del número pseudoaleatorio que se generará.

Para su funcionamiento, se hace pasar el EPC por el LFSR, bit a bit, introduciendo en primer lugar el bit más significativo. Tras haber introducido todo el EPC y al finalizar todos los sucesivos ciclos de desplazamiento, el contenido del LFSR será el primer número pseudoaleatorio generado de 16 bits (en principio, se establece esta longitud por necesidades del protocolo de comunicación). A partir de este resultado, el algoritmo puede extraer también las subsecuencias de N bits necesarias para cargar el *slot counter* de la etiqueta (que se encarga de seleccionar el instante temporal en el que lanzar la respuesta al lector). Para ello, una solución puede consistir simplemente en truncar el número generado de 16 bits a la longitud deseada. U otra solución, dado que se trata de un algoritmo liviano, puede ser la implementación de varios LFSR en una misma etiqueta, con distintos polinomios primitivos de acuerdo con las longitudes de números pseudoaleatorios necesarias para cada operación. Además, el contenido del LFSR se actualiza antes de cada generación con la información recibida del lector (mediante el parámetro Q del protocolo), lo que garantiza la adecuada generación de números pseudoaleatorios por parte de la etiqueta.

⁴ Propuestas iniciales publicadas en el *Congreso Internacional Smart SysTech 2016*, celebrado en Duisburg (Alemania).

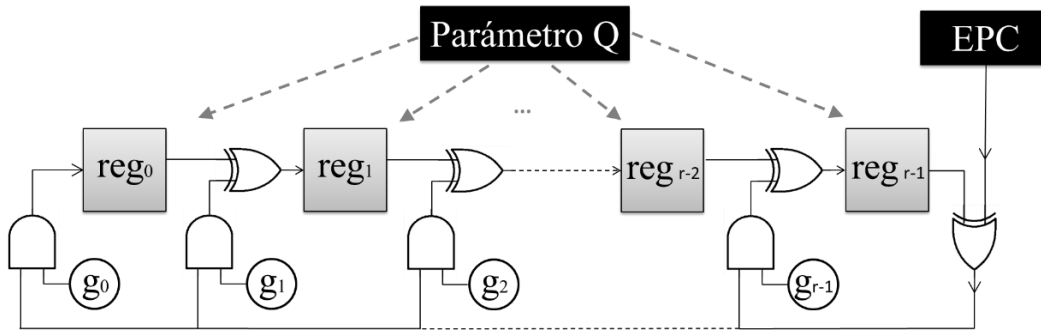


Figura 4.8. Esquema del algoritmo propuesto.

Gracias a este procedimiento, se asegura que el algoritmo propuesto es capaz de construir dos números pseudoaleatorios mientras se establece el canal de comunicación entre lector y etiqueta. El número pseudoaleatorio de 16 bits es utilizado como UID (respuesta de la etiqueta) y el otro (más corto) para la selección de la ranura temporal en la que contestará al lector.

Por otro lado, tal y como se contempla en la especificación *EPC Gen2*, el mecanismo de generación de números pseudoaleatorios debe ser capaz de generar y almacenar, al menos, dos números pseudoaleatorios diferentes mientras la etiqueta se encuentre activada y con energía (es decir, dentro del área de cobertura del lector y recibiendo su portadora). Para ello, se combina el resultado inicial obtenido en el LFSR con el código *StoredCRC*, una secuencia binaria que debe encontrarse en el banco de memoria de cada etiqueta, mediante una operación simple a nivel de bits: como el desplazamiento o la suma binaria. De tal forma que se obtiene un segundo valor pseudoaleatorio.

Por ejemplo, para generar el número pseudoaleatorio único que la etiqueta necesita para mandar como respuesta al lector (denominado UID o RN16, sección 4.1.3), en el LFSR debe emplearse un polinomio primitivo de grado 17. Ya que se necesita un número pseudoaleatorio de 16 bits y el resultado del LFSR tiene una longitud de $r-1$ bits, donde r es el exponente del término de mayor grado del polinomio. Mientras que para el caso del número pseudoaleatorio que debe emplearse para cargar el valor inicial del *slot counter* de la etiqueta, se precisa un polinomio primitivo de grado $N+1$, donde N es el valor del parámetro Q , cuyo valor es desconocido previamente y enviado por el lector (ligado al número de ranuras disponibles dentro de la ventana temporal para las respuestas de etiquetas establecida por el lector). Y que se corresponde con la longitud en bits del número pseudoaleatorio deseado en este caso.

Habitualmente los EPC se componen de 96 bits, los cuales se hacen circular por el LFSR según el algoritmo propuesto. Pero en ciertas aplicaciones logísticas, sucede que los bits más significativos del código (izquierda) contienen información que suele ser común a los conjuntos de etiquetas a identificar, por referirse al fabricante y tipo de producto; mientras que los bits menos significativos (situados a la derecha), se refieren al número de lote y de producto, por lo que suelen concentrar una mayor variación (Figura 4.7). Por lo que, con objeto de ahorrar tiempo y energía en el proceso de generación, se podría contemplar la posibilidad de truncar el EPC para quedarse únicamente con la parte de los bits menos significativos y que mayores variaciones presentan. Haciendo circular, por ejemplo, 36 bits en lugar de los 96 inicialmente propuestos. Sin embargo, para las pruebas realizadas, y puesto que se cumple con los tiempos de lectura establecido por la especificación, no se ha estimado necesario recurrir a esta posibilidad.

4.3.2. Adecuación a la especificación de EPC.

Tal y como se recoge en la especificación *EPC Gen2*, los generadores de números pseudoaleatorios que se implementen en las etiquetas deben satisfacer las siguientes restricciones de aleatoriedad:

- **Probabilidad de obtener un determinado número pseudoaleatorio:** la probabilidad de que el número generado tenga un determinado valor $RN16=j$, para cualquier valor de j , debe encontrarse en el siguiente rango:

$$0.8/2^{16} < P(RN16=j) < 1.25/2^{16} \quad (4.2)$$

En este caso, el algoritmo propuesto genera un $RN16$ que depende directamente del EPC que incluya cada etiqueta y que es desconocido antes de ser leído, por lo que:

$$P(RN16=j) = 1/2^{16} \quad (4.3)$$

- **Probabilidad de obtención de secuencias idénticas de forma simultánea:** la probabilidad de que dos o más etiquetas generen la misma secuencia de números pseudoaleatorios al mismo tiempo y durante el mismo proceso de lectura debe ser inferior a 0,1%. El resultado del algoritmo propuesto es un número de 16 bits, por tanto:

$$P(RN16=j) = 1/2^{16} = 1,53 \cdot 10^{-5} < 0,1\% \quad (4.4)$$

Y dicho resultado depende directamente del EPC de cada etiqueta, que es único a nivel mundial (por definición). Para los trabajos realizados se ha utilizado un EPC de 96 bits de longitud, por lo que la probabilidad de cada código es:

$$P(RN16=j) = 1/2^{96} = 1,26 \cdot 10^{-29} < 0,1\% \quad (4.5)$$

Además, el resultado puede ser distinto de acuerdo con el polinomio primitivo seleccionado para cada implementación del LFSR. Incluso considerando que únicamente hay disponible un polinomio primitivo, es decir, una única implementación del algoritmo para todos los EPC del mundo, la probabilidad de que se produzcan secuencias idénticas simultáneamente es:

$$P(RN16=j) = 2^{16}/2^{96} = 8,27 \cdot 10^{-25} < 0,1\% \quad (4.6)$$

- **Probabilidad de predicción de un número pseudoaleatorio:** conocidos los resultados obtenidos en los procesos de generación anteriores, la probabilidad de predecir un nuevo número pseudoaleatorio (en idénticas condiciones), al menos 10 ms después del anterior episodio de lectura (última vez que la etiqueta tuvo energía), no debe ser superior a 0,025%.

El método propuesto satisface esta condición porque el nuevo número pseudoaleatorio que se genera en la etiqueta depende de: el contenido del LFSR, que ha sido construido mediante un polinomio primitivo, el contenido del código *StoredCRC* y del resultado de la operación simple a nivel de bits. En todos los casos, estos valores son desconocidos antes de cualquier operación de lectura. Asimismo, la propuesta está abierta a que diferentes fabricantes utilicen diversos registros LFSR, con sus correspondientes polinomios primitivos, y distintas operaciones a nivel de bits para la implementación del algoritmo propuesto.

Adicionalmente, la probabilidad de predecir un número pseudoaleatorio generado por el método propuesto disminuye fuertemente dado que el contenido del LFSR se modifica antes de cada generación de acuerdo con valor del parámetro Q , enviado por el lector en cada proceso de lectura. Tal y como se ha descrito en la sección 4.1.3, se trata de un valor previamente desconocido por la etiqueta ya que el lector se lo envía en cada ronda de inventariado,

modificándose de forma dinámica durante todo el proceso de lectura para adaptarse al número de etiquetas que quedan por identificar dentro del área de cobertura del lector. Para lo que el lector va ajustando dicho valor en función de las ranuras vacías y de las colisiones detectadas en cada ronda.

4.3.3. Validación de la propuesta.

Teniendo en mente la importancia de los generadores de números pseudoaleatorios durante el transcurso del proceso de identificación de etiquetas, así como la relevancia de emplear uno u otro método para su obtención. Se ha realizado un estudio sobre la generación de números pseudoaleatorios en etiquetas reales. Con el objeto de obtener una fotografía de la situación y funcionamiento real de los generadores de números pseudoaleatorios en etiquetas comerciales, o al menos en una muestra de ellas, para encuadrar y poder evaluar el algoritmo propuesto de manera más objetiva⁵.

Para poder llevar a cabo el estudio, se han medido y analizando las características de aleatoriedad de secuencias reales de números pseudoaleatorios (RN16) generados por etiquetas comerciales. Además, se ha realizado el mismo estudio a una secuencia de números pseudoaleatorios obtenidos con el algoritmo propuesto, lo que permitirá su validación mediante la comparación directa de los resultados de la propuesta con los números pseudoaleatorios obtenidos de etiquetas comerciales reales.

Para la obtención de las secuencias de números pseudoaleatorios de las etiquetas comerciales (Figura 4.9), se ha empleado el sistema de adquisición de datos *Tagformance*®, de *Voyantic*®, que actúa como lector. En este extremo, cabe destacar que, para conseguir las secuencias numéricas analizadas en el estudio, las muestras se han obtenido una a una. Es decir, ha sido necesario realizar una medida para conseguir cada uno de los números pseudoaleatorios.



Figura 4.9. Una de las etiquetas evaluadas en el estudio.

Para la realización cada medida, el sistema envía un comando *Query*, tal cual se haría en un proceso de lectura de etiquetas común, capturando la respuesta recibida de la etiqueta. Posteriormente, se obtiene el valor del número pseudoaleatorio (RN16) generado por la etiqueta en cada respuesta y para cada etiqueta incluida en el estudio. El proceso se ha repetido hasta que todas las muestras han sido recogidas.

En este análisis simplificado únicamente se ha medido una etiqueta al mismo tiempo, para evitar problemas de comunicaciones y tener perfectamente identificada la etiqueta que proporcionaba el número pseudoaleatorio en cada medida. Para la realización de las medidas, las etiquetas evaluadas se han colocado frente a una antena UHF de tipo parche a 1 m de distancia y a 1,5 m sobre el suelo, bajo condiciones de espacio libre para las comunicaciones entre lector (equipo de medida) y etiqueta, ambos sintonizados a 868 MHz (Figura 4.10). Para este estudio, se han obtenido seis secuencias independientes de números pseudoaleatorios (RN16) de seis etiquetas distintas, donde cada una de las secuencias contiene 369 números diferentes [164].

⁵ Parte de los resultados han sido publicados en las *VI Jornadas Doctorales UCLM 2016*, celebradas en Toledo (España).

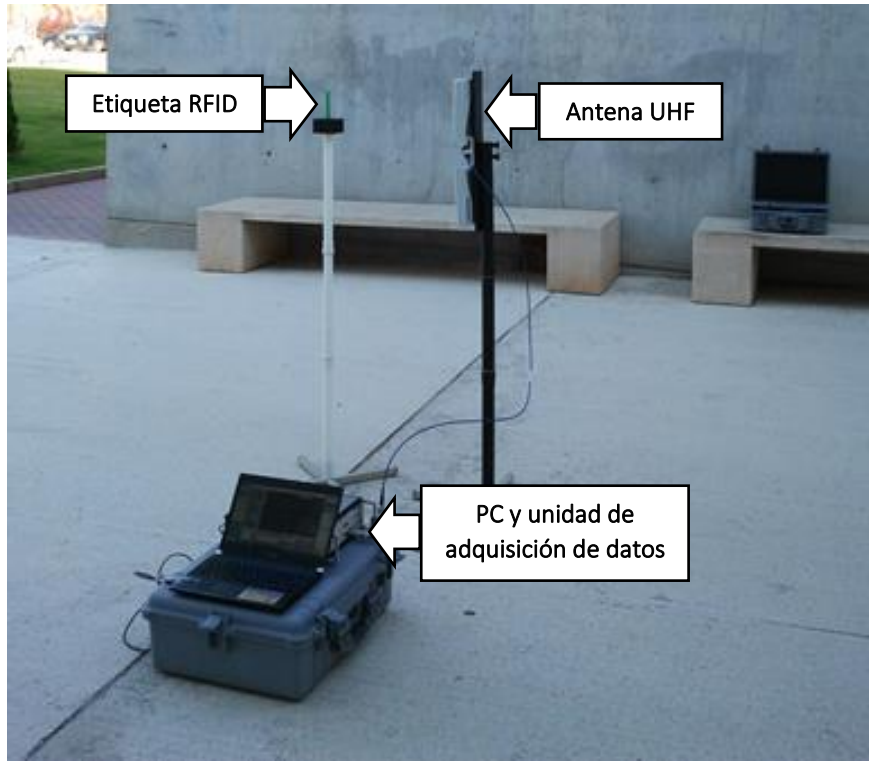


Figura 4.10. Disposición del equipamiento durante las medidas con etiquetas comerciales.

El análisis se divide en varios test de aleatoriedad, que se encuentran incluidos en la *NIST Statistical Test Suite* [165]–[168], para la evaluación de la aleatoriedad de las secuencias obtenidas, a partir de los números pseudoaleatorios medidos y con el algoritmo propuesto. Se ha aplicado un intervalo de confianza del 95% en todos los test realizados:

- Test de χ^2 : es la prueba más común para buscar uniformidad en series numéricas y especialmente diseñada para distribuciones discretas. A partir de los histogramas de las secuencias, las frecuencias observadas se comparan con las frecuencias de una distribución uniforme teórica (frecuencias esperadas). Teniendo en cuenta que el histograma tiene k rangos o intervalos y O_i e E_i son las frecuencias observadas y esperadas, respectivamente, el resultado estadístico χ^2 se define como:

$$\chi^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i} \quad (4.7)$$

- Test de series: se encarga de medir la correlación entre elementos adyacentes. En este caso, entre los números pseudoaleatorios generados por cada etiqueta y el algoritmo propuesto. Para esta prueba, cada uno de ellos es emparejado y clasificado, obteniendo un mapa de coordenadas que se divide en n^2 porciones, tomando n de acuerdo con el tamaño de la muestra (N). Siendo f_o la frecuencia esperada para cada porción del mapa y conocidas las frecuencias observadas y esperadas para cada porción del mapa, el resultado estadístico se obtiene como sigue:

$$X_0 = \frac{n^2}{N-1} \sum_{i=1}^n \sum_{j=1}^n \left(f_{o_{ij}} - \frac{N-1}{n^2} \right)^2 \quad (4.8)$$

- Test de huecos: se emplea para evaluar la recurrencia de cada número pseudoaleatorio en un cierto rango. Para ello, se cuentan el número de muestras que existen entre repeticiones de un

determinado número pseudoaleatorio y se aplica entonces el test de frecuencias (χ^2) para comparar con la longitud de huecos esperada.

- Tests de rachas: este tipo de pruebas son utilizadas para examinar la disposición o situación de los números en una secuencia, buscando subsecuencias repetidas dentro del grupo completo de números pseudoaleatorios de cada secuencia, para probar su independencia. Se llevan a cabo tres tipos de test distintos:
 - Test de rachas ascendentes y descendentes: siendo N el número total de rachas (crecientes y decrecientes), su media (μ_{ud}) y su varianza (σ_{ud}^2) vienen determinadas por:

$$\mu_{ud} = \frac{2N - 1}{3} \quad (4.9)$$

$$\sigma_{ud}^2 = \frac{16N - 29}{90} \quad (4.10)$$

Para un valor elevado de N , la distribución de las rachas (r) puede ser aproximada a una distribución normal tal y como se indica:

$$Z_0 = \frac{r - \mu_{ud}}{\sigma_{ud}} = \frac{r - [(2N - 1)/3]}{\sqrt{(16N - 29)/90}} \quad (4.11)$$

- Test de rachas por encima y por debajo de la media: este test se emplea para comprobar el comportamiento de las rachas por encima y por debajo de la media. Se trata de una prueba complementaria al test anterior y que asegura la aleatoriedad de la secuencia. Siendo n_a y n_b el número de rachas por encima (*above*) y por debajo (*below*), respectivamente y N el número total de rachas, su media (μ_{ab}) y su varianza (σ_{ab}^2), pueden expresarse como:

$$\mu_{ab} = \frac{2n_a n_b}{N} + \frac{1}{2} \quad (4.12)$$

$$\sigma_{ab}^2 = \frac{2n_a n_b (2n_a n_b - N)}{N^2 (N - 1)} \quad (4.13)$$

Para un valor elevado de N , la distribución de las rachas (r) puede ser aproximada a una distribución normal, en este caso:

$$Z_0 = \frac{r - \mu_{ab}}{\sigma_{ab}} = \frac{r - \left(\frac{2n_a n_b}{N}\right) - \frac{1}{2}}{\sqrt{\frac{2n_a n_b (2n_a n_b - N)}{N^2 (N - 1)}}} \quad (4.14)$$

- Test de longitud de las rachas: se trata de un test añadido a las dos pruebas anteriores y resulta necesario para evaluar la aleatoriedad de la longitud de las rachas y validar los resultados. El correspondiente test de frecuencias (test χ^2) viene determinado por:

$$\chi^2 = \sum_{i=1}^k \frac{[O_i - E(Y_i)]^2}{E(Y_i)} \quad (4.15)$$

Donde O_i es el número observado de rachas con longitud i . Y $E(Y_i)$, el valor esperado de la racha; que en caso de rachas ascendentes y descendentes y si $i \leq N - 2$, se define como:

$$E(Y_i) = \frac{2}{(i+3)} [N(i^2 + 3i + 1) - (i^3 + 3i^2 - i - 4)] \quad (4.16)$$

Y si $i = N - 1$:

$$E(Y_i) = \frac{2}{N!} \quad (4.17)$$

Y para rachas por encima y por debajo de la media, con una secuencia grande números pseudoaleatorios (N), se convierte en:

$$E(Y_i) = \frac{N\omega_i}{E(I)} \quad (4.18)$$

Donde:

$$\omega_i = \left(\frac{n_a}{N}\right)^i \left(\frac{n_b}{N}\right) + \left(\frac{n_a}{N}\right) \left(\frac{n_b}{N}\right)^i \quad (4.19)$$

$$E(I) = \frac{n_a}{n_b} + \frac{n_b}{n_a} \quad (4.20)$$

Los resultados de cada una de las pruebas anteriormente descritas se muestran en la Tabla 4.1. Donde en cada columna se detallan los valores de los resultados estadísticos de las pruebas realizadas para cada etiqueta medida⁶. Y el intervalo de valores para el que cada prueba es satisfactoria, se muestra en la última columna (más a la derecha). Estos rangos de valores son los mismos para todas las etiquetas dado que todas las secuencias de números pseudoaleatorios medidas y analizadas presentan el mismo tamaño.

Tabla 4.1. Resultados de las pruebas realizadas para las secuencias medidas.

TEST	RESULTADOS ESTADÍSTICOS						Intervalo de validación
	Etiqueta A	Etiqueta B	Etiqueta C	Etiqueta D	Etiqueta E	Etiqueta F	
χ^2	59.3062	85.0244	65.2412	77.1111	77.1455	80.6721	[57.1129, 87.743]
Series	76.1739	60.8696	88.6957*	59.4783	66.087	50.7826	[49.1105, 77.7454]
Huecos	3.6503	7.4033	2.451	4.5402	9.5646*	2.6942	[1.6103, 9.2364]
Rachas crecientes y decrecientes (χ^2)	3.0988	0.4912*	4.8163	7.2686*	5.2826	1.5757	[0.58437, 6.2514]
Longitud de las rachas	1,1552	0.041257	-0.94891	-1.1964	0.78388	-0.94891	[-1.96, 1.96]
Rachas sobre y bajo la media (χ^2)	9.4331*	2.8638	4.0394	4.1415	3.6268	4.7618	[1.6103, 9.2364]
Longitud de las rachas	0.74169	0.62686	1.2693	-1.449	0.77227	-0.60242	[-1.96, 1.96]

* fuera de rango.

⁶ Resultados publicados en las V Jornadas Doctorales UCLM 2015, celebradas en Ciudad Real (España).

En líneas generales, la mayoría de las secuencias de números pseudoaleatorios analizadas pasan la batería de pruebas realizadas. Por lo que se puede decir que dichas secuencias presentan buenas características de aleatoriedad, aunque los resultados no son excelentes. El test χ^2 es superado por todas las secuencias, mientras que los peores resultados son obtenidos del test de rachas crecientes y decrecientes. Los test de series, huecos y rachas por encima y por debajo de la media arrojan un caso fallido en cada uno de ellos. Sin embargo, la prueba de longitud de las rachas se cumple en todos los casos. Teniendo en cuenta los resultados para cada una de las secuencias, únicamente la secuencia medida en una etiqueta (etiqueta F) pasa satisfactoriamente todas las pruebas. En el resto de los casos, el resultado de una prueba estadística se encuentra fuera de rango para cada etiqueta. Aunque esto podría suponer un mal indicador para los generadores de números pseudoaleatorios que poseen las etiquetas bajo estudio, lo cierto es que las pruebas no son superadas por un escaso margen. Dichos valores se encuentran muy cerca de los límites de validación inferiores y superiores para cada test.

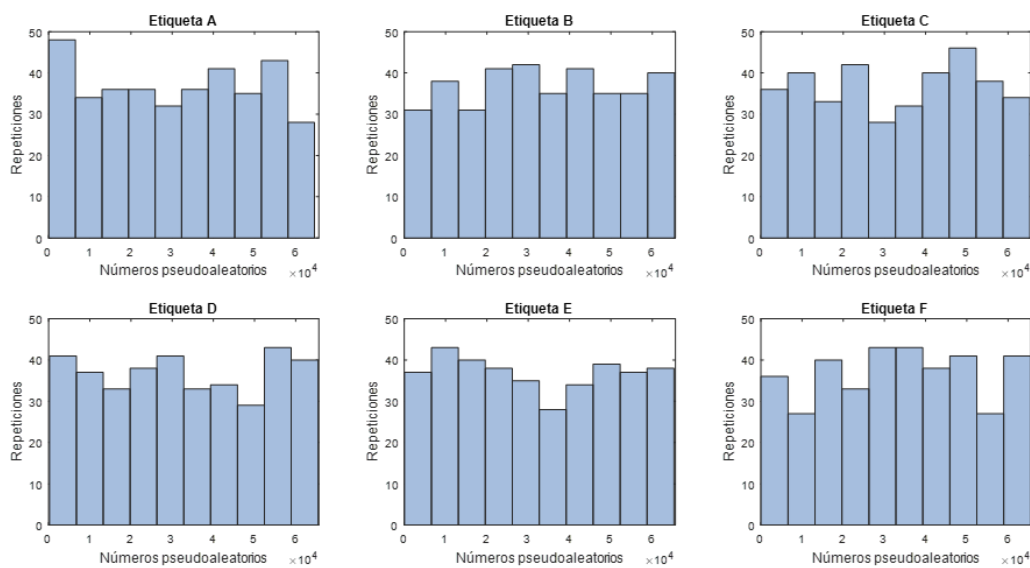


Figura 4.11. Histograma de las secuencias medidas en las etiquetas comerciales.

Por otro lado, se ha analizado de igual forma una secuencia de números pseudoaleatorios obtenida con el método propuesto. Los resultados se detallan en la Tabla 4.2, donde puede observarse como los resultados se encuentran dentro de los intervalos de validación para todas las pruebas realizadas. Lo que evidencia las buenas características de aleatoriedad de la secuencia de números generada a partir del algoritmo ultraligero propuesto.

Tabla 4.2. Resultados de las pruebas realizadas para el algoritmo propuesto.

TEST	RESULTADOS ESTADÍSTICOS	
	Algoritmo Propuesto	Intervalo de validación
χ^2	431.6	[363.2528, 435.6036]
Series	352.8274	[326.069, 394.7874]
Huecos	8.9288	[4.1682, 14.6837]
Rachas crecientes y decrecientes (χ^2)	1.0389	[0.58437, 6.2514]
Longitud de las rachas	0.21223	[-1.96, 1.96]
Rachas sobre y bajo la media (χ^2)	8.7413	[2.8331, 12.017]
Longitud de las rachas	-0.55558	[-1.96, 1.96]

Por último, para llevar a cabo una mejor evaluación de los resultados descritos y para compararlos con otras alternativas, se ha analizado también una secuencia de 10000 números obtenidos con el generador pseudoaleatorio LAMED, dado que se trata de un método científicamente verificado como un buen generador pseudoaleatorio [158]. Los resultados de estas pruebas estadísticas se recogen en la Tabla 4.3, donde queda de manifiesto que la secuencia de números generada con LAMED pasa satisfactoriamente la mayoría de las pruebas. Aunque, incluso en este caso, se falla en el test de rachas crecientes y decrecientes.

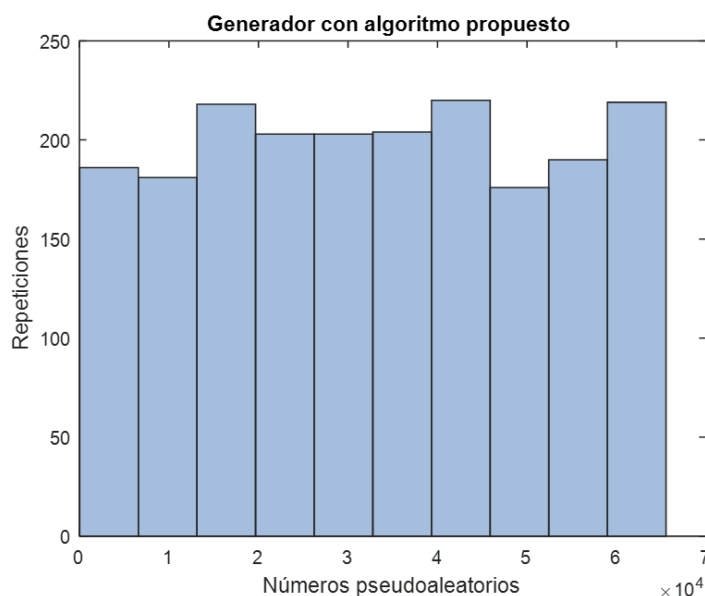


Figura 4.12. Histograma de la secuencia generada con el algoritmo propuesto.

Gráficamente, se puede observar como el histograma de la secuencia generada con LAMED (Figura 4.13) es más plano que el histograma de la secuencia obtenida con el método propuesto (Figura 4.12) y que los correspondientes a las secuencias medidas de las etiquetas comerciales (Figura 4.11). Destacando, que estas últimas presentan más irregularidades en la distribución de los valores obtenidos. Por lo que puede considerarse que las secuencias de números medidas son menos aleatorias que las obtenidas con el método propuesto o con el generador pseudoaleatorio LAMED. Ambos métodos ofrecen una distribución más uniforme en los números generados que los valores medidos en las etiquetas comerciales.

Tabla 4.3. Resultados de las pruebas realizadas para el generador LAMED.

