

Trabajo de Fin de Grado
Grado en Ingeniería de las Tecnologías de
Telecomunicación

Implementación de técnicas RF en control de activos
urbanos

Autor: Miguel Nájera Benítez

Tutor: Antonio Corral Aguilar

Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2020



Proyecto Fin de Carrera
Ingeniería de Telecomunicación

Implementación de técnicas RF en control de activos urbanos

Autor:
Miguel Nájera Benítez

Tutor:
Antonio Corral Aguilar
Profesor asociado

Departamento de Ingeniería Eléctrica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2020

Proyecto Fin de Carrera: Implementación de técnicas RF en control de activos urbanos

Autor: Miguel Nájera Benítez

Tutor: Antonio Corral Aguilar

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2020

El Secretario del Tribunal

Agradecimientos

Con este proyecto concluye mi formación académica realizada en la Universidad de Sevilla. Ha sido un camino que me ha hecho evolucionar no solo como ingeniero, sino como persona. Para mí, este aprendizaje ha sido algo más que la asimilación de los conceptos asociados a la ingeniería. El saber adoptar una actitud de visión global ante un problema, ver y entender cómo funciona algo, saber dónde no lo hace y poder dar la solución adecuada son las facultades que caracterizan la esencia del ingeniero. A partir de ahí, el innovar o crear cosas nuevas forma parte de la aventura.

Gracias a mis padres, sin ellos no habría sido posible nada de esto.

Gracias a mis amigos, por enriquecerme tanto dentro como fuera del ámbito laboral.

Gracias a mis profesores, tanto de la universidad como del colegio Salesianos de la Santísima Trinidad.

Gracias a mi maestro de Hapkido Javier Romero, por inculcarme la disciplina a través del deporte y las artes marciales, y a todos mis compañeros de la escuela Yong Mu Doyang.

Gracias a mis compañeros de Noxium, por ayudarme y orientarme.

Gracias a Antonio Corral, por darme la oportunidad de realizar este trabajo.

Miguel Nájera Benítez

Sevilla, 2020

RESUMEN

El objetivo de este proyecto ha sido la monitorización y control de contenedores de residuos urbanos. Para ello se ha integrado un sistema de adquisición de datos mediante tecnología RFID con posterior envío a base de datos centralizada.

Para el desarrollo del proyecto se han implementado las diferentes partes del sistema en un prototipo funcional, para dar lugar a la fabricación de un PCB final. Ha sido necesario el estudio de las comunicaciones entre las partes, así como el establecimiento de un diagrama de flujo que gestione la rutina del sistema.

Índice

Agradecimientos	ix
Resumen	xi
Índice	xii
Índice de Tablas	xiv
Índice de Figuras	xv
1. Introducción	1
2. Análisis del diseño	3
3. Implementación	7
3.1. <i>Descripción general de la solución</i>	7
3.2. <i>Desarrollo de la solución</i>	13
3.2.1. Estudio del lector RFID	14
3.2.2. Caracterización de la antena	20
3.2.3. Formato de trama de comunicaciones de la radio RFID	22
3.2.4. Remote Measure Unit	27
3.2.5. Alimentación del Sistema	28
3.2.6. Esquema general	29
3.2.7. Definición de protocolo de comunicaciones entre lector y RMU.	30
3.2.8. Diagrama de flujo de la RMU	31
3.2.9. Montaje del prototipo	33
3.2.10. Funcionamiento	34
3.2.11. Consumo	36
4. Pruebas, replanteo y resultados	37
4.1. <i>Primera prueba</i>	37
4.2. <i>Replanteo</i>	40
4.3. <i>Segunda prueba</i>	43
4.4. <i>Solución final y validación</i>	44
4.5. <i>Futuras mejoras</i>	46
4.6. <i>Estudio de costes</i>	47
4.7. <i>Demostración del piloto</i>	49
5. RFID y LPWAN en el futuro	51
6. Anexos	53
6.1. <i>Anexo A. Especificaciones técnicas lector HYM360.</i>	53
6.2. <i>Anexo B. Especificaciones técnicas antena HYN503.</i>	56
6.3. <i>Anexo C. Etiqueta pasiva HYT-MT-U031b.</i>	58
6.4. <i>Anexo D. Etiqueta pasiva ALN-9662.</i>	59
6.5. <i>Anexo E. Antecedentes de RFID</i>	61
6.6. <i>Anexo F. Fundamentos de RFID.</i>	63
6.1.1. Frecuencias de Trabajo	63

6.1.2.	Componentes del Sistema	65
6.7.	<i>Anexo G. Estándares y regularizaciones RFID</i>	90
6.1.3.	EPC Class 1 Gen 2	94
6.8.	<i>Anexo H. RFID y Código de barras óptico</i>	98
6.9.	<i>Anexo I. RFID y NFC</i>	101
6.10.	<i>Anexo J. Redes IoT</i>	103
6.1.4.	LoRaWAN	105
6.1.5.	SigFox	107
6.1.6.	Narrow Band	108
6.1.7.	Comparativa LoRaWAN/SigFox/NB	109
Referencias		114

ÍNDICE DE TABLAS

Tabla 1. Matriz de tecnologías candidatas.	3
Tabla 2. LPWAN vs Red de Telefonía vs ZigBee y 802.15.4.	4
Tabla 3. Matriz de tecnologías candidatas. (En rojo las descartadas, amarilla las posibles y verde las más adecuadas).	5
Tabla 4. Lista de materiales.	48
Tabla 5. Pronósticos sobre LPWAN.	52
Tabla 6. Prestaciones RFID según frecuencia de trabajo.	65
Tabla 7. Grado de atenuación según material.	72
Tabla 8. Comparativa Gen2 – Gen1.	97
Tabla 9. Comparativa RFID – Código de barras óptico	99
Tabla 10. Prestaciones RFID – Códigos de barras ópticos.	100
Tabla 11. Comparativa LoRa - NB.	110
Tabla 12. Detalles técnicos de tecnologías LPWAN.	111
Tabla 13. Diferentes costes de LoRa, NB y SigFox.	113

ÍNDICE DE FIGURAS

Figura 1. Esquema de funcionamiento general.	1
Figura 2. Diagrama de bloques del sistema.	7
Figura 3. Esquema del <i>Gateway</i> .	8
Figura 4. Esquemático de la fuente y radio RFID.	9
Figura 5. PCB de la fuente de alimentación, antena y radio RFID.	10
Figura 6. Rutina del <i>Gateway</i>	11
Figura 7. Plataforma Sócrates IoT.	12
Figura 8. Lector RFID HYM360.	13
Figura 9. Antena UHF RFID HYN503.	13
Figura 10. Etiquetas pasivas. Arriba la HYT-MT-U031b, abajo la ALN-9662.	14
Figura 11. Kit de desarrollo con lector HYM360.	14
Figura 12. Montaje con kit de desarrollo.	15
Figura 13. Software proporcionado por el fabricante.	15
Figura 14. Detalle de <i>Single Inv</i> , <i>Multiple</i> y <i>Clean</i> .	16
Figura 15. Detalle de parte media y superior del software.	16
Figura 16. Conexión establecida.	17
Figura 17. <i>Link Set</i> .	17
Figura 18. <i>Basic Settings</i> .	18
Figura 19. <i>Single Inv</i> .	18
Figura 20. <i>Multiple</i> .	19
Figura 21. Frequency hopping.	19
Figura 22. Antena HYN503.	20
Figura 23. Rango de lectura de antena HYN503 ante etiqueta ALN-9662.	20
Figura 24. Rango de lectura de antena HYN503 ante etiqueta HYT-MT-U031b.	21
Figura 25. Device Monitoring Studio.	22
Figura 26. Detalle de tráfico filtrado, tanto de entrada como de salida.	23
Figura 27. Formato de trama de transmisión de datos.	23
Figura 28. Formato de trama para comando <i>Single Inv</i> .	24
Figura 29. Formato de trama de respuesta para comando <i>Single Inv</i> .	24
Figura 30. Comando <i>Single Inv</i> en Docklight.	25
Figura 31. Formato de trama para comando <i>Multiple</i> .	25
Figura 32. Formato de trama de respuesta para comando <i>Multiple</i> .	25
Figura 33. Comando <i>Multiple</i> en Docklight.	25
Figura 34. Formato de trama para comando <i>Stop</i> .	26

Figura 35. Formato de trama de respuesta para comando <i>Stop</i> .	26
Figura 36. Comando <i>Stop</i> en Docklight.	26
Figura 37. Comando visualizado en osciloscopio.	27
Figura 38. Regulador LM 2840 YMK-ADJ	28
Figura 39. Conexión general del <i>Gateway</i> .	29
Figura 40. Diagrama de paso de mensajes del sistema.	30
Figura 41. Diagrama de flujo de la RMU.	31
Figura 42. Prototipo terminado con conector de alimentación (izquierda) y antena (derecha).	33
Figura 43. Inicio del programa.	34
Figura 44. Encendido del módem y bucle reposo/lectura múltiple.	34
Figura 45. Lectura de etiquetas.	35
Figura 46. Envío de datos. Detalle de envío por NB y 2G.	35
Figura 47. Trama de datos visualizada en la plataforma.	35
Figura 48. Consumo del equipo. En el eje vertical mA, en el eje horizontal segundos.	36
Figura 49. Prototipo // Solución inicial.	37
Figura 50. Toma de alimentación a cuadro eléctrico.	37
Figura 51. Cubo de basura a recoger.	38
Figura 52. Vista frontal de estructura recogedora de cubos, con antena HYN503 en la parte inferior.	38
Figura 53. Vista lateral de estructura recogedora de cubos, con antena HYN503 en parte media.	39
Figura 54. Ubicación, resaltada en amarillo, candidata para sistema de antenas.	40
Figura 55. Dipolo con cable coaxial, de 16 cm de un extremo a otro.	41
Figura 56. Pérdidas de retorno, -27dB, a la frecuencia de 866.3 MHz.	41
Figura 57. Medidas a tener en cuenta en el replanteo. En rojo, la disposición de los tres dipolos.	42
Figura 58. Dipolo en cobertura, y cobertura completa.	42
Figura 59. Conector tipo F y splitter de 3 entradas.	42
Figura 60. Segunda prueba con nuevo sistema de antenas.	43
Figura 61. Cobertura de la solución final.	44
Figura 62. Electrónica alojada en la cobertura final.	44
Figura 63. RMU y placa con la etapa de alimentación, antena y radio RFID.	45
Figura 64. Zona de lectura de la solución final.	45
Figura 65. Léon Theremin, 1927.	61
Figura 66. Historia de RFID.	62
Figura 67. Banda de frecuencias.	63
Figura 68. Pulsera impermeable de RFID a 125 KHz.	64
Figura 69. Comparativa UHF - HF & LF.	64
Figura 70. Antena y chip en tag RFID.	65
Figura 71. Tag pasivo.	67
Figura 72. Esquemático de un tag RFID pasivo.	67

Figura 73. Simplificación del “Backscatter Signaling”.	68
Figura 74. Backscatter modulado usando un transistor como switch.	69
Figura 75. Procesado de etiquetas pasivas.	69
Figura 76. Procesado de etiquetas activas.	70
Figura 77. Tags activos.	70
Figura 78. Comparativa de tags pasivos, semi-pasivos y activos.	71
Figura 79. Interferencia.	73
Figura 80. Interferencia mutua.	73
Figura 81. Etiquetas RFID sin memoria interna (izquierda), y con memoria interna (punto negro en imagen a la derecha).	74
Figura 82. Forma de las antenas RFID.	77
Figura 83. UPC.	77
Figura 84. EPC.	78
Figura 85. Campos del estándar GID-96.	79
Figura 86. Integración de un UPC en un EPC.	79
Figura 87. La pila EPC.	80
Figura 88. Estructura de la tecnología RFID.	81
Figura 89. Antena RFID interactuando con un Tag.	82
Figura 90. Transmisión y recepción de señales del lector RFID.	83
Figura 91. La señal recibida no está correlada con la señal de la etiqueta.	83
Figura 92. Codificación PIE. Se define Tari como el intervalo de tiempo de referencia para la señalización entre lector y tag, y es la duración de data-0, comprendida entre 6.25 μ seg y 25 μ seg.	84
Figura 93. Ejemplos de modulación de subportadora.	85
Figura 94. Símbolos FM0 y máquina de estado finito.	85
Figura 95. Símbolos Miller y máquina de estado finito.	86
Figura 96. Otros tipos de codificación RFID.	86
Figura 97. Lector RFID.	87
Figura 98. Arquitectura típica de un sistema RFID genérico.	88
Figura 99. ISO/IEC 14443.	91
Figura 100. Convenio de protocolo NFC.	92
Figura 101. Estructuras de códigos de barras: (a) unidimensional con codificación EAN 13	98
Figura 102. Sistema de pago mediante NFC.	102
Figura 103. LPWAN, en comparación a otras tecnologías inalámbricas.	103
Figura 104. Comparativa LPWAN – 3G/4G/5G – ZigBee.	104
Figura 105. Arquitectura LoRaWAN.	106
Figura 106. Estructura de la red LoRaWAN.	106
Figura 107. Arquitectura SigFox.	107
Figura 108. Arquitectura NB.	109
Figura 109. Ventajas de NB, LoRa y SigFox de cara a IoT.	112



1. INTRODUCCIÓN

“Nada en la vida es para ser temido, es sólo para ser comprendido. Ahora es el momento de entender más, de modo que podamos temer menos.”

- Marie Curie -

En la actualidad, la interconexión digital de objetos cotidianos forma parte de uno de los ámbitos tecnológicos en mayor desarrollo. Este concepto, denominado como *Internet of Things*, constituye un cambio en la calidad y forma de vida de la sociedad, ofreciendo una serie de servicios específicos en diversos campos, así como una gran cantidad de nuevas oportunidades de acceso a datos.

Uno de los pilares en los que se soporta IoT es la identificación y gestión de objetos de forma automática, de tal forma que sea posible conocer, entre otros aspectos, la ubicación y estado de un objeto específico, ya sea en un momento concreto o a lo largo de un intervalo de tiempo establecido.

Este trabajo pretende satisfacer la necesidad de monitorizar la recogida de cubos de residuos urbanos que realiza un camión dentro de su ruta habitual. Para ello se propone un sistema que identifica de forma individual cada cubo y envía tal identificación a una base de datos mediante tecnología inalámbrica. Es importante conocer de antemano de qué forma se desarrolla la actividad que va a realizar el camión en su itinerario.

La dinámica es la siguiente; el camión se detiene en cada punto de recogida, un operario acerca los cubos de las inmediaciones al camión y otro operario los coloca en la estructura de recogida de forma individual, o por parejas. Una vez el cubo se vacía, se deja en el punto donde se recogió y se continúa al siguiente punto de recogida.

El objetivo es detectar cada cubo que se vacía, de la forma más eficiente e inalámbricamente, con una tasa de envío de datos suficiente para poder considerarse “en tiempo real” y en zona urbana. Los datos identificados se irán transmitiendo a una base de datos centralizada, de tal forma que pueda consultarse en cualquier momento mediante una interfaz API.

El esquema completo de funcionamiento es el siguiente:

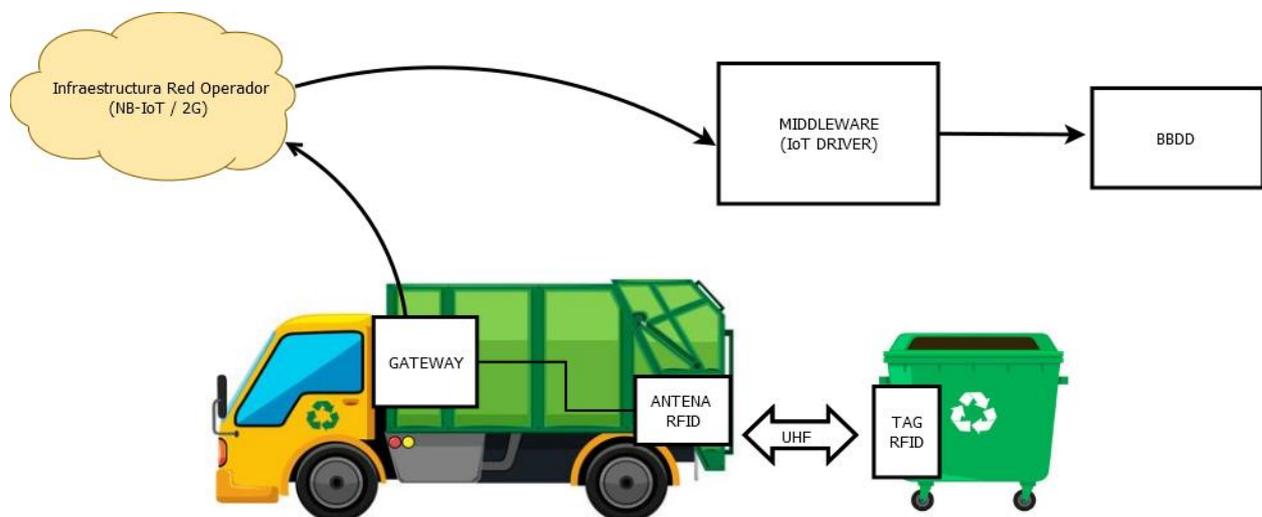


Figura 1. Esquema de funcionamiento general.

Se pueden distinguir las siguientes partes:

- **Tag RFID:** etiqueta pasiva que irá adherida a cada contenedor. Cada una de ellas posee un código único que identifica de manera singular cada contenedor de basura.
- **Antena RFID:** irá emplazada en un punto estratégico dentro del proceso de recogida de contenedores, de manera que pueda leer de forma fiable los tags mientras el cubo se vacía.
- **Gateway:** dispositivo encargado de realizar la lectura de tags. También realizará conexiones inalámbricas para el envío de datos.
- **Middleware:** quedará alojado en un servidor remoto con IP accesible, donde se recibirán los paquetes UDP que envíe el *Gateway*. Cuando la información sea recibida, la volcará a la base de datos.
- **BBDD:** base de datos SQL. Facilitará la monitorización de la actividad con una interfaz intuitiva y concisa.

Es importante señalar que la antena RFID y el *Gateway* se han representado de forma conceptual en este esquema general, es decir, que ambos elementos forman una sola unidad física, aunque en el esquema aparezcan como dos bloques unidos por una línea.

2. ANÁLISIS DEL DISEÑO

“Lo bueno de la ciencia es que es cierta, independientemente de si crees o no en ella.”

- Neil deGrasse Tyson-

Antes de implementar una solución funcional, se ha realizado un estudio de las tecnologías candidatas a formar parte del proyecto. Existen tres requisitos clave en la funcionalidad del equipo, a saber:

- Adquisición de datos del entorno: deberá realizarse de forma automática, precisa y rápida.
- Envío de datos a servidor: deberá tener la menor latencia posible.
- Protección física del equipo: El equipo deberá estar protegido del entorno de la forma más completa posible, teniendo en cuenta que estará expuesto a condiciones meteorológicas como sol, lluvia y viento.

Una vez considerados dichos requisitos, puede elaborarse una matriz donde se barajen todas las posibles soluciones a escoger. Para la protección del equipo se seleccionará aquella que cumpla con la norma CEI 60529, la cual se emplea para clasificar los diferentes grados de protección aportados por los contenedores que resguardan los componentes que constituyen un equipo. El primer dígito “x” representa la protección ante polvo, y el segundo dígito “y” representa la protección ante líquidos.

Adquisición de datos	Comunicaciones	Protección
Bluetooth	Narrow Band	IP [x][y]
ZigBee	LTE/4G	
RFID	LoRaWAN	
WiFi	SigFox	
Infrarrojos	Bluetooth	
Código de barras	ZigBee	
NFC	WiFi	
	WiMax	

Tabla 1. Matriz de tecnologías candidatas.