TEST	RESULTADOS ESTADÍSTICOS	
	LAMED	Intervalo de validación
χ^2	1930.8	[1918.4081, 2080.4483]
Series	1947.121	[1855.716, 2015.1404]
Huecos	5.1425	[4.8652, 15.98.72]
Rachas crecientes y decrecientes (χ^2)	9.7607*	[1.0636, 7.7794]
Longitud de las rachas	-0.93296	[-1.96, 1.96]
Rachas sobre y bajo la media (χ^2)	7.5084	[0.20198, 14.6837]
Longitud de las rachas	0.20198	[-1.96, 1.96]

* fuera de rango.

Tras la realización del estudio, se puede decir que la mayoría de las secuencias de números pseudoaleatorios analizadas pasan satisfactoriamente las pruebas de aleatoriedad realizadas. Por lo que se puede concluir que los resultados de las secuencias analizadas muestran una fuerte evidencia del comportamiento aleatorio aceptable que ofrecen los generadores de números pseudoaleatorios empleados en etiquetas RFID comerciales. En este sentido, las secuencias analizadas presentan una distribución aproximadamente uniforme para todo el rango de generación, siempre y cuando las secuencias sean adecuadamente generadas. Además, el hecho de que los resultados estadísticos se encuentren cerca de los límites de validación para las diferentes pruebas puede indicar que los generadores pseudoaleatorios que poseen las etiquetas analizadas tienen suficiente calidad para ser empleados únicamente en funciones comunes de identificación. Sin embargo, resultan poco apropiados cuando se necesitan mayores requisitos de seguridad y fiabilidad. Por lo que, los resultados inadecuados obtenidos en algunas de las pruebas pueden evidenciar que los PRNGs empleados en las etiquetas ofrecen una menor calidad de la que deberían tener.

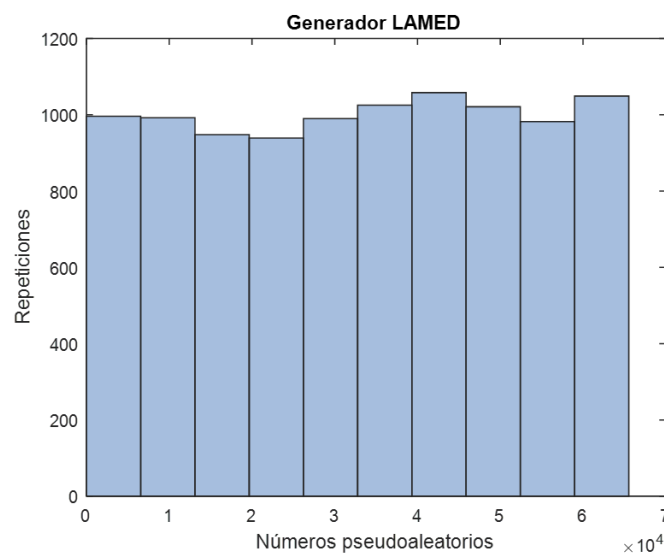


Figura 4.13. Histograma de la secuencia del generador LAMED.

4.4. Desarrollo de un emulador de etiquetas RFID pasivas.

En los últimos años se ha realizado un extenso trabajo en torno a las comunicaciones aéreas entre lectores y etiquetas para la tecnología RFID-UHF pasiva. Sin embargo, la mayoría de estos trabajos emplean protocolos y equipos estándar o no incluyen resultados físicos bajo condiciones reales y con componentes reales. Lo que suele deberse a la dificultad implícita de personalizar adecuadamente los chips de las etiquetas, con el fin de realizar las pruebas oportunas aplicando las soluciones propuestas.

Una vez estudiado y analizado en profundidad el protocolo de comunicación entre un lector y una etiqueta pasiva. Así como realizada la propuesta para la sustitución del generador de números pseudoaleatorios, que deben implementar las etiquetas, por un algoritmo más ligero. Un paso más es la realización de pruebas de funcionamiento. En este caso, aparte de los estudios y pruebas teóricas, se ha querido ir más allá y probar físicamente en la realidad el comportamiento de la propuesta.

No obstante, cabe en este punto destacar cuáles son las características físicas de una etiqueta RFID pasiva, en la que la mayor parte de la etiqueta se corresponde con la antena para la captación de la

señal de RF y es en un pequeño chip de pocas decenas de micras donde se encuentra toda la lógica. Por lo que las distintas partes hardware de una etiqueta RFID pasiva real presentan un diseño poco accesible a la hora de efectuarle modificaciones y realizar pruebas. Resultando bastante más complejas las modificaciones en la lógica interna de la etiqueta y el estudio de su comportamiento.

Siempre se podría optar por la alternativa de fabricar “ad hoc” un chip con las características deseadas. Pero esta resulta ser una opción inviable para nuestro equipo investigador, tanto de esfuerzo humano como económico. Siendo conscientes de que este tipo de fabricaciones se realiza a gran escala. Además, se ha de tener en cuenta que habría que repetir el proceso para cada modificación o prueba que se deseara realizar.

Otra solución que permite la realización de pruebas físicas reales es el uso de equipamiento de prueba y testeo, de tecnología RFID pasiva en este caso, existente en el mercado. De las diferentes alternativas que se pueden encontrar para evaluar y caracterizar sistemas RFID, se pueden destacar dos grupos principales de equipos: los sistemas basados en SDR (Software-Defined Radio, Sistemas de Radio definidos por Software) y los sistemas portátiles de medida.

Por un lado, los equipos de radiocomunicaciones basados en SDR se caracterizan porque todas o varias de las funciones de la capa física de comunicaciones se realizan mediante software [169], lo que les aporta gran flexibilidad y capacidad de reconfiguración. Es por ello por lo que este tipo de equipos se pueden adecuar de manera sencilla a las necesidades específicas para pruebas de etiquetas RFID. Un ejemplo es la solución de *National Instruments*® [170], que permite trabajar con etiquetas pasivas de RFID para la banda de UHF mediante el hardware *PXI*® y controlado por *LabVIEW*®. Aunque como contrapartida cabe destacar su elevado coste.

Por otro lado, los equipos portátiles de medida son los más extendidos para trabajar con comunicaciones aéreas en tecnología RFID-UHF pasiva. Se basan en actuar como un lector RFID y focalizan sus posibilidades en la evaluación del rendimiento y conformidad con los protocolos de etiquetas RFID. Por ejemplo, el sistema *Tagformance*®, de *Voyantic*®, que se presenta como una solución de medición completa de etiquetas RFID de alta precisión, está especialmente diseñado para caracterizar etiquetas y verificar aspectos relacionados con el cumplimiento de las normas y especificaciones de funcionamiento vigentes. Sin embargo, al no ser el propósito para el que fue diseñado, este sistema dispone de muy baja capacidad para incluir cambios en el protocolo de comunicaciones o para probar nuevas etiquetas y soluciones que no cumplan estrictamente con las normas existentes. Por su parte, el sistema *RFID Explorer*®, de *CISC Semiconductors*®, que trabaja en un rango de frecuencias de 800 MHz a 1 GHz, ampliable desde los 600 MHz hasta los 1,3 GHz. Fue inicialmente orientado para la caracterización de etiquetas y dispone de más parámetros configurables de otros sistemas, pero siempre limitados a los estándares y normas vigentes. También, este sistema añade una especie de emulador de etiqueta que permite el chequeo del comportamiento de los lectores RFID. Esta herramienta es capaz de medir la señal del lector, proporcionando información sobre el funcionamiento del enlace de comunicación desde el punto de vista de la etiqueta. Además, es capaz de generar la respuesta pertinente en cada caso. Sin embargo, nuevamente la configuración del equipo que se comercializa sólo ha sido diseñada para verificar el cumplimiento de lo que se está midiendo de acuerdo con las normas y protocolos existentes. En definitiva, todos estos equipos se suministran como una solución cerrada ya implementada, por lo que no permiten la realización de pruebas con nuevos algoritmos que se salgan fuera de los protocolos y normas de comunicación establecidas.

Por tanto, en el caso de que se precise de total flexibilidad y acceso para modificar distintos aspectos de los protocolos, o para probar otras propuestas de protocolos totalmente diferentes a lo que recogen los estándares actuales, sería necesario disponer de una solución completamente abierta. Esta

propuesta exhaustiva para el desarrollo de una plataforma completa que incluya emuladores de lector y etiqueta ha sido seguida durante los últimos años por otros grupos de investigación [171], [172]. En este sentido, los resultados presentados en [173] han propiciado varios trabajos. O en [174], donde se desarrolla un emulador multi-etiqueta para el ensayo de sistemas RFID. Pero de nuevo, estas nuevas soluciones se focalizan en la verificación de los lectores existentes y en la determinación de la eficiencia de los sistemas RFID, pero no en probar nuevos enfoques o propuestas de protocolos.

Tras analizar las posibles soluciones, finalmente se opta por desarrollar y construir una nueva plataforma hardware realista de bajo coste que permita emular el comportamiento real básico de una etiqueta RFID pasiva para la banda de UHF (Ultra High Frequency), sintonizada a una frecuencia de trabajo de 868 MHz. Y con el objetivo de crear una herramienta para realizar pruebas reales de nuevos cambios en los protocolos de comunicaciones empleados por las etiquetas RFID pasivas. Para ello, se propusieron las siguientes condiciones de diseño:

- La plataforma debe emular el comportamiento completo de una etiqueta RFID pasiva real y debe ser capaz de comunicarse con lectores RFID comerciales, como si se tratase de una etiqueta más.
- La plataforma debe cumplir con las especificaciones del protocolo de comunicación EPC Gen2 que define los requisitos físicos y lógicos de lectores y etiquetas RFID pasivas, que operen en el rango UHF (de 860 MHz a 960 MHz).
- La plataforma emuladora debe permitir una comunicación bidireccional con un lector RFID-UHF real. La ejecución de la rutina principal que se implemente en la plataforma deberá integrar el proceso de comunicación básico; es decir, recepción de la señal por parte del lector, generación de la respuesta por parte de la etiqueta y posterior envío al lector en caso de que fuera necesario.
- La plataforma debe ser flexible y parametrizable con el propósito de posibilitar el análisis y la modificación de los protocolos de comunicación entre lectores y etiquetas pasivas reales, supliendo las carencias del equipamiento comercial y de testeo que existe actualmente en el mercado. Además, debe proporcionar la flexibilidad necesaria para permitir la implementación de distintos protocolos de comunicación, así como la introducción de posibles ampliaciones o modificaciones de estos. En definitiva, debe permitir todos los cambios necesarios para poder llevar a cabo las pruebas que se deseen realizar.

Cabe destacar que a pesar de que la plataforma se comporta como una etiqueta pasiva, en realidad se trata de un sistema activo. Precisa de una fuente de alimentación propia para funcionar, debido a la necesidad de trabajar con un dispositivo flexible y potente que permita implementar fácilmente cambios en la lógica de la etiqueta emulada.

Con el objeto de poder llevar a cabo las pruebas de forma controlada, como lector RFID se empleará el sistema Tagformance®. Este equipo representa una solución más abierta que un lector RFID convencional, dado que permite configurar ciertos parámetros del protocolo a la hora de realizar las pruebas de comunicación.

Para la consecución de las tareas planteadas en el presente trabajo de investigación, se decide implementar el protocolo de comunicación hasta el instante en el que el lector identifica a la etiqueta (tiene conocimiento de su existencia). En este sentido, aunque la especificación EPC Gen2 contempla tres tipos de respuesta al lector por parte de las etiquetas, para este diseño únicamente se consideran las respuestas de tipo inmediato, que por otro lado son las más restrictivas y exigentes desde el punto de vista temporal. Es decir, se implementa la parte más crítica en la lectura de las etiquetas y que permite la realización de pruebas con la propuesta realizada en el punto 4.3 del documento, dejando el resto del protocolo para futuras versiones y/o ampliaciones.

4.4.1. Diseño y construcción del hardware.

Tras estudiar pormenorizadamente el funcionamiento del protocolo de comunicación, las limitaciones temporales suponen las restricciones más fuertes a la hora de plantear el diseño, puesto que la plataforma debe ser transparente para los lectores y transmitir la información en tiempo y forma, como lo haría una verdadera etiqueta pasiva. Tras evaluar las ventajas e inconvenientes de los sistemas y equipos comerciales existentes, se decide que la plataforma emuladora de etiquetas disponga de una FPGA como núcleo del sistema, lo que permitirá la rápida ejecución de las distintas operaciones para proporcionar a tiempo una respuesta válida al lector. Para lo que resulta imprescindible incluir en el diseño algunos interfaces de comunicación que interconecten las operaciones lógicas con las comunicaciones aéreas. Es decir, se precisa de un transceptor de UHF y, por consiguiente, de un microcontrolador rápido capaz de gestionar los flujos de información entre la FPGA el transceptor.

Por todo ello y teniendo en cuenta las características y prestaciones de los dispositivos electrónicos existentes en el mercado (como microprocesadores, microcontroladores, etc.), se decide implementar un sistema electrónico basado en el SoC (System on Chip) Zynq® 7000, que incorpora un microprocesador ARM de doble núcleo y una FPGA Artix7 en el mismo chip. Con este dispositivo se puede desarrollar un sistema de control y procesamiento potente y flexible: combinando la facilidad de programación y capacidades de comunicación de un microprocesador, con la potencia de cálculo y rendimiento de una FPGA. En su interior, ambos dispositivos interactúan mediante el bus AXI (Advanced eXtensible Interface), que permite el intercambio de información a gran velocidad. A este chip se le añade la circuitería necesaria para dotar al sistema de una interfaz para la comunicación aérea por radiofrecuencia⁷. El diagrama de bloques de la plataforma desarrollada se presenta en la Figura 4.14.

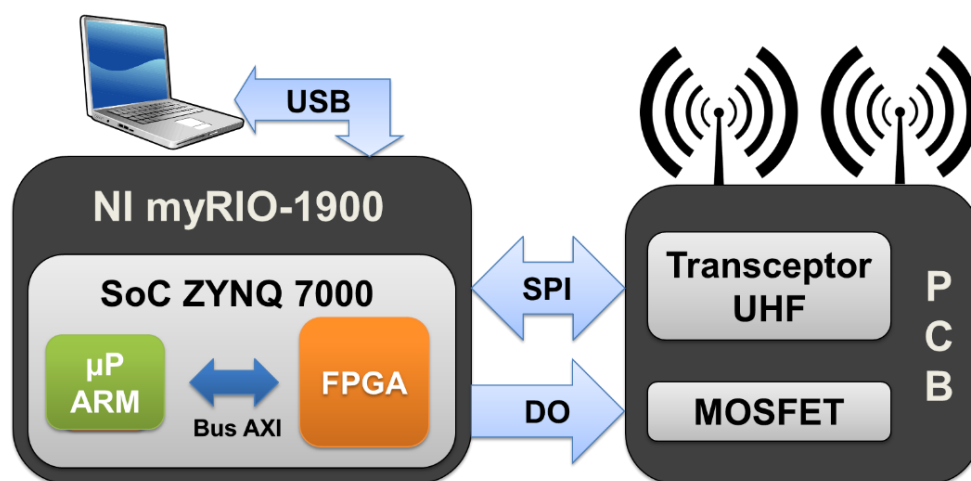


Figura 4.14. Diagrama de la plataforma emuladora de etiquetas RFID pasivas.

En una propuesta inicial, se comenzaron a gestionar directamente todos los recursos hardware mediante el desarrollo de controladores (drivers) de alto y bajo nivel, así como todo el software necesario para el funcionamiento de la plataforma. Para lo que se empleó el circuito del kit de evaluación ZC702 de Xilinx® (Figura 4.15), que permite el trabajo con los distintos interfaces y características del Zynq® 7000.

⁷ Resultados presentados en las IV Jornadas Doctorales de la UCLM 2014, celebradas en Cuenca (España).

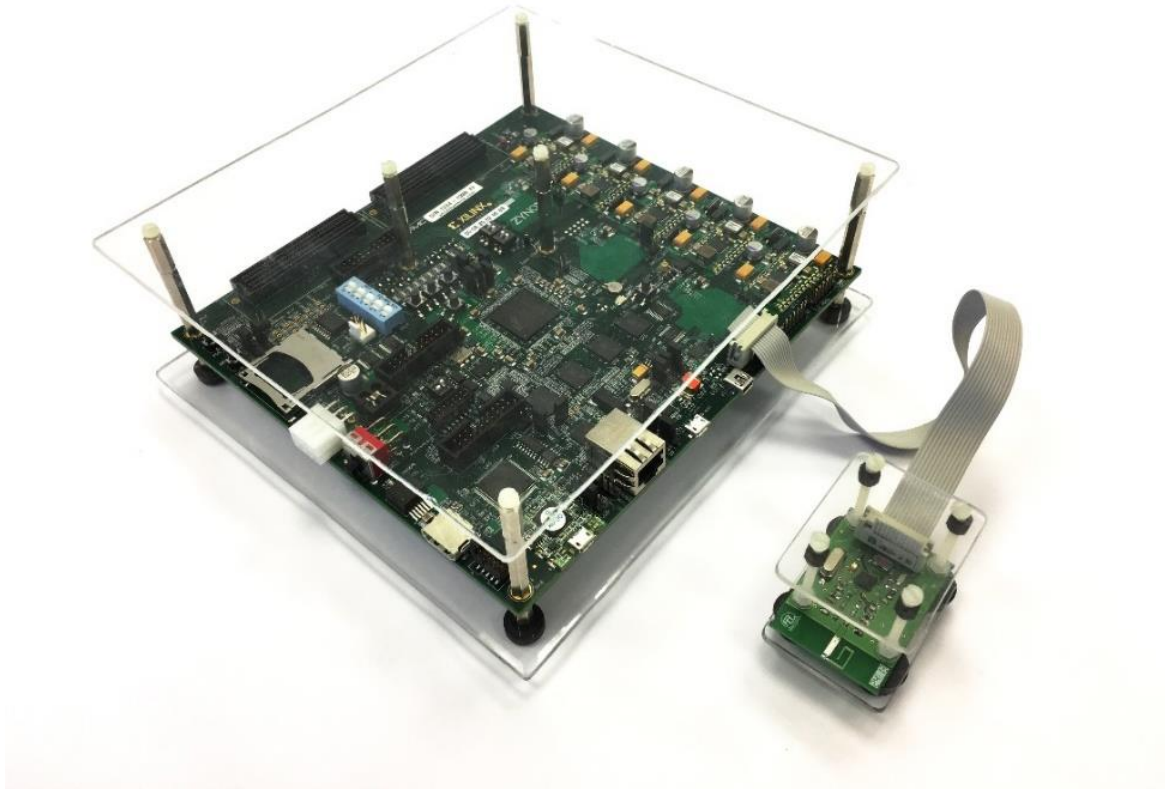


Figura 4.15. Prototipo del emulador de etiquetas desarrollado con la placa de pruebas del Zynq® 7000.

A este equipo se le añade una placa de circuito impreso (Printed Circuit Board, PCB), que se fabrica para albergar la interfaz para la comunicación aérea por radiofrecuencia (Figura 4.16). Cabe destacar que una etiqueta pasiva real posee una única antena por la que recibe la señal y envía su respuesta. Siendo esto lo que se pretendió emular con esta primera versión del hardware para la interfaz aérea: enviar y recibir las señales empleando las codificaciones y modulaciones adecuadas en cada caso. Mientras que una etiqueta pasiva comercial refleja la señal del lector modulando su respuesta sobre la misma, la plataforma desarrollada en esta primera versión incluye un sistema de comunicación completo e independiente con su propia referencia de reloj, lo que le permite generar su propia onda portadora para la transmisión.

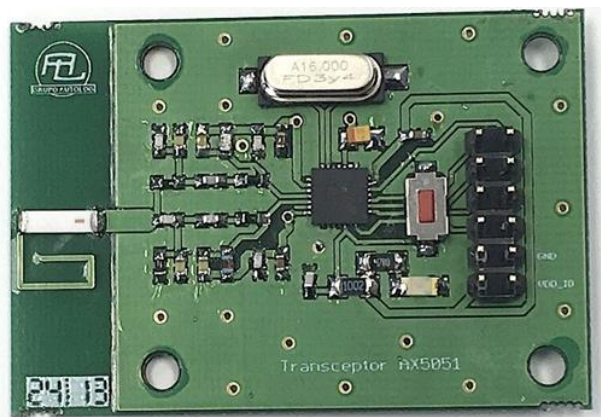


Figura 4.16. Primera versión de la PCB con la interfaz para la comunicación aérea en la banda de UHF.

Tras las primeras pruebas, la señal recibida del lector es decodificada de acuerdo con su codificación PIE. Previamente el emulador captura la señal utilizando un alto nivel de muestreo para evitar pérdidas

de información. Sin embargo, cuando la señal del emulador es enviada hacia el lector por el transceptor con su propia portadora, el lector realiza una recepción como la de la Figura 4.17, mientras que lo que se desea obtener es la envolvente de esa señal (Figura 4.18). Por lo que se observó que el lector no era capaz de interpretar los datos enviados desde el emulador (respuesta de la etiqueta). De donde se deduce que el lector no consigue filtrar una portadora distinta a la suya propia.

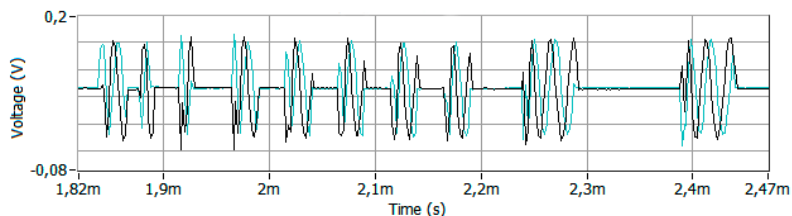


Figura 4.17. Forma de onda IQ obtenida de la señal recibida del emulador en el lector.

Una solución podría ser realizar un filtrado paso bajo de la señal en el lector para obtener la información de interés. Pero uno de los objetivos es que el emulador sea capaz de funcionar como una etiqueta pasiva real ante cualquier lector comercial. Por lo que se puede optar por otras soluciones en el lado de la etiqueta, como es la de utilizar la misma señal de reloj en el emulador trayéndola desde el lector con una conexión a su cable de antena para obtener la portadora original. Pero resulta otra solución poco viable, tanto desde el punto de vista técnico como por el motivo descrito anteriormente. No obstante, la solución debe pasar por actuar en el lado de la etiqueta.

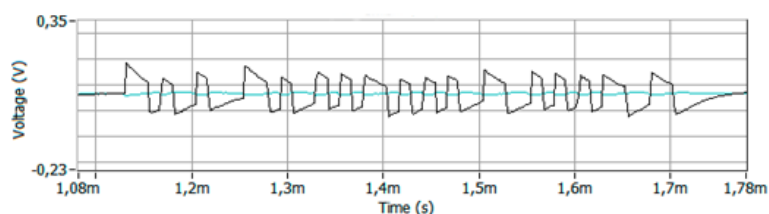


Figura 4.18. Forma de onda IQ de la respuesta de una etiqueta pasiva real en el lector.

En realidad, se estaba suplantando el proceso natural de respuesta de las etiquetas pasivas mediante la retrodispersión de la onda (fenómeno conocido como *backscatter*). De donde se deduce otra solución más directa que consiste en no utilizar el transceptor para la transmisión de la respuesta de la etiqueta y realizar una acción similar a la original de las etiquetas comerciales, imitando su funcionamiento real. Esto es, modular la respuesta de la etiqueta sobre la propia portadora emitida por el lector. Por lo que para replicar este comportamiento en la plataforma emuladora se necesita la separación física de los canales de transmisión y recepción en dos canales completamente independientes, puesto que no se trata de un circuito pasivo y la señal de RF será tratada de manera distinta en cada caso. Lo que se tradujo en el diseño y construcción de una nueva versión de la PCB con la interfaz para la comunicación aérea de la plataforma emuladora de etiquetas (Figura 4.19).

El trabajo directo con el hardware era una solución que requería de una gran inversión temporal y de recursos personales. Por lo que, para un desarrollo más rápido y ágil, finalmente se optó por emplear el equipo NI myRIO-1900 como núcleo lógico de operaciones de la plataforma⁸ (Figura 4.20), que está basado en el mismo SoC y puede ser programado mediante LabVIEW®. Aprovechando así las características que brinda esta tecnología para acelerar el desarrollo de la plataforma.

⁸ Resultados presentados en las VII Jornadas Doctorales de la UCLM 2017, celebradas en Albacete (España).

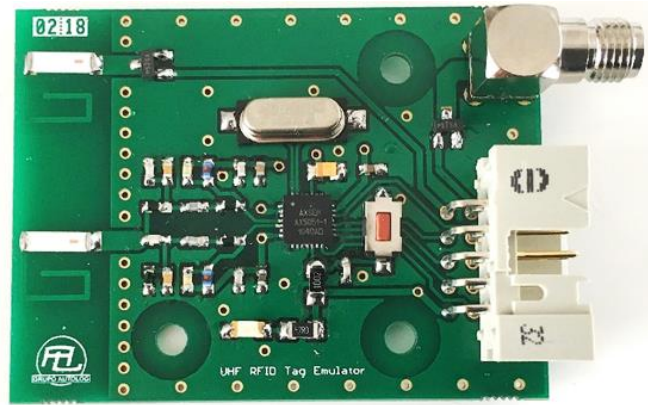


Figura 4.19. PCB definitiva con interfaces de comunicación para la plataforma emuladora de etiquetas.

Para recibir la señal que proviene del lector se emplea una antena tipo chip para la banda de UHF, sintonizada a 868 MHz, capaz de capturar las ondas electromagnéticas con diferentes polarizaciones. Dicha antena se encuentra conectada al transceptor de UHF AX5051, comandado mediante interfaz SPI. De este modo se asegura que el intercambio de datos entre el transceptor y el NI myRIO es lo suficientemente veloz. Lo que constituye un factor clave del desarrollo, puesto que en todo momento se pretende reducir el tiempo que transcurre desde que la señal se recibe hasta que se procesa y se realizan las operaciones oportunas como, por ejemplo, contestar al lector dentro del margen de tiempo esperado.



Figura 4.20. Plataforma con el emulador de etiquetas basado en myRIO y el sistema de medida empleado como lector.

Para enviar la señal con la respuesta al lector, se emplea otra antena similar que, conectada a tierra mediante un transistor MOSFET comandado por una salida digital (DO) del NI myRIO (Figura 4.21), se acoplará y desacoplará para generar una mayor o menor reflexión de la señal que proviene del lector. De forma que la información se transmite de manera similar a como lo haría una etiqueta pasiva real, emulando así su comportamiento. Además, en el diseño se incluye un conector SMA para proporcionar la posibilidad de conectar y emplear una antena externa (en vez de la integrada en la placa), con otras características para contestar al lector. Lo cual, dependiendo de la aplicación, puede resultar muy útil. Por ejemplo, si la respuesta de la plataforma no llega al lector con suficiente nivel de señal, se puede emplear una antena tipo parche para obtener mayores niveles de señal en la retrodispersión (*backscatter*).

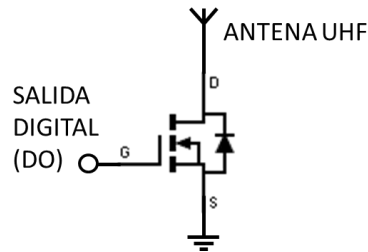


Figura 4.21. Circuito para la retrodispersión de la señal del lector.

Por último, el circuito fabricado se monta adecuadamente en el interior de una caja de material ABS para que no se produzcan interferencias y distorsiones en las señales de RF. De este modo se protegen los distintos elementos electrónicos, que son altamente sensibles a la electricidad estática. Dejando a la vista únicamente los conectores necesarios para el funcionamiento del emulador: el conector SMA para la conexión de la antena externa y un conector HARTING para conectar al NI myRIO (Figura 4.22).