Se hará un análisis de cada una de las tecnologías candidatas a grandes rasgos, descartando aquellas que sean incompatibles en primera aproximación, y profundizando en las que parezcan más prometedoras. Se dará una valoración en base al cumplimiento de requisitos para facilitar la selección.

Para las tecnologías de adquisición de datos se buscarán aquellas que cumplan características como bajo coste de identificación, autosuficiencia energética y corto alcance.

La tecnología Bluetooth opera a una frecuencia de 2.4 GHz, con un rango óptimo de 10 metros. Su limitado alcance hace que se descarte para el envío de datos, dado a que el camión operará en una zona urbana determinada. A pesar de poder comunicar dispositivos en un corto alcance de forma sencilla y cómoda, requiere de un emparejamiento manual, lo cual no es adecuado a la hora de identificar objetos que se van recogiendo de forma ágil.

ZigBee es una tecnología inalámbrica más centrada en aplicaciones domóticas e industriales. Opera a una distancia máxima de 100 metros, lo que la descarta para el envío de datos. Una de sus aplicaciones es la identificación de vehículos, siendo la alta fiabilidad y el bajo coste dos de sus requisitos. Posee una baja capacidad de transmisión, de unos 250 kbps, y un protocolo sencillo que puede ser implementado sin limitación en sistemas microcontroladores, por lo que podría resultar apropiado para la identificación de cubos.

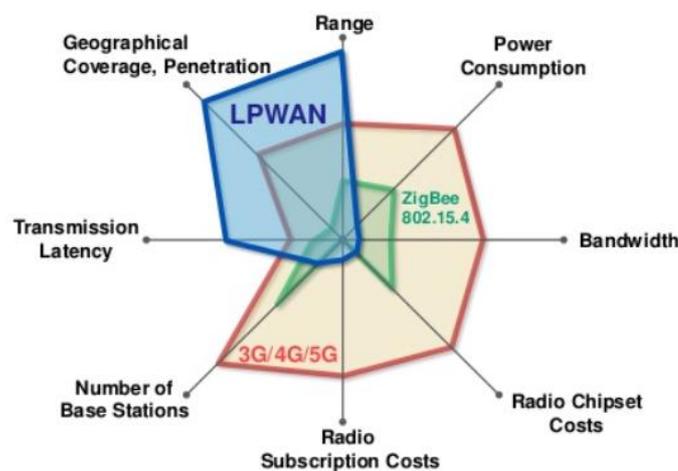


Tabla 2. LPWAN vs Red de Telefonía vs ZigBee y 802.15.4.

RFID tiene como objetivo la transmisión de datos a través de una etiqueta. Es una tecnología aplicada a la logística y seguimiento de activos, ya que no requiere línea de visión directa y puede identificar etiquetas en un rango entre 50cm y 100 metros. Las etiquetas pasivas tienen un coste muy bajo, en torno a 0,20 euros la unidad, y puede integrarse con otros elementos de control. Estas características hacen de RFID la candidata más prometedora. Puede encontrarse más información en el *Anexo F. Fundamentos de RFID*.

WiFi ofrece la posibilidad de crear una red inalámbrica a la que múltiples dispositivos pueden conectarse sin ningún problema de infraestructura ni gasto. Requiere de un establecimiento en la conexión que puede superar los 10 segundos, tiempo excesivo a la hora de identificar los cubos que se están vaciando. Además, habría que instalar un receptor en cada contenedor, lo que elevaría el coste. Para las comunicaciones tampoco resulta la opción óptima, ya que la distancia habitual de trabajo es de 50 metros. Puede aumentarse usando antenas específicas que amplían dicho rango a 30 km, pero su coste es elevado, en torno a 100 euros la antena. WiFi podría ser una alternativa si el camión almacenara los datos en su equipo y, al acabar el itinerario y dirigirse a la estación, volcara todos los datos de recogida al pasar por algún punto de acceso próximo. Sin embargo, esta opción descarta la idea de monitorizar en tiempo real la recogida de contenedores, lo que hace de WiFi una tecnología apenas apropiada en esta aplicación.

La tecnología infrarroja ofrece una velocidad de transmisión alta, alcanzando los 10Mbps, y utiliza un protocolo simple y componentes sumamente económicos. Sin embargo, la distancia de lectura es muy reducida, y es altamente sensible a objetos móviles que interfieran en la comunicación. De hecho, la propia luz solar puede interferir seriamente en la señal.

En lo referente a códigos de barras y NFC, se hace un análisis más específico en los anexos *H e I*. A grandes rasgos, NFC y los códigos de barras no resultan adecuados dado que las distancias máximas de lectura son de 20cm aproximadamente, y la información codificada en el código de barras es inalterable.

Para las tecnologías de comunicaciones, se buscarán aquellas que cumplan con características como cobertura geográfica, disponibilidad temporal, bajo coste de mantenimiento, compatibilidad evolutiva de redes y medio alcance con baja potencia.

Respecto a Narrow Band, LoRaWAN y SigFox, se ha hecho un estudio más detallado en el *Anexo J. Redes IoT*. Hay que mencionar brevemente que se ha seleccionado NB para las comunicaciones debido a su baja latencia y alta calidad de servicio, y que se adapta a zonas urbanas gracias a que se soporta en LTE. Además, NB posee un espectro licenciado y no tiene restricciones de potencia transmitida, superando también en seguridad a LoRaWAN y SigFox.

WiMax ofrece una red inalámbrica de área metropolitana, y posee un alcance de 50 km, con tasas de hasta 70 Mbps. Se usa especialmente en zonas alejadas de núcleos urbanos, por lo que a primera instancia no parece la mejor opción.

LTE ofrece rapidez, conexión en redes urbanas y menor saturación que la red 4G, aunque su coste es mayor que el de una LPWAN. Es por ello por lo que se dejará como solución posible pero no recomendable.

En cuanto a la protección, atendiendo a la norma CEI 60529 para el primer dígito, se necesita el aislamiento ante polvo, por lo que el mínimo valor admisible sería de 5. Respecto al segundo, no se requiere protección contra inmersión, pero sí contra chorros de agua y lluvia, por lo que el valor mínimo sería de 6. Así, se establecerá la protección como IP56 como mínimo.

Adquisición de datos	Comunicaciones	Protección
Bluetooth	Narrow Band	IP56
ZigBee	LTE/4G	
RFID	LoRaWAN	
WiFi	SigFox	
Infrarrojos	Bluetooth	
Código de barras	ZigBee	
NFC	WiFi	
	WiMax	

Tabla 3. Matriz de tecnologías candidatas. (En rojo las descartadas, amarilla las posibles y verde las más adecuadas).

Atendiendo a la tabla anterior, se han escogido las tecnologías RFID para la adquisición de datos y la tecnología Narrow Band - IoT para las comunicaciones del equipo con la base de datos. Además, se ha añadido en la funcionalidad una conmutación a 2G si, tras un período de tiempo, fuera imposible realizar la conexión mediante NB-IoT por motivos de cobertura, por ejemplo.

Respecto a la alimentación del sistema, la fuente deberá regular una tensión constante a partir del cuadro eléctrico del camión, que alimente los equipos electrónicos. Para ello se empleará el convertidor buck que cumpla la especificación conveniente.

3. IMPLEMENTACIÓN

“La ciencia puede divertirnos y fascinarnos, pero es la ingeniería la que cambia el mundo.”

- Isaac Asimov -

3.1. Descripción general de la solución

El sistema constará de un dispositivo *Gateway* instalado en el camión, el cual identificará los cubos que se van recogiendo y enviará los datos inalámbricamente a la base de datos. Mediante una API, se podrán consultar los mensajes que se reciben.

El diagrama de bloques completo, incluyendo el dispositivo *Gateway*, es el siguiente:

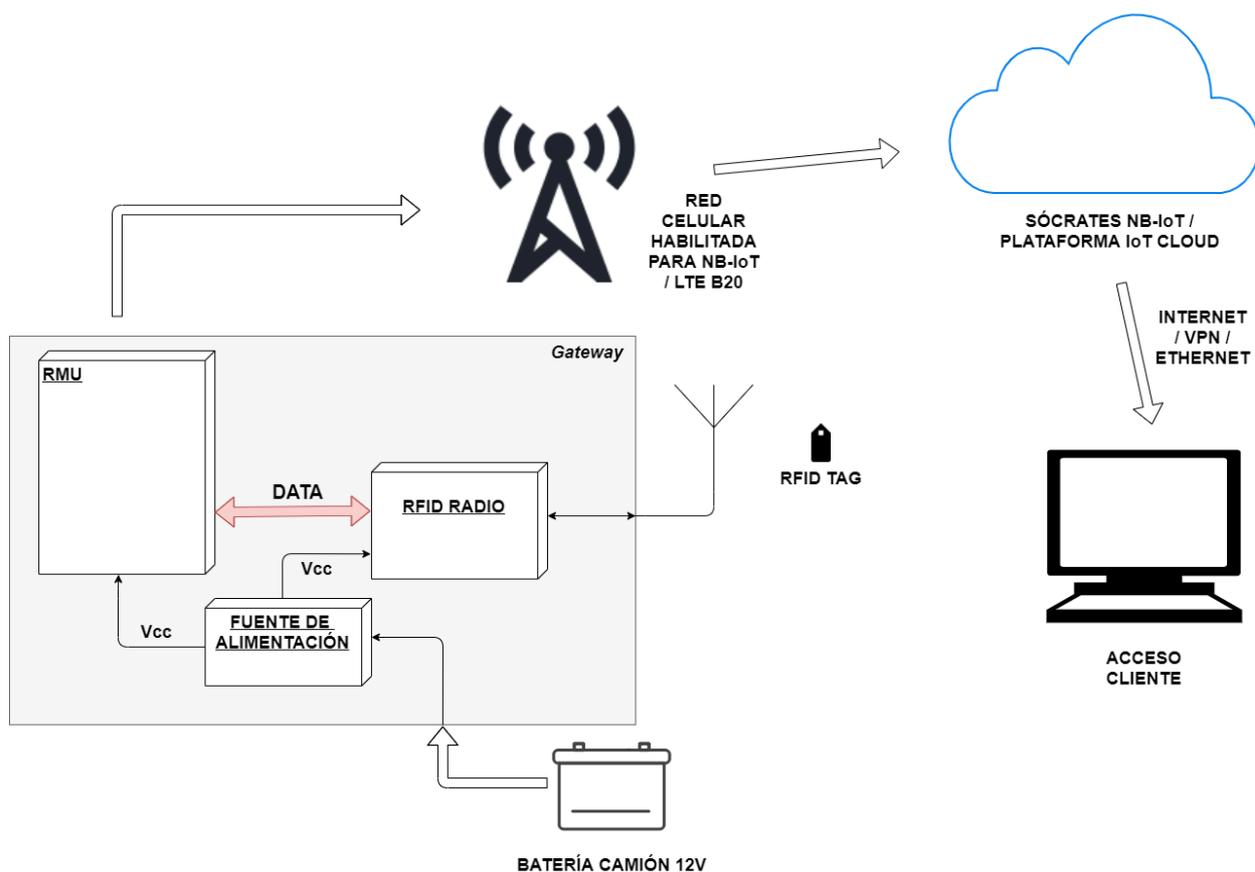


Figura 2. Diagrama de bloques del sistema.

Para la radio RFID se ha elegido el lector HYM360 de la compañía Winnix. Ofrece un kit de desarrollo y software, lo que permite estudiar las comunicaciones y conectarlo a otro dispositivo maestro que le envíe comandos.

Para la RMU (Remote Measure Unit) se ha elegido el dispositivo del mismo nombre de la compañía Noxium.

Es una pasarela abierta IoT para transportar información por paquetes al servidor IP fijado de forma fiable, segura y encriptada. A su vez dispone de diversas interfaces locales de comunicaciones para la programación y monitorización de comandos. Hará las veces de maestro, controlará el modo de funcionamiento del lector RFID y enviará los datos a la nube. Funciona con un modo de operación optimizado y baja tasa de envío de datos en la red.

Para la fuente se ha elegido el integrado LM2840XMK, el cual hará posible la conexión del dispositivo a la batería del camión.

El dispositivo *Gateway* es el siguiente:

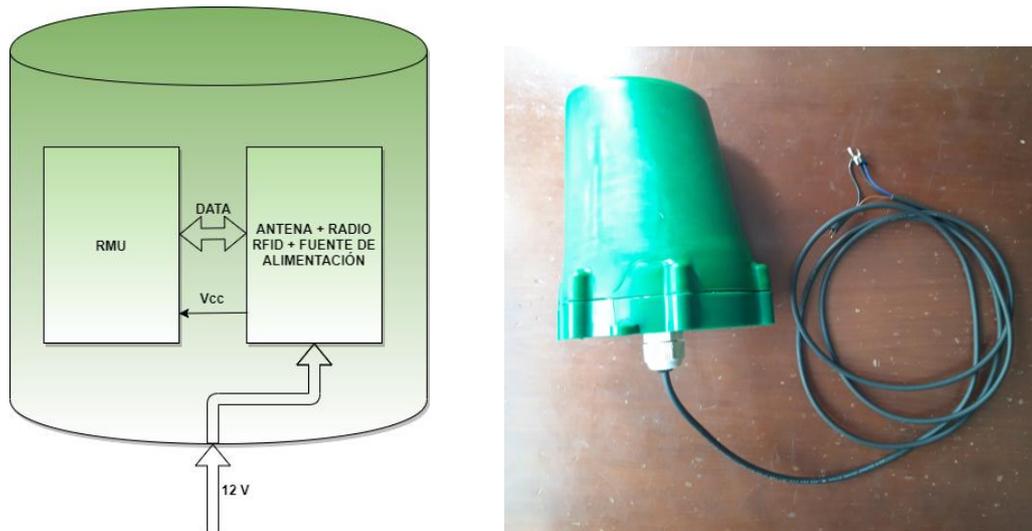


Figura 3. Esquema del *Gateway*.

En él se alojan dos unidades:

- La RMU, descrita anteriormente.
- El PCB, que integrará la radio RFID, la antena y da fuente de alimentación.

Ambas irán enfrentadas en estructura de mezzanina, y unidas mediante torretas.

El esquemático del PCB donde se integran la radio RFID y la fuente es el siguiente:

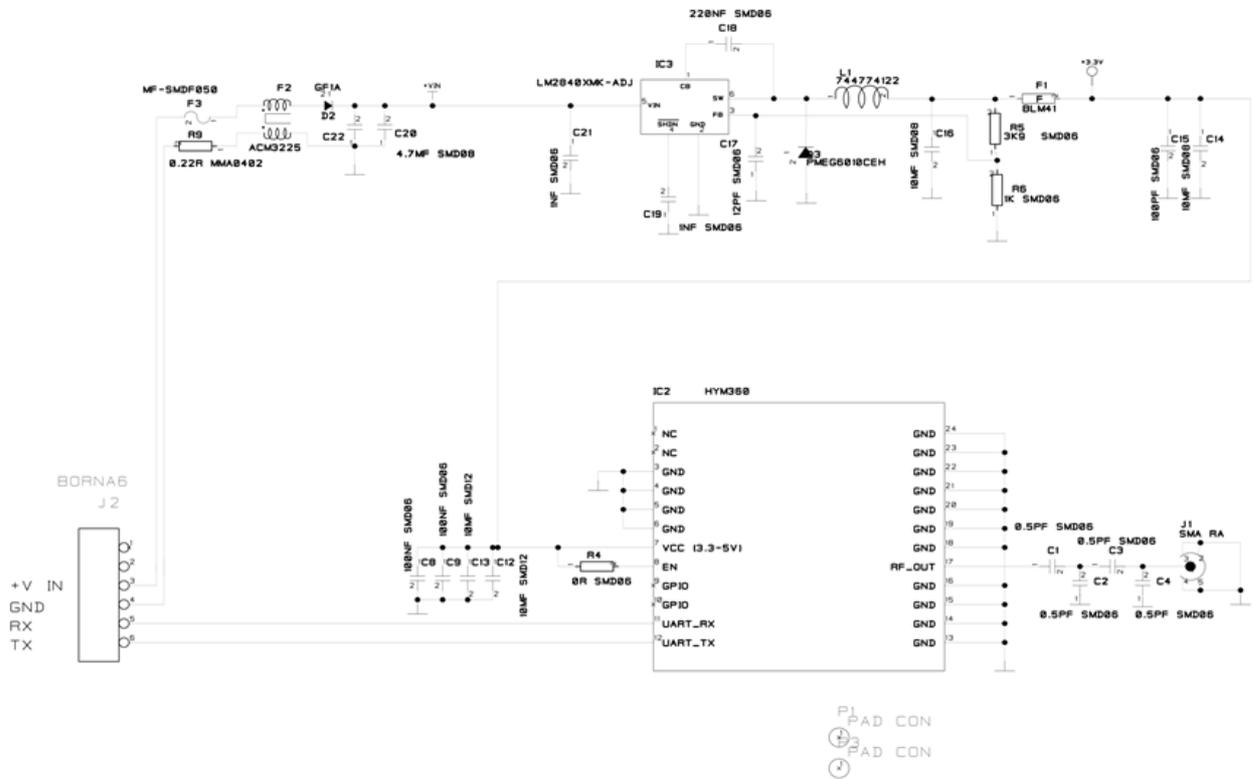


Figura 4. Esquemático de la fuente y radio RFID.

Se puede observar una primera etapa de protección de polaridad, por si se conectara accidentalmente al revés. A continuación, la fuente que proporcionará una tensión estable a la salida de 3.7V tanto al lector HYM360 como a la RMU, la cual no se ha incluido en el esquemático por motivos de confidencialidad. Por último, el lector RFID y la antena. El conector tendrá como entradas:

- La tensión de entrada +Vin; procedente de la batería del camión a 12V.
- El pin de recepción de datos del lector RFID, el cual será pin de transmisión de la RMU.
- El pin de transmisión de datos del lector RFID, el cual será pin de recepción de la RMU.

A continuación se muestra el PCB donde se ha integrado la antena, la fuente de alimentación y la radio RFID. La antena es de tipo meandro y, aunque la optimización se vuelve más crítica y sus pérdidas son más altas que un dipolo estándar, mejora la omnidireccionalidad y ofrece unos requisitos de espacio más pequeños.

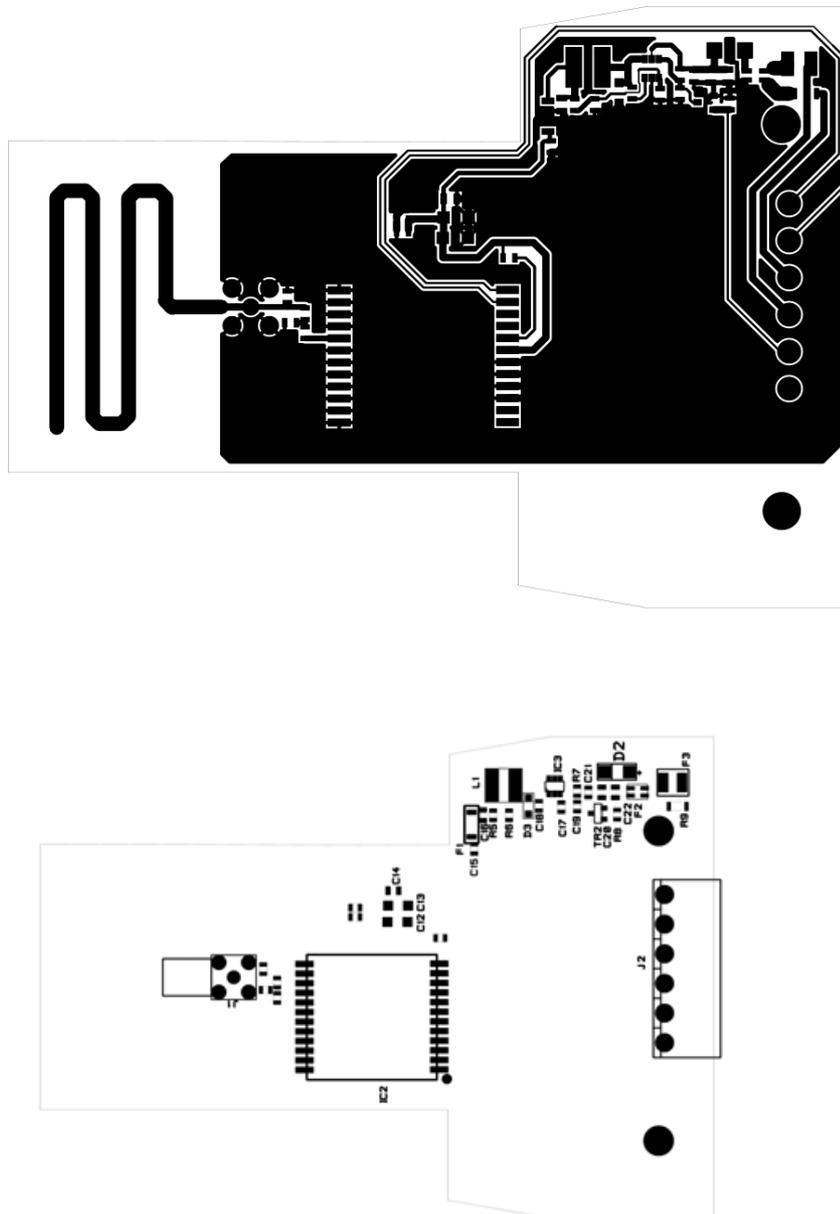


Figura 5. PCB de la fuente de alimentación, antena y radio RFID.

La rutina que sigue el *Gateway* es la siguiente; la radio RFID recibirá comandos de la RMU para realizar diversas funciones. Éstas se definen como:

- Escucha simple, realizada mediante el comando *Single Inv.*
- Escucha a discreción (o continua), realizada mediante el comando *Multiple.*
- Detención de escucha a discreción, realizada mediante el comando *Stop.*

Una escucha se define técnicamente como una portadora que la antena propaga al medio con objeto de energizar

un tag y realizar el proceso de backscattering (más información en *Anexo F. Fundamentos de RFID*). Esta escucha puede realizarse de forma masiva, es decir, el módulo RFID emite entre 20 y 30 portadoras por segundo, o de forma individual, en la que solo se emite una portadora.

Inicialmente, se necesita saber si hay o no cubos en el sistema de recogida del camión. Para ello, la radio RFID emite de forma continua durante T1 segundos, y permanece en reposo T2 segundos. Con esta dinámica se consiguen dos cosas; la primera, reducir el consumo del dispositivo y, la segunda, evitar que el módulo RFID se sobrecaliente. En este bucle, señalado en la figura inferior con un rectángulo discontinuo rojo, se permanece hasta que un tag próximo al sistema conteste a la radio RFID. Este bucle modela la dinámica del camión cuando se está desplazando de un punto de recogida a otro.

Cuando el camión se detiene en un punto de recogida y un operario coloca un cubo en el sistema de vaciado, el tag del cubo, que ahora se encuentra en la distancia de lectura efectiva de la antena, se energiza y contesta, enviando su ID. El módulo RFID lo recibe, pasando al siguiente bucle. En éste, la radio envía cada T_SingInv (tiempo entre lecturas individuales) una lectura simple, que el tag contestará mientras el cubo se esté vaciando.

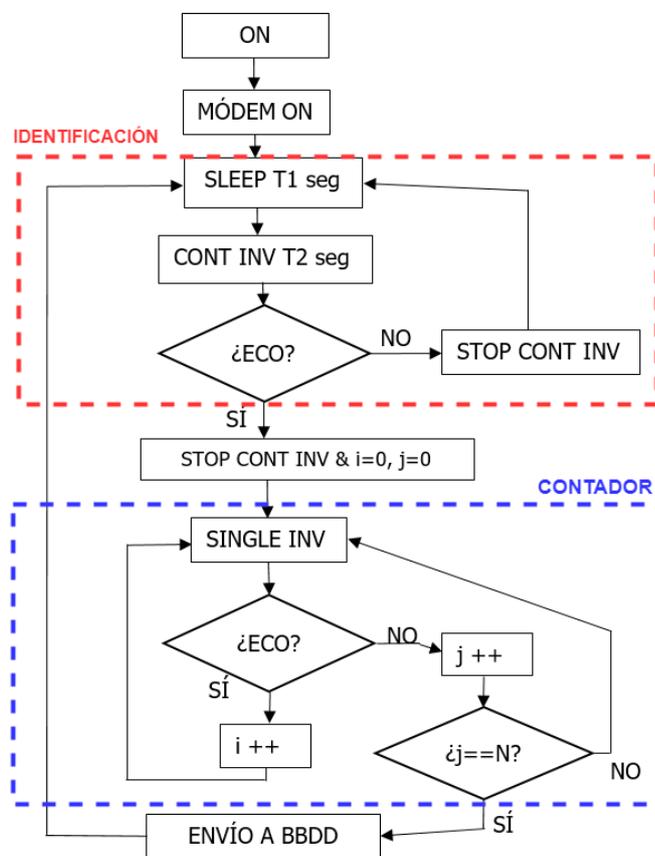


Figura 6. Rutina del Gateway

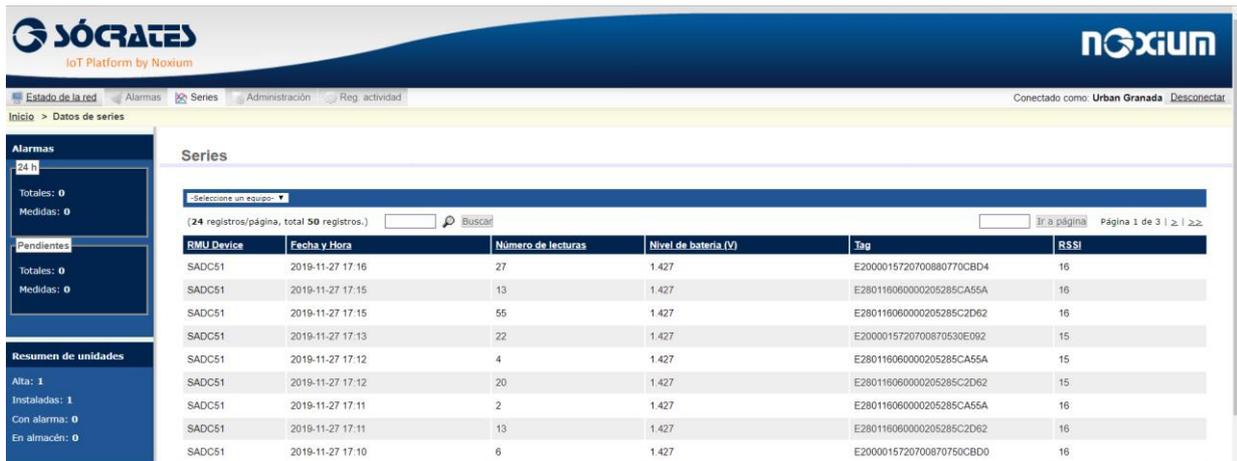
Dos contadores gestionan este bucle. El primero; i , aumenta en uno cada vez que una escucha simple es contestada exitosamente por un tag. De esta manera, i se incrementará en uno cada T_SingInv mientras el cubo se esté vaciando, es decir, mientras se encuentra sujeto al sistema de vaciado y a una distancia de lectura efectiva de la antena.

El segundo índice, j , sirve para salir del bucle. Cuando el cubo se vacía y se retira del sistema de recogida, el Gateway necesita saber que ese cubo ya ha sido procesado. Este evento se gestiona de la siguiente manera; cuando el cubo se retira, el módulo RFID sigue haciendo lecturas simples, pero esta vez el tag no contestará ya que no se encuentra dentro de la distancia de lectura de la antena. De tal manera, cuando una lectura sencilla no tiene respuesta, se incrementa en uno el índice j , de forma que cuando llegue a N lecturas simples insatisfactorias se da ese cubo como retirado, y se procede a enviar al servidor la información del tag. Dicha información

contiene el ID del tag, y el número de veces que se ha leído el cubo (valor del índice i).

Como el cambio de cubo del sistema de recogida puede hacerse de forma ágil y dinámica, es posible que un segundo cubo se coloque en el sistema de recogida durante el intervalo de escuchas simples insatisfactorias que esté realizando el módulo RFID antes de enviar los datos. En este caso, el módulo almacenaría los datos del primer cubo procesado, y comenzaría a contar el segundo. Este solapamiento podría repetirse con todos los cubos de un mismo punto. Una vez acabada la gestión de un punto de recogida, se mandaría un mensaje con todos los ID's identificados, y cuántas veces se ha leído cada uno.

El acceso a los datos se realizará a través de la plataforma IoT Sócrates, proporcionada por la compañía Noxium. En ella podemos observar los campos que se rellenan de forma automática.



The screenshot shows the 'Sócrates IoT Platform by Noxium' interface. The main content area displays a table titled 'Series' with the following data:

RMU Device	Fecha y Hora	Número de lecturas	Nivel de batería (V)	Tag	RSSI
SADC51	2019-11-27 17:15	27	1.427	E2000015720700880770C8D4	16
SADC51	2019-11-27 17:15	13	1.427	E280116060000205285CA55A	16
SADC51	2019-11-27 17:15	55	1.427	E280116060000205285C2D62	16
SADC51	2019-11-27 17:13	22	1.427	E2000015720700870530E092	15
SADC51	2019-11-27 17:12	4	1.427	E280116060000205285CA55A	15
SADC51	2019-11-27 17:12	20	1.427	E280116060000205285C2D62	15
SADC51	2019-11-27 17:11	2	1.427	E280116060000205285CA55A	16
SADC51	2019-11-27 17:11	13	1.427	E280116060000205285C2D62	16
SADC51	2019-11-27 17:10	6	1.427	E2000015720700870750C8D0	16

Figura 7. Plataforma Sócrates IoT.

En la imagen anterior pueden comprobarse los campos RMU Device, que corresponde al ID del dispositivo, junto a los campos fecha y hora, número de lecturas (índice i), ID del tag y RSSI. Los datos se envían como cadena de caracteres y se presenta en la plataforma de manera ordenada para tener un control de los datos en “tiempo real”.

3.2. Desarrollo de la solución

En este apartado se expone el procedimiento seguido a la hora de integrar todos los elementos del equipo. En primer lugar se elaboró un prototipo inicial con el que se realizaron las pruebas. Dicho prototipo se detalla en este apartado. Finalmente, a raíz de dichas pruebas, se llegó a un replanteo del diseño para dar lugar a la solución final, descrita en el capítulo siguiente.

Primeramente, se ha adquirido un lector RFID. Dicho módulo cumple con el protocolo EPC C1 G2, su frecuencia de trabajo abarca de los 840 a los 960 MHz, con una antena estándar de 2 dBi, y distancia de lectura de hasta 2 metros. Con un bajo consumo de energía, una fuente de alimentación simple y un circuito de interfaz, se puede establecer un sistema RFID estable y de alto rendimiento. Es adecuado para el comercio minorista, control de acceso, industria médica, seguimiento de alimentos, anti-falsificación...

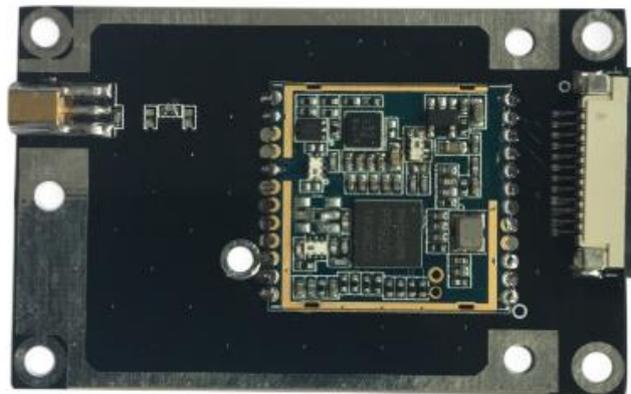


Figura 8. Lector RFID HYM360.

Las especificaciones técnicas de este lector quedan adjuntadas en el *Anexo A*.

La antena que se ha empleado ha sido la siguiente:



Figura 9. Antena UHF RFID HYN503.

Los detalles técnicos de la antena se adjuntan en el *Anexo B*. Es una antena general para aplicaciones UHF con alta ganancia y bajo VSWR¹. La antena es adecuada para entornos severos por su diseño impermeable con doble junta de silicona y refuerzo de la carcasa.

¹ [37] Voltage Standing Wave Ratio, denominado en castellano Relación de Onda Estacionaria. La Relación de Onda Estacionaria o ROE se refiere a la razón geométrica existente entre el valor máximo y el valor mínimo de la amplitud de voltaje observado en una condición de onda estacionaria eléctrica como sería a lo largo de una línea de transmisión. Este fenómeno se explica mediante los conceptos de onda directa y

Por último, se han adquirido dos tipos diferentes de etiquetas. Las primeras se describen en el Anexo C. Las segundas se detallan en el anexo D. **Ambas son pasivas.**



Figura 10. Etiquetas pasivas. Arriba la HYT-MT-U031b, abajo la ALN-9662.

3.2.1. Estudio del lector RFID

Para realizar las primeras pruebas de funcionamiento y familiarizarse con la dinámica de estos dos elementos, se incluía un kit de desarrollo.



Figura 11. Kit de desarrollo con lector HYM360.

onda reflejada. La relación de onda estacionaria es un número positivo sin dimensiones y siempre mayor o igual a uno. Si la onda reflejada es cero, no existirán máximos ni mínimos, o en otras palabras la amplitud es constante, y por lo tanto el valor ROE=1. Por el contrario, si existe una onda reflejada, aparecerán voltajes máximos y mínimos y el ROE será >1 . En el límite, si toda la onda directa se refleja habrá valores máximos y puntos donde el voltaje mínimo es cero, en este último caso el ROE será infinito.

En primer lugar, se estudiaron las comunicaciones que emplea el lector, es decir, los mensajes que envía y recibe en su ciclo de trabajo. Para ello se hizo el siguiente montaje, conectando el kit de desarrollo al portátil mediante un cable USB-RS232.

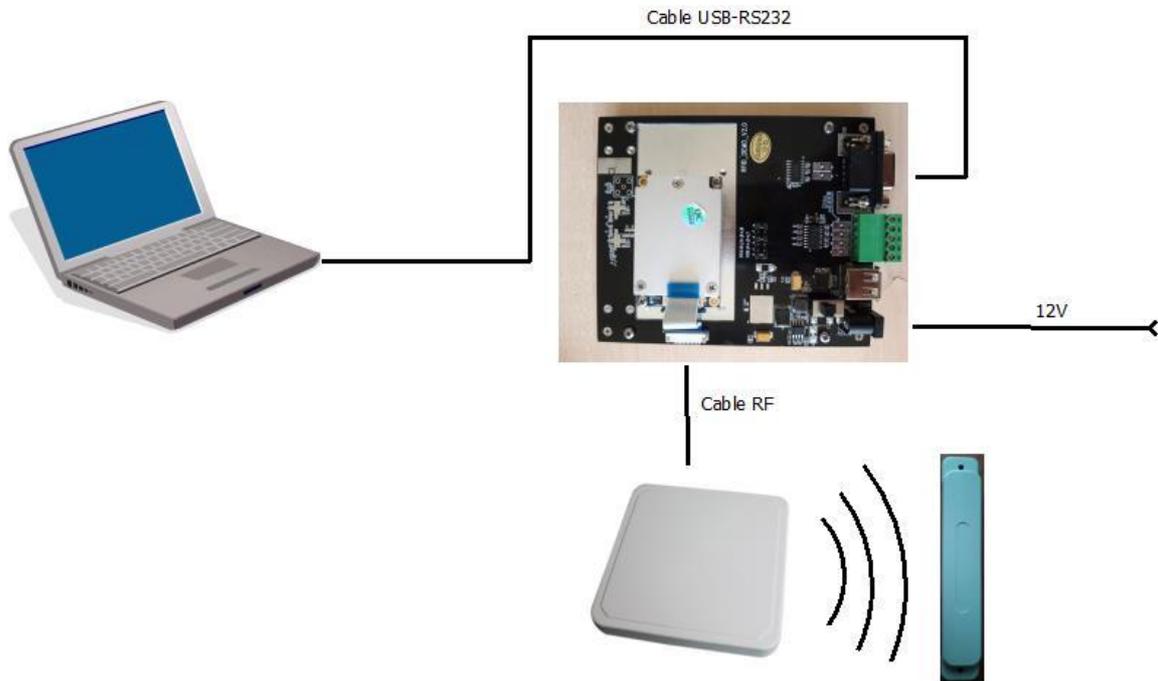


Figura 12. Montaje con kit de desarrollo.

El software, proporcionado por el fabricante, permite enviar comandos al lector mediante una interfaz sencilla. Pueden realizarse algunos ajustes previos como la tasa de baudios, el idioma y el puerto por el que se va a realizar la conexión.

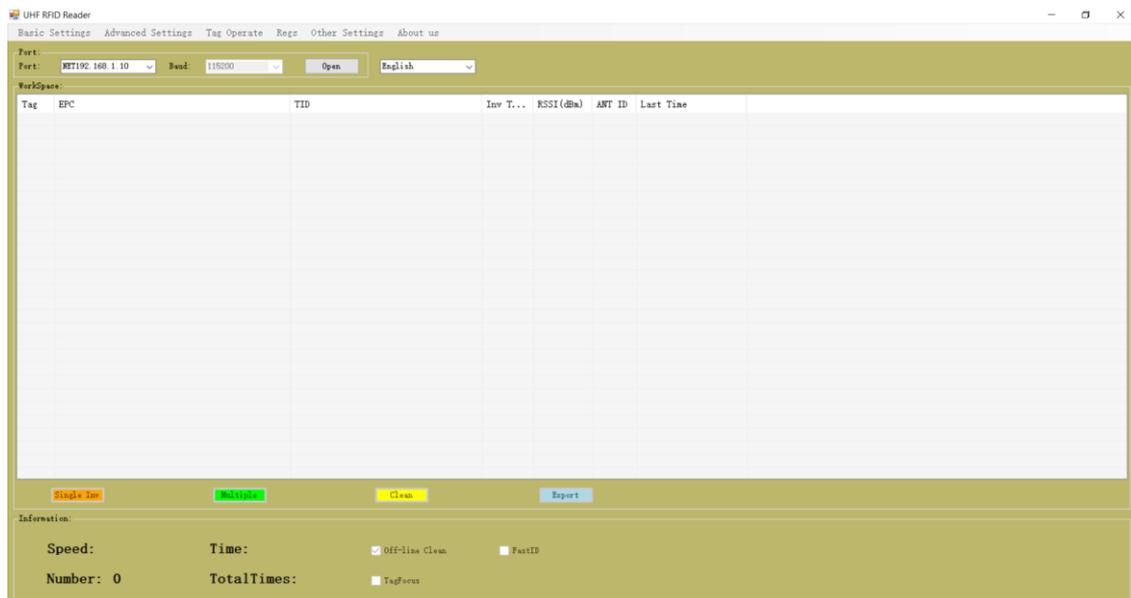


Figura 13. Software proporcionado por el fabricante.