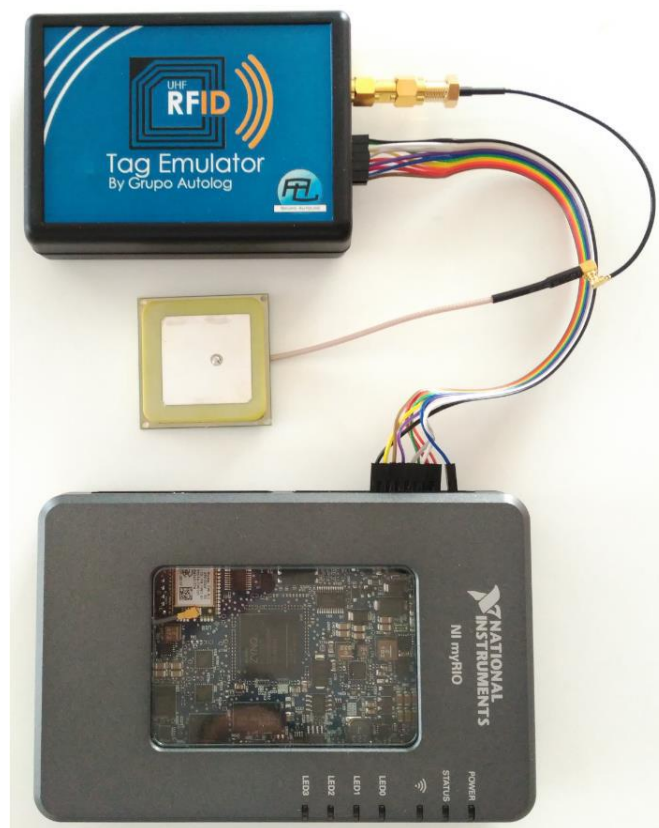


Figura 4.22. Plataforma emuladora de etiquetas RFID pasivas.

4.4.2. Implementación del software.

Para dotar de funcionalidad al hardware descrito en el punto anterior se desarrolla, mediante LabVIEW, todo el software necesario para el manejo y control de la plataforma emuladora⁹. Dada la complejidad del programa a desarrollar y la cantidad de parámetros que hay que gestionar, se opta por implementar

⁹ Parte del desarrollo definitivo de este dispositivo ha sido objeto del Trabajo Fin de Máster en Ingeniería Industrial de Alberto Flores Fernández en la E.T.S. de Ingeniería Industrial de la UCLM (julio de 2018), bajo la continua supervisión del doctorando como codirector de este.

un software modular, dividido en partes o módulos que a su vez son invocados por otros módulos cuando es preciso. Esta característica permite que el programa sea fácilmente escalable de cara a futuros trabajos y/o ampliaciones.

Debido a las fuertes restricciones temporales con las que se ha de cumplir, todos los procesos principales de la plataforma que requieren un mayor cómputo se han implementado en la FPGA. Empleándose el microprocesador, por tanto, para gobernar el transceptor y gestionar los flujos de información con la FPGA. De tal forma que esta distribución permite que la plataforma emuladora sea transparente para el lector, comportándose como una etiqueta pasiva real.

El programa principal (Figura 4.23) comienza con la inicialización de variables, drivers y funciones necesarias para el control de todas las operaciones de la FPGA y el transceptor de UHF. Una vez se han realizado estas operaciones, el sistema entra en modo recepción, donde se busca cualquier señal válida que provenga de un lector y se capturan los datos. Gracias a la alta velocidad de procesamiento que posee la FPGA, el sistema es capaz de preparar a tiempo la respuesta para su transmisión cuando se finaliza toda la recepción de la señal del lector. A continuación, el emulador cambia la configuración de modo recepción a modo transmisión y envía, en caso necesario, la respuesta solicitada por el lector. Para finalizar el ciclo, el sistema vuelve de nuevo a modo recepción a la espera de que lleguen nuevos datos.

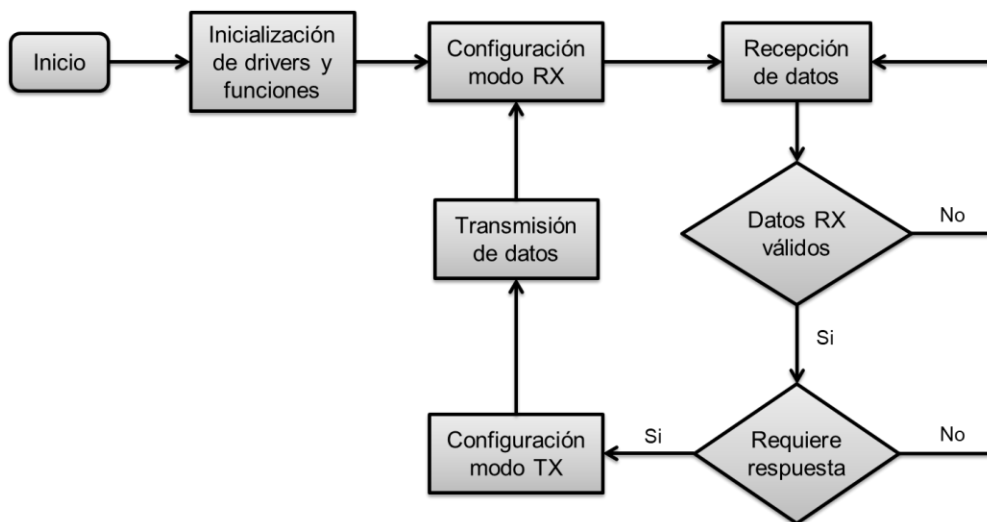


Figura 4.23. Flujograma del programa principal del emulador de etiquetas.

Por otro lado, también se han desarrollado los drivers necesarios para gestionar el transceptor con la FPGA mediante la interfaz SPI, para obtener una mayor velocidad de respuesta del emulador. Así como el control de la retrodispersión de la señal de respuesta a través de una salida digital que comanda el transistor MOSFET. En el interior del transceptor, la información se gestiona a través de una pila FIFO donde el bit más significativo se procesa en primer lugar. Procediéndose de igual modo a la hora de emitir mensajes hacia el lector. Para esta versión de la plataforma, la parte correspondiente al banco de memoria interna de la etiqueta se ha implementado de acuerdo con un EPC de 96 bits.

Dada la complejidad de todo el software, el programa se ha dividido en partes más pequeñas, empleando el paradigma de la programación modular. Dentro de LabVIEW, la modularidad del programa se traduce en crear secciones más pequeñas de código conocidas como *subVI*. Estas unidades de código gráfico tienen las mismas características que los *VI*, con la única diferencia de que los primeros son llamados a través de los segundos. Por lo que, un *subVI* puede entenderse como una subrutina en lenguajes de programación basados en texto. Gracias a esta técnica se ha podido abordar con éxito la

creación del software necesario para el funcionamiento de la plataforma emuladora, puesto que se permite dividir el código en pequeñas partes que son más fácilmente implementables en el lenguaje de programación.

Además de desarrollar las funciones propias de una etiqueta pasiva real, se ha diseñado una interfaz gráfica que se muestra en la pantalla del ordenador (Figura 4.24). Ésta permite la interacción del usuario con la plataforma y está conectada a la NI myRIO para monitorizar la evolución del proceso de comunicación que esté llevando a cabo la plataforma en cada momento. También se han implementado funcionalidades adicionales para facilitar el trabajo con la plataforma emuladora como son el encendido y apagado de la etapa de radiofrecuencia para habilitar o deshabilitar las comunicaciones aéreas (modo *stand-by*), o la posibilidad de poner en pausa el sistema en cualquier momento, congelando todos los procesos. Gracias a esta interfaz se proporciona el fácil acceso a todos los datos que circulan por el interior del chip de una etiqueta real, como parámetros de comandos recibidos, números aleatorios generados o valor de BLF calculado. Lo que permite exportar y emplear esta información para su posterior procesamiento y análisis.

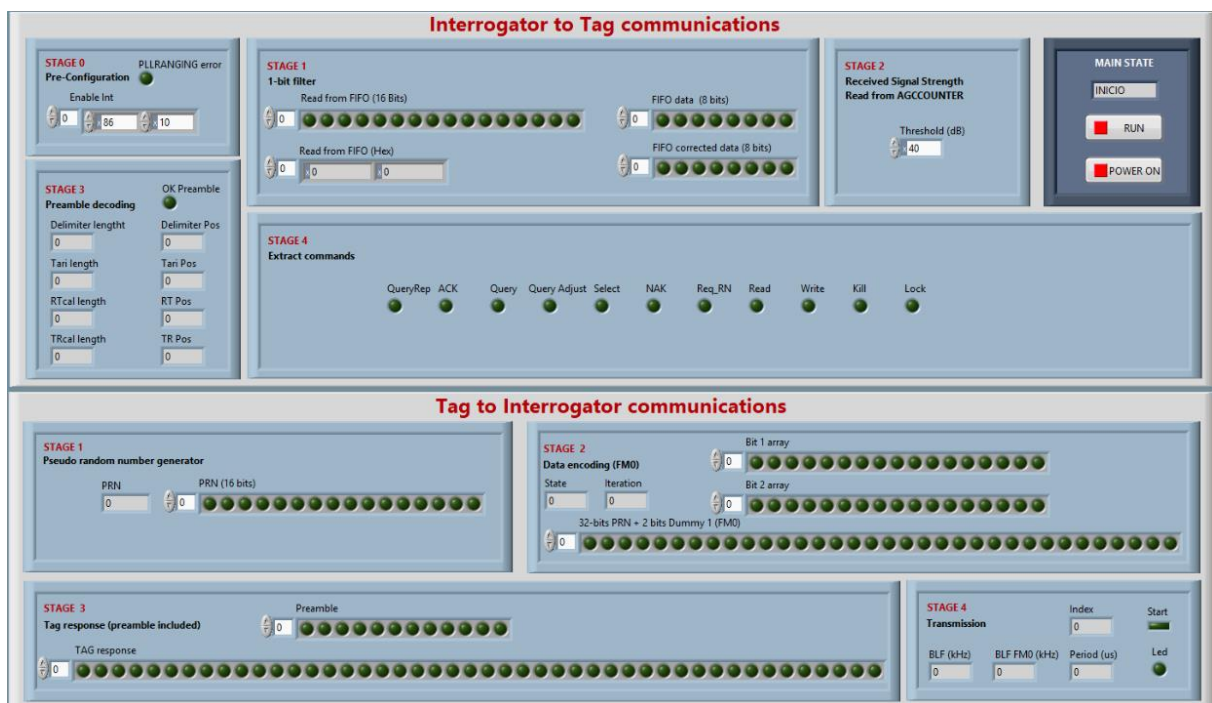


Figura 4.24. Pantalla principal del módulo monitorización de la plataforma.

4.4.3. Funcionamiento y pruebas realizadas.

Una vez la plataforma se encuentra en funcionamiento, es capaz de recibir y enviar datos de acuerdo con la especificación EPC Gen2, tal y como lo haría una etiqueta pasiva real. Sin embargo, a diferencia de ésta, que se activa cuando incide sobre ella señal del lector y funciona con la energía de la propia señal, la plataforma no captura la energía para funcionar de la señal de RF y dispone de un suministro externo continuo de energía. Ya que resulta imposible alimentar y hacer funcionar el emulador de etiquetas únicamente con señal de RF.

4.4.3.a. Comunicación desde el lector hacia el emulador de etiquetas.

En un sistema RFID pasivo, siempre es el lector el encargado de iniciar las comunicaciones, puesto que tiene que suministrar a las etiquetas la energía necesaria para que funcionen. Pero a diferencia de una

etiqueta pasiva real, el emulador de etiquetas, una vez puesto en marcha, se encuentra la mayor parte del tiempo trabajando en modo recepción: recibiendo señales e interpretando la información entrante, en busca de una señal válida del lector RFID (Figura 4.25) para actuar en consecuencia. Para ello, la señal que se recibe en el puerto de la antena se muestrea cada $2\ \mu\text{s}$ y es demodulada mediante el esquema ASK en el transceptor. Después, la FPGA analiza los datos para detectar un preámbulo (*preamble*) cuando se está esperando el primer comando del lector, o una ventana de sincronización (*frame-sync*) para cualquier otro comando. En este instante, todos los datos que no sean un *preamble* o un *frame-sync* son descartados como ruido.

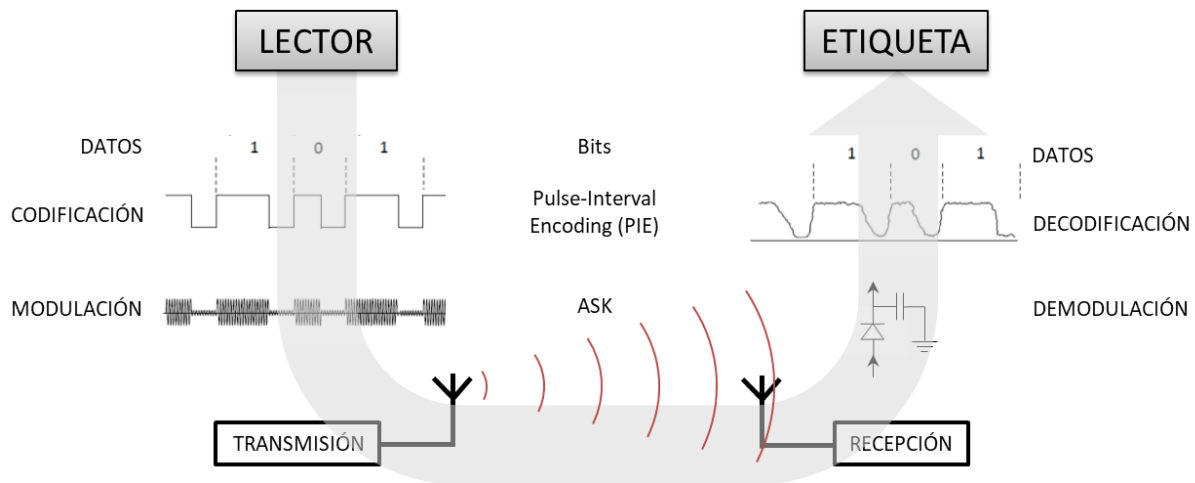


Figura 4.25. Flujo y transformación de la información desde el lector a la etiqueta.

El *preamble* (Figura 4.26) sirve para sincronizar y ajustar las variables y mecanismos que intervienen en la comunicación y que los datos se reciban adecuadamente. Consta de: un intervalo de señal, denominado *delimiter*, a nivel bajo y con una longitud fija en torno a los $12,5\ \mu\text{s}$; el símbolo de un dato "0", que tiene una duración igual que el parámetro *Tari*, por lo que debe encontrarse entre los $6,25\ \mu\text{s}$ y $25\ \mu\text{s}$ (establecido en la especificación EPC Gen2); el parámetro *RTcal* (Reader to Tag Calibration, o calibración del lector hacia la etiqueta), que consiste en un pulso con una duración de un dato "0" más la duración de un dato "1"; y por último, el parámetro *TRcal* (Tag to Reader Calibration, o calibración de la etiqueta hacia el lector), cuya duración especifica el valor de la *Backscatter Link Frequency* (BLF, o frecuencia del enlace por retrodispersión), que se emplea a la hora de contestar al lector. Además, *RTcal* y *TRcal* deben cumplir que $1,1 \cdot RTcal \leq TRcal \leq 3 \cdot RTcal$. Y un *frame-sync* es un *preamble* sin el *TRcal*.

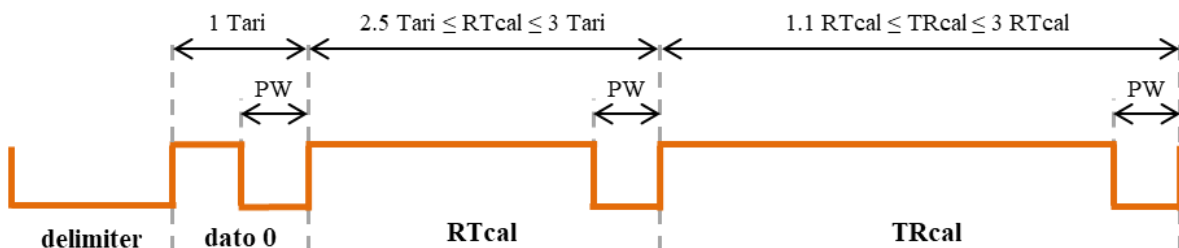


Figura 4.26. Preámbulo del comando del lector [16].

Cuando la plataforma emuladora detecta un preámbulo o una ventana de sincronización, la FPGA se encarga de medir la duración de los valores de *Tari*, *RTcal* y *TRcal*. Para posteriormente decodificar el mensaje de acuerdo al patrón PIE (Pulse Interval Encoding, o codificación por ancho entre pulsos), y teniendo en cuenta el valor *pivot*, que es igual a $RTcal/2$, procediendo de la siguiente forma: si un símbolo tiene una duración menor a *pivot*, se interpreta como un dato "0" y si es mayor, un dato "1".

Todos los símbolos terminan con el mismo intervalo de señal a nivel bajo (Figura 4.2). La señal recibida es decodificada por la FPGA que posteriormente lleva a cabo distintas operaciones, dependiendo del comando recibido, para generar una respuesta al lector apropiada.

4.4.3.b. Comunicación desde el emulador de etiquetas hacia el lector.

En el instante en el que la respuesta ha sido generada, la plataforma entra en el modo de transmisión y prepara los datos para ser enviados, ya que las etiquetas pasivas deben codificar sus respuestas empleando esquemas FM0 o Miller.

Para llevar a cabo la codificación FM0, se invierte la fase de la señal codificada en cada flanco de la señal binaria original, es decir, cada vez que se termina un símbolo. Y se incorpora una inversión adicional en mitad de un dato “0”. Consecuentemente, la codificación FM0 tiene memoria y el nivel de señal de un determinado símbolo depende del nivel de los símbolos codificados inmediatamente anteriores. En cambio, para la codificación Miller se realiza una inversión de fase en mitad de un dato “1” y únicamente se invierte la fase entre dos datos “0” consecutivos. Para finalizar la codificación Miller, la señal resultante en banda base se multiplica por una onda cuadrada a M veces la velocidad de los datos. M es un parámetro que se encuentra dentro del paquete de datos del comando que inicia la ronda de inventariado de etiquetas (comando *Query*). La velocidad de los datos de la subportadora se ajusta para que sea igual al valor BLF, estableciéndose así la velocidad para el enlace entre la etiqueta y el lector. La ecuación (4.21) describe cómo se obtiene este valor, donde DR (*Divided Ratio*) es otro parámetro que se obtiene del paquete de datos del comando *Query*.

$$BLF = \frac{DR}{TRcal} \quad (4.21)$$

El mensaje de la etiqueta comienza con un preámbulo determinado, que es distinto para cada esquema de codificación (FM0 o Miller) y sirve para sincronizar al receptor (el lector RFID en este caso) para que pueda llevar a cabo una correcta decodificación. Además, en ambos casos, el mensaje finaliza incorporando un dato “1” adicional, denominado *dummy*.

Para implementar las codificaciones FM0 y Miller, que son esquemas de tipo bifase, se duplican los datos de acuerdo con el símbolo correspondiente. De tal manera que se pueda emular la inversión de fase en mitad del símbolo o la violación de código que es necesario realizar en el preámbulo FM0 del mensaje de respuesta de la etiqueta. Por ejemplo, para que un dato “0” esté codificado con FM0, la señal debe tener una inversión de fase en mitad del símbolo, para lo que la FPGA del emulador de etiquetas debe cambiar ese dato “0” por dos datos “01” o “10”, dependiendo del símbolo que lo preceda. A continuación, se aplica una codificación NRZ a la señal obtenida en la conversión anteriormente descrita. Transmitiéndose, por último, mediante la modulación digital en amplitud (ASK) al doble de la velocidad establecida para el enlace, cumpliendo así con el valor de BLF establecido.

Para transmitir información al lector (Figura 4.27), las etiquetas pasivas reales utilizan la retrodispersión (*backscatter*) de la señal que proviene del lector, reflejándola en mayor o menor medida. Siendo esa señal reflejada en la etiqueta la que llega nuevamente al lector con la información incorporada, la cual es interpretada por éste para extraer la respuesta enviada por la etiqueta.

Desde el punto de vista de la etiqueta, la generación de la señal de respuesta por retrodispersión depende de las características de su antena, así como de sus habilidades para originar una mayor o menor reflexión de la portadora del lector, modulando y transmitiendo así su respuesta. Para emular este comportamiento en la plataforma desarrollada, la señal resultante de todo el proceso se conduce a la salida digital de la FPGA que comanda el MOSFET que se encuentra conectado entre la antena para la respuesta y tierra, propiciando que se acople y desacople la antena a la velocidad adecuada. De tal

forma que se consigue que se produzca una mayor o menor reflexión de la portadora del lector en cada instante de tiempo.

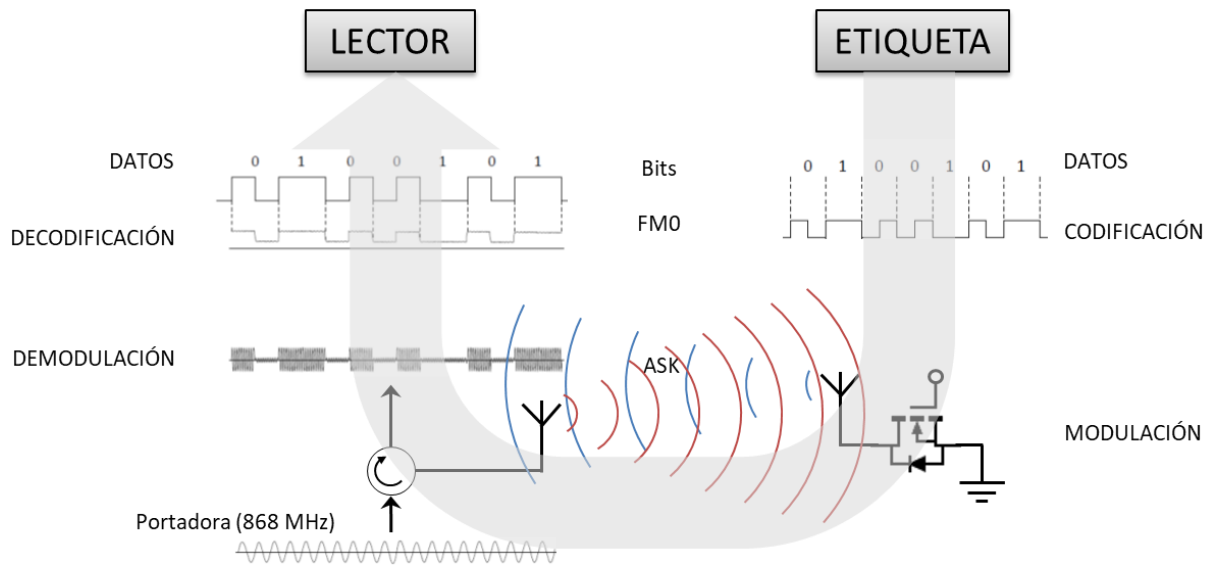


Figura 4.27. Flujo y transformación de la información desde la etiqueta al lector.

4.4.3.c. Pruebas de comunicación.

Además de las pruebas que se han ido realizando durante el desarrollo y que han permitido, por ejemplo, lograr la correcta emulación del proceso de *backscatter*. Para comprobar el correcto funcionamiento de la plataforma emuladora de etiquetas desarrollada, se han realizado una serie de pruebas de comunicación reales con el lector de RFID, observando que se comporta como si fuera una etiqueta RFID pasiva real.

En una primera etapa, las pruebas se centraron en la captura e interpretación de la señal transmitida por el lector. Consiguiéndose, tras la realización de unos pequeños ajustes, recibir de forma correcta la información enviada por el lector. A continuación, las pruebas se focalizaron en comprobar que el emulador de etiquetas generaba una respuesta adecuada a tiempo con los parámetros recibidos del lector. En último lugar, se realizaron pruebas de transmisión de la respuesta de la etiqueta y de recepción en el lector, observando que la señal recibida era interpretada por el lector de manera correcta.

A modo de ejemplo de las pruebas realizadas, la Figura 4.28 muestra el resultado del envío de un comando *Query* por parte del lector y su posterior respuesta por parte de la etiqueta. Cabe destacar que, dentro de todo el proceso de identificación de etiquetas, este comando es el primero que requiere la generación y envío de una respuesta por parte de la etiqueta. Por lo que es el punto crítico y clave para una correcta identificación de éstas ya que, un error en la transmisión, una colisión, o el efecto captura, pueden ocasionar que cualquier etiqueta quede sin identificar. Es a partir de este momento, cuando el lector tendrá conocimiento de la existencia de las etiquetas que hayan contestado. Por lo que se podrán identificar adecuadamente.

Los resultados obtenidos son satisfactorios. En todos los casos, la señal recibida en el lector es similar a la señal que se recibe de una etiqueta RFID pasiva real. Por lo que queda demostrado que el emulador de etiquetas desarrollado se comporta como una etiqueta pasiva. Consiguiendo así, la creación de una plataforma flexible y reconfigurable de bajo coste con la que hacer pruebas reales libremente. Tanto a

nivel de cambios en el protocolo de comunicación, como en las operaciones que tienen lugar en la lógica interna de la etiqueta.

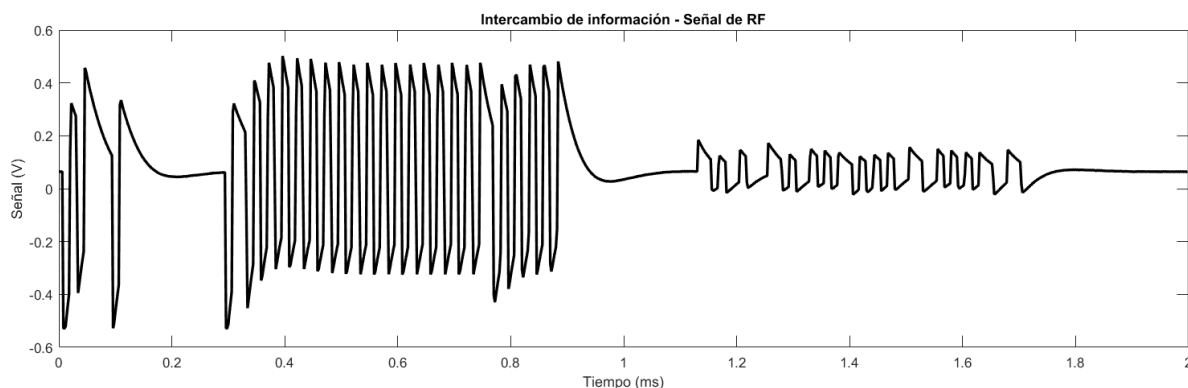


Figura 4.28. Señal emitida por el lector (a la izquierda) y señal recibida del emulador de etiquetas (a la derecha).

4.4.4. Implementación física del algoritmo ultraligero propuesto.

Para tener un análisis más completo y comprobar la viabilidad real de la propuesta anteriormente realizada, aparte de las pruebas teóricas y simulaciones, el algoritmo propuesto en la sección 4.3 se ha implementado en el emulador de etiquetas desarrollado, que replica el comportamiento de una etiqueta pasiva real¹⁰. Esta implementación en un dispositivo real permite comprobar los recursos que realmente necesitan cada una de las operaciones que se realizan para las diferentes soluciones. Además, permite comparar la propuesta con otras alternativas existentes en la actualidad.