En la parte inferior de la pantalla pueden apreciarse cuatro pulsadores, teniendo especial interés tres de ellos. El primero de ellos, *Single Inv*, realiza una única lectura del entorno. El segundo, *Multiple*, realiza un barrido constante del entorno en busca de etiquetas. Por último, *Clean*, limpia la pantalla de tags leídos para empezar desde el principio.

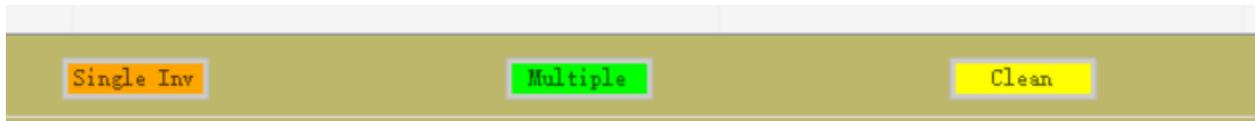


Figura 14. Detalle de *Single Inv*, *Multiple* y *Clean*.

En la parte media y superior de la pantalla, se puede apreciar la tabla vacía de tags, incluyendo su EPC, TID, el número de veces que se ha leído, su RSSI en dBm, el ID de la antena (en caso de tener más de una), y la hora a la que se leyó por última vez. Este formato nos permite confirmar que el lector puede leer más de un tag. Nótese que la barra superior, en la figura 52, se muestra en translúcido, dejando tales ajustes disponibles solo cuando la conexión esté abierta.

Una vez terminadas las conexiones dispuestas en la Figura 51, se ajusta la tasa de baudios a 115200 (recomendación del fabricante) y se pulsa *Open* para abrir la conexión.

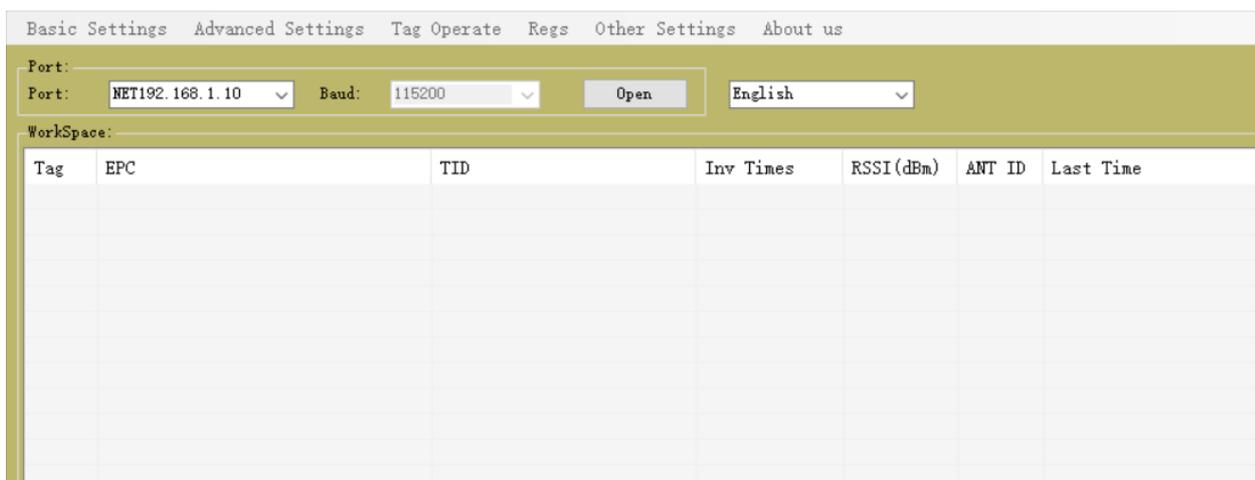


Figura 15. Detalle de parte media y superior del software.

Una vez abierta la conexión, podemos comprobar que la barra, antes translúcida, pasa a ser accesible.

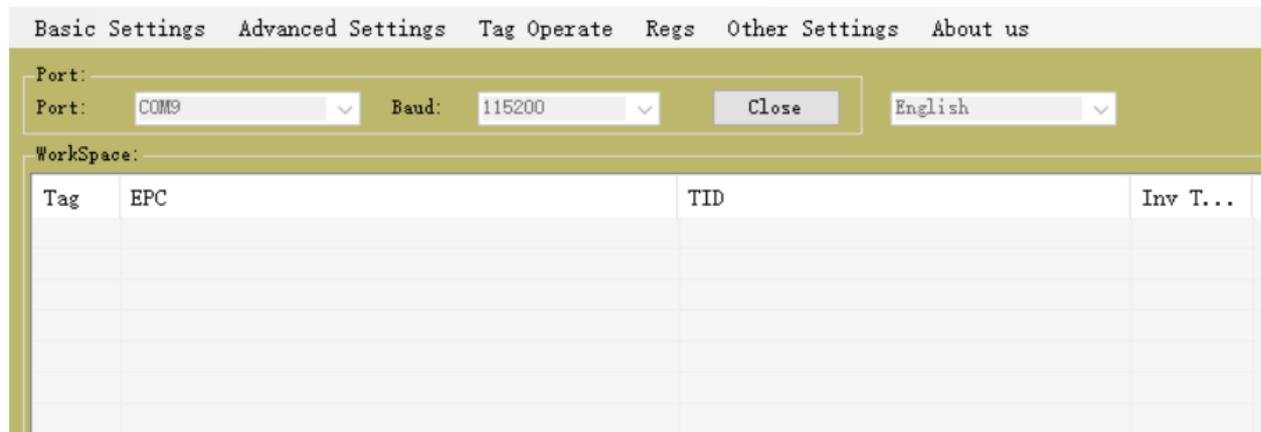


Figura 16. Conexión establecida.

Si se exploran los ajustes básicos, se pueden establecer valores como:

- Potencia de transmisión: se ha fijado el valor a la máxima potencia admisible, 25 dBm.
- Región de operación: Europa, en esta selección el lector trabajará con frecuencias comprendidas entre 865.7 MHz y 867.5 MHz.

En la Figura 57 se pueden comprobar ciertos parámetros de interés, como la versión del dispositivo o la temperatura del micro. Otros valores aparecen con el valor *Get Failed*. Esto se debe a que el modelo de este lector es, en cuanto a prestaciones, de los más limitados, y este software + kit de desarrollo pueden soportar también lectores más avanzados que si admiten ajustes más complejos, como la posibilidad de usar más de una antena, frecuencias de salto (FHSS)...

Por curiosidad hay que comentar que el lector admite un ajuste en la modulación del enlace, tal como se muestra en la siguiente pestaña:

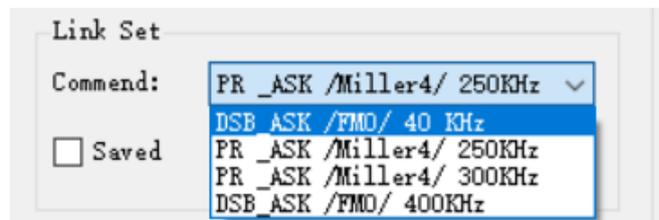


Figura 17. Link Set.

The screenshot shows the 'Basic Settings' window with the following sections:

- Tx Power:** Tx Power: 30 (Set), Saved: 25 (Get)
- Region Set:** Region: China2 (Set), Saved: Europe (Get)
- FHSS:** num: 0 (Add), Freq: 922.375 MHz (Set), Default (Get)
- Ant Set:** Ant Set: ANT1 (Set), Saved: ANT3, ANT4 (Get)
- Version Info:** Software: V2.1.4, Hardware: 1.31 (Get), Firmware: 3.01, ModuleID: 00000000
- Temperature:** Temp: 20 °C (Get)
- Link Set:** Commend: PR_ASK / Miller4 / 250KHz (Set, Get)
- Temperature protect:** Temp Protect (checkbox)
- Ant work time (ms):** ANT1: 0, ANT2: 0, ANT3: 0, ANT4: 0 (Set, Get)
- Interval time (ms):** Interval time: (Set, Get)
- Buzzer:** Ring (button)
- GPIO:** GPIO (GPIO1~4 is input, GPIO5~8 is output), GPIO1-8 (checkboxes), Get OK (Get)

Figura 18. *Basic Settings.*

Se deja de lado la pestaña de *Advanced Settings* ya que todos los parámetros ajustables aquí, como filtros, algoritmos o contraseñas, no tienen relevancia, debido a que, como se comentó antes, este lector no funciona con tales prestaciones.

Una vez situada la etiqueta a una distancia cercana (10 cm) de la antena, se procede a comprobar la lectura.

Pulsando el botón de *Single Inv*, se obtiene el siguiente resultado:

Tag	EPC	TID	Inv T...	RSSI (dBm)	ANT ID	Last Time
1	E2-80-11-60-60-00-02-05-28-5C-2D-62		1	0	1	19/06/2019 16:33:30

Figura 19. *Single Inv.*

Donde se pueden observar el EPC, número de veces leído (1), la antena (en este caso una), y la hora de lectura.

El valor de RSSI se corresponde a 0 debido a que el lector no ofrece este parámetro.

Pulsando el botón de *Multiple*, se observa lo siguiente:

Tag	EPC	TID	Inv T...	RSSI (dBm)	ANT ID	Last Time
1	E2-00-00-15-72-07-00-87-07-50-CB-D0		43	0	1	19/06/2019 16:39:54
2	E2-80-11-60-60-00-02-05-28-5C-2D-62		132	0	1	19/06/2019 16:39:54
3	E2-00-00-15-72-07-00-87-05-20-E3-24		23	0	1	19/06/2019 16:39:54
4	E2-00-00-15-72-07-00-88-03-40-EE-27		159	0	1	19/06/2019 16:39:53

Figura 20. *Multiple*.

El software muestra todos los tags leídos en las inmediaciones de la antena. Nótese que el campo TID se muestra vacío debido, una vez más, a las limitaciones del HYM360. También señalar el principio de la cabecera de los tags. Los de pegatina comienzan con los octetos E2-00-00... mientras que los de adherencia magnética empiezan con E2-80-11... Por último, anotar la velocidad de lectura de etiquetas. Dicha cifra se señala en la parte inferior izquierda del software, y no es un valor estable. Varía en el tiempo en función de la distancia y número de tags y, tras una serie de pruebas, se llegó a la conclusión de acotar la velocidad de lectura a un margen entre 20 y 30 lecturas por segundo, debido al carácter pseudoaleatorio de dicha variable.

Por último, hay que comentar que el lector emite realizando saltos de frecuencia (frequency hopping) de 600kHz, es decir, 865.7 MHz, 866.3 MHz, 866.9 MHz y 867.5 MHz. Esto se hace para resolver problemas de interferencia destructiva.

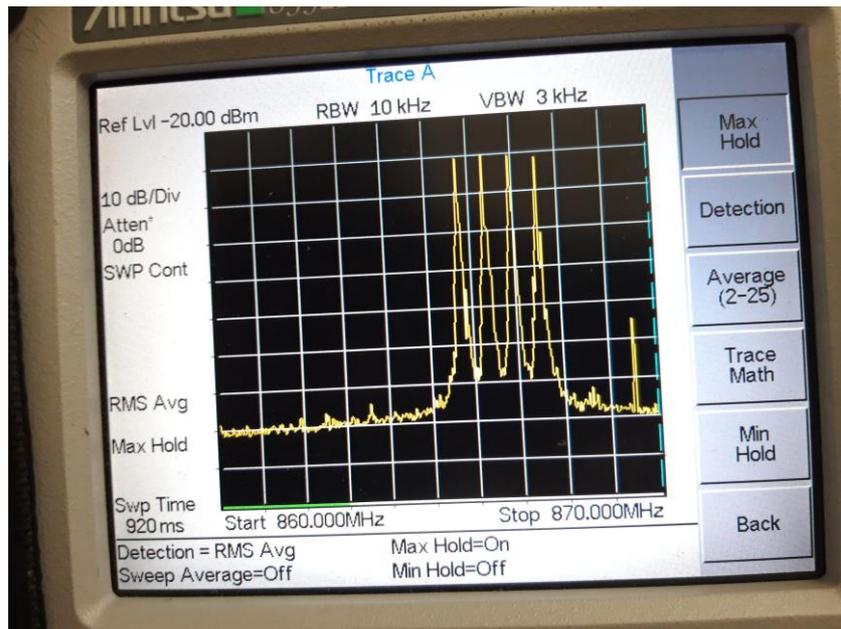


Figura 21. Frequency hopping.

En la imagen anterior se pueden observar las cuatro frecuencias de salto. Hay que aclarar que para dicha medida se ha realizado un *Max and Hold*, de modo que el analizador de espectro represente los máximos de la señal capturada y los mantenga en la representación.

3.2.2. Caracterización de la antena

A continuación, se realizó un estudio de la radiación de la antena, para obtener el área alrededor de ésta en la cual los tags serían legibles. Dicho estudio se ha llevado a cabo de forma experimental, es decir, haciendo barridos en modo *Multiple* y esbozando un diagrama de radiación acorde a los límites de lectura. Se ha realizado con ambas etiquetas. Dado que el plano vertical y horizontal es el mismo, solo se ha esbozado uno de ellos.



Figura 22. Antena HYN503.

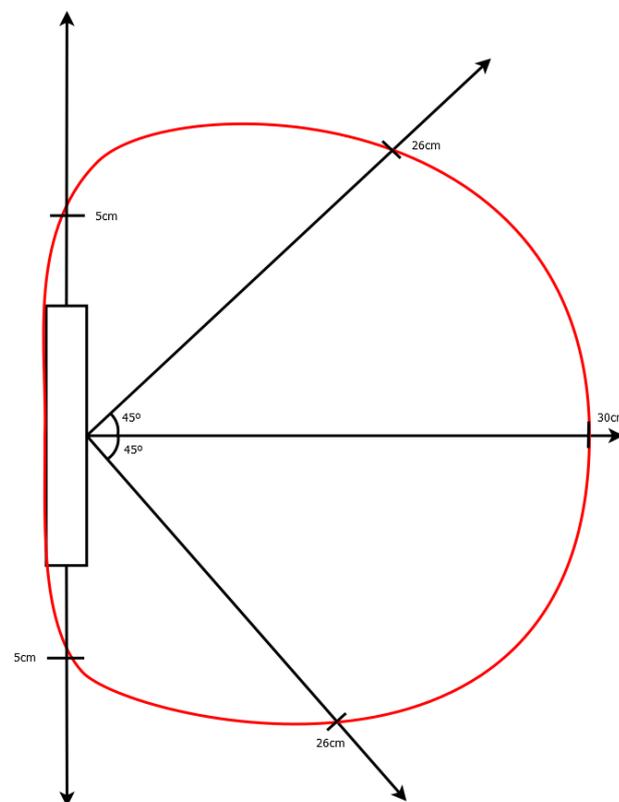


Figura 23. Rango de lectura de antena HYN503 ante etiqueta ALN-9662.

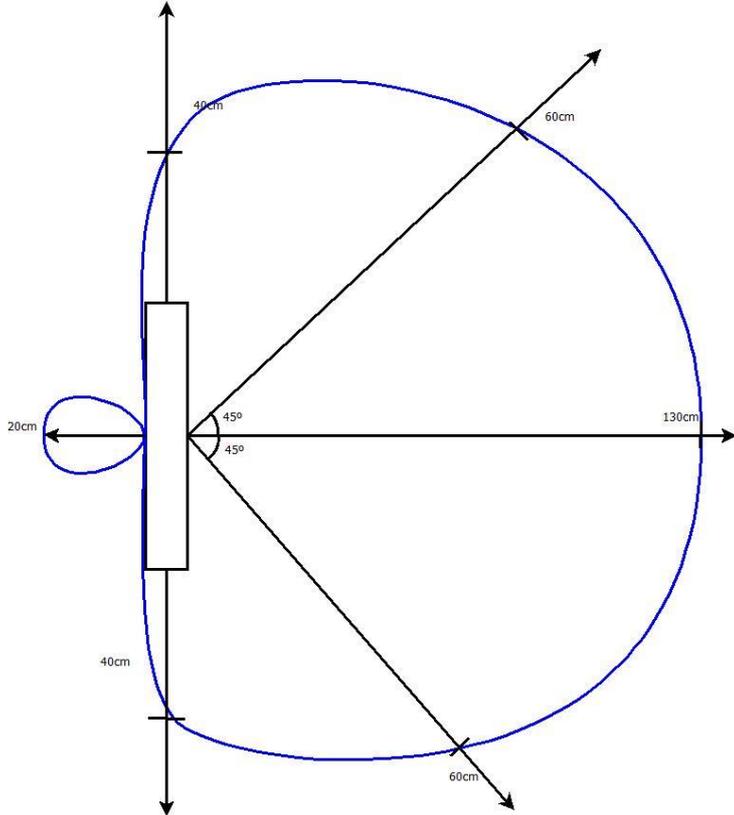


Figura 24. Rango de lectura de antena HYN503 ante etiqueta HYT-MT-U031b.

Ante tales resultados, la etiqueta HYT-MT-U031b muestra un alcance mayor a la ALN-9662.

3.2.3. Formato de trama de comunicaciones de la radio RFID

Tras caracterizar la antena y obtener un área efectiva de lectura, se ha pasado a estudiar con más profundidad las comunicaciones entre el lector y el software proporcionado por el fabricante. Para ello se ha empleado el software Device Monitoring Studio, en el cual se puede ver el tráfico de datos por el puerto de comunicaciones que se seleccione. Con el software preparado se realizaron las mismas pruebas antes descritas (*Single Inv*, *Multiple*, *Stop*) y se observaron los siguientes resultados.

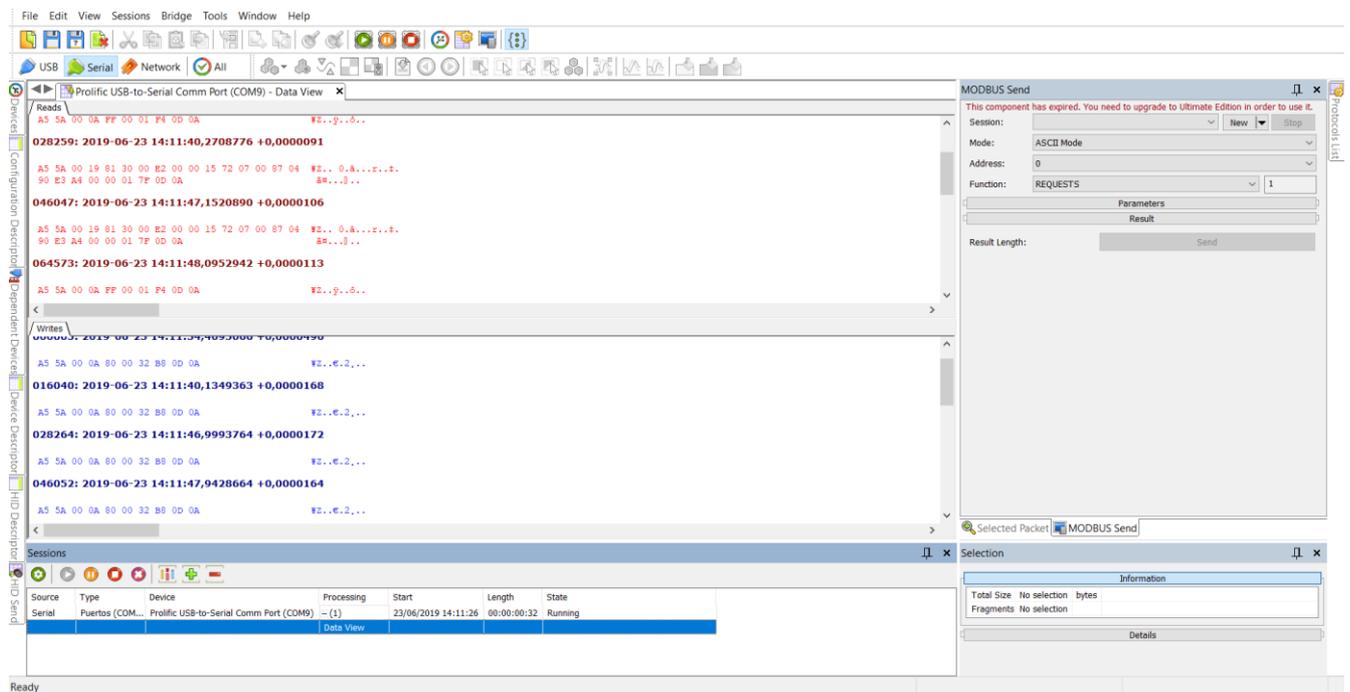


Figura 25. Device Monitoring Studio.

Puede observarse un intercambio de tramas hexadecimales entre el lector y el software, por lo que hay que centrarse en buscar el formato de trama adecuado para poder transmitir comandos al lector directamente desde un micro u otro elemento externo que pueda ir montado en el prototipo.

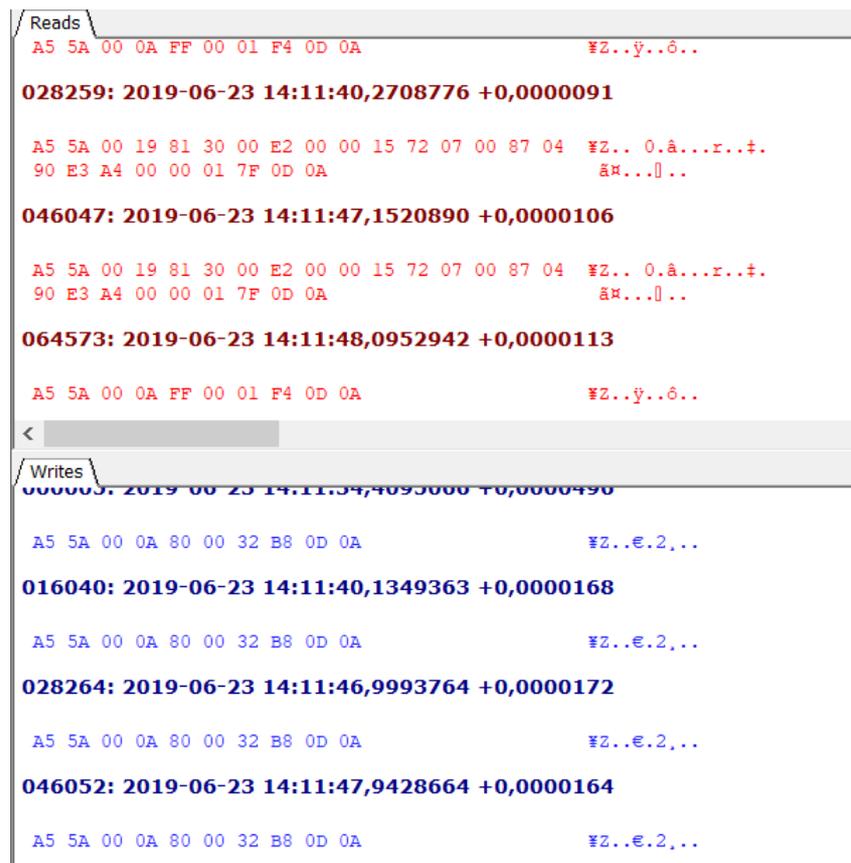


Figura 26. Detalle de tráfico filtrado, tanto de entrada como de salida.

Analizando las tramas enviadas y recibidas para cada orden, se buscó el formato adecuado que permitiera una programación flexible y adecuada a las necesidades del prototipo, con idea de poder establecer un protocolo de comunicaciones entre el lector y el dispositivo que mandara los comandos. Una vez encontrado, se estableció el siguiente formato:

Header	Length	Command	Data	Check code	End
2 bytes	2 bytes	1 byte	N bytes	1 byte	2 bytes

Figura 27. Formato de trama de transmisión de datos.

El protocolo de comunicaciones se basa en UART² y USB. Tiene una tasa de 115200 baudios.

² [38] Universal Asynchronous Receiver-Transmitter. Es el dispositivo que controla los puertos y dispositivos serie. Se encuentra integrado en la placa base o en la tarjeta adaptadora del dispositivo.

Las funciones principales de chip UART son: manejar las interrupciones de los dispositivos conectados al puerto serie y convertir los datos en formato paralelo, transmitidos al bus de sistema, a datos en formato serie, para que puedan ser transmitidos a través de los puertos y viceversa.

El controlador del UART es el componente clave del subsistema de comunicaciones series de una computadora. El UART toma bytes de datos y transmite los bits individuales de forma secuencial. En el destino, un segundo UART reensambla los bits en bytes completos. La transmisión serie de la información digital (bits) a través de un cable único u otros medios es mucho más efectiva en cuanto a costo que la transmisión en paralelo a través de múltiples cables. Se utiliza un UART para convertir la información transmitida entre su forma secuencial y paralela en cada terminal de enlace. Cada UART contiene un registro de desplazamiento que es el método fundamental de conversión entre las forma secuencial y paralela.

Se buscaron las diferentes tramas para los distintos comandos de interés, con sus respectivas tramas de respuesta. Empleando el software Docklight, se envió cada comando en hexadecimal para verificar la respuesta del lector, comprobando que el formato establecido encajaba con el tráfico que había sido filtrado al principio.

Lectura Simple

Header		Length		Command	Data		Check code
0xA5	0x5A	0x00	0x0A	0x80	Timeout (MSB)	Timeout (LSB)	0xxx
End							
0x0D	0x0A						

Figura 28. Formato de trama para comando *Single Inv.*

Siendo el Check Code la XOR de todos los campos, a excepción de header y tail.

El Timeout está en milisegundos. Si el lector encuentra un tag, o el timeout llega a cero, el lector se detendrá y mandará la respuesta.

Por tanto, la trama deseada tendrá esta forma:

A5-5A-00-0A-80-00-32-B8-0D-0A.

La respuesta tiene este formato:

Header		Length		Command	Data		
0xA5	0x5A	0x00	0xxx	0x81	PC (MSB)	PC (LSB)	EPC (MSB)
Data							
EPC	EPC	EPC	EPC	EPC	EPC	EPC	EPC
Data					Check code	End	
EPC	EPC	EPC (LSB)	RSSI (MSB)	RSSI (LSB)	Ant Num.	0xxx	0x0D 0x0A

Figura 29. Formato de trama de respuesta para comando *Single Inv.*

Comparando con la trama recibida en Device Monitoring Studio, se puede deducir que la trama de respuesta es:

A5-5A-00-19-81-30-00-E2-80-11-60-60-00-02-05-28-5A-15-84-00-00-01-3E-0D-0A

Se ha resaltado en rojo el ID de la etiqueta, parámetro a obtener. Cabe destacar que cuando no se detecta etiqueta, la trama que se recibe es la siguiente:

A5-5A-00-0A-FF-00-01-F4-0D-0A

siendo FF el octeto "Command" de respuesta cuando hay algún error. Esta trama va a resultar clave para consideraciones futuras.

El UART normalmente no genera directamente o recibe las señales externas entre los diferentes módulos del equipo. Usualmente se usan dispositivos de interfaz separados para convertir las señales de nivel lógico del UART hacia y desde los niveles de señalización externos.

Las señales externas pueden ser de variada índole. Ejemplos de estándares para señalización por voltaje son RS-232, RS-422 y RS-485.

Con Docklight, se envió la trama en hexadecimal por puerto serie, obteniéndose la siguiente respuesta:

```
[TX] - A5 5A 00 0A 80 00 32 B8 0D 0A
[RX] - A5 5A 00 19 81 30 00 E2 80 11 60 60 00 02 05 28 5A 15 84 00 00 01 3E 0D 0A
```

Figura 30. Comando *Single Inv* en Docklight.

La respuesta se corresponde con el formato esperado, lo que nos da evidencias de que se encontró el formato correcto.

Lectura Continua

Header		Length		Comman d	Data		Check code
0xA5	0x5A	0x00	0x0A	0x82	Num[1]	Num[0]	0xxx
End							
0x0D	0x0A						

Figura 31. Formato de trama para comando *Multiple*.

El campo “Data” indica el número de veces que se va a leer. Si se pone a 0, la lectura será infinita, y el lector no atenderá otros comandos hasta que se le envíe el comando *Stop*. Si, por ejemplo, se pone a 0x2710, se leerá 10000 veces. No olvidar el Check Code (XOR de todos los campos, exceptuando header y tail) en función del campo “Data”. La trama deseada es la siguiente:

A5-5A-00-0A-82-00-00-88-0D-0A

Header		Length		Comman d	Data		
0xA5	0x5A	0x00	0xxx	0x83	PC (MSB)	PC (LSB)	EPC (MSB)
Data							
EPC	EPC	EPC	EPC	EPC	EPC	EPC	EPC
Data						Check code	End
EPC	EPC	EPC (LSB)	RSSI (MSB)	RSSI (LSB)	Ant Num.	0xxx	0x0D 0x0A

Figura 32. Formato de trama de respuesta para comando *Multiple*.

Comparando con la trama recibida en Device Monitoring Studio, se puede deducir que la trama de respuesta es:

A5-5A-00-19-83-30-00-E2-80-11-60-60-00-02-05-28-5A-15-84-00-00-01-3C-0D-0A

siendo en rojo el ID de la etiqueta, parámetro a obtener.

Se realizaron las mismas comprobaciones en Docklight para el comando *Multiple*:

```
[TX] - A5 5A 00 0A 82 00 00 88 0D 0A
[RX] - A5 5A 00 19 83 30 00 E2 80 11 60 60 00 02 05 28 5A 15 84 00 00 01 3C
01 3C 0D 0A A5 5A 00 19 83 30 00 E2 80 11 60 60 00 02 05 28 5A 15 84 00 00
00 00 01 3C 0D 0A A5 5A 00 19 83 30 00 E2 80 11 60 60 00 02 05 28 5A 15 84
15 84 00 00 01 3C 0D 0A A5 5A 00 19 83 30 00 E2 80 11 60 60 00 02 05 28 5A
28 5A 15 84 00 00 01 3C 0D 0A A5 5A 00 19 83 30 00 E2 80 11 60 60 00 02 05 28 5A
```

Figura 33. Comando *Multiple* en Docklight.

Como curiosidad, se ha medido con un osciloscopio la señal en los pines de entrada y salida del lector, obteniéndose el siguiente resultado.

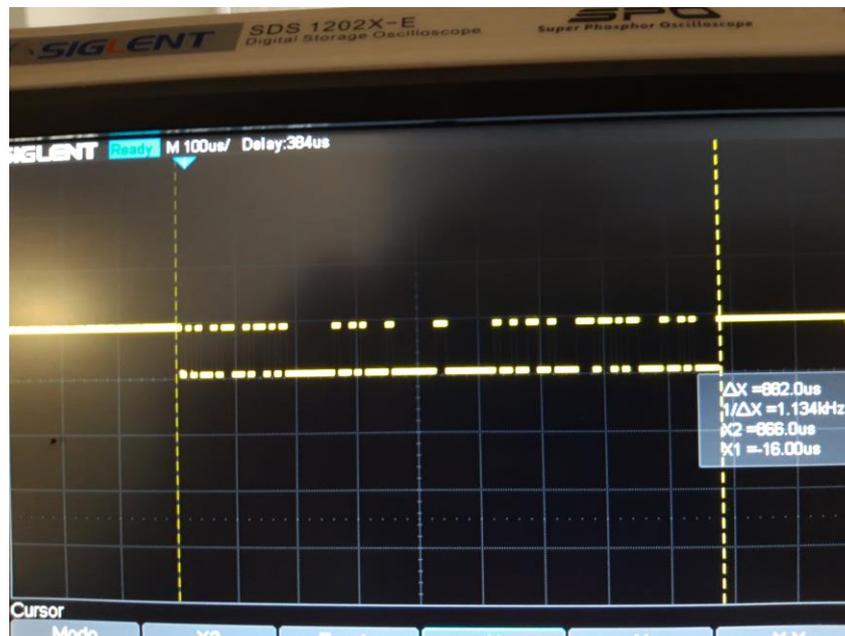


Figura 37. Comando visualizado en osciloscopio.

En la imagen anterior se puede apreciar la codificación seguida para un comando, y el tiempo que dura dicha señal, en este caso 882 microsegundos.

3.2.4. Remote Measure Unit

Una vez definidas las tramas adecuadas para controlar el lector, y poder obtener los ID's de los tags en las respuestas, se ha requerido de otro elemento que sea el que precisamente envíe los comandos. Todas las pruebas hasta ahora realizadas se han hecho utilizando un equipo portátil como origen de órdenes al lector, sin embargo, de cara al prototipo final, no puede integrarse de esta forma. Hace falta un elemento que sea el que haga las veces de “cerebro” del dispositivo *Gateway*, y realice además los envíos al servidor. Se ha elegido NB-IoT como tecnología de comunicación inalámbrica debido a su calidad de servicio y su baja latencia. No ofrece el mayor rango de alcance ni el mejor coste, sin embargo, esta aplicación se desarrolla en un entorno urbano, por lo que la cobertura LTE no es un problema. En cuanto al coste, esta aplicación está diseñada para una flota de camiones de recogida de basura, la cual no exige un elevado número de dispositivos.

Dicho elemento va a ser un dispositivo electrónico denominado RMU (Remote Measure Unit), y va a realizar el envío de comandos al lector y el envío de datos mediante el módem. Como se comentó anteriormente, la RMU es un dispositivo multitecnología de comunicaciones LTE-M & LTE-NB, de la compañía Noxium, que dispone de diversas interfaces locales de comunicaciones para la programación y monitorización de comandos. Es una pasarela abierta IoT para transportar información por paquetes al servidor IP fijado de forma fiable, segura y encriptada, por medio de comandos.

3.2.5. Alimentación del Sistema

Para la alimentación se puede disponer de la batería del camión, por lo que se puede hacer una toma directamente de ella a 12 voltios.

La RMU se alimenta a 3.7 voltios, por lo que se ha añadido un regulador al dispositivo para realizar la conversión.

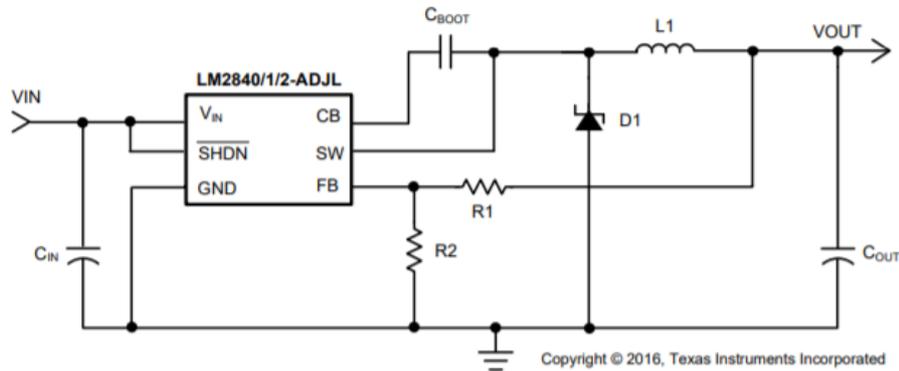


Figura 38. Regulador LM 2840 YMK-ADJ

Para obtener la salida deseada, se ha consultado el datasheet del dispositivo y se ha realizado el cálculo para obtener unos valores de R1 y R2 que den a la salida 3.7 voltios. Puede recibir a la entrada hasta 42 voltios, así que cumple los requisitos para ser conectado directamente a la batería del camión.

$$V_{out} = 0.765 \left(1 + \frac{R1}{R2} \right)$$

R2 está comprendida entre 100Ω y 10KΩ. Fijando Vout a 3.7 voltios y R2 a 1KΩ, se obtiene:

$$R1 = 1K \left(\frac{3.7}{0.765} - 1 \right) = 3.836K\Omega$$

Por lo que se fija R1 a 3.9KΩ.

El lector admite una alimentación entre 3.3 y 5 voltios, por lo que se alimentará desde la RMU. Se ha hecho un ajuste en la RMU para sacar dos pines de alimentación a 3.7 voltios y, mediante un transistor, se enciende o apaga el lector en función del estado del proceso. De tal forma se reduce su consumo y se evitan temperaturas elevadas.

3.2.6. Esquema general

Recapitulando, se tienen tres elementos clave a integrar:

- Lector RFID, que lee etiquetas próximas de forma simple o continua, y las envía.
- RMU, que envía los comandos oportunos al lector, y recibe las respuestas. También establece la conexión al servidor.
- Regulador, que adapte el voltaje de entrada del dispositivo al voltaje de funcionamiento de la RMU.

Atendiendo a los pines de cada dispositivo, una configuración global sería la siguiente:

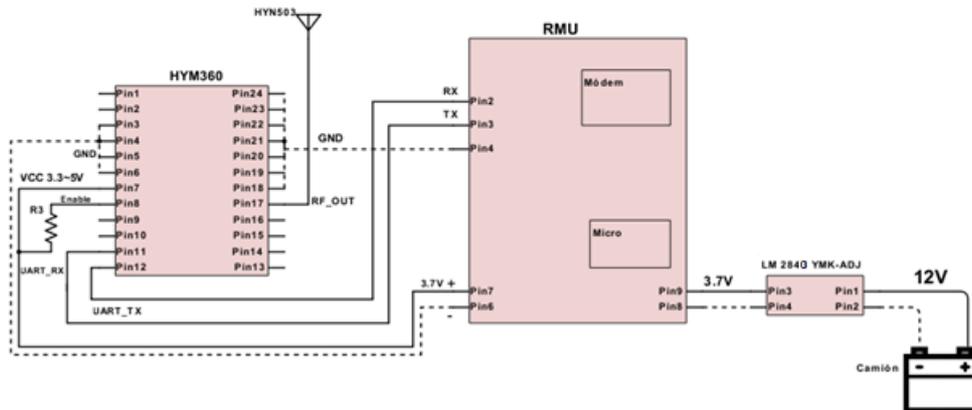


Figura 39. Conexión general del Gateway.

Configuración de pines HYM360

- 1~2: NC
- 3~6 & 13~16 & 18~24: GND
- 7: VDD3.3~5V, Input
- 8: EN, Input
- 9~10: GPIO, Output
- 11: UART_RX, Input
- 12: UART_TX, Output
- 17: RFOUT, Input & Output

Configuración de pines RMU

- 2: RX, Input
- 3: TX, Output
- 4 & 6 & 8: GND
- 7: VDD, Output
- 9: VCC, Input
- Además, existen 3 pines de comunicación con el módem, RT, TX y GND. Se conectan a conversor TTL-USB.