Una vez programado el algoritmo propuesto en el emulador de etiquetas, que principalmente consiste en la implementación del LFSR, se procede a su puesta en marcha. En primer lugar, se obtiene la información necesaria para el funcionamiento del algoritmo como es el parámetro Q , que se obtiene del comando *Query* enviado por el lector. Este valor se carga directamente en el LFSR, que inicialmente se encuentra vacío, actuando como semilla para la generación del número pseudoaleatorio. Paralelamente, se rescata el EPC, de 96 bits en este caso, que se encuentra en el banco de memoria del emulador y se prepara para introducirlo en el LFSR. Cabe recordar que este código es único para cada etiqueta y se graba en su memoria durante el proceso de fabricación de acuerdo con los estándares actualmente vigentes. A continuación, se hace circular cada uno de los bits que forman este EPC por el LFSR, comenzando por el bit más significativo. Tras la introducción de todo el código, el primer número pseudoaleatorio generado se obtiene del contenido del LFSR. A partir de esta secuencia binaria, se realizan las operaciones oportunas según requieran los distintos comandos que intervengan en la comunicación, como puede ser hacer uso del parámetro *Stored-CRC* alojado en la memoria de la etiqueta u obtener subsecuencias del número pseudoaleatorio generado; tal y como se ha expuesto en la descripción del funcionamiento de la propuesta.

Por otra parte, con el objeto de comparar el algoritmo propuesto para la generación de números pseudoaleatorios con otras soluciones que se emplean en la actualidad, también se han implementado en el emulador de etiquetas dos métodos alternativos a la propuesta y de los más comunes como son: los generadores congruenciales lineales (LCG, Linear Congruential Generators) y los generadores congruenciales multiplicativos (MCG, Multiplicative Congruential Generators). Lo que permite evaluar,

¹⁰ Resultados publicados en el *Congreso Internacional Smart SysTech 2017*, celebrado en Múnich (Alemania).

por tanto, la eficiencia y funcionamiento del algoritmo propuesto frente a otras posibles soluciones. La implementación de ambos métodos se ha realizado siguiendo las recomendaciones marcadas en [175].

Para poder evaluar la eficiencia de estos algoritmos, se consideran como variables cuantitativas medibles los recursos hardware de la FPGA [176] que se utilizan para la implementación de cada uno de los mecanismos generadores. Así como el tiempo necesario para la ejecución de cada uno de ellos. Además, en el análisis también se incluyen los recursos necesarios para la implementación de toda la lógica de la etiqueta.

También cabe destacar, para un mejor entendimiento de la comparativa realizada, que los recursos disponibles en la PFGA se dividen en: bloques lógicos, que hacen referencia a los grupos totalmente configurables de puertas lógicas; LTUs, que son unos grupos de puertas lógicas ya predefinidos y conectados por hardware; registros, para albergar información y variables; bloques de memoria RAM; y DSP48s, que son unas unidades rápidas de procesamiento equivalentes a cientos de grupos de bloques lógicos.

En la Figura 4.29 se pueden observar: la cantidad de recursos empleados para implementar el algoritmo propuesto para la generación de números pseudoaleatorios, respecto del total de recursos lógicos disponibles en la PFGA del emulador; junto con la cantidad de recursos utilizados para los métodos LCG y MCG; y frente al total de recursos necesarios para la implementación de toda la lógica de la etiqueta. Puede observarse como los métodos LCG y MCG necesitan aproximadamente la misma cantidad de recursos. Contrastando notablemente con la menor cantidad de recursos necesarios para implementar el algoritmo propuesto. Además, en las pruebas realizadas se ha observado que para la ejecución de los algoritmos LCG y MCG, se requiere un tiempo medio de ejecución de 75 ns, mientras que el algoritmo propuesto se ejecuta en 50 ns. Lo que supone un ahorro temporal considerable que puede emplearse para realizar otras operaciones y que la etiqueta sea más eficiente.

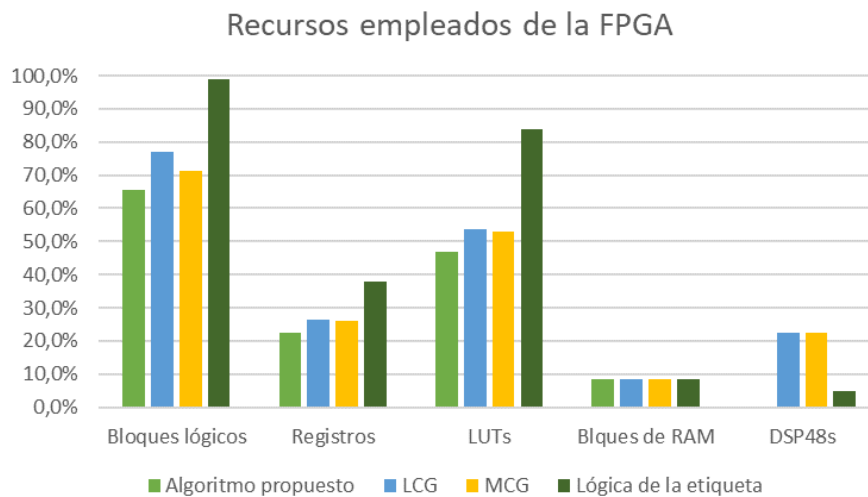


Figura 4.29. Recursos de la FPGA necesarios para la implementación de cada método.

Los resultados obtenidos ponen de manifiesto que la estrategia para generar números pseudoaleatorios conlleva algo más de la mitad del total de los recursos necesarios para implementar la lógica completa de una etiqueta real. Lo que resulta bastante ilustrativo sobre qué partes de la lógica interna de las etiquetas requieren de mayor cantidad de recursos. Este hecho invita a tener en cuenta que la implementación de un método u otro para la generación de números pseudoaleatorios implica la necesidad de emplear más o menos recursos hardware. Por lo que, escogiendo métodos más ligeros, como el algoritmo ultraligero propuesto, permitiría la fabricación de chips más sencillos para las

etiquetas pasivas de RFID, tanto desde el punto de vista de los recursos necesarios (hardware y software), como de la cantidad de operaciones que tiene que realizar y que en la práctica se traduce en tiempo. Es decir, con el algoritmo propuesto se obtendrían nuevos chips que realizarían las mismas funciones que los actuales y que se podrían construir con menos recursos materiales, lo que también puede repercutir en un abaratamiento de los costes de producción. Y donde la ejecución de los comandos que impliquen el uso del generador de números pseudoaleatorios se realizaría de forma más rápida.

4.5. Comportamiento de la BLF en etiquetas reales.

Tanto para desarrollar el emulador de etiquetas pasivas, como para realizar la propuesta de sustitución del generador de números pseudoaleatorios por el algoritmo ultraligero descrito anteriormente, ha sido necesario llevar a cabo un profundo trabajo con el protocolo de comunicación en RFID. Gracias, en parte, a lo que se ha adquirido un gran conocimiento sobre cómo son y cómo se producen las comunicaciones entre un lector y una etiqueta RFID. Lo cual, ha permitido fijar el foco sobre algunos aspectos que, a priori, no se les ha dado importancia y han sido pasados por alto.

De algunos de los trabajos desarrollados en los últimos años para mejorar la tecnología RFID pasiva, como en [177], se desprende la evidencia de que cada etiqueta pasiva de RFID responde al lector con una velocidad ligeramente distinta a la que en un principio (teóricamente) espera el lector. Hecho que además se ha constatado mientras se realizaban las medidas para el análisis de los números pseudoaleatorios generados en etiquetas reales.

En principio, este efecto es algo común en cualquier dispositivo que utilice osciladores, debido a la propia naturaleza de los mismos. Pero dada la peculiaridad de las comunicaciones RFID y la particularidad de este hecho, se decidió medir y analizar la velocidad de transmisión de datos a la que las etiquetas responden al lector para averiguar si esas variaciones podían presentar algún patrón o comportamiento determinado¹¹. Para, dado el caso, aplicar este fenómeno a otros procesos que se llevan a cabo en las etiquetas RFID pasivas. Por ejemplo, la simplificación de los generadores de números pseudoaleatorios empleados en las etiquetas a la vez que se mejoran sus prestaciones es una posible aplicación de este estudio, ya que estas variaciones podrían ser utilizadas como semilla. Abriendo la puerta a otras funcionalidades como podría ser la mejora de las posibilidades de incluir encriptación en las etiquetas.

4.5.1. Frecuencia de enlace por retrodispersión.

En la práctica, el proceso de identificación de etiquetas RFID pasivas consiste en un diálogo entre el lector y cada etiqueta mediante el que se obtienen los códigos unívocos de todas y cada una de las etiquetas presentes en el rango de cobertura del lector. Tal y como se ha descrito en la sección 4.1.3, esta comunicación comienza con la emisión de una portadora a la frecuencia de trabajo por parte del lector. Sobre esta señal se modulará la codificación de los comandos que emita el lector, que serán recibidos e interpretados por las etiquetas. Y donde la respuesta de cada etiqueta será la reflexión de la misma portadora del lector modulada con la información que cada una de ellas deba transmitir.

¹¹ Parte de este trabajo ha sido realizado durante la estancia de investigación en la Universidad Técnica de Múnich, TUM (Múnich, Alemania), en otoño de 2016 y bajo la supervisión de E. Biebl y K. Finkenzeller.

Para responder físicamente al lector y dado que las etiquetas RFID pasivas carecen de fuente de alimentación independiente, cada etiqueta modula y refleja (*backscatter*) la señal del lector, obteniéndose en la antena del lector una señal $a_t(t)$ definida por la ecuación (4.22). Donde x_b , f_c y ϑ_b , son la señal moduladora con los datos binarios de respuesta, la frecuencia de la portadora emitida por el lector y el desfase introducido por la etiqueta, respectivamente [178]. Y describiéndose la señal binaria de respuesta en el lector como dos valores diferentes de intensidad de señal: el valor modulado y el no modulado.

$$a_t(t) = x_b(t) \cdot \cos(2\pi f_c t + \theta_b) \quad (4.22)$$

La velocidad de transmisión de datos a la que una etiqueta debe responder al lector coincide con el valor de la frecuencia subportadora a la que la etiqueta pasiva modula la portadora emitida por el lector (en este caso una onda continua a 868 MHz, banda de UHF), para elaborar la respuesta por retrodispersión. Ese valor de frecuencia de la subportadora se denomina *Backscatter-Link Frequency (BLF)*, según la especificación EPC Gen2 [16]. Su valor se obtiene a partir de la ecuación (4.21), para la que cabe recordar que *DR* (Divided Ratio) es un parámetro enviado por el lector en el comando *Query* y *TRcal* es un intervalo de tiempo que se obtiene directamente del preámbulo que precede a dicho comando. Por tanto, el valor de la frecuencia de la subportadora que contiene la información de respuesta de una etiqueta RFID pasiva, depende de la información que el lector haya emitido y está directamente relacionada con el valor medido del intervalo *TRcal* por parte de la etiqueta.

En este sentido, cabe destacar que toda implementación de soluciones lógicas en circuitos integrados (chips), conlleva la aparición de incertidumbres en los valores de los distintos parámetros y operaciones. Además, debido a que las etiquetas RFID pasivas deben ser cada vez más baratas, se construyen con componentes que presentan unas tolerancias considerables. Por lo que valores como la medida del parámetro *TRcal* u otras operaciones pueden variar ligeramente de unas etiquetas a otras. E incluso producirse este efecto para una misma etiqueta en distintos instantes de tiempo. Además, entendiendo las etiquetas pasivas como un sistema aislado, carecen de referencia externa con la que poder comparar si los valores medidos o los resultados de las operaciones que realiza son correctos o se han desviado respecto al valor esperado.

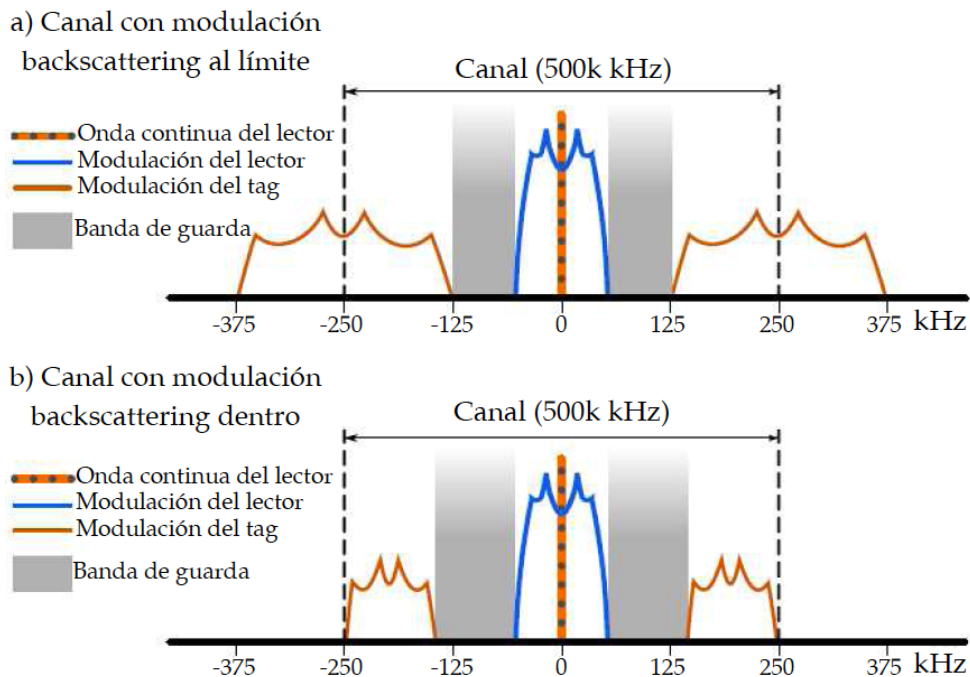


Figura 4.30. Espectro del canal de comunicación entre el lector y la etiqueta [16].

Como consecuencia de la modulación de la portadora por parte del lector, aparece una subportadora (valor de BLF) en el espectro que es la que contiene la información de la etiqueta. La Figura 4.30 muestra la distribución de las señales del lector y la etiqueta en el canal de comunicación. En este caso la frecuencia máxima de la subportadora de la etiqueta (BLF) es de 250kHz, lo que da lugar a los dos picos laterales separados 500 kHz de anchura sobre la frecuencia central en banda base; la cual se corresponde con la portadora original del lector y es de 868 MHz. Cuanto mayor es la frecuencia de la subportadora, más alejados están los lóbulos laterales de la portadora del lector. Por lo que le resulta más fácil filtrar su propia portadora para extraer la respuesta de la etiqueta (señal de backscattering).

Teniendo en cuenta este fenómeno y remarcando el hecho de que una etiqueta calcula la frecuencia de la subportadora con la que debe responder al lector, en base a la información contenida en la señal que éste le envía, tal y como se ha comentado anteriormente. Cada etiqueta contestará al lector a una frecuencia ligeramente distinta (superior o inferior) a la esperada por el lector. Por ello, en la especificación EPC Gen2 se recoge que este valor de frecuencia para la respuesta de la etiqueta (BLF) debe estar dentro de un determinado rango. Y que, a su vez, este valor se mantenga estable durante la comunicación con el lector. En la Tabla 4.4 se muestran algunas de estas tolerancias.

Tabla 4.4. Tolerancias permitidas para el valor de BLF [16].

DR	TRcal ($\mu\text{s} \pm 1\%$)	BLF (kHz)	Tolerancia (Tª nominal)	Variación durante la retrodispersión
64/3	33.3	640	+/- 15%	+/- 2.5%
	33.3 < TRcal < 66.7	320 < BLF < 640	+/- 22%	+/- 2.5%
	66.7	320	+/- 10%	+/- 2.5%
	66.7 < TRcal < 83.3	256 < BLF < 320	+/- 12%	+/- 2.5%
	83.3	256	+/- 10%	+/- 2.5%
	83.3 < TRcal ≤ 133.3	160 ≤ BLF < 256	+/- 10%	+/- 2.5%
	133.3 < TRcal ≤ 200	107 ≤ BLF < 160	+/- 7%	+/- 2.5%
	200 < TRcal ≤ 225	95 ≤ BLF < 107	+/- 5%	+/- 2.5%
8	17.2 ≤ TRcal a 25	320 < BLF ≤ 465	+/- 19%	+/- 2.5%
	25	320	+/- 10%	+/- 2.5%
	25 < TRcal < 31.25	256 < BLF < 320	+/- 12%	+/- 2.5%
	31.25	256	+/- 10%	+/- 2.5%
	31.25 < TRcal < 50	160 < BLF < 256	+/- 10%	+/- 2.5%
	50	160	+/- 7%	+/- 2.5%
	50 < TRcal ≤ 75	107 ≤ BLF < 160	+/- 7%	+/- 2.5%
	75 < TRcal ≤ 200	40 ≤ BLF < 107	+/- 4%	+/- 2.5%

Realizando un análisis en frecuencia de la señal de respuesta que proviene de la etiqueta y capta el lector, se observa como la mayor parte de la energía se concentra en torno al valor de la subportadora (BLF). A la vez que puede apreciarse claramente en el espectro la desviación de la subportadora respecto a la frecuencia inicialmente esperada por el lector. Por lo que analizando el espectro de todas las señales recibidas en el lector puede diferenciarse cada una de las respuestas correspondientes a cada una de las etiquetas que contestan al lector.

Este comportamiento ha sido aprovechado en [177], donde se propone su uso para minimizar el número de colisiones entre respuestas de etiquetas así como evitar el efecto captura. Siendo posible, gracias al análisis espectral del preámbulo de la señal que recibe el lector como respuesta. La Figura 4.31 muestra las frecuencias obtenidas empleando un análisis FFT para un ejemplo realizado con cuatro etiquetas comerciales dentro del área de cobertura del lector. Para ese caso se han obtenido picos de frecuencia de 313 kHz, 320 kHz, 330 kHz y 352 kHz. Estas frecuencias son los primeros armónicos de las subportadoras moduladas binariamente de cada etiqueta y que coinciden con los valores de las BLF respectivos de las cuatro etiquetas. En caso de colisión o de que varias etiquetas contesten en el mismo instante de tiempo, el problema se detectaría fácilmente, dado que el espectro de la señal muestra el número de etiquetas distintas que han participado en esa respuesta. Por lo tanto, el lector puede actuar en consecuencia e identificar de forma adecuada cada una de ellas.

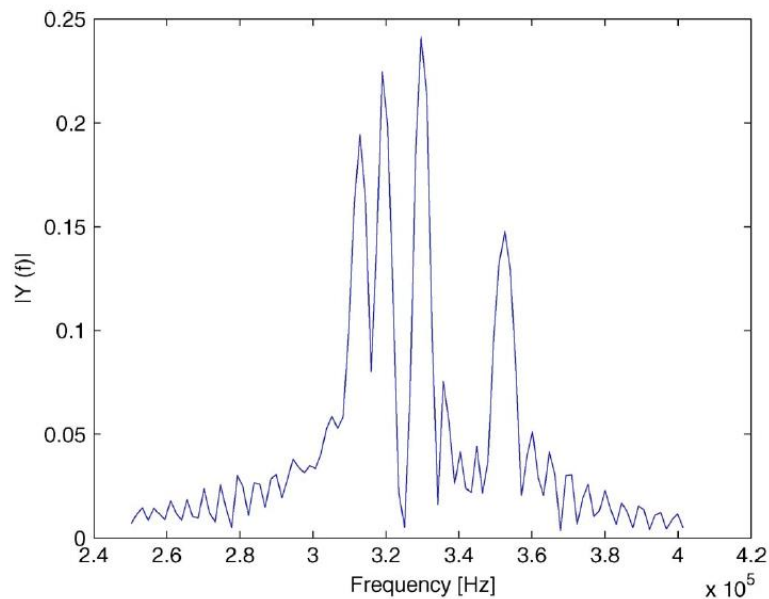


Figura 4.31. FFT de la señal que llega al lector con varias subportadoras de etiquetas comerciales distintas [177].

4.5.2. Medida y caracterización de la BLF.

Teniendo en cuenta la evidencia de que la subportadora con la que una etiqueta pasiva de RFID responde al lector (BLF) presenta una ligera desviación respecto al valor teórico al que debería responder, este fenómeno puede interpretarse como un signo de singularidad de cada una de las etiquetas que participan en el proceso de identificación. Por lo que se propone realizar un estudio¹² para caracterizar este comportamiento físico y natural, por otra parte, de las etiquetas RFID pasivas para la banda de UHF. De tal forma que se pueda establecer si esta característica singular de cada una de ellas puede ser empleada en los procesos de comunicación entre el lector y la etiqueta.

Dado que está probado que distintas etiquetas presentan un BLF distinto y puesto que se desea conocer el alcance y aplicabilidad de este fenómeno, este estudio se ha diseñado para abarcar el caso más restrictivo: caracterizar una única etiqueta. Consiguiendo así que los resultados puedan extrapolarse al resto de etiquetas. Por tanto, el estudio se centra en una etiqueta comercial escogida de entre las más comunes y utilizadas en la industria.

¹² Resultados publicados en *Revista Iberoamericana de Automática e Informática Industrial*, Vol. 17, Núm. 1, pp 76-83, enero de 2020. Edit: CEA. JCR: 1.313-T3 (Automation & Control Systems 46/62).

La obtención del valor de la subportadora que contiene la información que envía la etiqueta (BLF) se realiza directamente mediante la captura y análisis de la señal recibida de la misma. A partir de estos datos, se estudia y analiza la variación de este parámetro a lo largo del tiempo y bajo varios supuestos.

4.5.2.a. Configuración de la medida.

Los valores de BLF se conseguirán gracias a la captura de la señal que proviene de la etiqueta mediante un sistema de adquisición de datos, que analiza la señal recibida y obtiene el valor de este parámetro. En esta ocasión, el equipo de medida empleado y que actúa como lector/analizador, ha sido el sistema *RFID Xplorer*, de CISCO® Semiconductor. El montaje para la medida ha conestado de una antena UHF tipo parche de 5 dBi, un circulator de radiofrecuencia que permite aislar la señal de transmisión de la de recepción y la unidad de adquisición de datos. Para su manejo, basta con conectarla a un puerto USB de un ordenador con capacidad suficiente para ejecutar adecuadamente el programa que recoge y analiza los datos.

Para la realización de las medidas, la etiqueta pasiva se ha colocado a una distancia de 50 cm en línea recta respecto de la antena, de manera que sobre la etiqueta incida la mayor cantidad de radiación posible (Figura 4.32). Todas las medidas se realizan bajo condiciones de espacio libre y a una temperatura de 20°C.

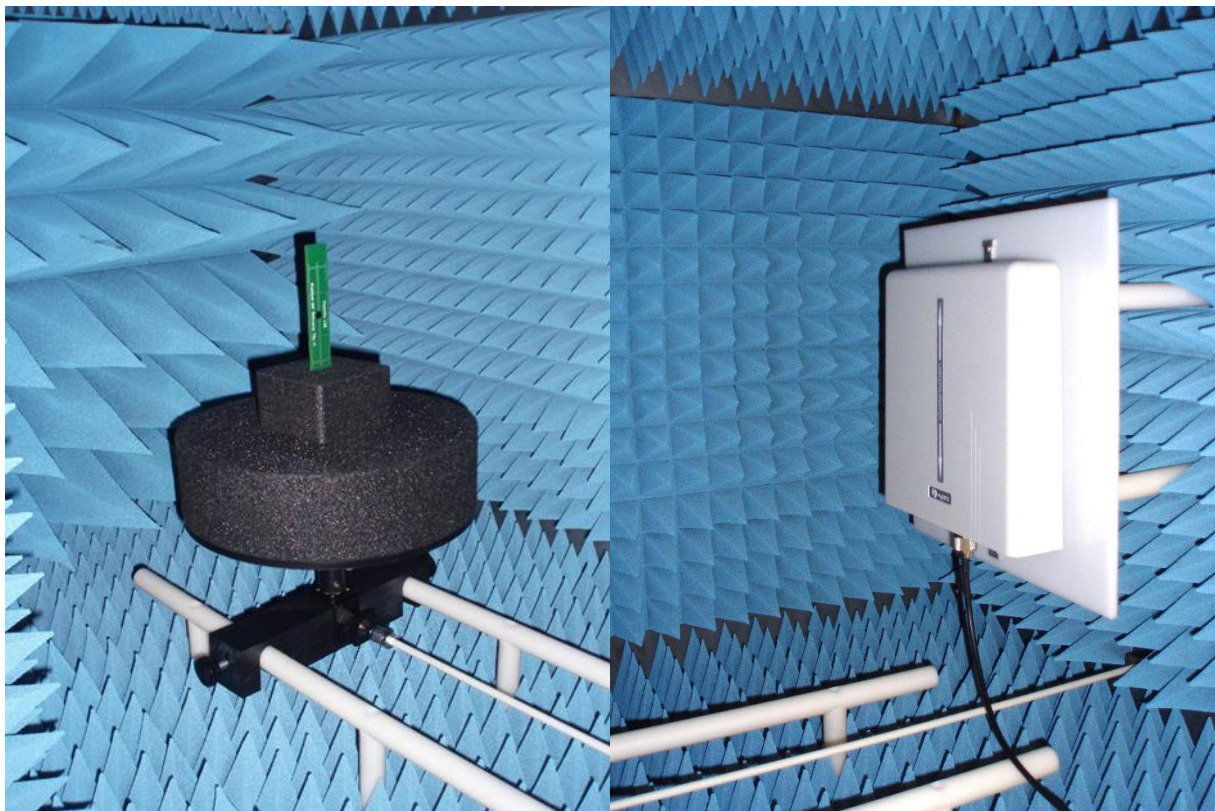


Figura 4.32. Disposición el equipamiento de medida durante las medidas realizadas.

Las medidas se llevan a cabo mediante el lanzamiento de una secuencia de comandos por parte del lector (equipo de medida), que se corresponden con los empleados en un proceso de lectura habitual. Además, dado que el equipo de medida permite escoger la secuencia de comandos a utilizar, se plantea la realización de dos estudios diferentes: uno para caracterizar la variación del valor de BLF de la etiqueta entre distintas respuestas independientes y otro para observar su variación al responder a distintos comandos durante el proceso de retrodispersión, es decir, durante el mismo proceso comunicativo o diálogo establecido con el lector.

Durante todas las medias, el equipo de medida, que actúa como lector, ha sido configurado de modo que emite un preámbulo cuyo parámetro TR_{cal} tiene una duración de $66.656 \mu s$ y el parámetro DR del comando *Query* toma el valor $64/3$. Por lo que teniendo en cuenta la ecuación (4.21), en teoría cabría esperar un valor de BLF de $320,05 \text{ kHz}$ como subportadora de respuesta por parte de la etiqueta en todos los casos.

4.5.2.b. Estudio para respuestas independientes.

Por un lado, se estudia la variación del BLF de la etiqueta para respuestas independientes (*different backscattering*). Es decir, se realizan en distintos momentos, simulando distintos procesos de lectura. Para ello, se lanzan únicamente comandos *Query* y se mide la subportadora en la que la etiqueta ha transmitido los datos de respuesta a este comando. Con el propósito de obtener una muestra representativa del fenómeno, se han realizado 50 repeticiones independientes del proceso. Y cuyos resultados pueden verse en la Figura 4.33, donde se muestra el valor medio, máximo y mínimo de BLF para cada una de las veces que se ha realizado el experimento. El valor medio de BLF de todas las respuestas medidas es $425,43 \text{ kHz}$, siendo los valores máximo y mínimo recogidos $482,21 \text{ kHz}$ y $300,7 \text{ kHz}$, respectivamente.

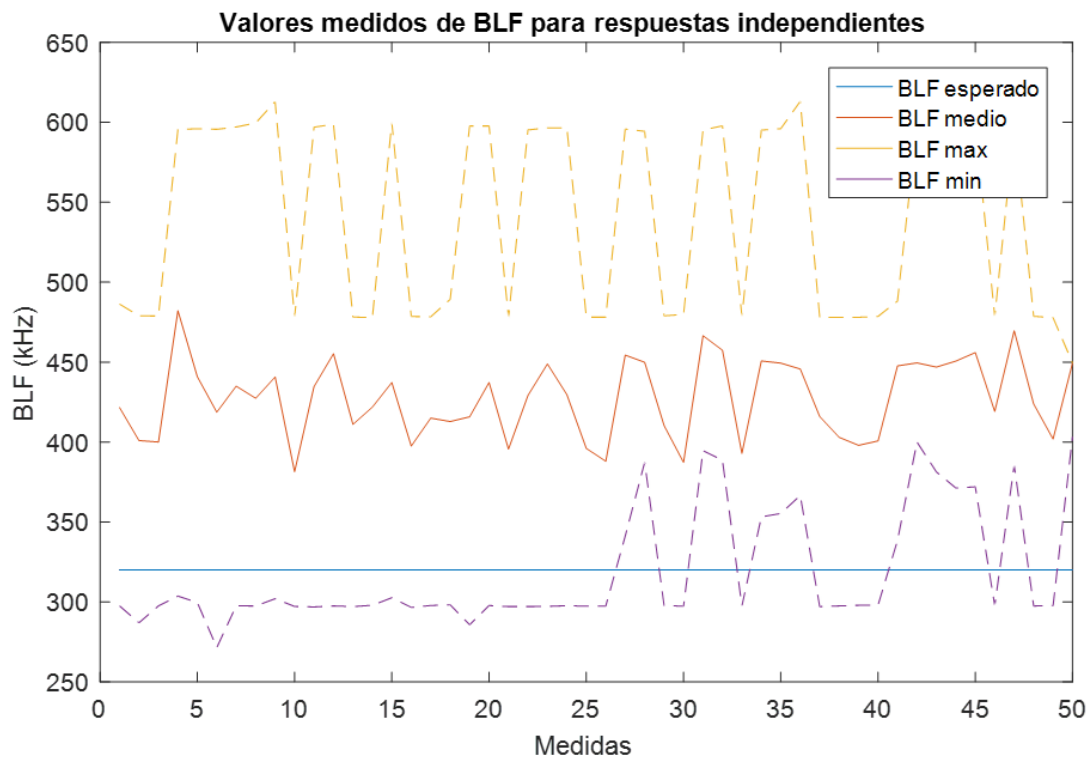


Figura 4.33. Resultados de las medidas para respuestas independientes.

Contrastando los resultados obtenidos con las especificaciones que se supone deben cumplir las etiquetas (recogidas en la Tabla 4.4), se observa como prácticamente en la mayoría de las pruebas realizadas, la subportadora que contiene la información de respuesta de la etiqueta (BLF) excede de la tolerancia admisible ($\pm 22\%$). Por lo que cabe destacar que, desde este punto de vista, la etiqueta no cumple con la especificación *EPC Gen2*.

4.5.2.c. Estudio durante el proceso de retrodispersión.

Por otro lado, se analiza la evolución del BLF entre las distintas respuestas de la etiqueta al lector dentro de un mismo proceso de identificación (*during backscattering*). Para lo que se lanza la secuencia de

comandos que se sucede en un proceso de identificación real: Query – ACK – Req_RN, obteniéndose el valor de BLF para cada una de las respuestas a los comandos anteriores. En este caso, el proceso se ha repetido en 10 ocasiones y los resultados pueden observarse en la Tabla 4.5. Además, se ha añadido en cada fila el margen de tolerancia que recoge la especificación EPC Gen2, que es el intervalo en el que se deben encontrar todos los valores de BLF durante todo el proceso de comunicación. Se puede apreciar cómo este requisito se cumple para la mayoría de los casos.

A la vista de los resultados obtenidos se puede concluir que, aunque la etiqueta no cumple con la especificación EPC Gen2 en cuanto al valor de BLF con el que responde al lector y se aleja del valor esperado considerablemente, este valor se mantiene relativamente estable una vez se ha iniciado la comunicación. Es decir, una vez que la etiqueta es alimentada por la onda del lector y calcula el valor de BLF, éste no sufre prácticamente variaciones durante ese periodo energético.

Tabla 4.5. Variaciones de BLF durante la retrodispersión.

Medida	BLF (kHz) para cada comando			Margen de tolerancia ($\pm 2,5\%$)	
	Query	ACK	Req_RN	Min.	Max.
1	381,05	386,52	400,31*	371,52	390,58
2	409,66	398,91	401,83	399,42	419,90
3	399,63	394,98	390,16	389,64	409,62
4	448,83	446,88	449,74	437,61	460,05
5	450,69	443,73	451,34	439,42	461,96
6	394,03	388,16	396,34	384,18	403,88
7	449,61	453,26	466,09*	438,37	460,85
8	453,45	450,63	450,39	442,11	464,79
9	401,53	394,72	409,89	391,49	411,57
10	399,58	391,81	395,01	389,59	409,57

* fuera de rango.

4.5.3. Análisis y aplicación de los resultados.

Los resultados obtenidos en los experimentos realizados ponen en evidencia las grandes tolerancias existentes en las etiquetas RFID pasivas, debido en parte a su constitución física y los componentes que la forman. Aun así, a pesar de la gran dispersión de los valores de BLF de la etiqueta bajo estudio, el lector ha sido capaz de interpretar la señal reflejada por la etiqueta en todos los casos. Lo que por otro lado demuestra la fiabilidad y robustez de la tecnología RFID.

Una vez caracterizado el comportamiento de este parámetro y puesto de manifiesto que lleva acarreada una gran incertidumbre, cabe preguntarse si esta peculiaridad se podría utilizar para mejorar la usabilidad y funcionamiento de la tecnología RFID pasiva. En este sentido y en línea con los trabajos descritos en el apartado 4.3 del presente documento, dado que una de las principales características obtenidas en el parámetro BLF es la incertidumbre, puede contemplarse la posibilidad de emplear este comportamiento como fuente de aleatoriedad para la generación de números pseudoaleatorios en la etiqueta RFID pasiva.

Comparando la secuencia del valor medio de BLF obtenido para cada una de las medidas realizadas con una secuencia normal de números aleatorios, cuyos parámetros característicos sean la media y la

desviación típica de la secuencia medida, se observa como los resultados obtenidos en las medidas pueden asemejarse a una secuencia de números aleatorios (Figura 4.34). Teniendo en cuenta que el este estudio se ha centrado en el análisis de una única etiqueta y que los valores medidos de BLF serán distintos si realizamos las medidas a otras etiquetas, se añade, si cabe, mayor incertidumbre y aleatoriedad al comportamiento de este parámetro cuantas más etiquetas estén involucradas en un proceso de lectura. Por lo que no parece descabellado emplear esta variación de la BLF de la etiqueta para la obtención de números aleatorios o pseudoaleatorios que ella misma debe generar durante los procesos de comunicación con el lector.

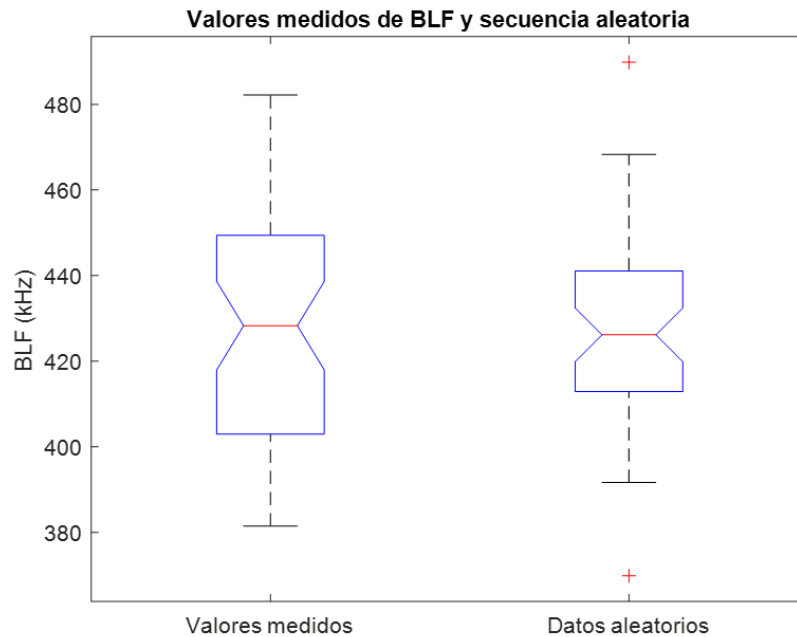


Figura 4.34. Comparación entre los valores medidos de BLF y una secuencia aleatoria de datos.

Conociendo que la etiqueta pasiva de RFID calcula la BLF según la ecuación (4.21). Sabiendo que el DR es un parámetro fijo que puede tomar los valores de 8 y $64/3$. Y que el valor del TR_{cal} se obtiene a partir de la medida que la etiqueta hace sobre el preámbulo de la señal que envía el lector. Si el lector no modifica ninguno de estos parámetros, el resultado de BLF no debería variar. Pero lejos de obtenerse un valor único de BLF en los experimentos realizados, los resultados obtenidos muestran que la etiqueta calcula y responde con distinto BLF cada vez que ésta es interpelada para ello. De donde se desprende que el valor de la subportadora en la que la etiqueta contesta al lector depende directamente de la precisión en la medida del TR_{cal} y en cómo se lleve a cabo el cálculo de la BLF.

Por un lado, el uso de componentes de bajo coste para abaratar el precio de las etiquetas, como un sistema de reloj de baja frecuencia, causa errores en las medidas de los parámetros que el lector envía a las etiquetas y contribuye a la variación en la BLF. Además, estas posibles fuentes de error se ven acentuadas por los procesos de fabricación física de las etiquetas, que introducen mayores incertidumbres [179]. Por otro lado, los procesos de cálculo que lleva a cabo una etiqueta deben ser sencillos, por lo que puede que la precisión con la que se calcula el valor de BLF añada nuevos errores al valor final que se obtiene para este parámetro. En la Figura 4.35 se representan los valores de BLF medidos frente a uno de los casos más desfavorables, como es el supuesto de que la etiqueta únicamente contemple 1 Byte para calcular el valor de BLF (256 valores posibles). En ella se observa como incluso en este caso, la probabilidad de obtener un mismo valor de BLF es muy baja. Además, en caso de mejorarse la precisión en el cálculo (asignando mayor cantidad de bytes para codificar este valor), habrá más valores posibles y la probabilidad de que un valor de BLF se repitiese sería

prácticamente nula. Con lo que se demuestra nuevamente que el valor de BLF que calcula una etiqueta RFID pasiva puede asemejarse a una fuente de aleatoriedad.

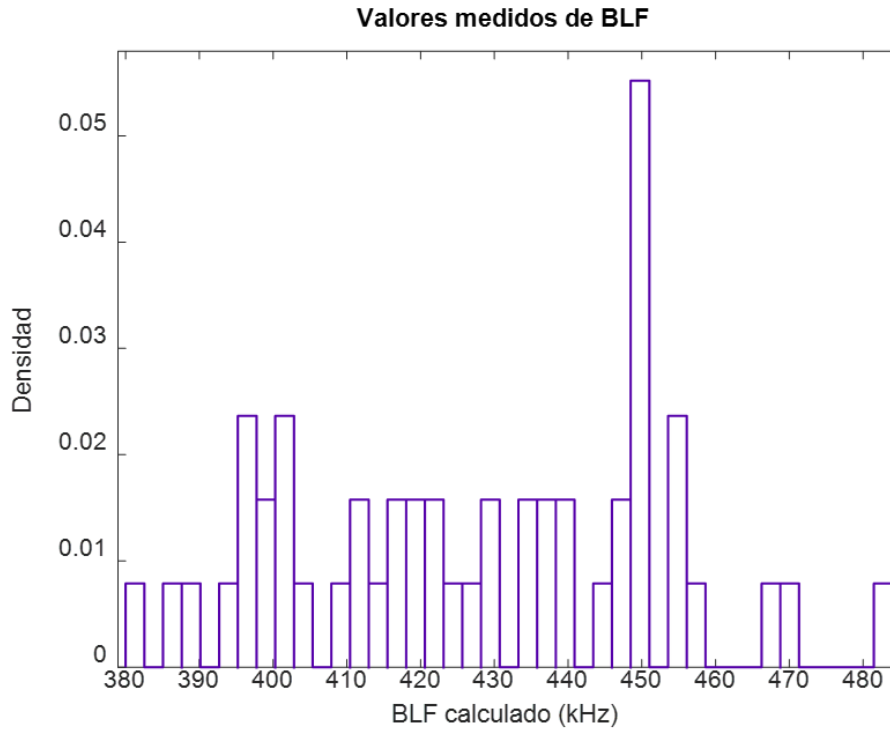


Figura 4.35. Distribución de valores de BLF calculados con una precisión de 1 Byte.

A partir de los valores medidos de BLF y dadas las evidencias anteriormente mencionadas, se ha realizado una ligera transformación mediante operaciones sencillas para tratar de obtener una secuencia de números que se asemeje a una secuencia de aleatoria o pseudoaleatoria de números en un determinado rango de interés. Esta sencilla transformación persigue el objetivo de comprobar si la variación del parámetro BLF, que a priori no sería buena, es apta para emplearse en otros ámbitos, como en los protocolos de comunicación entre etiqueta pasiva de UHF y lector RFID. Además, cabe tener en cuenta que el hecho de emplear operaciones sencillas responde al objetivo de minimizar en la medida de lo posible las operaciones lógicas que se deban realizar en las etiquetas, para que su potencial pueda ser aprovechado en otras nuevas funcionalidades.

En primer lugar, se obtiene la desviación de los valores de BLF medidos (BLF_{medido}) respecto al valor teórico esperado (BLF_{esp}), tal y como se muestra en la ecuación (4.23).

$$BLF_{diff} = BLF_{medido} - BLF_{esp} \quad (4.23)$$

Dado que todos los valores de BLF_{diff} se encuentran en el rango de unos 100 kHz. Y teniendo en cuenta que las etiquetas deben ser capaces de generar números aleatorios de 16 bits. Se escala y normaliza el valor de BLF_{diff} obtenido al rango $[0, 2^{16}]$ según se describe en la ecuación (4.24). Los resultados de esta transformación junto con una secuencia de valores aleatorios de una distribución discreta uniforme se presentan en la Figura 4.36. En ella se observa como la secuencia de números obtenida se puede asemejar a una secuencia de números aleatorios de 16 bits.

$$BLF_{NORM} = \frac{BLF_{diff} - \min(BLF_{diff})}{\max(BLF_{diff}) - \min(BLF_{diff})} \cdot 2^{16} \quad (4.24)$$

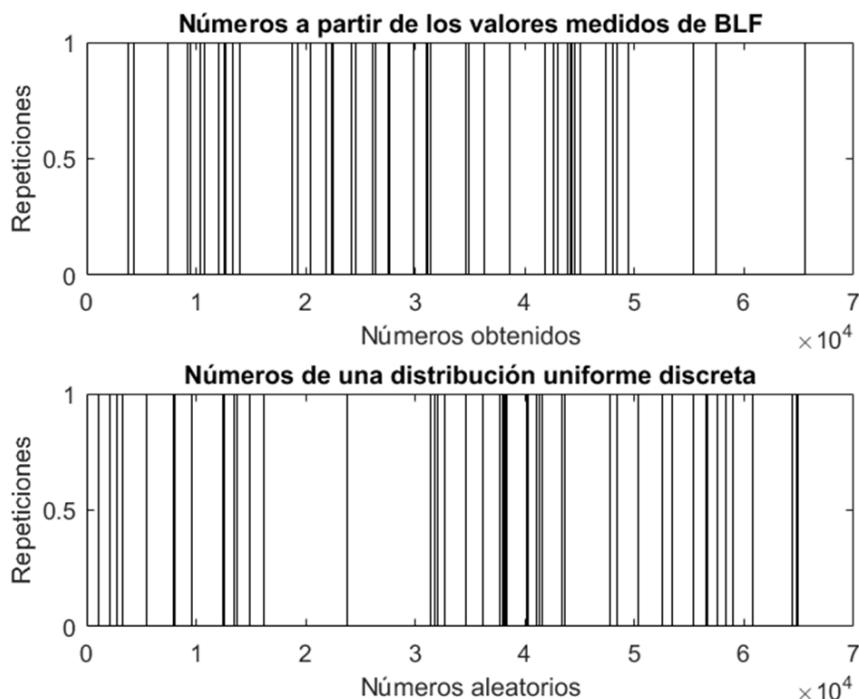


Figura 4.36. Comparación entre los valores obtenidos de BLF_{NORM} y una secuencia de números aleatorios.

A la vista de los resultados anteriores, se ha estudiado la aleatoriedad de las secuencias de números obtenidos mediante los mismos test estadísticos que los empleados en la sección 4.3.3. Concretamente, el estudio se ha realizado para la secuencia correspondiente a la diferencia entre el valor de BLF medido y el valor teórico esperado (BLF_{diff}). Así como para la misma secuencia normalizada por el procedimiento descrito anteriormente (BLF_{NORM}). En la Tabla 4.6 se muestran los resultados de pruebas estadísticas realizadas. En ella se observa como la secuencia modificada mediante operaciones sencillas (secuencia normalizada) pasa casi satisfactoriamente la mayoría de los test, mientras que la secuencia obtenida directamente a partir de los valores medidos presenta dificultades considerables en ciertos test.

Tabla 4.6. Resultados de las pruebas de aleatoriedad a las secuencias de BLF.

TEST	RESULTADOS ESTADÍSTICOS		
	BLF_{diff}	BLF_{NORM}	Intervalo de validación
χ^2	16.4*	13.8	[4.1682, 14.6837]
Series	4.0816	3.3061*	[3.4895, 13.3613]
Huecos	1.7247	4.8313*	[0.21072, 4.6052]
Rachas crecientes y decrecientes (χ^2)	0.10971	0.80294	[0.015971, 2.7055]
Longitud de las rachas	0	-1.025	[-1.96, 1.96]
Rachas sobre y bajo la media (χ^2)	10.6557*	0.58862	[0.015971, 2.7055]
Longitud de las rachas	2.2531*	0.18985	[-1.96, 1.96]

* fuera de rango.

Los resultados obtenidos en estos últimos test de aleatoriedad evidencian que las secuencias de números analizadas, a partir de los valores BLF normalizado, pueden asemejarse a secuencias de números pseudoaleatorios generadas por etiquetas RFID pasivas comerciales. Por lo que, dado el caso, podría utilizarse el valor de BLF como semilla en los algoritmos de generación de números pseudoaleatorios de las etiquetas, o incluso utilizar directamente el valor de BLF. Además, dado que

este parámetro varía durante el proceso de comunicación con el lector, tal y como ha quedado demostrado, puede emplearse como fuente de aleatoriedad para tareas más complejas que tienen lugar entre la etiqueta y el lector, como la criptografía.

4.6. Discusión de resultados y sus aplicaciones.

A tenor de los trabajos desarrollados en torno al protocolo de comunicación entre lectores y etiquetas de RFID pasivas para la banda de UHF, así como del análisis de los distintos resultados obtenidos, se posibilita la elaboración fundamentada de determinadas propuestas encaminadas a contribuir en la mejora del funcionamiento y en el uso de la tecnología RFID¹³. En este sentido, se pueden proponer variaciones que hagan los protocolos de comunicación entre la etiqueta pasiva y el lector de RFID más seguros y eficientes.

Puesto que los algoritmos para la implementación de los generadores de números pseudoaleatorios suponen una gran parte del peso de la lógica utilizada en las etiquetas RFID pasivas y en vista de los resultados obtenidos, podría reconsiderarse la necesidad de emplear un generador robusto de números pseudoaleatorios de alta calidad en las etiquetas pasivas. Posiblemente esta función debería ser asumida por otro mecanismo más ligero, lo que simplificaría considerablemente la lógica interna de las etiquetas. En este sentido, el algoritmo ultraligero propuesto se erige como una opción plausible para ello. Además, cabe la posibilidad de sustituir el parámetro Q, que quizás en ciertas ocasiones pueda no proporcionar suficiente variabilidad durante los procesos de lectura, por otro valor. A tal efecto, una buena alternativa sería emplear las variaciones que presenta el parámetro BLF que, tal y como se ha comprobado, presentan un comportamiento bastante aleatorio.

La sustitución de los PRNG en las etiquetas RFID pasivas debe ser reconsiderada a la vista del comportamiento no exhaustivamente aleatorio de las secuencias analizadas, especialmente en el caso de etiquetas comerciales. Propuesta que toma mayor relevancia cuando se considera que su uso mayoritariamente es para la realización de operaciones simples, como es el caso de la obtención del número UID requerido por las etiquetas en el proceso de identificación.

Además, cabe señalar que la razón principal por la que actualmente las etiquetas no incluyen cifrado es por el consumo energético de los algoritmos necesarios. Al reducir el consumo de energía del PRNG, el aumento de la capacidad de la etiqueta puede utilizarse para mejorar los niveles de seguridad e integridad de los datos que se transmiten. Aunque para ello, siempre se ha de tener en cuenta que las técnicas de seguridad y los procesos de cifrado también requieren el uso de un PRNG.

La inclusión de mecanismos de seguridad y operaciones que requieran un mayor procesamiento de la información en las etiquetas contribuye a atajar algunos de los problemas que se le han venido atribuyendo a esta tecnología, como son la privacidad y la autenticidad de las comunicaciones. Mientras que el primer término se refiere al problema de que haya lectores maliciosos que capturen la información de cualquier etiqueta, la autenticación hace referencia a que cualquier lector puede recoger información errónea procedente de etiquetas malintencionadas, especialmente las falsificadas. Para evitar este tipo de problemas y gracias a las propuestas que surgen a partir de los resultados de los trabajos realizados, se puede considerar la implementación de soluciones basadas en: autenticación simétrica mutua, en la que ambos extremos conocen y comparten una clave secreta; autenticación

¹³ Resultados parciales presentados en la VII Jornada de Investigación de la Escuela de Ingeniería Minera e Industrial de Almadén (Universidad de Castilla – La Mancha. 27 de septiembre de 2018).

mediante claves derivadas, en la que cada uno de los dispositivos posee una clave distinta privada y la información se comparte con claves derivadas de las privadas, que actúan como llave para acceder al contenido de los mensajes; o transferencia cifrada de mensajes, donde los datos se transforman en datos cifrados aplicando una clave secreta y un algoritmo secreto. De esta forma se protege la información frente a posibles atacantes externos, tanto pasivos (que intentan espiar las comunicaciones para descubrir información confidencial con fines ilícitos), como activos (que manipulan las comunicaciones para modificarlas en su propio beneficio). Siendo, además, una de las preocupaciones derivadas de la implantación de la IoT y todas las tecnologías implicadas [180].

En cuanto a los resultados que se desprenden de la caracterización de la BLF, la fuerte desviación respecto al valor teórico de BLF al que debería contestar la etiqueta, puede ser una evidencia de las grandes tolerancias que presentan los elementos físicos que se encuentran en las mismas. Hecho que puede ser debido, en parte, al imperativo que marca el mercado de lograr etiquetas RFID pasivas lo más baratas posibles. En contrapartida para la tecnología, esto supone que al no cumplirse fielmente todas las especificaciones se puedan producir errores de funcionamiento. Y que, en última instancia, causan fallos de lectura y que algunas etiquetas RFID pasivas no sean correctamente identificadas.

En cambio, se plantea la posibilidad de emplear en positivo estas grandes tolerancias e incertidumbres encontradas en las etiquetas como fuentes de aleatoriedad (semilla) para su aplicación en otros procesos que la etiqueta pasiva de RFID tiene que llevar a cabo. Además, en el caso concreto del parámetro BLF, se ha puesto de manifiesto cómo puede emplearse como fuente de aleatoriedad para su uso en las comunicaciones entre la etiqueta y el lector. E incluso para ciertas aplicaciones, podría ser suficiente con emplear esta característica aleatoria del parámetro BLF y eliminar el generador de números pseudoaleatorios de la etiqueta. Lo que simplificaría enormemente la circuitería lógica del chip. Aunque en contrapartida, también se estarían limitando las funcionalidades de la etiqueta.

Cabe resaltar que el tipo de etiqueta que se ha empleado para el estudio no cumple con la especificación EPC Gen2, en cuanto a que la etiqueta responde a una frecuencia bastante superior al valor que teóricamente debería responder, de acuerdo con los parámetros iniciales marcados por el lector al comienzo del ciclo de lectura. Se ha de tener en cuenta que para el estudio se ha escogido uno de los modelos de etiqueta más empleado actualmente en el mercado, por lo que de este estudio se desprende la evidencia de que las etiquetas comerciales no cumplen con la especificación que se supone deberían cumplir. A priori, los resultados de caracterización de la BLF podrían extrapolarse al resto de etiquetas RFID pasivas, dado que todas ellas se producen en masa y con los mismos componentes. Si bien los valores concretos de BLF serán distintos, lo que no cambiará será su comportamiento a lo largo del tiempo, puesto que todas las etiquetas funcionan igual. No obstante, se podría ampliar el mismo estudio para respuestas independientes con otras etiquetas, lo que permitiría obtener una comparación de resultados entre distintas etiquetas. Así como estudiar también la variación de la BLF durante el mismo proceso de lectura (*backscattering*) para un mayor número de comandos.

En cualquier caso, puede resultar bastante interesante un estudio más profundo de este fenómeno, ya que cada etiqueta responde con valor de subportadora ligeramente distinta. Lo cual, puede entenderse como una característica diferenciadora de cada una de las etiquetas que pueden estar presentes en el área de cobertura de un lector de RFID. Además, dado que también se producen variaciones (aunque de menor magnitud), durante las respuestas a los distintos comandos de un mismo proceso de identificación, también podrían emplearse éstas como semilla para procesos de seguridad y criptografía durante la comunicación entre etiqueta y lector.

En este sentido, se puede contemplar la posibilidad de realizar alguna modificación en los valores de *TRcal* medido en las etiquetas para que los valores de BLF resultantes se adecúen mejor a las exigencias

de aleatoriedad que deben cumplir este tipo de fuentes, según las características recogidas en la especificación EPC Gen2. De tal forma que puedan ser directamente utilizados como fuente pseudoaleatoria, evitando complicar en exceso la lógica interna de las etiquetas.

En definitiva, al emplear la variación de la BLF para otros fines o al sustituir el generador de números pseudoaleatorios por otro mecanismo más ligero, se persigue conseguir etiquetas pasivas más eficientes. Es decir, que posean las mismas funcionalidades, pero minimizando su carga computacional y sacándole el máximo provecho posible a los recursos que ellas mismas ya poseen. De este modo se contribuye a un ahorro de energía por parte de la etiqueta pasiva para realizar sus funciones. Por lo que este nuevo excedente de energía que se crea puede ser aprovechado para llevar a cabo nuevas tareas, como las relacionadas con la seguridad y que a esta tecnología se le están demandando. O visto desde otro punto de vista, al precisar de menos cantidad de energía para funcionar, los lectores serían capaces de detectar etiquetas que se sitúen más lejos de lo que lo hacen en la actualidad.

En este sentido se propone la creación de dos clases de etiquetas RFID pasivas para la banda de UHF: etiquetas de clase robusta y etiquetas de clase ligera. Si bien ambos tipos de etiquetas deben cumplir con todos los requisitos establecidos en los protocolos de comunicación para asegurar la compatibilidad entre lectores y etiquetas de RFID ya existentes.

Por un lado, si un nuevo mecanismo puede sustituir a los generadores de números pseudoaleatorios existentes, ofreciendo mejores características en términos de eficiencia y fácil implementación, aparecería un nuevo tipo de etiquetas simplificadas, denominadas etiquetas de clase ligera o *light-class labels*. Por lo tanto, el proceso de fabricación de estas se simplificaría y, por consiguiente, los costes de este tipo de etiquetas se reducirían considerablemente. Estas etiquetas ligeras podrían emplearse en aplicaciones que no requieran de grandes prestaciones, como es el caso de los procesos de identificación, que son la mayoría de las tareas en las que se utiliza la tecnología RFID. Además, esta clase de etiquetas sería ampliamente utilizada por multitud de sectores a nivel mundial, ya que, con una diminuta inversión, se dotaría a los objetos que identifiquen de todo el valor añadido que proporciona el uso de esta tecnología, como pasar a formar parte del IoT.