Una vez encendido el equipo, la RMU comenzará realizando una lectura a discreción al entorno. Cuando encuentra un tag, éste responde mandando su ID y la RMU detiene la lectura continua. En este punto, se realizan lecturas individuales periódicas hasta que se deja de obtener respuesta. Esto se hace con la siguiente idea; mientras el camión está vaciando un cubo, la antena lee periódicamente del entorno cada Tiempo_SingInv segundos. El cubo, cuyo tag está colocado de forma estratégica para que permanezca cerca de la antena, es alzado por el mecanismo de recogida para ser vaciado. En este proceso, puede darse el caso en que una lectura resulte sin respuesta por diversos motivos; el cubo se ha salido de la zona de lectura puntualmente en el proceso de vaciado, alguna interferencia... de tal manera que hay que tener en cuenta una posible lectura errónea. Es por eso por lo que se añadirá un contador de “lecturas sin respuesta” para considerar estas posibles perturbaciones. El equipo considerará que un cubo ha sido liberado por el camión cuando ha realizado N lecturas al medio y no ha tenido respuesta. Este número N será suficiente grande como para descartar las posibles perturbaciones antes comentadas, pero no tanto como para ralentizar de forma severa el protocolo.

Mientras el cubo se vacía, el lector manda lecturas individuales periódicas que son respondidas por la etiqueta. Una vez se ha dejado de leer la etiqueta N veces, se envía la información al servidor y se repite el proceso.

3.2.8. Diagrama de flujo de la RMU

Atendiendo al diagrama establecido en el apartado anterior, se ha desarrollado el siguiente diagrama de flujo:

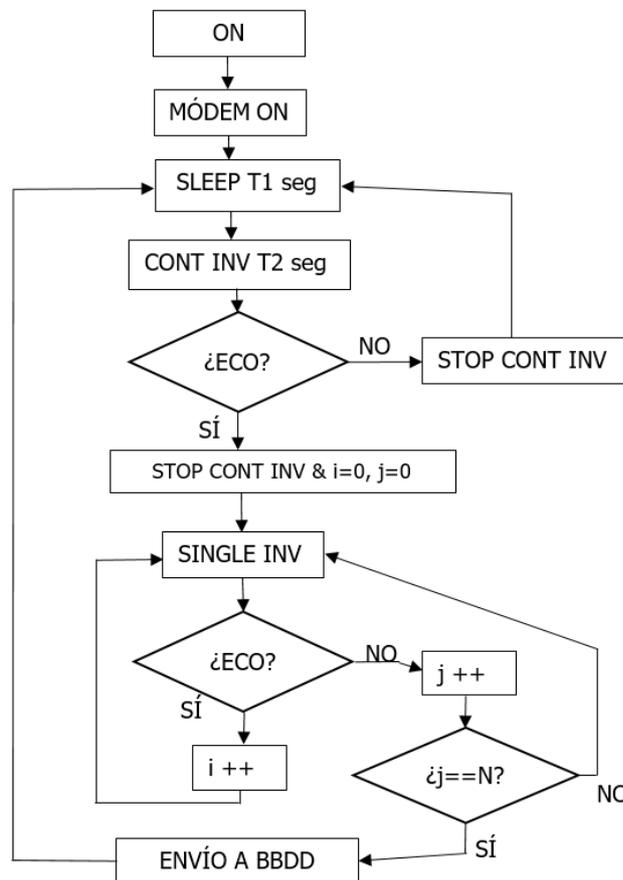


Figura 41. Diagrama de flujo de la RMU.

Al encenderse el equipo, lo primero que se hace es encender el módem debido a que requiere un tiempo de aproximadamente 2 minutos en encender y establecer la cobertura NB.

Una vez encendido, la RMU ejecutará un bucle de exploración del medio. Apagará el lector durante T1 segundos, lo encenderá y hará una lectura continua del medio T2 segundos. En caso de no haber encontrado etiquetas cerca volverá apagarlo. El objetivo de este bucle es diverso. El lector consume 630 mA a 3.7 voltios en lectura continua, por lo que someter al lector a dicho régimen de forma ininterrumpida dispararía el

consumo, aparte de elevar la temperatura del lector de forma significativa a unos 50° C, lo cual, a largo plazo, puede deteriorar o incluso inutilizar completamente el *Gateway*.

Una vez recibido un eco de la etiqueta del cubo que se está recogiendo, se detiene la lectura a discreción. Se iguala un índice a cero y se hace una lectura individual cada *Tiempo_SingInv*. Cada vez que se tiene una respuesta se incrementa el índice *i*. Como se comentaba antes, existe otro índice, *j*, que cuenta las veces que una de las lecturas individuales no ha dado respuesta. Esto es posible gracias a que el lector devuelve la trama

A5-5A-00-0A-FF-00-01-F4-0D-0A

cuando no ha leído ninguna etiqueta. Una vez el índice *j* ha igualado el parámetro *N*, el bucle de lectura sale y se pasa a enviar los datos por el módem. Una vez enviado se vuelve al principio, en busca de más tags.

Para una primera consideración, se han fijado los índices a:

- T1 (tiempo que el dispositivo está en reposo) = 2 segundos.
- T2 (tiempo que el dispositivo está realizando lecturas a discreción) = 1 segundo.
- *Tiempo_SingInv* (tiempo entre lecturas individuales) = 1 segundo.
- *N* (número de lecturas fallidas hasta considerar cubo como recogido) = 5.

El paquete de datos final a enviar es:

{f, o, t, r, d}

siendo

- *f*: origen de envío; SADC51.
- *o*: destino; RHOST.
- *t*: tipo de conexión; read.
- *d*: datos. Este campo es, a su vez, otro paquete con sus campos propios:

{ID, H, S, T, U, ST, B, I, E}

siendo

- *ID*: número de paquete que se envía. Cuando solo se envía un paquete vale "-1".
- *H*: fecha y hora de la RMU.
- *S*: ID del tag.
- *T*: tipo de dispositivo que envía los datos.
- *U*: unidades.
- *ST*: momento de la muestra.
- *B*: batería.
- *I*: número de veces que se ha leído.
- *E*: datos de ingeniería separados por coma, como la batería.

3.2.9. Montaje del prototipo

En este apartado se desarrolla el montaje de la solución inicial, no siendo ésta la definitiva. La solución final nace a raíz de las pruebas y el replanteo expuestos en el capítulo siguiente. Por tanto, lo que aquí se expone consta como el final del prototipo.

La electrónica irá protegida en una cobertura específica para ser instalada en el camión. Ésta cumple el estándar de protección IP67.

El conector que se ha empleado para la alimentación es un M8 de tres polos; positivo, negativo y otro que se ha dejado para pasar la señal de comunicación de la RMU hacia fuera del dispositivo, y poder monitorizar la actividad del mismo. Para ello, mediante un adaptador TTL-USB, se visualizará el estado del módem de la RMU. Sin esa toma, no sabríamos en qué estado se encuentra el dispositivo. Para la antena se empleará un conector TNC hembra.

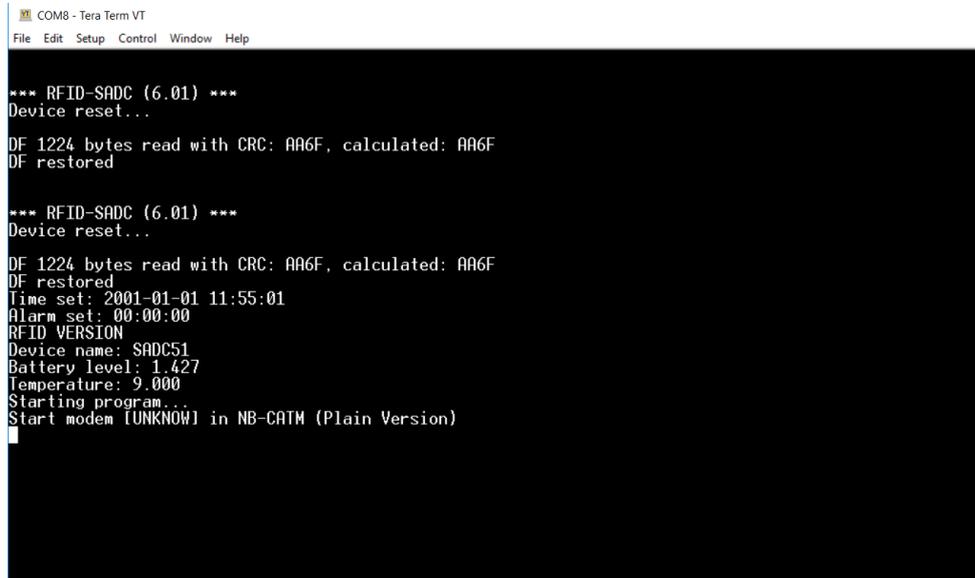
Se han soldado los cables en los pines de comunicación y alimentación del lector. Dichos cables tienen en su extremo libre un conector que permite deshacer las conexiones en caso de separar algún componente.



Figura 42. Prototipo terminado con conector de alimentación (izquierda) y antena (derecha).

3.2.10. Funcionamiento

Una vez terminado el montaje del dispositivo, con el micro programado y la antena en posición, se han realizado pruebas de funcionamiento monitorizando la actividad de la RMU mediante un adaptador TTL-USB. Para empezar el proceso, solo hay que darle alimentación al sistema.



```

COM8 - Tera Term VT
File Edit Setup Control Window Help

*** RFID-SADC (6.01) ***
Device reset...

DF 1224 bytes read with CRC: AA6F, calculated: AA6F
DF restored

*** RFID-SADC (6.01) ***
Device reset...

DF 1224 bytes read with CRC: AA6F, calculated: AA6F
DF restored
Time set: 2001-01-01 11:55:01
Alarm set: 00:00:00
RFID VERSION
Device name: SADC51
Battery level: 1.427
Temperature: 9.000
Starting program...
Start modem [UNKNOWN] in NB-CATM (Plain Version)

```

Figura 43. Inicio del programa.

En primer lugar, siguiendo el diagrama de flujo establecido, se realizará el encendido del módem.



```

COM8 - Tera Term VT
File Edit Setup Control Window Help

AT+CEREG?
AT+QCFG="band",F,0,0,1
AT+QCFG="nwscanseq",010302,1
AT+QCFG="nwscanmode",1,1
AT+COPS=1,2,"21407",0
AT+QICSGP=1,1,"sm2ms.movistar.es"
AT+CGREG?
AT+CGREG=2
AT+CEREG?
AT+CSQ
AT+QIOPEN=1,1,"UDP","37.187.50.42",8090
AT+QISEND=1,92
["f": "SADC51", "o": "RHOST", "i": "sync", "l": "7", "E": "SADC51,1.427,9.000,0,0,0,0,16", "F": "800C"]AT+QIRD=1,512
Time set: 2019-07-01 10:23:07
AT+QIRD=1,512
AT+CMGR=1
AT+QICLOSE=1
AT+COPS=2
AT+QIDEACT=1
AT+CFUN=0
I2C Eeprom Stat: Regs: 0 [0x0000 - 0x0000]
End modem
Starting program...
UART9 OPEN HEARTBEAT
DF Current CRC: 224C
Writed 1224 bytes in DF success.

```

Figura 44. Encendido del módem y bucle reposo/lectura múltiple.

Una vez el módem recibe la trama de sincronización, comienza el primer bucle del diagrama. Se permanece en este estado hasta que se lee una etiqueta.

```

COM8 - Tera Term VT
File Edit Setup Control Window Help
AT+CFUN=0
I2C Eeprom Stat: Regs: 0 [0x0000 - 0x0000]
End modem
Starting program...
UART9 OPEN HEARTBEAT
DF Current CRC: 224C
Wrote 1224 bytes in DF success.
NZ("F": "RFID", "T": "2019-07-01 10:24:13", "S": "E2000015720700880770CBD4", "V": "1")
NZ("F": "RFID", "T": "2019-07-01 10:24:14", "S": "E2000015720700880770CBD4", "V": "2")
NZ("F": "RFID", "T": "2019-07-01 10:24:15", "S": "E2000015720700880770CBD4", "V": "3")
NZ("F": "RFID", "T": "2019-07-01 10:24:16", "S": "E2000015720700880770CBD4", "V": "4")
NZ("F": "RFID", "T": "2019-07-01 10:24:17", "S": "E2000015720700880770CBD4", "V": "5")
NZ("F": "RFID", "T": "2019-07-01 10:24:18", "S": "E2000015720700880770CBD4", "V": "6")
NZ("F": "RFID", "T": "2019-07-01 10:24:19", "S": "E2000015720700880770CBD4", "V": "7")
NZ("F": "RFID", "T": "2019-07-01 10:24:20", "S": "E2000015720700880770CBD4", "V": "8")
NZ("F": "RFID", "T": "2019-07-01 10:24:21", "S": "E2000015720700880770CBD4", "V": "9")
NZ("F": "RFID", "T": "2019-07-01 10:24:22", "S": "E2000015720700880770CBD4", "V": "10")
NZ("F": "RFID", "T": "2019-07-01 10:24:23", "S": "E2000015720700880770CBD4", "V": "11")
NZ("F": "RFID", "T": "2019-07-01 10:24:24", "S": "E2000015720700880770CBD4", "V": "12")
NZ("F": "RFID", "T": "2019-07-01 10:24:25", "S": "E2000015720700880770CBD4", "V": "13")
NZ("F": "RFID", "T": "2019-07-01 10:24:26", "S": "E2000015720700880770CBD4", "V": "14")
NZ("F": "RFID", "T": "2019-07-01 10:24:27", "S": "E2000015720700880770CBD4", "V": "15")
NZ("F": "RFID", "T": "2019-07-01 10:24:28", "S": "E2000015720700880770CBD4", "V": "16")
NZ("F": "RFID", "T": "2019-07-01 10:24:29", "S": "E2000015720700880770CBD4", "V": "17")
NZ("F": "RFID", "T": "2019-07-01 10:24:30", "S": "E2000015720700880770CBD4", "V": "18")
NZ("F": "RFID", "T": "2019-07-01 10:24:31", "S": "E2000015720700880770CBD4", "V": "19")
NZ("F": "RFID", "T": "2019-07-01 10:24:32", "S": "E2000015720700880770CBD4", "V": "20")
NZ("F": "RFID", "T": "2019-07-01 10:24:33", "S": "E2000015720700880770CBD4", "V": "21")
NZ("F": "RFID", "T": "2019-07-01 10:24:34", "S": "E2000015720700880770CBD4", "V": "22")
NZ("F": "RFID", "T": "2019-07-01 10:24:35", "S": "E2000015720700880770CBD4", "V": "23")
NZ("F": "RFID", "T": "2019-07-01 10:24:36", "S": "E2000015720700880770CBD4", "V": "24")
NZ("F": "RFID", "T": "2019-07-01 10:24:37", "S": "E2000015720700880770CBD4", "V": "25")
    
```

Figura 45. Lectura de etiquetas.

Una vez leída una etiqueta, se hacen lecturas individuales cada segundo hasta que se dejan de leer tags.

```

COM8 - Tera Term VT
File Edit Setup Control Window Help
NZ("F": "RFID", "T": "2019-07-01 10:24:31", "S": "E2000015720700880770CBD4", "V": "19")
NZ("F": "RFID", "T": "2019-07-01 10:24:32", "S": "E2000015720700880770CBD4", "V": "20")
NZ("F": "RFID", "T": "2019-07-01 10:24:33", "S": "E2000015720700880770CBD4", "V": "21")
NZ("F": "RFID", "T": "2019-07-01 10:24:34", "S": "E2000015720700880770CBD4", "V": "22")
NZ("F": "RFID", "T": "2019-07-01 10:24:35", "S": "E2000015720700880770CBD4", "V": "23")
NZ("F": "RFID", "T": "2019-07-01 10:24:36", "S": "E2000015720700880770CBD4", "V": "24")
NZ("F": "RFID", "T": "2019-07-01 10:24:37", "S": "E2000015720700880770CBD4", "V": "25")
NZ("F": "RFID", "T": "2019-07-01 10:24:38", "S": "E2000015720700880770CBD4", "V": "26")
NZ("F": "RFID", "T": "2019-07-01 10:24:39", "S": "E2000015720700880770CBD4", "V": "27")
UART9 CLOSED HEARTBEAT
("F": "RFID", "TT": "2019-07-01 10:24:39", "TX": "27", "TG": "0")
Start modem [MOV] in 2G-3G (Plain Version)
ATE0
AT&W
AT+CGREG?
AT+CEREG=2
AT+CEREG?
AT+CSQ
AT+QIOPEN=1,1,"UDP","37.187.50.42",8090
AT+QISEND=1,217
("F": "SADC51", "o": "RHOST", "l": "read", "c": "1", "d": [{"ID": "-1", "H": "2019-07-01 10:24:39", "S": "E2000015720700880770CBD4", "T": "04", "U": "0", "ST": "2019-07-01 10:24:39", "B": "1", "I": "27", "E": "SADC51.1.427.9.000.0.0.0.0.15"}]JAI+QIRD=1,512
AT+QIRD=1,512
AT+CMGR=1
AT+QICLOSE=1
AT+COPS=2
AT+QIDEACT=1
AT+CFUN=0
I2C Eeprom Stat: Regs: 0 [0x0000 - 0x0000]
End modem
("F": "RFID", "TT": "2019-07-01 10:24:39", "TX": "27", "TG": "0")
UART9 OPEN HEARTBEAT
DF Current CRC: FF26
Wrote 1224 bytes in DF success.
    
```

```

UART9 CLOSED HEARTBEAT
("F": "RFID", "TT": "2019-06-04 09:26:54", "TX": "31", "TG": "0")
Start modem [MOV] in NB-CATM (Plain Version)
ATE0
AT&W
    
```

Figura 46. Envío de datos. Detalle de envío por NB y 2G.

Una vez se dejan de leer tags, se envían los datos. En este caso se estableció la conexión mediante 2G para comprobar bien la conmutación entre NB y 2G.

RMU Device	Fecha y Hora	Número de lecturas	Nivel de batería (V)	Tag
SADC51	2019-07-01 12:24	27	1.453	E2000015720700880770CBD4

Figura 47. Trama de datos visualizada en la plataforma.

3.2.11. Consumo

Se ha esbozado una gráfica con el consumo en cada uno de los estados del equipo, así como el tiempo aproximado que se encuentra en cada uno de ellos.

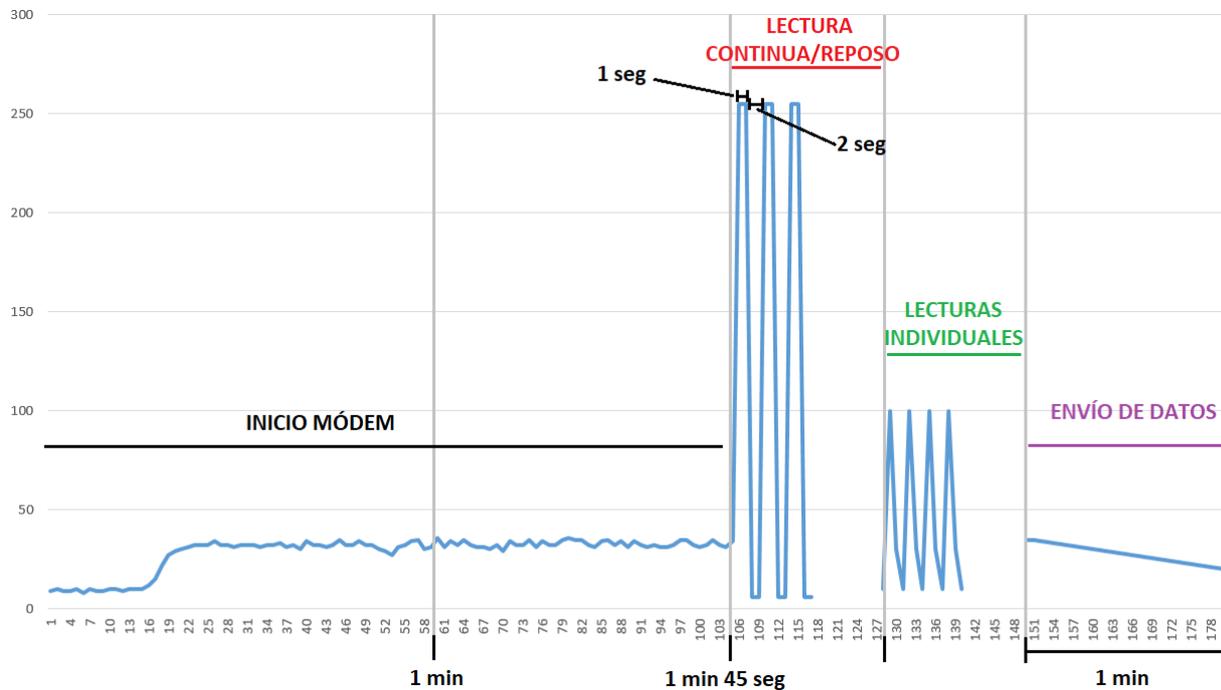


Figura 48. Consumo del equipo. En el eje vertical mA, en el eje horizontal segundos.