Por otro lado, se encontrarían las etiquetas de clase robusta o *strong-class labels*. Este tipo se asemejaría a las etiquetas empleadas actualmente, aunque asegurando que, al menos, se cumple con todas las especificaciones y requerimientos recogidos en los protocolos de comunicación. Para ello, se emplearían componentes de mayor calidad para su fabricación e incluso se podrían añadir nuevas funcionalidades que compliquen la circuitería del chip, a pesar de que esto supondría un incremento en el precio final de las etiquetas de esta clase. Podrían emplearse en aplicaciones en las que a la etiqueta se le requiera gran carga computacional, como podría ser el cifrado de todos los datos que contenga el banco de memoria o la encriptación de todas las comunicaciones. Por lo que esta clase de etiquetas estaría más orientada a aplicaciones más específicas, donde la inversión necesaria para la adquisición de las etiquetas seguiría siendo diminuta en comparación con el valor del objeto al que identifican. Por ejemplo, una etiqueta pasiva que incluya todo el historial médico de un paciente deberá cumplir con unas fuertes exigencias de seguridad, debido a la sensibilidad de la información que almacena.

Con la propuesta de estas dos clases de etiquetas pasivas de RFID se pretende contribuir al impulso definitivo que necesita la tecnología para ser acogida por todos los usuarios como una tecnología fiable y que aporta valor añadido a todos los productos asociados a cada etiqueta.

Capítulo 5.

Conclusiones.

A pesar de ser una tecnología relativamente joven, la identificación por radiofrecuencia (RFID) ha experimentado un gran desarrollo y una rápida evolución durante los últimos años. Prueba de ello es que algunos de sus avances han emergido con tanta fuerza que se han convertido en tecnologías con entidad propia, como las redes inalámbricas de sensores y todas sus variantes.

Con la realización de esta tesis se pone en valor el potencial de esta tecnología como clave para la adecuada implantación global del Internet de las Cosas. Se ha comprobado que aún queda camino por recorrer y la tecnología aún tiene nichos por explorar, quedando constatado que lejos de estar obsoleta o haber pasado de moda, la tecnología RFID está más viva que nunca.

Por su parte, los resultados de los trabajos desarrollados arrojan nuevas oportunidades en cuanto al funcionamiento y uso de la tecnología RFID, colaborando y contribuyendo también en su mejora y, en última instancia, a que esta tecnología sea adoptada de forma masiva en todo el mundo.

5.1. Trabajos realizados y resultados obtenidos.

A partir del estudio pormenorizado del funcionamiento del protocolo de comunicaciones aéreas entre lectores y etiquetas pasivas de RFID, para la banda de UHF, ha sido posible el desarrollo de trabajos y realización de propuestas encaminadas a contribuir en la mejora del funcionamiento y el uso de esta tecnología.

Desde la simple identificación de objetos a través de señales de radiofrecuencia, la tecnología ha experimentado una continua evolución y crecimiento. La incorporación de sensores a las etiquetas, inicialmente pasivas, para obtener alguna información adicional, ha permitido el surgimiento de las redes inalámbricas de sensores (WSN) como una tecnología con entidad propia. A partir de la que derivan otras como las WSN y las WBAN, ampliando el catálogo de servicios que este tipo de redes pueden prestar. Ejemplos de ello han sido los estudios y desarrollos realizados en este campo, poniendo especial énfasis en las comunicaciones de estas tecnologías. Como el sistema de monitorización del consumo eléctrico real de maquinaria o el sistema inteligente para el uso eficiente de la energía, que contribuyen a la eficiencia energética y optimizan la utilización de los recursos energéticos disponibles en cada momento. O el sistema de seguridad activa para la monitorización de personas, que incrementa notablemente la seguridad física de las personas y resulta especialmente útil en situaciones de riesgo.

El uso de este tipo de tecnologías y aplicaciones ha propiciado la aparición del Internet de las Cosas (Internet of Things, IoT). Este paradigma va a modificar notablemente la forma actual de trabajar y hacer las cosas cambiando la realidad por completo, empleando la tecnología para que los procesos se realicen con mayor control y calidad. Como ocurre, por ejemplo, con el sistema automático de monitorización y seguimiento de muestras descrito.

Además, estos desarrollos han servido para poner de manifiesto la importancia y utilidad de la identificación automática de las cosas. A partir de la cual surge toda una serie de datos e información que conforman un conjunto de características de valor añadido a los productos y objetos asociados, que son proporcionadas por el uso de las distintas tecnologías implicadas. De entre las que cabe destacar la RFID (Identificación por Radiofrecuencia), como la tecnología para la identificación rápida y automática por excelencia, siendo clave para la implantación masiva del Internet de las Cosas (IoT) a nivel mundial.

Pero para poder llevar a cabo una instalación exitosa de los sistemas RFID se debe, por un lado, conocer a fondo la tecnología; y por otro, saber cómo se comportarán estos sistemas en los entornos en los que operan. En esta línea se ha desarrollado y construido un sistema de medida para la caracterización electromagnética de materiales y soluciones constructivas, que contribuye a averiguar el comportamiento real de la señal de radiofrecuencia cuando incide sobre una determinada superficie, estableciendo qué cantidad de energía es reflejada o qué porción de señal la atraviesa. Lo que permite tanto a instaladores como usuarios actuar en consecuencia para lograr el funcionamiento óptimo de la tecnología RFID u otras similares que utilicen el mismo medio de propagación.

Según la especificación EPC Gen2, ampliamente adoptada por la industria a nivel mundial para el uso de tecnología RFID, las etiquetas comerciales pasivas de RFID para la banda de UHF necesitan implementar un generador de números pseudoaleatorios. Debido a la relevancia de estos números para el funcionamiento correcto del protocolo de comunicación y, por tanto, de esta tecnología (especialmente en el proceso de identificación), es crucial asegurar la precisión y buenas prestaciones del mecanismo generador.

Se han obtenido valores de números pseudoaleatorios de etiquetas reales y la mayoría de las secuencias de números pseudoaleatorios analizadas satisfacen adecuadamente las pruebas de aleatoriedad realizadas. Lo cual permite concluir que los generadores que están siendo utilizados en etiquetas RFID comerciales tienen unas prestaciones adecuadas. Pero los resultados también evidencian que esos generadores no serían apropiados en caso de utilidades más exigentes y que requieren mayores prestaciones, como operaciones relacionadas con la seguridad y privacidad de la información. Por lo que se puede concluir que los resultados obtenidos en algunas de las pruebas ponen de manifiesto unas prestaciones de los generadores de números pseudoaleatorios implementados en las etiquetas inferiores a lo esperado.

En esta línea se propone un algoritmo ultraligero para la generación de números pseudoaleatorios que puede ser una alternativa al mecanismo que actualmente se implementa en las etiquetas RFID-UHF comerciales. Como se ha demostrado, la propuesta cumple con los requisitos de la especificación EPC Gen2, reduce sustancialmente la complejidad lógica del chip de la etiqueta y supone una menor carga computacional, ya que únicamente requiere de varias funciones lógicas livianas y algunas operaciones de acceso a la memoria para ser implementada en una solución ASIC (Application-Specific Integrated Circuit, Circuito Integrado de Aplicación Específica).

La utilización del algoritmo propuesto implica que la etiqueta necesita un menor tiempo para calcular su respuesta, por lo que el proceso de identificación podría realizarse de forma más rápida. Pudiéndose aprovechar ese tiempo sobrante para realizar otras tareas o para añadir nuevas funcionalidades a la etiqueta.

Además, las etiquetas que utilicen este método necesitarán capturar menos energía de la onda portadora para su funcionamiento. Con lo que también podrán utilizar la energía excedente para mejorar su alcance, provocando que los lectores vean incrementada su área efectiva de cobertura. O bien, para realizar nuevas operaciones que actualmente no pueden llevar a cabo, como las relacionadas con la seguridad y la encriptación de la información.

En cualquier caso, la utilización del método propuesto puede suponer una mejora apreciable en las prestaciones de las etiquetas. Lo que también ha sido comprobado gracias a la implementación de la propuesta en el emulador físico de etiquetas pasivas, que ha sido desarrollado y que se comporta e interactúa con el lector como una etiqueta pasiva real. Además, este emulador se presenta como una solución de bajo coste abierta, flexible y reconfigurable, que es fácilmente adaptable a cualquier tipo de prueba relacionada con las comunicaciones o con el funcionamiento de la propia etiqueta. Permite observar y controlar los parámetros internos de la etiqueta, así como todos los flujos de datos que suceden durante los procesos de comunicación, obteniéndose resultados reales de las pruebas en las que se emplee el emulador y sin necesidad de desarrollar chips ad-hoc de etiquetas UHF pasivas reales.

De entre los muchos aspectos que entran en juego durante las comunicaciones entre lectores y etiquetas pasivas de RFID, ha llamado la atención el hecho probado de que cada etiqueta responde al lector con una velocidad de transmisión de datos distinta a la esperada. En base a lo que se ha llevado a cabo un estudio para caracterizar el comportamiento de la BLF (Backscatter-Link Frequency), o subportadora de respuesta de una etiqueta RFID pasiva, a lo largo del tiempo.

Los resultados muestran una fuerte desviación respecto al valor teórico al cual la etiqueta debería responder cada vez que ésta es interpelada por el lector. Incluso sobrepasando en algunos casos los límites marcados al respecto por las especificaciones. Lo que evidencia que las etiquetas comerciales tampoco cumplen con el protocolo de comunicaciones en este extremo. En cambio, una vez establecido el enlace e iniciado el diálogo entre lector y etiqueta, el valor de la BLF permanece relativamente estable, produciéndose también ligeras variaciones aleatorias, aunque de mucha menor magnitud que las anteriores. Además, ha quedado demostrado que esta variación tiene un comportamiento altamente aleatorio en todos los casos. Por lo que se plantea la posibilidad de utilizar este comportamiento como fuente de aleatoriedad para su uso en los protocolos de comunicación. Abriendo la puerta a implementar nuevas funcionalidades en las etiquetas y empleando unos recursos de los que ya disponen.

Gracias a las propuestas realizadas, la capacidad liberada en la etiqueta en términos de proporción del circuito utilizado y de la energía necesaria para funcionar, puede ser utilizada en la implementación de prestaciones adicionales. Esto incluiría la incorporación en las etiquetas de protocolos de autenticación y operaciones que impliquen niveles de seguridad mejorados, como es el caso del encriptado de la información. Lo cual requiere de unas altas capacidades de aleatoriedad, incluso mejores que las proporcionadas por los generadores que se utilizan actualmente. Sin embargo, el método ultraligero propuesto para la generación de números pseudoaleatorios podría alcanzar las prestaciones necesarias con la utilización propuesta del parámetro BLF en el algoritmo de generación descrito. Además, para este proceso de encriptado se cuenta también con la ventaja adicional de que el parámetro BLF, que como se ha visto tiene una componente aleatoria, adquiere un valor que varía en cada sesión de lectura pero que es conocido durante cada intercambio de información tanto por la etiqueta como por el lector.

Con todo ello, se ha pretendido contribuir a la evolución y el desarrollo de las distintas tecnologías con las que se ha trabajado para, en definitiva, impulsar la implantación masiva del IoT. Específicamente, se ha dado un mayor peso a la tecnología RFID, sin la que sería inviable que el IoT se convierta en una realidad global.

5.2. Aportaciones.

Del conjunto de resultados que se han ido obteniendo de cada uno de los trabajos desarrollados durante esta tesis, han ido surgiendo y tomando forma diversas contribuciones constatables que perdurarán en el tiempo y podrán ser empleadas para seguir trabajando y avanzando en la evolución de la tecnología RFID y el IoT. Todas y cada una de las aportaciones de esta tesis han contribuido a alcanzar con creces los objetivos planteados en su inicio.

En el ámbito de las WSN se encuentran la red inalámbrica de sensores creada para monitorizar el consumo energético real de la electricidad, la red inalámbrica de sensores y actuadores empleada para controlar y gestionar el uso de los recursos energéticos disponibles en cada momento, la red de seguridad activa para la monitorización de personas y los módulos cosechadores de energía. Aparte de ser herramientas útiles para las aplicaciones para las que han sido desarrolladas en todos los casos, estos equipos también sirven como plataformas de pruebas para futuros trabajos y/o usos.

Aterrizando en el mundo de las comunicaciones de los sistemas RFID pasivos, se dispone de un completo sistema de medida, específicamente diseñado y construido, para la caracterización electromagnética de materiales y soluciones constructivas a escala real totalmente operativo que permite obtener información sobre el comportamiento de las señales de radiofrecuencia al interactuar con ellos. Además, este sistema permite ampliar sus prestaciones para que sus resultados puedan aplicarse a diversas tecnologías que utilicen la radiofrecuencia.

En el campo de los protocolos de comunicación entre lectores y etiquetas RFID UHF pasivas, dada la relevancia de los números pseudoaleatorios para el buen funcionamiento de los mismos, se encuentra la propuesta de un novedoso algoritmo ultraligero para la generación de números pseudoaleatorios, que cumple con las especificaciones actualmente vigentes en este ámbito y supone una reducción de la carga computacional de las etiquetas. En este sentido, se propone la sustitución de los generadores de números pseudoaleatorios actuales por la propuesta realizada. De tal forma que las etiquetas que la implementen verían reducida la complejidad lógica de su chip y necesitarían menos energía para su funcionamiento. Por lo que los lectores mejorarían su alcance sin ningún cambio ni esfuerzo por su parte.

Además, gracias a la caracterización de la BLF como una novedosa fuente de aleatoriedad de las etiquetas, se abre la posibilidad de plantear cambios y mejoras de los protocolos de comunicación, protegiendo la información frente a posibles amenazas, así como de implementar nuevas funcionalidades en las etiquetas empleando los recursos de los que ya disponen en la actualidad.

También, en este ámbito, se dispone de una plataforma altamente flexible y reconfigurable, específicamente diseñada y desarrollada, totalmente operativa que emula el comportamiento de una etiqueta pasiva real y que puede ser empleada para la realización de cualquier tipo de pruebas en las que estén involucradas etiquetas pasivas de RFID-UHF, de las que se obtendrán datos reales de funcionamiento.

Por último, se propone la creación de dos clases distintas de etiquetas RFID pasivas para la banda de UHF: unas etiquetas de clase ligera (*light-class labels*), gracias a la incorporación de las propuestas realizadas en este ámbito y que suponen una simplificación respecto a las actuales, pero manteniendo su funcionalidad y orientadas a ser usadas a gran escala en labores meramente de identificación; y unas etiquetas de clase robusta (*strong-class labels*), con más cantidad de recursos para incorporar nuevas funcionalidades que requieran mayor carga computacional y orientadas a aplicaciones específicas.

Por otro lado, prestando atención a la producción científica también se hallan una serie de publicaciones, comunicaciones orales y contribuciones, que se han ido elaborando y publicando durante la realización de la tesis y que se agrupan en los siguientes apartados:

REVISTAS CIENTÍFICAS INDEXADAS:

- **Blanco, J.;** García, A.; Cañas, V. “Análisis y Caracterización de la Frecuencia de Enlace por Retro-dispersión en Sistemas UHF-RFID Pasivos”. Revista Iberoamericana de Automática e Informática Industrial, Vol. 17, Núm. 1, pp 76-83, enero de 2020. Edit: CEA. e-ISSN 1697-7920. DOI: 10.4995/riai.2019.11115.
- **Blanco, J.;** García, A.; Cañas, V. “Analysis and improvements of the pseudorandom number generation in passive UHF-RFID tags”. Future Generation Computer Systems, Vol. 99, pp 115-123, octubre de 2019. Edit: Elsevier. ISSN 0167-739X. DOI: 10.1016/j.future.2019.04.021.
- Quintana, S.; Blas, J.M.; Peña, J.; **Blanco, J.;** García, L.D.; Pastor, J.M. “Design and Operation of a Real-Scale Electromagnetic Shielding Evaluation System for Reinforced Composite Construction Materials”. Journal of Materials in Civil Engineering, Vol. 30, Issue 8, agosto de 2018. Edit. ASCE. ISSN: 0899-1561. DOI: 10.1061/(ASCE)MT.1943-5533.0002323.
- **Blanco, J.;** García, A.; de las Morenas, J. “Design and Implementation of a Wireless Sensor and Actuator Network to Support the Intelligent Control of Efficient Energy Usage” Sensors, 18(6), 1892, Junio de 2018. Edit. MDPI. EISSN: 1424-8220. DOI: 10.3390/s18061892.
- De las Morenas, J.; García, A.; **Blanco, J.** "Prototype Traceability System for the Dairy Industry". Computers and Electronics in Agriculture, Vol. 101, pp. 34-41, febrero de 2014. Edit. Elsevier. ISSN: 0168-1699. DOI: 10.1016/j.compag.2013.12.011.

CONGRESOS INTERNACIONALES:

- **Blanco, J.;** García, A.; Pastor, J.M.; Cañas, V. “A multi-purpose UHF RFID Tag Emulator for Communication Protocols Testing”. Smart SysTech 2017: European Conference on Smart Systems and Technologies, 20-21 de junio de 2017, Múnich (Alemania). ISSN: 0932-6022. ISBN: 978-3-8007-4428-2.
- **Blanco, J.;** Pastor, J. M.; García, A. “Improvements and Applications of RFID Technology as a key factor for the Smart Automation”. RFID-Anwendertag 2016: AutoID – Basis für Industrie 4.0, RFID-Anwenderzentrum München, 18 de noviembre de 2016, Garching (Alemania).
- García, A.; De la Vara, J.A.; **Blanco, J.;** Sánchez-Crespo, S.; Molina, A. "TRAZALE: Un sistema de monitorización para muestras de leche en Castilla-La Mancha. I.- Seguimiento y transporte mediante RFID". SEOC 2016 XLI Congreso Nacional y XVII Congreso Internacional de la Sociedad Española de Ovinotecnia y Caprinotecnia. 14-16 de septiembre de 2016, Talavera de la Reina (España). ISBN: 978-84-608-8680-8.
- **Blanco, J.;** García, A.; Pastor, J.M.; Cañas, V.J.; de las Morenas, J. “Ultra-lightweight Algorithm for Generating Pseudo-random Number Sequences in Passive UHF-RFID Tags”. Smart SysTech 2016: European Conference on Smart Systems and Technologies, 7-8 de junio de 2016, Duisburg (Alemania). ISSN: 0932-6022. ISBN: 978-3-8007-4229-5.

- **Blanco, J.**; García, A.; de las Morenas, J. "Smart Management System for an Efficient Energy Use". Energy and Environment Knowledge Week International Congress, 30 - 31 de octubre de 2014, Toledo (España). ISBN: 978-84-607-1162-0.
- **Blanco, J.**; García, A.; de las Morenas, J. "Safety Wristband for Active Security Network", Smart SysTech 2014: 10th European Conference on Smart Systems and Technologies, 1 - 2 de julio de 2014, Dortmund (Alemania). ISBN: 978-3-8007-3626-3. ISSN: 0932-6022.
- Zangróniz, R.; García-Higuera, A.; **Blanco, J.**; de las Morenas, J. "Low-Cost Wireless System for Measuring Energy Efficiency in Industry", Smart SysTech 2013: 9th European Conference on Smart Systems and Technologies, 11 - 12 de junio de 2013, Erlangen/Nuremberg (Alemania). ISBN: 978-3-8007-3521-1. ISSN: 0932-6022.

CONGRESOS NACIONALES:

- **Blanco, J.** "La tecnología RFID como factor clave de la Industria 4.0: Protocolos de comunicación aérea en etiquetas UHF pasivas", VII Jornada de Investigación de la Escuela de Ingeniería Minera e Industrial de Almadén (Universidad de Castilla – La Mancha. 27 de septiembre de 2018).
- **Blanco, J.**; Pastor, J. M.; García, A. "Diseño e Implementación de un Dispositivo para la Emulación de Etiquetas RFID Pasivas en la Banda de UHF". VII Jornadas Doctorales UCLM 2017, 7 de noviembre de 2017, Albacete (España). ISBN: 978-84-17238-22-3.
- **Blanco, J.**; Pastor, J. M.; García, A. "Algoritmo Ultraligero para la Generación de Números Pseudoaleatorios en Etiquetas RFID pasivas". VI Jornadas Doctorales UCLM 2016, 18 de octubre de 2016, Toledo (España). ISBN: 978-84-16393-82-4.
- **Blanco, J.**; Pastor, J. M.; García, A. "Análisis de técnicas anticolidión para protocolos de comunicación en UHF con etiquetas RFID pasivas". V Jornadas Doctorales UCLM 2015, 6 de octubre de 2015, Ciudad Real (España). ISBN: 978-84-16393-18-3.
- **Blanco, J.**; Pastor, J. M.; García, A. "Plataforma para la Evaluación de Protocolos de Comunicación en Sistemas RFID Pasivos". IV Jornadas Doctorales UCLM 2014, 7 de octubre de 2014, Cuenca (España).

CAPÍTULO DE LIBRO:

- San José, J.I.; **Blanco, J.**; de Dios, J.J.; Zangróniz, R.; Pastor, J.M. "La identificación por radiofrecuencia (RFID) y sus aplicaciones". Investigación y Transferencia en la Escuela Politécnica de Cuenca, pp. 289-311. Ed.: Escuela Politécnica de Cuenca, Universidad de Castilla – La Mancha (España), junio 2015. ISBN: 978-84-608-1482-5.

PATENTE:

- García, A.; Zangróniz, R.; De Las Morenas, J.; **Blanco, J.** "Sistema Automático de Monitorización y Seguimiento de Muestras". Patente de invención presentada por la UCLM en la Oficina Española de Patentes y Marcas el 14 de enero de 2013 con referencia ES201300070, número de solicitud P201300070, fecha de concesión el 18 de agosto de 2015 y número de publicación ES2518615.

5.3. Propuestas de trabajos futuros.

Los diferentes trabajos que se han ido desarrollando a lo largo de la tesis, han sentado las bases para proponer otros nuevos que han surgido a partir de los resultados obtenidos en varios ámbitos.

En la línea de trabajo de las redes inalámbricas de sensores y todas sus variantes se propone la mejora de los sistemas y dispositivos desarrollados mediante la incorporación de nuevos elementos, como aplicaciones para dispositivos móviles que proporcionen una fácil monitorización y gestión de los sistemas en cualquier entorno. Además, los sistemas desarrollados pueden emplearse como plataforma de pruebas para nuevos planteamientos y/o aplicaciones. Así como utilizarlos para seguir contribuyendo a la implantación del IoT, donde la maquinaria y los dispositivos se conectarán directamente a los servicios web para la toma distribuida de decisiones.

Al igual que sucede en otros muchos campos científicos, disponer de herramientas que permitan simular situaciones reales conlleva múltiples ventajas, tanto a niveles de recursos materiales como temporales. Aunque ésta debe entenderse como un complemento a los comportamientos reales que se estén estudiando.

En este sentido, en la línea de la caracterización electromagnética de materiales, resultaría muy útil la creación de un software de simulación para sistemas RFID. Poniendo el foco en cómo se propagan las señales de radiofrecuencia y cómo les afecta el entorno en el que se implante el sistema. Para que tanto instaladores como expertos pudiesen emplearlo para mejorar el funcionamiento y la eficiencia en las instalaciones reales de sistemas RFID. Por lo que se propone la creación de una herramienta de simulación¹ que debería contar con varios módulos o partes:

- Un primer módulo en el que modelar las características físicas del espacio en el que funcionará la tecnología RFID, como puede ser una nave industrial, una habitación, etc.
- Un segundo módulo de materiales, que incorpore información sobre el comportamiento electromagnético, al menos, de los materiales más comunes. Así como del comportamiento de las ondas electromagnéticas en su presencia. Para ello sería necesario crear una base de datos que se alimentaría de los resultados de ensayos reales, como los descritos en el punto 3.3.2.
- Un módulo de cálculo, basado en la teoría electromagnética y de propagación de las ondas, que junto con los parámetros electromagnéticos de cada uno de los materiales que forman el espacio físico modelado, permita el cálculo de la propagación de las ondas electromagnéticas en un área de interés (simulando el área de cobertura de un lector RFID).
- Un módulo de representación gráfica que permita la visualización de los resultados con gráficos 2D y 3D. Lo que facilitaría la interpretación de los resultados de la simulación.

Además, este tipo de herramienta alertaría prematuramente ante posibles problemas de comunicación o funcionamiento del sistema RFID por la aparición de interferencias que distorsionen la señal electromagnética. Como, por ejemplo, la existencia de una estantería metálica cerca de un lector RFID en una nave industrial.

En los trabajos desarrollados en torno al protocolo de comunicaciones aéreas entre lector y etiquetas RFID pasivas, el algoritmo ultraligero propuesto para la generación de números pseudoaleatorios sólo

¹ Los primeros trabajos en esta línea fueron desarrollados durante la estancia de investigación realizada en la Universidad Técnica de Múnich, TUM (Alemania). Aunque finalmente ha quedado parada al exceder el objeto de la presente tesis, debido en parte a la gran cantidad de recursos temporales y materiales que se precisan para llevarse a cabo.

se ha utilizado para las operaciones de identificación de las etiquetas, que no obstante suponen la mayoría de las acciones en las que intervienen etiquetas RFID. Pero resultaría interesante averiguar su respuesta ante otras operaciones distintas que se lleven a cabo en la etiqueta. Además, la propuesta puede ser también evaluada en condiciones reales de trabajo, con distintos lectores comerciales y en presencia de otras etiquetas comerciales [152]. Todo ello permitiría también establecer si la utilización de esta nueva clase de etiquetas ligeras (simplificadas) tiene algún efecto en las prestaciones de la tecnología RFID que se está implantando en la actualidad y si puede ser utilizada con seguridad y garantías.

Por otro lado, resultaría interesante sustituir el actual LFSR del algoritmo propuesto por un registro de desplazamiento con realimentación no lineal (NLFSR: Non-Linear Feedback Shift Register), para averiguar el efecto que tendría este nuevo mecanismo en la generación de números pseudoaleatorios. Probablemente con esto se mejoraría la calidad del generador, aunque a cambio de requerir más cantidad recursos para su funcionamiento.

A partir de la caracterización de la BLF de respuesta de las etiquetas pasivas, se plantea la necesidad de diseñar algoritmos sencillos que permitan emplear la variación de los valores de BLF, puesta de manifiesto en los trabajos desarrollados, para otros usos. Por ejemplo, ajustarla a los requisitos que se recogen en la especificación EPC Gen2 y poder emplear dicha variación como fuente de aleatoriedad fiable. Así como estudiar la viabilidad de emplear la BLF de cada etiqueta como elemento diferenciador de cada una de ellas frente al lector en los procesos de identificación.

Por todo ello, se plantea además la posibilidad de proponer mejoras o cambios en los protocolos de comunicación entre lector y etiquetas RFID UHF pasivas, ya que hay varios motivos para ello y que van desde la mejora en el rendimiento de las comunicaciones hasta permitir la inclusión de encriptación en todos los intercambios de información entre etiquetas y lectores.

En definitiva, tras la realización de esta tesis doctoral, con los resultados obtenidos y los trabajos futuros planteados, se sientan las bases de una línea investigadora a la que poder dedicarse de manera profesional.

Referencias.