Desde que se da alimentación, el equipo emplea un tiempo aproximado de 1 minuto y 45 segundos en arrancar el módem, según la cobertura. En este intervalo consume una media de 40 mA.

Después, pasa al estado de reposo/lectura hasta que encuentra un tag. En este estado consume 6 mA en reposo y 255 mA en lectura continua.

Cuando encuentra un tag, se pasa al estado de lecturas individuales, en las que se dan picos de 100 mA y se decrece hasta aproximadamente 10 mA hasta la siguiente lectura.

Por último, cuando se han acabado de leer tags, se procede a enviar los datos al servidor. En este período se consume una media de 30 mA.

4. PRUEBAS, REPLANTEO Y RESULTADOS

En este capítulo se desarrollan las pruebas realizadas al prototipo descrito en el capítulo anterior. A raíz de éstas, se aplicaron las modificaciones que llevaron a la solución final.

4.1. Primera prueba

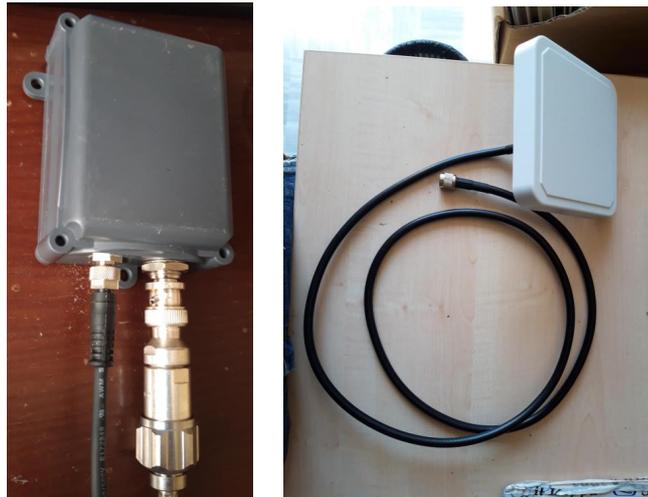


Figura 49. Prototipo // Solución inicial.

Una vez preparado el prototipo (*Gateway* + antena) se ha procedido a realizar una primera prueba de campo. Para ello, se ha tomado la alimentación del cuadro eléctrico del camión, se ha instalado el *Gateway* en un lugar apropiado, lo más cubierto posible, y se ha instalado la antena en la estructura de recogida de cubos.



Figura 50. Toma de alimentación a cuadro eléctrico.

La toma se realizó a 12 voltios en el cuadro eléctrico y, aprovechando la propia electrónica del camión, dicha toma estará al voltaje deseado cuando se arranque, por lo que puede aprovecharse a modo de “interruptor”.

La dinámica a la hora de recoger los cubos es la siguiente; el camión se para en cada punto de recogida. Un operario lleva los cubos de las inmediaciones al camión mientras otro los va situando en la estructura. Ésta puede recoger cubos de forma individual, es decir, a derecha o izquierda de la estructura, o de forma paralela, situando dos cubos al mismo tiempo, uno a cada lado. Tal colocación la decide sobre la marcha el operario, por lo que a efectos funcionales se considerará aleatoria. Una vez situados uno o dos cubos, se alza la estructura, se vacían y se baja, dejando los cubos en el suelo. Una vez se termina con un punto se desplaza al siguiente y se repite el proceso.



Figura 51. Cubo de basura a recoger.



Figura 52. Vista frontal de estructura recogedora de cubos, con antena HYN503 en la parte inferior.

La antena intentó colocarse en la parte baja de la estructura. En la parte inferior la instalación resultó imposible debido a la hidráulica del camión, que ocupaba la parte de atrás y la antena interfería en su movimiento.



Figura 53. Vista lateral de estructura recogedora de cubos, con antena HYN503 en parte media.

Acto seguido, se trató de colocar en la parte media, pero tampoco resultó un punto adecuado ya que, aparte de no abarcar el ancho suficiente donde los cubos eran puestos, la antena impactaba directamente con los cubos mientras se alzaba la estructura.

Dado que la estructura puede soportar un cubo a la izquierda, un cubo a la derecha, o dos cubos en todo el ancho, se necesita un área de lectura que abarque todo ese ancho. Con la antena HYN503 resulta imposible cubrir toda esa zona. Además, la propia estructura metálica alteraba las lecturas, dependiendo de la ubicación de la antena.

Esta primera prueba no resultó exitosa, por lo que se tomaron medidas y se realizaron fotos con objeto de realizar un replanteo eficiente.

4.2. Replanteo

Lo primero fue trazar la zona crítica en la que iban a ser leídas las etiquetas. Además, la propia estructura metálica de la estructura resultaba un obstáculo añadido, ya que las lecturas no eran limpias si había elementos metálicos entre la antena y el tag. Se decidió implantar un **nuevo sistema de tres antenas** que abarcara toda el área crítica. Dada la ubicación candidata, y la distancia a la que se debe leer, se decidió que la antena adecuada sería el dipolo.

Este nuevo sistema de antenas a instalar debía estar lo más cerca posible de los cubos, sin metal en medio y abarcar todo el ancho de la zona de colocación de cubos, 76 cm. Con estas limitaciones, se decidió diseñar el sistema de tres dipolos en la zona resaltada en la imagen siguiente.

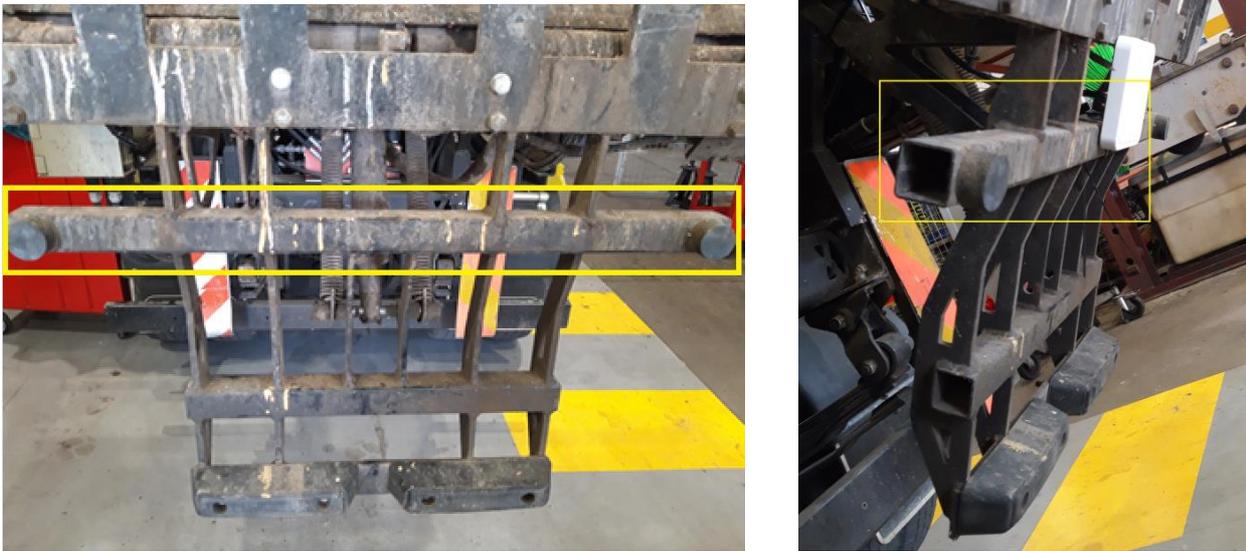


Figura 54. Ubicación, resaltada en amarillo, candidata para sistema de antenas.

En esta ubicación, tres dipolos abarcarían toda la zona de lectura de tags, al mismo tiempo que estarían colocadas a escasos centímetros de la etiqueta. Hay que tener en cuenta que pasar de una a tres antenas reduciría la potencia de emisión en cada una a la tercera parte, por eso la cercanía al tag resulta imprescindible.

Una forma sencilla de elaborar un dipolo en media longitud de onda es empleando un cable coaxial. Retirando la cubierta y dejando el vivo (conductor interno) a un lado y la malla (conductor externo) a otro se obtiene un dipolo aceptable. La longitud del dipolo se ha calculado de forma adecuada a la frecuencia de trabajo del lector:

$$\lambda = \frac{c}{f} = \frac{3 \cdot 10^8 \text{ m/s}}{865 \cdot 10^6 \text{ Hz}} = 0,3468208 \text{ m}$$

Por tanto, $\frac{\lambda}{2} = 0,1734104 \text{ m} = 17,34 \text{ cm}$



Figura 55. Dipolo con cable coaxial, de 16 cm de un extremo a otro.

A partir del resultado obtenido teóricamente, se ha realizado un ajuste experimental utilizando un medidor de pérdidas de retorno. Así, se han ido recortando cada rama del dipolo progresivamente para sintonizarlo con la máxima precisión posible. Esto se ha comprobado midiendo las pérdidas de retorno cada vez que se realizaba un corte. La imagen siguiente muestra las pérdidas, donde se puede apreciar un ancho de banda de unos 45MHz a -15dB.

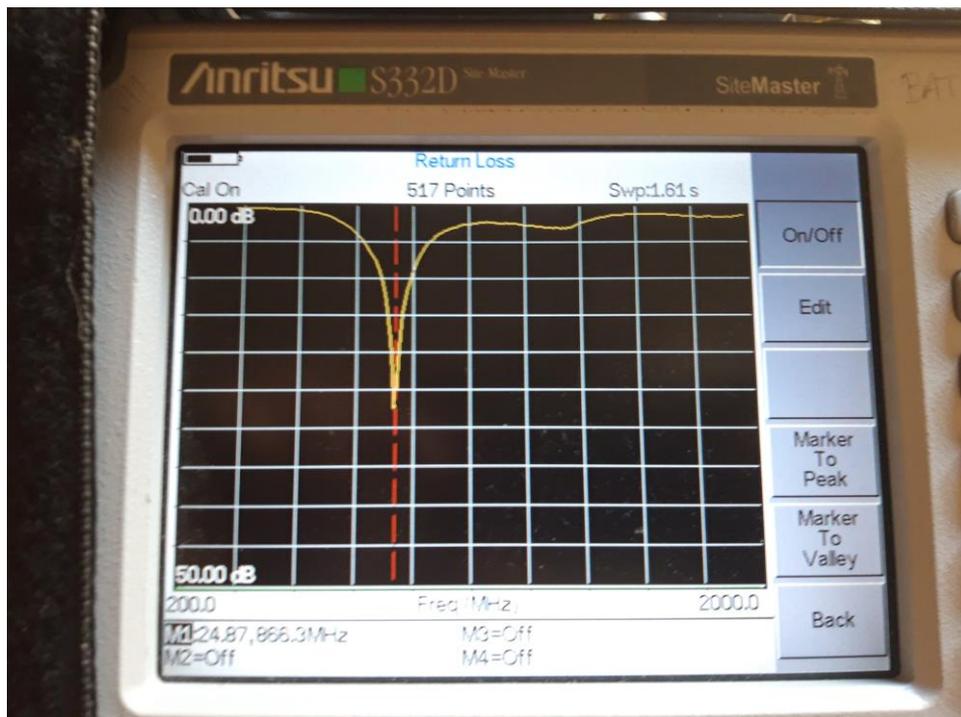


Figura 56. Pérdidas de retorno, -27dB, a la frecuencia de 866.3 MHz.

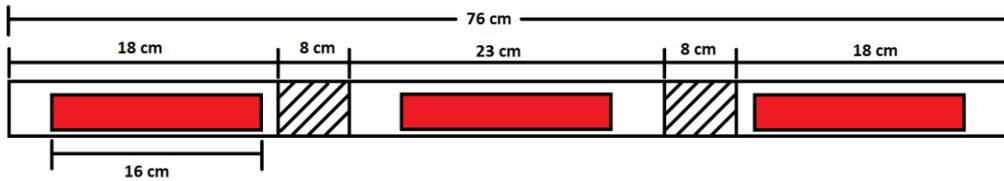


Figura 57. Medidas a tener en cuenta en el replanteo. En rojo, la disposición de los tres dipolos.

Una vez elaborados y sintonizados los tres dipolos, se han preparado unas protecciones de PVC de dimensiones similares a la superficie metálica a las cuales van a ir sujetas. Para una prueba de prototipo, la sujeción se realizará con bridas con protección ultravioleta.



Figura 58. Dipolo en cobertura, y cobertura completa.

Los tres dipolos irán conectados al lector mediante un splitter, y conectores tipo F. Se ha empleado cable RG-223 de cada dipolo al splitter y del splitter al *Gateway*.



Figura 59. Conector tipo F y splitter de 3 entradas.

4.3. Segunda prueba

Una vez preparado el *Gateway* con el sistema de tres antenas se realizaron pruebas de lectura en una barra metálica que simula la estructura de recogida del camión. Gracias a las medidas tomadas en la primera prueba se pudo simular de forma práctica la estructura de recogida de residuos.



Figura 60. Segunda prueba con nuevo sistema de antenas.

Con esta nueva disposición, se realizaron las mismas pruebas de radiación con cada dipolo, resultando un alcance de 8 cm de lectura en dirección saliente a la estructura. De dicha forma, el área efectiva de lectura quedaba cubierto, pudiéndose identificar más de un tag. Sin embargo, el carácter poco robusto de las coberturas no resultó suficiente para validar la solución.

4.4. Solución final y validación

Buscando una cobertura sólida, se optó por la siguiente:



Figura 61. Cobertura de la solución final.

La electrónica quedaría alojada y protegida dentro de la misma. Gracias a las ranuras a ambos lados, la mezzanina quedaría estable y firme dentro de la misma.



Figura 62. Electrónica alojada en la cobertura final.

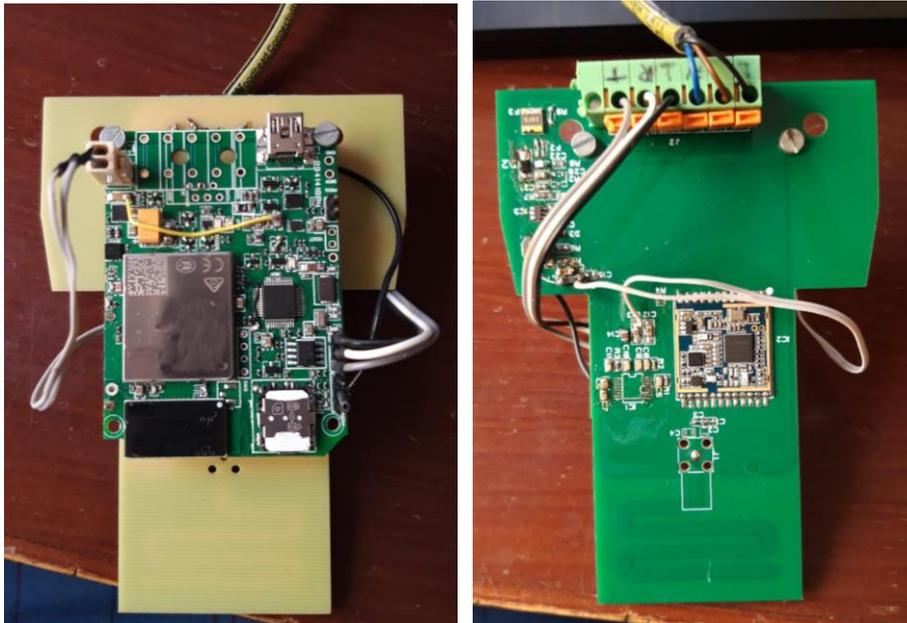


Figura 63. RMU y placa con la etapa de alimentación, antena y radio RFID.

Se realizaron pruebas de lectura para comprobar la eficiencia de la antena de meandro, obteniéndose una distancia efectiva de 25 centímetros en el plano saliente a la estructura. De esta manera, el esquema de instalación final sería de dos dispositivos a ambos lados de la estructura de recogida, abarcando todo el ancho de lectura.

La solución final también ofrece la posibilidad de leer más de una etiqueta en su ciclo de trabajo, solapándose de manera pseudoaleatoria el orden de lectura. Este comportamiento se debe a la propia naturaleza de la radiofrecuencia, haciéndose imposible la lectura de más de una etiqueta en el mismo instante de tiempo.

Esta configuración facilita la instalación, anclando ambas carcasas a la estructura con un único cable de alimentación al cuadro eléctrico del camión.

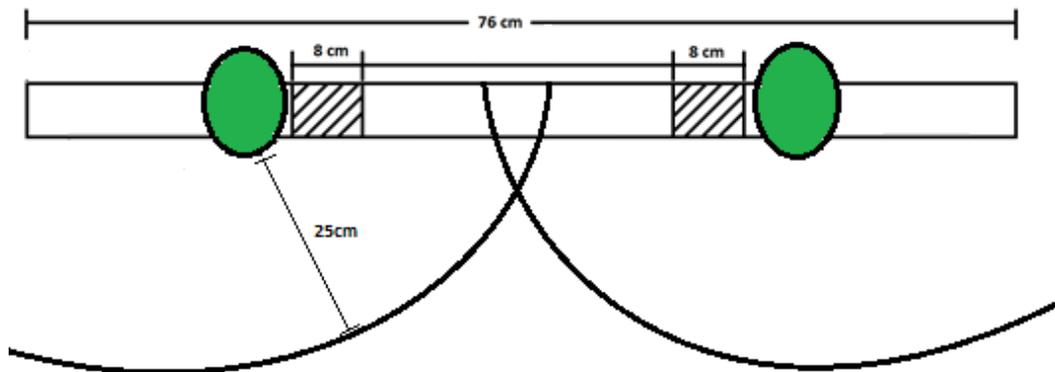


Figura 64. Zona de lectura de la solución final.

4.5. Futuras mejoras

Como posibles futuras mejoras de este prototipo, se dejan propuestas las siguientes:

- Dada la configuración del *Gateway*, los tiempos de reposo y lectura no están totalmente adaptados a un proceso real. Sería interesante poder modificar dichas constantes en tiempo real, así como el número de lecturas no exitosas necesarias para pasar al envío de datos. Esto podría realizarse mediante el paso de parámetros al *Gateway* en tiempo real, definiendo algún estado intermedio de configuración. De esta manera, el dispositivo estaría bien dimensionado.
- El carácter secuencial de lectura y envío de etiquetas puede generar intervalos de tiempo en los que el dispositivo no esté leyendo etiquetas. Esto puede optimizarse paralelizando ambos procesos, dando lugar a una lectura totalmente independiente del envío de datos.

4.6. Estudio de costes

Se ha elaborado una lista de materiales con los costes aproximados de cada uno de los elementos necesarios para llevar a cabo este desarrollo. Se recogen los datos en la siguiente tabla.