- [1] K. Finkenzeller, *RFID Handbook*. Chichester, UK: John Wiley & Sons, Ltd, 2010.
- [2] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2. pp. 381–394, Feb. 2006, doi: 10.1109/JSAC.2005.861395.
- [3] A. Alwadi, A. Gawanmeh, S. Parvin, and J. N. Al-Karaki, "Smart Solutions for RFID based Inventory Management Systems: A Survey," *Scalable Comput. Pract. Exp.*, vol. 18, no. 4, pp. 347–360, Nov. 2017, doi: 10.12694/scpe.v18i4.1333.
- [4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/J.FUTURE.2013.01.010.
- [5] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: A systematic mapping," *J. Syst. Softw.*, vol. 132, pp. 186–203, Oct. 2017, doi: 10.1016/J.JSS.2017.05.125.
- [6] A. Badru and N. Ajayi, "Adoption of RFID in large-scale organisation — A review of challenges and solutions," in *2017 IST-Africa Week Conference (IST-Africa)*, May 2017, pp. 1–10, doi: 10.23919/ISTAFRICA.2017.8102394.
- [7] J. Landt, "The history of RFID," *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, Oct. 2005, doi: 10.1109/MP.2005.1549751.
- [8] H. Bhatt and B. Glover, *RFID Essentials*, vol. 159, no. 12. O'Reilly, 2006.
- [9] J. Bamfield, "Electronic Article Surveillance: management learning in curbing theft," in *Crime At Work*, Palgrave Macmillan UK, 2005, pp. 156–174.
- [10] M. W. Khan *et al.*, "A pilot study on the reproductive risks of maternal exposure to magnetic fields from electronic article surveillance systems," *Int. J. Radiat. Biol.*, vol. 94, no. 10, pp. 902–908, Oct. 2018, doi: 10.1080/09553002.2018.1439197.
- [11] L. Kumari, K. Narsaiah, M. K. Grewal, and R. K. Anurag, "Application of RFID in agri-food sector," *Trends in Food Science and Technology*, vol. 43, no. 2. Elsevier Ltd, pp. 144–161, Jun. 01, 2015, doi: 10.1016/j.tifs.2015.02.005.
- [12] S. S. Al-Ghawji, S. A. Hussain, M. A. Al Rahbi, and S. Z. Hussain, "Automatic toll e-ticketing system for transportation systems," in *2016 3rd MEC International Conference on Big Data and Smart City, ICBDS C 2016*, Apr. 2016, pp. 284–288, doi: 10.1109/ICBDSC.2016.7460382.

- [13] K. Ok, V. Coskun, M. N. Aydin, and B. Ozdenizci, "Current benefits and future directions of NFC services," in *ICEMT 2010 - 2010 International Conference on Education and Management Technology, Proceedings*, 2010, pp. 334–338, doi: 10.1109/ICEMT.2010.5657642.
- [14] GS1, "EPC Information Services (EPCIS) Standard." pp. 1–138, 2016.
- [15] AIM, "RAIN RFID - A world of business & consumer connectivity." <https://rainrfid.org/> (accessed Jul. 06, 2020).
- [16] GS1, "EPCTM Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface. Version 2.1." pp. 1–152, 2018.
- [17] ISO, *ISO/IEC 18000-6 - Information technology. Radio frequency identification for item management. Parameters for air interface communications at 860 MHz to 960 MHz General*. 2013.
- [18] "AIM - AIM Home." <https://www.aimglobal.org/> (accessed Jul. 06, 2020).
- [19] M. Forouzandeh and N. C. Karmakar, "Chipless RFID tags and sensors: A review on time-domain techniques," *Wireless Power Transfer*, vol. 2, no. Special Issue 2. Cambridge University Press, pp. 62–77, 2015, doi: 10.1017/wpt.2015.10.
- [20] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Networks*, 2002, doi: 10.1016/S1389-1286(01)00302-4.
- [21] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Networks*, 2008, doi: 10.1016/j.comnet.2008.04.002.
- [22] S. Srivastava, M. Singh, and S. Gupta, "Wireless Sensor Network: A Survey," in *2018 International Conference on Automation and Computational Engineering, ICACE 2018*, 2018, doi: 10.1109/ICACE.2018.8687059.
- [23] R. Lin, Z. Wang, and Y. Sun, "Energy efficient medium access control protocols for wireless sensor networks and its state-of-art," in *IEEE International Symposium on Industrial Electronics*, 2004, doi: 10.1109/ISIE.2004.1571886.
- [24] W. K. G. Seah, A. E. Zhi, and H. P. Tan, "Wireless Sensor Networks Powered by Ambient Energy Harvesting (WSN-HEAP) - Survey and challenges," in *Proceedings of the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2009*, 2009, doi: 10.1109/WIRELESSVITAE.2009.5172411.
- [25] S. Wang, X. Gao, and L. Zhuo, "Survey of network coding and its benefits in energy saving over wireless sensor networks," in *ICICS 2009 - Conference Proceedings of the 7th International Conference on Information, Communications and Signal Processing*, 2009, doi: 10.1109/ICICS.2009.5397467.
- [26] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," *IEEE Commun. Surv. Tutorials*, 2013, doi: 10.1109/SURV.2012.062612.00084.
- [27] M. M. Wang, J. N. Cao, J. Li, and S. K. Dasi, "Middleware for wireless sensor networks: A survey," *J. Comput. Sci. Technol.*, 2008, doi: 10.1007/s11390-008-9135-x.
- [28] D. Baghyalakshmi, J. Ebenezer, and S. A. V. Satyamurty, "WSN based temperature monitoring for High Performance Computing cluster," in *International Conference on Recent Trends in Information Technology, ICRTIT 2011*, 2011, doi: 10.1109/ICRTIT.2011.5972379.

-
- [29] J. G. Escribano and A. García, "Human condition monitoring in hazardous locations using pervasive RFID sensor tags and energy-efficient wireless networks," *J. Zhejiang Univ. Sci. C*, vol. 13, no. 9, pp. 674–688, 2012, doi: 10.1631/jzus.C1100318.
 - [30] A. El Kouche, L. Al-Awami, H. Hassanein, and K. Obaia, "WSN application in the harsh industrial environment of the oil sands," in *IWCMC 2011 - 7th International Wireless Communications and Mobile Computing Conference*, 2011, doi: 10.1109/IWCMC.2011.5982603.
 - [31] H. C. Lee, "Towards a general wireless sensor network platform for outdoor environment monitoring," in *Proceedings of IEEE Sensors*, 2012, doi: 10.1109/ICSENS.2012.6411207.
 - [32] T. Kalaivani, A. Allirani, and P. Priya, "A survey on Zigbee based wireless sensor networks in agriculture," in *TISC 2011 - Proceedings of the 3rd International Conference on Trendz in Information Sciences and Computing*, 2011, doi: 10.1109/TISC.2011.6169090.
 - [33] A. Guinard, M. S. Aslam, D. Pusceddu, S. Rea, A. McGibney, and D. Pesch, "Design and deployment tool for in-building wireless sensor networks: A performance discussion," in *Proceedings - Conference on Local Computer Networks, LCN*, 2011, doi: 10.1109/LCN.2011.6115530.
 - [34] IEEE, "IEEE Standard for Low-Rate Wireless Networks," 2016. doi: 10.1109/IEEESTD.2016.7460875.
 - [35] T. Heo *et al.*, "Multitiered and Distributed WSN for Cooperative Indoors Environment Management," *Mob. Inf. Syst.*, vol. 2017, pp. 1–12, 2017, doi: 10.1155/2017/6979178.
 - [36] J. Bhola and S. Soni, "A study on research issues and challenges in WSN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 1667–1671, doi: 10.1109/WiSPNET.2016.7566423.
 - [37] K. Mikhaylov and J. Petäjäjärvi, "Design and Implementation of The Plug&Play Enabled Flexible Modular Wireless Sensor and Actuator Network Platform," *Asian J. Control*, vol. 19, no. 4, pp. 1392–1412, Jul. 2017, doi: 10.1002/asjc.1492.
 - [38] T. R. Sheltami, A. A. Al-Roubaiey, and A. S. H. Mahmoud, "A survey on developing publish/subscribe middleware over wireless sensor/actuator networks," *Wirel. Networks*, vol. 22, no. 6, pp. 2049–2070, Aug. 2016, doi: 10.1007/s11276-015-1075-0.
 - [39] T. Oda, R. Obukata, M. Ikeda, L. Barolli, and M. Takizawa, "Design and Implementation of a Simulation System Based on Deep Q-Network for Mobile Actor Node Control in Wireless Sensor and Actor Networks," in *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2017, pp. 195–200, doi: 10.1109/WAINA.2017.67.
 - [40] K. Ozero, T. Oda, D. Elmazi, and L. Barolli, "Design and Implementation of a Simulation System Based on Genetic Algorithm for Node Placement in Wireless Sensor and Actor Networks," in *Advances on Broad-Band Wireless Computing, Communication and Applications*, L. Barolli, F. Khafa, and K. Yim, Eds. Cham: Springer International Publishing, 2017, pp. 673–682.
 - [41] W. Chen, H. Miao, J. Liu, B. Qi, and N. Sun, "Actuators task assignment algorithm and its application for WSN," in *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2017, pp. 309–313, doi: 10.1109/SNPD.2017.8022738.
 - [42] F. Januario, A. Santos, L. Palma, A. Cardoso, and P. Gil, "A distributed multi-agent approach for resilient supervision over a IPv6 WSN infrastructure," in *2015 IEEE International Conference on Industrial Technology (ICIT)*, 2015, vol. 2015-June, no. June, pp. 1802–1807, doi:

- 10.1109/ICIT.2015.7125358.
- [43] R. Mahjoub and K. Elleithy, "Efficient Actor Recovery Paradigm for Wireless Sensor and Actor Networks," *Sensors*, vol. 17, no. 4, p. 858, Apr. 2017, doi: 10.3390/s17040858.
 - [44] R. A. Uthra, S. V. Kasmir Raja, A. Jeyasekar, and A. J. Lattanze, "A probabilistic approach for predictive congestion control in wireless sensor networks," *J. Zhejiang Univ. Sci. C*, vol. 15, no. 3, pp. 187–199, 2014, doi: 10.1631/jzus.C1300175.
 - [45] M. Sha, D. Gunatilaka, C. Wu, and C. Lu, "Empirical Study and Enhancements of Industrial Wireless Sensor–Actuator Network Protocols," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 696–704, Jun. 2017, doi: 10.1109/JIOT.2017.2653362.
 - [46] W. Cui, X. Meng, B. Yang, H. Yang, and Z. Zhao, "An efficient lossy link localization approach for wireless sensor networks," *Front. Inf. Technol. Electron. Eng.*, vol. 18, no. 5, pp. 689–707, 2017, doi: 10.1631/FITEE.1601247.
 - [47] X. Bai, M. Cao, L. Liu, J. Panneerselvam, and Q. Sun, "Efficient estimation and control of WSANs for the greenhouse environment," in *Proceedings of the 9th International Conference on Utility and Cloud Computing - UCC '16*, 2016, pp. 369–374, doi: 10.1145/2996890.3007853.
 - [48] E. Yoon, J. Park, and C. Yu, "Thermal energy harvesting circuit with maximum power point tracking control for self-powered sensor node applications," *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 2, pp. 285–296, Apr. 2018, doi: 10.1631/FITEE.1601181.
 - [49] E. Kulla, M. Ikeda, and L. Barolli, "Energy-Aware Actor Selection Methods in WSAN," in *2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2015, pp. 27–32, doi: 10.1109/BWCCA.2015.100.
 - [50] C. de Farias *et al.*, "A control and decision system for smart buildings using wireless sensor and actuator networks," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 1, pp. 120–135, 2014, doi: 10.1002/ett.2791.
 - [51] H. D. Chinh, S. S. Shetty, M. Gupta, and S. K. Panda, "A wireless sensor and actuator network (WSAN) framework for personalized thermal comfort in office buildings," in *2016 IEEE International Conference on Sustainable Energy Technologies (ICSET)*, 2016, pp. 42–47, doi: 10.1109/ICSET.2016.7811754.
 - [52] A. D'Elia *et al.*, "A self-powered WSAN for energy efficient heat distribution," in *2016 IEEE Sensors Applications Symposium (SAS)*, 2016, pp. 1–6, doi: 10.1109/SAS.2016.7479818.
 - [53] T. Labeodan, C. De Bakker, A. Rosemann, and W. Zeiler, "On the application of wireless sensors and actuators network in existing buildings for occupancy detection and occupancy-driven lighting control," *Energy Build.*, vol. 127, pp. 75–83, Sep. 2016, doi: 10.1016/j.enbuild.2016.05.077.
 - [54] A. Syahrani, G. A. A. Putri, A. R. Pratama, G. D. Putra, W. Najib, and Widyawan, "WSAN-based energy efficient system in building: A monitoring and scheduling," in *2014 Makassar International Conference on Electrical Engineering and Informatics (MICEEI)*, Nov. 2014, no. November, pp. 59–64, doi: 10.1109/MICEEI.2014.7067311.
 - [55] A. González-Potes, W. A. W. Mata-López, A. M. A. Ochoa-Brust, C. E. Pozo, and C. Escobar-del Pozo, "Smart Control of Multiple Evaporator Systems with Wireless Sensor and Actuator Networks," *Energies*, vol. 9, no. 3, p. 142, Feb. 2016, doi: 10.3390/en9030142.
 - [56] A. Anvari-Moghaddam, H. Monsef, A. Rahimi-Kian, J. M. Guerrero, and J. C. Vasquez, "Optimized energy management of a single-house residential micro-grid with automated demand

- response,” in *2015 IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6, doi: 10.1109/PTC.2015.7232243.
- [57] T. Zhang *et al.*, “Current trends in the development of intelligent unmanned autonomous systems,” *Front. Inf. Technol. Electron. Eng.*, vol. 18, no. 1, pp. 68–85, Jan. 2017, doi: 10.1631/FITEE.1601650.
- [58] E. Jovanov and A. Milenkovic, “Body area networks for ubiquitous healthcare applications: Opportunities and challenges,” in *Journal of Medical Systems*, Oct. 2011, vol. 35, no. 5, pp. 1245–1254, doi: 10.1007/s10916-011-9661-x.
- [59] I. Cianci, G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, “Content centric services in smart cities,” in *Proceedings - 6th International Conference on Next Generation Mobile Applications, Services, and Technologies, NGMAST 2012*, 2012, pp. 187–192, doi: 10.1109/NGMAST.2012.20.
- [60] L. H. Wang, T. Y. Chen, S. Y. Lee, and H. Chen, “Implementation of a personal health monitoring system in cardiology application,” in *IEEE Asia-Pacific Conference on Circuits and Systems, Proceedings, APCCAS*, Dec. 2012, pp. 236–239, doi: 10.1109/APCCAS.2012.6419015.
- [61] Y. P. Hsu and D. J. Young, “Skin-surface-coupled personal health monitoring system,” in *Proceedings of IEEE Sensors*, 2013, doi: 10.1109/ICSENS.2013.6688176.
- [62] M. Frost, G. Marcu, R. Hansen, K. Szaántó, and J. E. Bardram, “The MONARCA self-assessment system: Persuasive personal monitoring for bipolar patients,” in *2011 5th International Conference on Pervasive Computing Technologies for Healthcare and Workshops, PervasiveHealth 2011*, 2011, pp. 204–205, doi: 10.4108/icst.pervasivehealth.2011.246050.
- [63] S. Yang and M. Gerla, “Personal gateway in mobile health monitoring,” in *2011 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2011*, 2011, pp. 636–641, doi: 10.1109/PERCOMW.2011.5766966.
- [64] S. H. Toh, S. C. Lee, and W. Y. Chung, “WSN based personal mobile physiological monitoring and management system for chronic disease,” in *Proceedings - 3rd International Conference on Convergence and Hybrid Information Technology, ICCIT 2008*, 2008, vol. 1, pp. 467–472, doi: 10.1109/ICCIT.2008.392.
- [65] Y. F. Lee, “Personal medical monitoring system: Addressing interoperability,” *IT Prof.*, vol. 15, no. 5, pp. 31–37, 2013, doi: 10.1109/MITP.2012.90.
- [66] H. Na and Y. Choi, “Conceptual design of personal wellness record for mobile health monitoring,” in *2013 IEEE 2nd Global Conference on Consumer Electronics, GCCE 2013*, 2013, pp. 410–411, doi: 10.1109/GCCE.2013.6664873.
- [67] R. Megret *et al.*, “Wearable video monitoring of people with age dementia: Video indexing at the service of helthcare,” in *2008 International Workshop on Content-Based Multimedia Indexing, CBMI 2008, Conference Proceedings*, 2008, pp. 101–108, doi: 10.1109/CBMI.2008.4564934.
- [68] M. D. L. A. C. León, J. I. N. Hipólito, and J. L. García, “A security and privacy survey for WSN in e-Health applications,” in *CERMA 2009 - Electronics Robotics and Automotive Mechanics Conference*, 2009, pp. 125–130, doi: 10.1109/CERMA.2009.47.
- [69] O. Garcia-Morchon and H. Baldus, “The ANGEL WSN security architecture,” in *Proceedings - 2009 3rd International Conference on Sensor Technologies and Applications, SENSORCOMM 2009*, 2009, pp. 430–435, doi: 10.1109/SENSORCOMM.2009.71.
- [70] L. Rong, “A study of the security monitoring system in coal mine underground based on WSN,” in *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN*

- 2011, 2011, pp. 91–93, doi: 10.1109/ICCSN.2011.6013669.
- [71] A. Hu, “Applications of environmental security monitoring based on WSN in substation,” in *Proceedings - 4th International Congress on Image and Signal Processing, CISP 2011*, 2011, vol. 5, pp. 2806–2808, doi: 10.1109/CISP.2011.6100752.
 - [72] F. Viani, G. Oliveri, M. Donelli, L. Lizzi, P. Rocca, and A. Massa, “WSN-based solutions for security and surveillance,” in *European Microwave Week 2010, EuMW2010: Connecting the World, Conference Proceedings - European Microwave Conference, EuMC 2010*, 2010.
 - [73] City Government of Busan, “Global Smart City.” <http://k-smartcity.kr/english/index.php> (accessed Jul. 06, 2020).
 - [74] V. Pradhan, V. S. K. Murthy Balijepalli, and S. A. Khaparde, “An Effective Model for Demand Response Management Systems of Residential Electricity Consumers,” *IEEE Syst. J.*, vol. 10, no. 2, pp. 434–445, 2016, doi: 10.1109/JSYST.2014.2336894.
 - [75] V. Marinakis and H. Doukas, “An Advanced IoT-based System for Intelligent Energy Management in Buildings,” *Sensors*, vol. 18, no. 2, p. 610, Feb. 2018, doi: 10.3390/s18020610.
 - [76] E. Fotopoulou *et al.*, “Providing Personalized Energy Management and Awareness Services for Energy Efficiency in Smart Buildings,” *Sensors*, vol. 17, no. 9, p. 2054, Sep. 2017, doi: 10.3390/s17092054.
 - [77] W. Sun, F. R. Yu, T. Tang, and S. You, “A Cognitive Control Method for Cost-Efficient CBTC Systems With Smart Grids,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 568–582, 2017, doi: 10.1109/TITS.2016.2586938.
 - [78] F. Terroso-Saenz, A. González-Vidal, A. P. Ramallo-González, and A. F. Skarmeta, “An open IoT platform for the management and analysis of energy data,” *Futur. Gener. Comput. Syst.*, Sep. 2017, doi: 10.1016/J.FUTURE.2017.08.046.
 - [79] S. Akbari, “Energy harvesting for wireless sensor networks review,” in *2014 Federated Conference on Computer Science and Information Systems, FedCSIS 2014*, Oct. 2014, pp. 987–992, doi: 10.15439/2014F85.
 - [80] A. S. Weddell, M. Magno, G. V. Merrett, D. Brunelli, B. M. Al-Hashimi, and L. Benini, “A Survey of Multi-Source Energy Harvesting Systems,” in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, 2013, pp. 905–908, doi: 10.7873/DATE.2013.190.
 - [81] T. V. Galchev, J. McCullagh, R. L. Peterson, and K. Najafi, “Harvesting traffic-induced vibrations for structural health monitoring of bridges,” *J. Micromechanics Microengineering*, 2011, doi: 10.1088/0960-1317/21/10/104005.
 - [82] C. Dagdeviren *et al.*, “Conformal piezoelectric energy harvesting and storage from motions of the heart, lung, and diaphragm,” *Proc. Natl. Acad. Sci. U. S. A.*, vol. 111, no. 5, pp. 1927–1932, Feb. 2014, doi: 10.1073/pnas.1317233111.
 - [83] C. Dagdeviren *et al.*, “Recent progress in flexible and stretchable piezoelectric devices for mechanical energy harvesting, sensing and actuation,” *Extrem. Mech. Lett.*, vol. 9, pp. 269–281, 2016, doi: 10.1016/j.eml.2016.05.015.
 - [84] F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of things,” *International Journal of Communication Systems*, vol. 25, no. 9. John Wiley & Sons, Ltd, pp. 1101–1102, Sep. 01, 2012, doi: 10.1002/dac.2417.
 - [85] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

-
- [86] F. Gregorio, G. González, C. Schmidt, and J. Cousseau, "Internet of Things," in *Signals and Communication Technology*, Springer, 2020, pp. 217–245.
 - [87] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, "Middleware for internet of things: A survey," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2015.2498900.
 - [88] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018, doi: 10.1016/J.FUTURE.2017.07.060.
 - [89] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014, doi: 10.1109/JIOT.2014.2306328.
 - [90] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," *Comput. Networks*, vol. 148, pp. 241–261, Jan. 2019, doi: 10.1016/j.comnet.2018.12.008.
 - [91] H. Kagermann, W. Lukas, and W. Wahlster, "Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution.," *VDI nachrichten* 13, 2011.
 - [92] J. Lee, B. Bagheri, and H. A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015, doi: 10.1016/j.mfglet.2014.12.001.
 - [93] P. García Ansola, A. García, J. de las Morenas, J. García Escribano, and F. J. Otamendi, "ZigID: Improving visibility in industrial environments by combining WSN and RFID," *J. Zhejiang Univ. A*, vol. 12, no. 11, pp. 849–859, Nov. 2011, doi: 10.1631/jzus.A1100024.
 - [94] A. Soia, O. Konnikova, and E. Konnikov, "The internet of things," in *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020*, 2019, pp. 8587–8591, doi: 10.4018/ijhiot.2018010101.
 - [95] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, "Intelligent Manufacturing in the Context of Industry 4.0: A Review," *Engineering*, vol. 3, no. 5, pp. 616–630, Oct. 2017, doi: 10.1016/J.ENG.2017.05.015.
 - [96] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4. IEEE Computer Society, pp. 2233–2243, Nov. 01, 2014, doi: 10.1109/TII.2014.2300753.
 - [97] M. P. Borrás, M., Roca, M.I., Berruga, I., Molina, A., Beltrán, M.C., Molina, "Influencia de la refrigeración de las muestras sobre los métodos microbiológicos de detección de inhibidores en leche de oveja," in *XXXIII Jornadas científicas y X Internacionales de la Sociedad Española de Ovinotecnia y Caprinotecnia*, 2008, pp. 397–402.
 - [98] A. Bekkali, S. Zou, A. Kadri, M. Crisp, and R. V. Penty, "Performance Analysis of Passive UHF RFID Systems under Cascaded Fading Channels and Interference Effects," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 3, pp. 1421–1433, 2015, doi: 10.1109/TWC.2014.2366142.
 - [99] M. Victoria Bueno-Delgado and P. Pavon-Marino, "A centralized and aligned scheduler for passive RFID dense reader environments working under EPCglobal standard," *Simul. Model. Pract. Theory*, vol. 34, pp. 172–185, May 2013, doi: 10.1016/j.simpat.2012.07.006.
 - [100] J. S. Choi, M. Kang, R. Elmasri, and D. W. Engels, "Investigation of impact factors for various performances of passive UHF RFID system," in *2011 IEEE International Conference on RFID-Technologies and Applications, RFID-TA 2011*, 2011, pp. 152–159, doi: 10.1109/RFID-

- TA.2011.6068631.
- [101] ISO/IEC JTC 1, *ISO/IEC 7498-1:1994(en), Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model — Part 1*. 2002.
 - [102] Á. Cardama *et al.*, *Antenas*. 2002.
 - [103] K. T. Selvan and R. Janaswamy, “Fraunhofer and Fresnel Distances : Unified derivation for aperture antennas,” *IEEE Antennas Propag. Mag.*, vol. 59, no. 4, pp. 12–15, Aug. 2017, doi: 10.1109/MAP.2017.2706648.
 - [104] A. L. Bleda, G. Santa, A. J. Jara, R. Maestre, and A. Gomez Skarmeta, “Evaluation of the electromagnetic absorption in furniture for the integration of UHF-RFID tags,” in *2011 IEEE International Conference on RFID-Technologies and Applications, RFID-TA 2011*, 2011, pp. 81–88, doi: 10.1109/RFID-TA.2011.6068620.
 - [105] OMS, “Los campos electromagnéticos y la salud pública.” <https://www.who.int/peh-emf/publications/facts/fs304/es/> (accessed Jul. 06, 2020).
 - [106] B. S. Çiftler, A. Kadri, and I. Guvenc, “Experimental performance evaluation of passive UHF RFID systems under interference,” in *2015 IEEE International Conference on RFID Technology and Applications, RFID-TA 2015*, Jan. 2016, pp. 81–86, doi: 10.1109/RFID-TA.2015.7379802.
 - [107] A. Ameli, P. U. Jung, and C. B. Park, “Electrical properties and electromagnetic interference shielding effectiveness of polypropylene/carbon fiber composite foams,” *Carbon N. Y.*, vol. 60, pp. 379–391, Aug. 2013, doi: 10.1016/j.carbon.2013.04.050.
 - [108] D. Asprone *et al.*, “Assessment of the Electromagnetic Disturbance of a Glass Fiber Reinforced Composite Fencing Structure,” *J. Compos. Constr.*, vol. 14, no. 5, pp. 629–635, Oct. 2010, doi: 10.1061/(ASCE)CC.1943-5614.0000121.
 - [109] I. Choi, J. G. Kim, I. S. Seo, and D. G. Lee, “Radar absorbing sandwich construction composed of CNT, PMI foam and carbon/epoxy composite,” *Compos. Struct.*, vol. 94, no. 9, pp. 3002–3008, Sep. 2012, doi: 10.1016/j.compstruct.2012.04.009.
 - [110] I. Choi, D. Lee, and D. G. Lee, “Hybrid composite low-observable radome composed of E-glass/aramid/epoxy composite sandwich construction and frequency selective surface,” *Compos. Struct.*, vol. 117, no. 1, pp. 98–104, Nov. 2014, doi: 10.1016/j.compstruct.2014.06.031.
 - [111] G. Kulkarni, N. Velhal, V. Phadtare, and V. Puri, “Enhanced electromagnetic interference shielding effectiveness of chemical vapor deposited MWCNTs in X-band region,” *J. Mater. Sci. Mater. Electron.*, vol. 28, no. 10, pp. 7212–7220, May 2017, doi: 10.1007/s10854-017-6402-z.
 - [112] P. C. Kim and D. G. Lee, “Composite sandwich constructions for absorbing the electromagnetic waves,” *Compos. Struct.*, vol. 87, no. 2, pp. 161–167, Jan. 2009, doi: 10.1016/j.compstruct.2008.05.015.
 - [113] M. Sedlacik, M. Mrlik, V. Babayan, and V. Pavlinek, “Magnetorheological elastomers with efficient electromagnetic shielding,” *Compos. Struct.*, vol. 135, pp. 199–204, Jan. 2016, doi: 10.1016/j.compstruct.2015.09.037.
 - [114] J. M. Thomassin, C. Jérôme, T. Pardoen, C. Bailly, I. Huynen, and C. Detrembleur, “Polymer/carbon based composites as electromagnetic interference (EMI) shielding materials,” *Materials Science and Engineering R: Reports*, vol. 74, no. 7. Elsevier Ltd, pp. 211–232, Jul. 01, 2013, doi: 10.1016/j.mser.2013.06.001.
 - [115] C. J. vo. Klemperer and D. Maharaj, “Composite electromagnetic interference shielding materials for aerospace applications,” *Compos. Struct.*, vol. 91, no. 4, pp. 467–472, Dec. 2009, doi:

- 10.1016/j.compstruct.2009.04.013.
- [116] B. Wang, Z. Guo, Y. Han, and T. Zhang, "Electromagnetic wave absorbing properties of multi-walled carbon nanotube/cement composites," *Constr. Build. Mater.*, vol. 46, pp. 98–103, Sep. 2013, doi: 10.1016/j.conbuildmat.2013.04.006.
 - [117] L. B. Wang, K. Y. See, Y. Ling, and W. J. Koh, "Study of Metal Foams for Architectural Electromagnetic Shielding," *J. Mater. Civ. Eng.*, vol. 24, no. 4, pp. 488–493, Apr. 2012, doi: 10.1061/(ASCE)MT.1943-5533.0000403.
 - [118] Z. J. Wang, K. Z. Li, and C. Wang, "Freezing-thawing effects on electromagnetic wave reflectivity of carbon fiber cement based composites," *Constr. Build. Mater.*, vol. 64, pp. 288–292, Aug. 2014, doi: 10.1016/j.conbuildmat.2014.04.091.
 - [119] D. Micheli, A. Delfini, F. Santoni, F. Volpini, and M. Marchetti, "Measurement of electromagnetic field attenuation by building walls in the mobile phone and satellite navigation frequency bands," *IEEE Antennas Wirel. Propag. Lett.*, vol. 14, pp. 698–702, 2015, doi: 10.1109/LAWP.2014.2376811.
 - [120] D. Micheli *et al.*, "Electromagnetic characterization and shielding effectiveness of concrete composite reinforced with carbon nanotubes in the mobile phones frequency band," *Mater. Sci. Eng. B Solid-State Mater. Adv. Technol.*, vol. 188, pp. 119–129, Oct. 2014, doi: 10.1016/j.mseb.2014.07.001.
 - [121] R. A. Khushnood, S. Ahmad, P. Savi, J. M. Tulliani, M. Giorcelli, and G. A. Ferro, "Improvement in electromagnetic interference shielding effectiveness of cement composites using carbonaceous nano/micro inerts," *Constr. Build. Mater.*, vol. 85, pp. 208–216, Jun. 2015, doi: 10.1016/j.conbuildmat.2015.03.069.
 - [122] E. B. Savage, J. L. Gilbert, W. A. Radasky, and M. J. Madrid, "An alternative EM shielding effectiveness measurement method for buildings," in *2010 Asia-Pacific Symposium on Electromagnetic Compatibility, APEMC 2010*, 2010, pp. 138–141, doi: 10.1109/APEMC.2010.5475830.
 - [123] G. Bantsis, S. Mavridou, C. Sikilidis, M. Betsiou, N. Oikonomou, and T. Yioultsis, "Comparison of low cost shielding-absorbing cement paste building materials in X-band frequency range using a variety of wastes," *Ceram. Int.*, vol. 38, no. 5, pp. 3683–3692, Jul. 2012, doi: 10.1016/j.ceramint.2012.01.010.
 - [124] L. Baoyi, D. Yuping, and L. Shunhua, "The electromagnetic characteristics of fly ash and absorbing properties of cement-based composites using fly ash as cement replacement," *Constr. Build. Mater.*, vol. 27, no. 1, pp. 184–188, Feb. 2012, doi: 10.1016/j.conbuildmat.2011.07.062.
 - [125] J. Chen, D. Zhao, H. Ge, and J. Wang, "Graphene oxide-deposited carbon fiber/cement composites for electromagnetic interference shielding application," *Constr. Build. Mater.*, vol. 84, pp. 66–72, Jun. 2015, doi: 10.1016/j.conbuildmat.2015.03.050.
 - [126] S. D. Hutagalung, N. H. Sahrol, Z. A. Ahmad, M. F. Ain, and M. Othman, "Effect of MnO₂ additive on the dielectric and electromagnetic interference shielding properties of sintered cement-based ceramics," *Ceram. Int.*, vol. 38, no. 1, pp. 671–678, Jan. 2012, doi: 10.1016/j.ceramint.2011.07.055.
 - [127] I. W. Nam, H. K. Kim, and H. K. Lee, "Influence of silica fume additions on electromagnetic interference shielding effectiveness of multi-walled carbon nanotube/cement composites," *Constr. Build. Mater.*, vol. 30, pp. 480–487, May 2012, doi: 10.1016/j.conbuildmat.2011.11.025.
 - [128] A. P. Singh *et al.*, "Multiwalled carbon nanotube/cement composites with exceptional

- electromagnetic interference shielding properties,” *Carbon N. Y.*, vol. 56, pp. 86–96, May 2013, doi: 10.1016/j.carbon.2012.12.081.
- [129] D. M. Pozar, *Microwave Engineering, 4th Edition*. 2012.
- [130] GS1 AISBL, “GS1.” <https://www.gs1.org/> (accessed Jul. 06, 2020).
- [131] AIM, “RAIN RFID.” <https://rainrfid.org/> (accessed Jul. 06, 2020).
- [132] L. Arjona, H. Simon, and A. Ruiz, “Energy-Aware RFID Anti-Collision Protocol,” *Sensors*, vol. 18, no. 6, p. 1904, Jun. 2018, doi: 10.3390/s18061904.
- [133] L. Duan, X. Zhang, Z. J. Wang, and F. Duan, “A Feasible Segment-by-Segment ALOHA Algorithm for RFID Systems,” *Wirel. Pers. Commun.*, vol. 96, no. 2, pp. 2633–2649, Sep. 2017, doi: 10.1007/s11277-017-4316-y.
- [134] Y. Chen, J. Su, and W. Yi, “An Efficient and Easy-to-Implement Tag Identification Algorithm for UHF RFID Systems,” *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1509–1512, Jul. 2017, doi: 10.1109/LCOMM.2017.2649490.
- [135] J. Su, Z. Sheng, D. Hong, and G. Wen, “An Effective Frame Breaking Policy for Dynamic Framed Slotted Aloha in RFID,” *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 692–695, 2016, doi: 10.1109/LCOMM.2016.2521839.
- [136] S. K. Wijayasekara, A. Robithoh, P. Sasithong, P. Vanichchanunt, S. Nakpeerayuth, and L. Wuttisittikulij, “A Reduced Complexity of Vahedi’s Tag Estimation Method for DFSA,” *Eng. J.*, vol. 21, no. 6, pp. 111–125, Oct. 2017, doi: 10.4186/ej.2017.21.6.111.
- [137] Haifeng Wu and Yu Zeng, “Passive RFID Tag Anticollision Algorithm for Capture Effect,” *IEEE Sens. J.*, vol. 15, no. 1, pp. 218–226, Jan. 2015, doi: 10.1109/JSEN.2014.2339653.
- [138] H. Choi, H. Kim, and S. Choi, “Capture-Aware Couple-Resolution Blocking Protocol in RFID Systems,” *Wirel. Pers. Commun.*, vol. 93, no. 4, pp. 969–986, Apr. 2017, doi: 10.1007/s11277-016-3940-2.
- [139] H. Wu, Y. Wang, and Y. Zeng, “Capture-aware Bayesian RFID tag estimate for large-scale identification,” *IEEE/CAA J. Autom. Sin.*, vol. 5, no. 1, pp. 119–127, Jan. 2018, doi: 10.1109/JAS.2017.7510757.
- [140] Hung-Yu Chien, “SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity,” *IEEE Trans. Dependable Secur. Comput.*, vol. 4, no. 4, pp. 337–340, Oct. 2007, doi: 10.1109/TDSC.2007.70226.
- [141] W. Yong, L. Qing, W. Lei, and S. Hao, “Research on Anti-Collision Algorithm in Radio Frequency Identification Technology,” in *2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, Aug. 2017, pp. 239–244, doi: 10.1109/IHMSC.2017.167.
- [142] S. Xiaohao and L. Baolong, “An Investigation on Tree-Based Tags Anti-collision Algorithms in RFID,” in *2017 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, Sep. 2017, no. 3, pp. 5–11, doi: 10.1109/ICCNEA.2017.19.
- [143] Y. Bai, L. Yang, G. Zhang, and Y. Xu, “An improved binary search RFID anti-collision algorithm,” in *2017 12th International Conference on Computer Science and Education (ICCSE)*, Aug. 2017, no. Iccse, pp. 435–439, doi: 10.1109/ICCSE.2017.8085531.
- [144] Z. Fu, F. Deng, and X. Wu, “Design of a Quaternary Query Tree ALOHA Protocol Based on Optimal Tag Estimation Method,” *Information*, vol. 8, no. 1, p. 5, Dec. 2016, doi: 10.3390/info8010005.
- [145] J. Liu and Q. Feng, “A blocking collision tracking tree algorithm in mobile RFID systems,” in *2017*

- Progress In Electromagnetics Research Symposium - Spring (PIERS)*, May 2017, pp. 2520–2525, doi: 10.1109/PIERS.2017.8262177.
- [146] B. Liu and X. Su, “An Anti-Collision Algorithm for RFID Based on an Array and Encoding Scheme,” *Information*, vol. 9, no. 3, p. 63, Mar. 2018, doi: 10.3390/info9030063.
 - [147] H. Landaluce, A. Perallos, E. Onieva, L. Arjona, and L. Bengtsson, “An Energy and Identification Time Decreasing Procedure for Memoryless RFID Tag Anticollision Protocols,” *IEEE Trans. Wirel. Commun.*, vol. 15, no. 6, pp. 4234–4247, 2016, doi: 10.1109/TWC.2016.2537800.
 - [148] W. Shoufeng, Z. Dongchen, X. Xiaoyan, S. Shumeng, and W. Tinglan, “A novel anti-collision scheme for RFID systems,” in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Mar. 2014, pp. 458–461, doi: 10.1109/WF-IoT.2014.6803210.
 - [149] N. Bagheri, P. Alenaby, and M. Safkhani, “A new anti-collision protocol based on information of collided tags in RFID systems,” *Int. J. Commun. Syst.*, vol. 30, no. 3, p. e2975, Feb. 2017, doi: 10.1002/dac.2975.
 - [150] K.-S. Huang, C.-K. Hwang, B.-K. Lee, and I.-H. Chung, “An exact closed-form formula of collision probability in diverse multiple access communication systems with frame slotted aloha protocol,” *J. Franklin Inst.*, vol. 354, no. 13, pp. 5739–5752, Sep. 2017, doi: 10.1016/j.jfranklin.2017.05.028.
 - [151] J. Vales-Alonso, V. Bueno-Delgado, E. Egea-Lopez, F. J. Gonzalez-Castaño, and J. Alcaraz, “Multiframe maximum-likelihood tag estimation for RFID anticollision protocols,” *IEEE Trans. Ind. Informatics*, vol. 7, no. 3, pp. 487–496, Aug. 2011, doi: 10.1109/TII.2011.2158831.
 - [152] P. Solic, J. Maras, J. Radic, and Z. Blazevic, “Comparing theoretical and experimental results in Gen2 RFID throughput,” *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 1, pp. 349–357, 2017, doi: 10.1109/TASE.2016.2532959.
 - [153] D. C. Ranasinghe, D. W. Engels, and P. H. Cole, “Low cost RFID systems: confronting security and privacy,” *Pap. Auto-ID*, 2005, [Online]. Available: <http://autoidlabs.eleceng.adelaide.edu.au/sites/default/files/publications/papers/AUTOIDLABS-WP-SWNET-013.pdf>.
 - [154] P. Peris-lopez and L. A. Entrena, “Cryptographically Secure Pseudo-Random Bit Generator for RFID Tags,” *Int. Conf. Internet Technol. Secur. Trans.*, 2010.
 - [155] J. Chen, A. Miyaj, H. Sato, and C. Su, “Improved Lightweight Pseudo-Random Number Generators for the Low-Cost RFID Tags,” in *2015 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 17–24, doi: 10.1109/Trustcom.2015.352.
 - [156] E. Taqieddin, H. Al-Dahoud, M. Mowafi, and O. Banimelhem, “An Enhanced EPC Gen2v2 RFID Authentication and Ownership Management Protocol,” in *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*, Oct. 2017, vol. 2017-Octob, pp. 683–689, doi: 10.1109/LCN.2017.126.
 - [157] H. Nomaguchi, A. Miyaji, and C. Su, “Evaluation and Improvement of Pseudo-Random Number Generator for EPC Gen2,” in *2017 IEEE Trustcom/BigDataSE/ICSS*, Aug. 2017, pp. 721–728, doi: 10.1109/Trustcom/BigDataSE/ICSS.2017.305.
 - [158] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, “LAMED — A PRNG for EPC Class-1 Generation-2 RFID specification,” *Comput. Stand. Interfaces*, vol. 31, no. 1, pp. 88–97, Jan. 2009, doi: 10.1016/j.csi.2007.11.013.
 - [159] K. Mandal, X. Fan, and G. Gong, “Design and Implementation of Warbler Family of Lightweight

- Pseudorandom Number Generators for Smart Devices,” *ACM Trans. Embed. Comput. Syst.*, vol. 15, no. 1, pp. 1–28, Feb. 2016, doi: 10.1145/2808230.
- [160] Z. Shi, J. Chen, S. Chen, and S. Ren, “A lightweight RFID authentication protocol with confidentiality and anonymity,” in *Proceedings of 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2017*, Mar. 2017, pp. 1631–1634, doi: 10.1109/IAEAC.2017.8054290.
 - [161] Z. Shi, F. Wu, C. Wang, and S. Ren, “A Lightweight RFID Authentication Protocol with Forward Security and Randomized Identifier,” Springer, Cham, 2016, pp. 1–13.
 - [162] V. Sharma, A. Vithalkar, and M. Hashmi, “Lightweight security protocol for chipless RFID in Internet of Things (IoT) applications,” in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, Jan. 2018, pp. 468–471, doi: 10.1109/COMSNETS.2018.8328246.
 - [163] GS1, “EPC Tag Data Standard,” *Differences*, pp. 1–200, 2014, [Online]. Available: <http://www.gs1.org/gsmp/kc/epcglobal/tds/>.
 - [164] Raosoft, “Sample size calculator.” <http://www.raosoft.com/samplesize.html> (accessed Jul. 06, 2020).
 - [165] D. Biebighauser, “Testing Random Number Generators,” *University of Minnesota*, 2000. <http://www-users.math.umn.edu/~garrett/students/reu/pRNGs.pdf> (accessed Jul. 06, 2020).
 - [166] M. Rütli and P. M. Troyer, *A Random Number Generator Test Suite for the C++ Standard*. Institute for Theoretical Physics - ETH Zürich, 2004.
 - [167] X. Meng, “Test for Random Numbers,” *Department of Computer Science - Bucknell University*, 2002. <http://www.eg.bucknell.edu/~xmeng/Course/CS6337/Note/master/node36.html> (accessed Jul. 06, 2020).
 - [168] L. E. Bassham *et al.*, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-22r1a.
 - [169] T. F. Collins, R. Getz, D. Pu, and A. M. Wyglinski, *Software Defined Radio For Engineers*. Artech House, 2018.
 - [170] “Using National Instruments Software and Hardware to Develop and Test RFID Tags - National Instruments.” <https://www.ni.com/en-us/innovations/case-studies/19/using-national-instruments-software-and-hardware-to-develop-and-test-rfid-tags.html> (accessed Jul. 06, 2020).
 - [171] M. Winkler, T. Faseth, H. Arthaber, and G. Magerl, “An UHF RFID tag emulator for precise emulation of the physical layer,” *Microw. Conf. (EuMC), 2010 Eur.*, no. September, pp. 273–276, 2010.
 - [172] M. Winkler, T. Faseth, J. Steininger, and H. Arthaber, “Implementation of a receiver for an EPC tag emulator for performance evaluation,” *Microw. Conf. (EuMC), 2011 41st Eur.*, no. October, pp. 119–122, 2011, [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6101763.
 - [173] O. Abdelmalek, D. Hely, and V. Beroulle, “EPC Class 1 GEN 2 UHF RFID tag emulator for robustness evaluation and improvement,” in *2013 8th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, Mar. 2013, pp. 20–24, doi: 10.1109/DTIS.2013.6527771.
 - [174] Q. Peng, C. Zhang, and Z. Wang, “A multi-tag emulator for the UHF RFID system,” *IEEE Trans.*

-
- Instrum. Meas.*, vol. 63, no. 6, pp. 1461–1469, 2014, doi: 10.1109/TIM.2013.2289701.
- [175] P. L’Ecuyer, “Tables of linear congruential generators of different sizes and good lattice structure,” *Math. Comput.*, vol. 68, no. 225, pp. 249–261, Jan. 1999, doi: 10.1090/S0025-5718-99-00996-5.
- [176] “Introduction to FPGA Hardware Concepts (FPGA Module) - LabVIEW 2018 FPGA Module Help - National Instruments.” https://zone.ni.com/reference/en-XX/help/371599P-01/lvfpgaconcepts/fpga_basic_chip_terms/ (accessed Jul. 06, 2020).
- [177] I. Bratuz, A. Vodopivec, and A. Trost, “Resolving Collision in EPCglobal Class-1 Gen-2 System by Utilizing the Preamble,” *IEEE Trans. Wirel. Commun.*, vol. 13, no. 10, pp. 5330–5339, Oct. 2014, doi: 10.1109/TWC.2014.2350975.
- [178] Dawei Shen, G. Woo, D. P. Reed, A. B. Lippman, and Junyu Wang, “Separation of multiple passive RFID signals using Software Defined Radio,” in *2009 IEEE International Conference on RFID*, Apr. 2009, pp. 139–146, doi: 10.1109/RFID.2009.4911203.
- [179] H. Salah, H. A. Ahmed, J. Robert, and A. Heuberger, “FFT Based Rate Estimation for UHF RFID Systems,” in *Smart SysTech 2015: European Conference on Smart Objects, Systems, and Technologies*, 2015, pp. 1–5.
- [180] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, Oct. 2014, doi: 10.1007/s11276-014-0761-7.

Listado de tablas.

Tabla 4.1. Resultados de las pruebas realizadas para las secuencias medidas.	80
Tabla 4.2. Resultados de las pruebas realizadas para el algoritmo propuesto.	81
Tabla 4.3. Resultados de las pruebas realizadas para el generador LAMED.	82
Tabla 4.4. Tolerancias permitidas para el valor de BLF [16].	100
Tabla 4.5. Variaciones de BLF durante la retrodispersión.	104
Tabla 4.6. Resultados de las pruebas de aleatoriedad a las secuencias de BLF.	107

Listado de figuras.

Figura 2.1. Ejemplos de etiquetas con tecnología NFC (CC).	20
Figura 2.2. Lector y etiqueta RFID pasiva en funcionamiento.....	22
Figura 2.3. Etiqueta RFID pasiva y esquema de funcionamiento de su circuito integrado (CI).	23
Figura 2.4. Rangos de frecuencias para el funcionamiento de la tecnología UHF-RFID en el mundo (CC).	23
Figura 2.5. Partes de la tecnología RAIN RFID [15].....	24
Figura 2.6. Interior del prototipo del nodo sensor de la red.....	26
Figura 2.7. Lógica de funcionamiento del sistema desarrollado para el control del uso de la energía. .	29
Figura 2.8. Interior del prototipo de router desarrollado para crear la WSN.	30
Figura 2.9. Pruebas de laboratorio del sistema final antes de ser implantado.	30
Figura 2.10. Exterior (a) e interior (b) de la pulsera Inteligente desarrollada.	33
Figura 2.11. Dispositivos fijos y móviles de la red desarrollada.	33
Figura 2.12. Pantalla del software de gestión y control de la red de seguridad activa.	34
Figura 2.13. Exterior (a) e interior (b) del módulo cosechador de energía desarrollado.	37
Figura 2.14. Módulo cosechador de energía en el interior de un nodo.....	38
Figura 2.15. Sistema de trazabilidad para el proceso de recogida de muestras de leche.....	41
Figura 2.16. Sistema inalámbrico de trazabilidad para el proceso de recogida de muestras.	42
Figura 2.17. Dispositivo USB para el enlace de comunicación por radiofrecuencia.....	43
Figura 2.18. Evolución de la temperatura de las muestras en el interior de la nevera.	43
Figura 2.19. Ejemplo de ruta de recogida de muestras.	44
Figura 3.1. Diferencias entre campo cercano y campo lejano (CC).....	47
Figura 3.2. Ondas en un determinado instante para los campos eléctrico y magnético (CC).....	47
Figura 3.3. Espectro electromagnético y sus aplicaciones (Fuente: http://www.electromagneticos.es).	49
Figura 3.4. Red de dos puertos.	51
Figura 3.5. Diagrama del sistema de medida para la caracterización electromagnética de materiales.	52
Figura 3.6. Cavidades que forman la cámara anecoica electromagnética.	53
Figura 3.7. Estructura metálica y acabado de la cámara diseñada y fabricada.	53
Figura 3.8. Material absorbente electromagnético que recubre las paredes interiores de la cámara. .	54
Figura 3.9. Interiores de las cámaras emisora (a) y receptora (b).....	54
Figura 3.10. Equipo de medida electromagnética de materiales completo.	55
Figura 3.11. Disposición de las antenas en el interior de la cámara para la medida.....	56
Figura 3.12. Resultados de las medidas en vacío, sin muestra de material, del equipo.	57
Figura 3.13. Energía reflejada en función de la frecuencia para las muestras analizadas.	58

Figura 3.14. Energía absorbida en función de la frecuencia para las muestras analizadas.	58
Figura 4.1. Información a través del enlace de comunicación con modulación ASK [16].	63
Figura 4.2. Codificación por ancho de pulso (PIE) [16].	63
Figura 4.3. Codificación FMO de los datos para enviarlos al lector [16].	64
Figura 4.4. Secuencias de datos FMO [16].	64
Figura 4.5. Secuencia de comandos entre lector y etiqueta.	67
Figura 4.6. Algoritmo para la obtención del parámetro Q propuesto en EPC Gen2 [16].	68
Figura 4.7. Ejemplo de EPC de 96 bits.	74
Figura 4.8. Esquema del algoritmo propuesto.	75
Figura 4.9. Una de las etiquetas evaluadas en el estudio.	77
Figura 4.10. Disposición del equipamiento durante las medidas con etiquetas comerciales.	78
Figura 4.11. Histograma de las secuencias medidas en las etiquetas comerciales.	81
Figura 4.12. Histograma de la secuencia generada con el algoritmo propuesto.	82
Figura 4.13. Histograma de la secuencia del generador LAMED.	83
Figura 4.14. Diagrama de la plataforma emuladora de etiquetas RFID pasivas.	86
Figura 4.15. Prototipo del emulador de etiquetas desarrollado con la placa de pruebas del Zynq® 7000.	87
Figura 4.16. Primera versión de la PCB con la interfaz para la comunicación aérea en la banda de UHF.	87
Figura 4.17. Forma de onda IQ obtenida de la señal recibida del emulador en el lector.	88
Figura 4.18. Forma de onda IQ de la respuesta de una etiqueta pasiva real en el lector.	88
Figura 4.19. PCB definitiva con interfaces de comunicación para la plataforma emuladora de etiquetas.	89
Figura 4.20. Plataforma con el emulador de etiquetas basado en myRIO y el sistema de medida empleado como lector.	89
Figura 4.21. Circuito para la retrodispersión de la señal del lector.	90
Figura 4.22. Plataforma emuladora de etiquetas RFID pasivas.	90
Figura 4.23. Flujograma del programa principal del emulador de etiquetas.	91
Figura 4.24. Pantalla principal del módulo monitorización de la plataforma.	92
Figura 4.25. Flujo y transformación de la información desde el lector a la etiqueta.	93
Figura 4.26. Preámbulo del comando del lector [16].	93
Figura 4.27. Flujo y transformación de la información desde la etiqueta al lector.	95
Figura 4.28. Señal emitida por el lector (a la izquierda) y señal recibida del emulador de etiquetas (a la derecha).	96
Figura 4.29. Recursos de la FPGA necesarios para la implementación de cada método.	97
Figura 4.30. Espectro del canal de comunicación entre el lector y la etiqueta [16].	99
Figura 4.31. FFT de la señal que llega al lector con varias subportadoras de etiquetas comerciales distintas [177].	101
Figura 4.32. Disposición el equipamiento de medida durante las medidas realizadas.	102
Figura 4.33. Resultados de las medidas para respuestas independientes.	103
Figura 4.34. Comparación entre los valores medidos de BLF y una secuencia aleatoria de datos.	105
Figura 4.35. Distribución de valores de BLF calculados con una precisión de 1 Byte.	106
Figura 4.36. Comparación entre los valores obtenidos de BLF _{NORM} y una secuencia de números aleatorios.	107

Glosario.

ABS	Acrilonitrilo butadieno estireno
ACK	Acknowledgement, reconocimiento
ASIC	Application-Specific Integrated Circuit, circuito integrado de aplicación específica
ASK	Amplitude-shift keying, modulación por desplazamiento de amplitud
BAP	Battery Assisted Passive RFID Tags, etiquetas pasivas asistidas por batería
BLF	Backscatter-Link Frequency, Frecuencia de Enlace por Retrodispersión
BST	Binary Searching Tree, árbol binario de búsqueda
CPS	Cyber-Physical Systems, sistemas ciber-físicos
CRC	Cyclic-Redundancy Check, Código de Redundancia Cíclica
CTT	Collision Tracking Tree, árbol de rastreo de colisiones
CW	Continuous Wave, onda continua
DFSA	Dynamic Frame Slotted Aloha
DNI	Documento Nacional de Identidad
DR	Divided Ratio, proporción de división
DSB-ASK	Double-sideband amplitude-shift keying, modulación en amplitud de doble banda lateral
EAS	Electronic Article Surveillance
EPC	Electronic Product Code, Código Electrónico de Producto
EPCIS	Electronic Product Code Information System
FFD	Full Function Devices, Dispositivos de Funcionalidad Completa
FPGA	Field-programmable gate array, matriz programable de puertas lógicas
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
ID	Identificación
IoT	Internet of Things, Internet de las Cosas
IQ	Magnitudes de la constelación para la modulación QAM
ISO	International Organization for Standardization
LCG	Linear Congruential Generator, generador congruencial lineal
LFSR	Linear Feedback Shift Register, registro de desplazamiento con realimentación lineal
LTE	Long Term Evolution
LTU	Grupo de puertas lógicas predefinido
MAC	Media Access Control, Control de Acceso al Medio
MCG	Multiplicative Congruential Generator, generador congruencial multiplicativo
MSB	Most Significant Bit, bit más significativo
NFC	Near Field Communication
OSI	Open System Interconnection

PCB	Printed Circuit Board, placa de circuito impreso
PET	Polietileno tereftalato
PIE	Pulse-Interval Encoding, codificación por ancho entre pulsos
PLC	Power Line Communications
PRNG	Pseudo-Random Number Generator, Generador de Números Pseudoaleatorios
PRNGs	Pseudo-Random Number Generators, Generadores de Números Pseudoaleatorios
PR-ASK	Phase-reversal amplitude shift keying, modulación en amplitud con inversión de fase
PSK	Phase-shift keying, modulación por desplazamiento de fase
PW	Pulse Width
QAM	Quadrature Amplitude Modulation, modulación de amplitud en cuadratura
QT	Query Tree, árbol de consulta
RAE	Real Academia Española
RAM	Random Access Memory, memoria de acceso aleatorio
RF	Radio-Frequency, Radiofrecuencia
RFID	Radio-Frequency IDentification, Identificación por Radiofrecuencia
RN16	Número aleatorio de 16 bits
RX	Recepción de señal
SDR	Software-Defined Radio, sistemas de radio definidos por software
SoC	System on Chip, sistema electrónico en un único chip
SSB-ASK	Single-sideband amplitude-shift keying, modulación en amplitud de simple banda lateral
TX	Transmisión de señal
UE	Unión Europea
UID	Unique IDentifier
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
VAC	Voltaje de Corriente Alterna
VDC	Voltaje de Corriente Directa (continua)
VI	Virtual Instrument, instrumento virtual
WBAN	Wireless Body Area Network, Red Inalámbrica de Ámbito Personal
WSN	Wireless Sensor Network, Red Inalámbrica de Sensores
WSAN	Wireless Sensor and Actuator Network, Red Inalámbrica de Sensores y Actuadores

Parte de los trabajos llevados a cabo en esta tesis han sido financiados por el Ministerio de Educación, Cultura y Deporte, dentro Programa Estatal de Promoción del Talento y su Empleabilidad, mediante la Ayuda para contratos predoctorales de Formación de Profesorado Universitario (FPU), referencia: FPU13/01582 (BOE-A-2014-9081); y la Ayuda de movilidad para estancias breves a beneficiarios del subprograma de Formación del Profesorado Universitario, referencia: EST15/00367.