Ítem	Cantidad	Valor	Tecnología	Fabricante	Coste unidad (€) y Lote
Kit de desarrollo RFID	1	-	-	Winnix	40
Antena HYN503.	1	-	-	Winnix	50
Lector RFID HYM360.	2	-	-	Winnix	70
Tag RFID HYT-MT-U031b	2	-	-	Winnix	1.30
Tag RFID ALN-9662.	30	-	-	ALIEN	0.5 (x100)
Cable coaxial RG-223	3 metros	-	-	-	15
Cable multihilo de datos	2 metros	-	-	-	20
RMU	1	-	-	Noxium	-
PCB	1	-	-	-	-
Regulador	1	LM 2840 YMK-ADJ	-	Texas Instruments	4
Fusible	1	MF-F050	SMD	Mouser	0.43 (x10)
Resistencia	1	0.22 Ω	SMD0402	RS PRO	1.30 (x5)
Resistencia	1	0 Ω	SMD0603	RS PRO	0.009 (x5000)
Resistencia	1	3.9 k Ω	SMD0603	TE Connectivity	0.349 (x10)
Resistencia	1	1 k Ω	SMD0603	RS PRO	0.002 (x5000)
Diodo	1	GF1A	SMD	Vishay	0.18 (x10)
Diodo Schottky	1	PMEG6010CEH	SMD	Mouser	0.266 (x10)
Condensador	4	4.7 μ F	SMD0805	Würth	0.451 (x10)
Condensador	1	220 nF	SMD0603	AVX	0.127 (x50)

Condensador	1	12 pF	SMD0603	AVX	0.153 (x50)
Condensador	2	10 uF	SMD0603	AVX	0.196 (x50)
Condensador	1	10 uF	SMD1206	AVX	0.441 (x50)
Condensador	1	100 pF	SMD0603	AVX	0.27 (x50)
Condensador	2	100 nF	SMD0603	Syfer	0.24 (x10)
Bobina	1	22 uH	SMD	Würth	0.34 (x5)
Conector tipo F	4	-	-	-	0.15
Conector M8 tres polos	2	-	-	-	8
Conector TNC hembra	1	-	-	-	2.65
Cobertura prototipo	1	--	-	-	10
Coberturas antenas dipolo	3	-	-	-	30
Splitter	1	-	-	-	3
Cobertura final	1	-	-	-	20
Bridas	30	-	-	-	3.95

Tabla 4. Lista de materiales.

4.7. Demostración del piloto

En la defensa de este proyecto se realizará, al final de la presentación, una demostración del funcionamiento del sistema.

La demo consistirá en una simulación en directo de la rutina del equipo. Se conectará el mismo a una fuente de alimentación que emulará el cuadro eléctrico del sistema. Para esta demo, se ha preparado un terminal de salida añadido con objeto de mostrar la actividad del módem. Para ello se empleará el software TeraTerm. Una vez el dispositivo arranque y establezca cobertura, se aproximarán diversos tags para verificar la correcta lectura de los mismos. Estas aproximaciones emularán el vaciado de los cubos de residuos. Una vez se hayan dejado de aproximar tags, el equipo deberá enviar los datos a la plataforma IoT, la cual mostrará los datos de recepción del mismo modo que los mostraría al cliente.

5. RFID Y LPWAN EN EL FUTURO

"Dejen que el futuro diga la verdad y evalúe a cada uno de acuerdo a sus trabajos y a sus logros. El presente es de ellos, pero el futuro, por el cual trabajé tanto, es mío".
- Nikola Tesla -

RFID es una tecnología que, a pesar de sus más de 70 años de existencia, sigue evolucionando y reinventándose. Hoy en día sigue totalmente vigente en diferentes industrias e incluso puede perfilarse como determinante en proceso de digitalización del sector retail. [1] Sin embargo, a pesar del avance significativo del protocolo Gen II del EPCglobal, existen muchas cuestiones que hay que atender, como son:

- Seguridad: El EPC Gen II no soporta criptografía y existen pocos productos RFID que tengan funciones de encriptación en el mercado. Hoy en día cualquier control de acceso se realiza usando contraseñas, y existen aplicaciones RFID que requieren un robusto sistema de seguridad, como son por ejemplo la inclusión de esta tecnología en los pasaportes.
- Electromagnetismo de RFID: En presencia de metales o líquidos el funcionamiento de las etiquetas UHF disminuye considerablemente, ya que estos materiales pueden impedir la propagación de la señal.
- Fabricación: Las etiquetas RFID se aplican después de la fabricación, por ello hace que las etiquetas RFID sean muy aún demasiado caras.
- Sensores: A pesar de la promesa de que existan RFID con sensores (Clase 3) todavía no están comercialmente disponibles, sobre todo en el dominio pasivo. Principalmente esto es debido a la memoria de almacenamiento de la etiqueta, ya que en el caso de las etiquetas pasivas la capacidad de almacenamiento es bastante reducida.
- Innovaciones en los lectores: Los lectores RFID hoy en día son genéricos. Esto es una desventaja debido a que los lectores están sobrecargados con funcionalidades innecesarias para servir a un número demasiado elevado de funciones. En ellos se incluyen muchas funciones para que puedan servir posteriormente para cualquier aplicación para los que sean requeridos, cuando se debería plantear la posibilidad de fabricar lectores con unas determinadas funcionalidades dependiendo de la aplicación para la cual éste se va a utilizar.

Todas estas cuestiones son tratadas para que en un futuro la tecnología RFID pueda mejorar solventando todas sus actuales desventajas, pero como es lógico surgirán nuevas cuestiones que ayudarán al desarrollo futuro de RFID, permitiendo que no sea una tecnología de identificación estancada, como es hoy la innovación en el código de barras, ya que es una tecnología que promete en diversos campos.

[2] Respecto a las LPWAN, hay que mencionar que surgieron como alternativa viable a las tecnologías inalámbricas tradicionales para proporcionar conectividad de área amplia de bajo consumo y rentable para IoT. A medida que la cantidad de dispositivos IoT conectados aumenta de 7 miles de millones en 2018 a 22 miles de millones en 2025, se espera que las LPWAN sean un motor clave para el crecimiento. En un reciente informe de mercado que incluye un análisis exhaustivo de LPWAN, IoT Analytics estima que LPWAN será la tecnología de comunicación IoT de más rápido crecimiento en los próximos 5 años, con un número de dispositivos conectados a LPWAN que crecen un 109% por año y prevé que supere los 1.000 millones en 2023.

Hoy en día, el mercado de LPWAN se encuentra todavía en una fase temprana y se caracteriza por un alto grado de fragmentación tecnológica (IoT Analytics investigó 16 tecnologías de LPWAN y aún hay más) y una huella

de red que está lejos de ser global. Sin embargo, el análisis del mercado sugiere que esto se está consolidando rápidamente en torno a algunas tecnologías clave.

Según las estimaciones, en 2017, LoRa fue el líder general del mercado si se contabilizan las implementaciones de redes tanto públicas como privadas, mientras que Sigfox era líder en términos de conexiones a través de redes públicas, con la gran mayoría concentrada en Europa. Al contar con redes tanto públicas como privadas, NB-IoT y LoRa ya representan aproximadamente el 70% del mercado actual y se espera que aumenten su participación en el mercado a casi el 85% en los próximos 5 años.

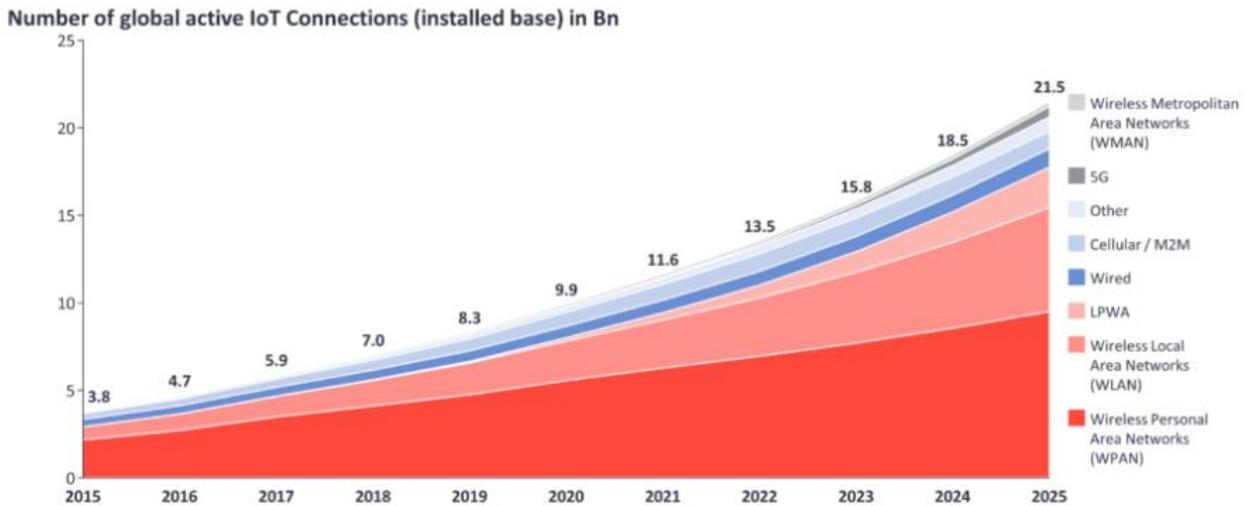


Tabla 5. Pronósticos sobre LPWAN.

[3] De la misma manera, LPWAN servirá de soporte para otras tecnologías recién implantadas. 5G, por ejemplo, está pensado para la conexión de grandes dispositivos, como teléfonos móviles y ordenadores. Es aquí donde las redes LPWAN despejarán al 5G de dispositivos que no requieran tanta potencia o Wi-Fi, trabajando en paralelo para mantener conexiones que necesiten menos caudal de datos, como sensores de alumbrado público, contadores de agua, gestores de aparcamientos, electrodomésticos... permitiendo así configuración de grandes redes destinadas al control inteligente de las ciudades.

6. ANEXOS

A continuación se desarrollan los diversos anexos que reúnen información más detallada sobre los temas tratados en apartados anteriores. Se deja en esta sección aspectos más técnicos, como datasheets, estudios más profundos sobre las tecnologías protagonistas en este proyecto, fundamentos teóricos de la tecnología RFID, sus estándares y sus antecedentes históricos. También se refleja la evolución del prototipo inicial.

6.1. Anexo A. Especificaciones técnicas lector HYM360.

Datos técnicos

No.	Item	Technical Date	Unit	Remark
1	Fixed Current	≤ 380	mA	25dBm
2	Standby Current	≤ 1	mA	EN Pin Low Level
3	Frequency Range	840~960	MHz	
4	Default Working Frequency	Hopping Frequency	MHz	Frequency Interval 250KHz
5	Fixed Power	25	dBm	Max 27dBm
6	Stepping Interval	1	dBm	10~25dBm adjustable by soft
7	Label Protocol	EPC C1G2 /ISO18000-6C		
8	Starting Time	≤ 50	ms	
9	VSWR	≤ 1.5		
10	Max Reading Range	2	m	2dBi Antenna

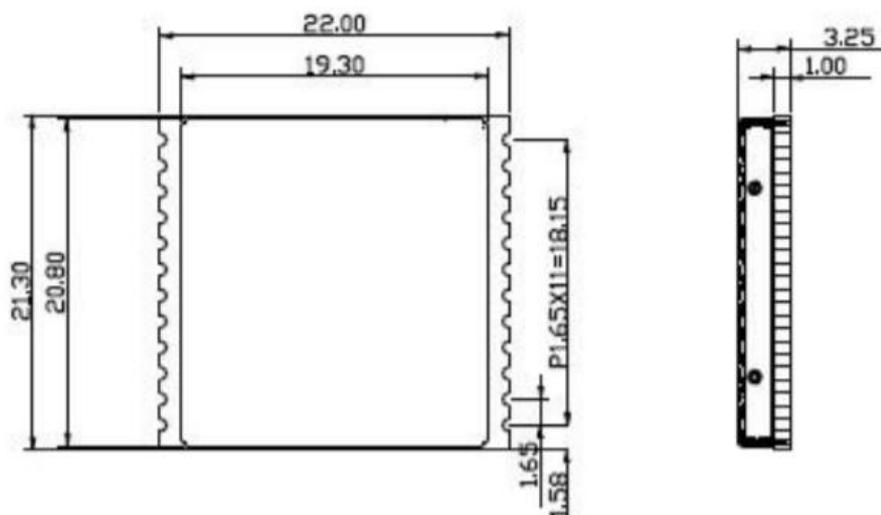
Características DC

Data	Min Value	Typical Value	Max Value	Unit	Remark
Voltage of Power	3.3	4.2	5	V	DC
Input High Level	2	3.3	3.5	V	GPIO
	2	-	5	V	EN
Input Low Level	-0.5	0	0.5	V	GPIO
	-	-	0.18	V	EN
Output High Level	2.3	-	3.3	V	GPIO
Output Low Level	0	-	1	V	GPIO
Enable Current	2	5	25	μ A	$V_{EN} \geq 2V$

Requerimientos en la antena

No.	Item	Technical Data	Unit	Remark
1	VSWR	≤ 1.5		

Dimensiones



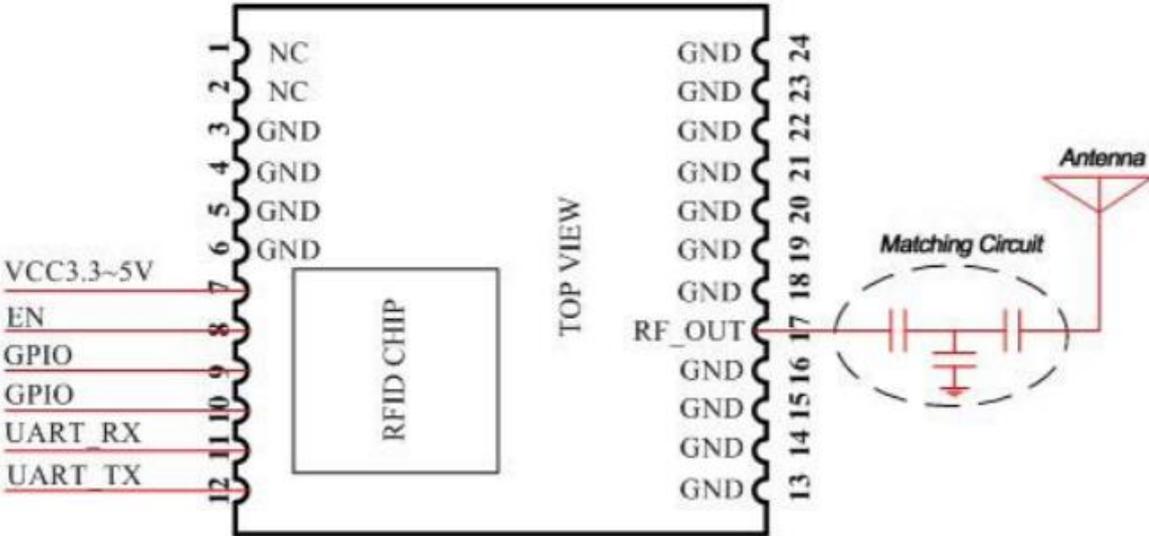
Interfaz

PIN	Signal Name	Signal Direction	Function/Compatibility Description
1~2	NC		NC
3~6	GND	-	Module Connecting Ground
7	VDD	Input	Module Supplying power
8	EN	Input	Module Enabling, Highly Effective
9	GPIO	Output	
10	GPIO	Output	
11	UART_RX	Input	
12	UART_TX	Output	
13~16	GND	-	Module connecting ground
17	RFOUT	Bidirection	Module Radio frequency Input and output interface
18~24	GND	-	Module connecting ground

Requisitos de entorno

No.	Item	Technical Data	Unit	Remark
1	Working temperature	-20~+70	℃	
2	Storage temperature	-40~+85	℃	
3	Relative humidity	10%~90%	RH	

Pinout



6.2. Anexo B. Especificaciones técnicas antena HYN503.

Prestaciones

- Frecuencia: 860 – 960 MHz.
- ROE Máxima: $\leq 1.3:1$
- Ganancia: > 9 dBi
- Ancho de haz campo H: 70°
- Ancho de haz campo E: 70°
- Polarización: circular
- Humedad relativa: 5% ~ 95%
- Impedancia de entrada: 50Ω
- Conector: N-50KFD (Tipo N hembra)

Características físicas

- Tamaño: 258mm x 258 mm x 56 mm
- Peso: 0.91 kg
- Material: Acrilonitrilo-estireno-acrilato plástico.
- Color: blanco.
- Grado de protección: IP67
- Temperatura de operación: $-40^\circ \text{C} \sim +85^\circ \text{C}$
- Temperatura de almacenamiento: $-40^\circ \text{C} \sim +85^\circ \text{C}$

Diagrama de radiación

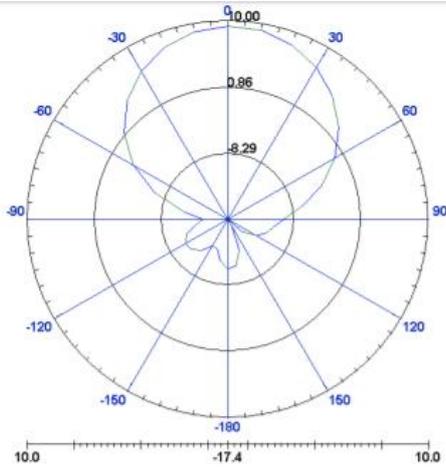


Figure 7. The radiation pattern(E side)

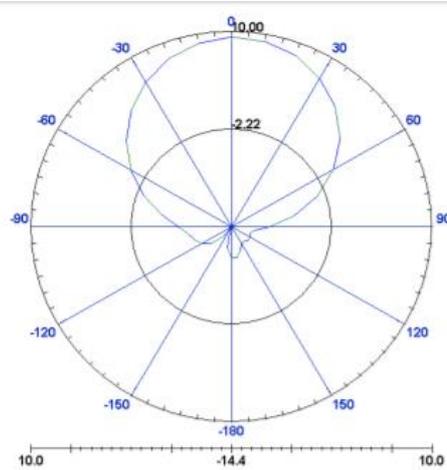
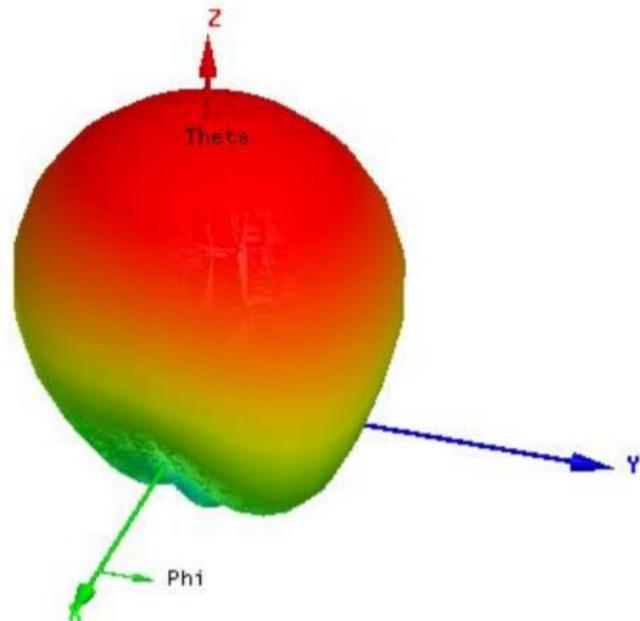
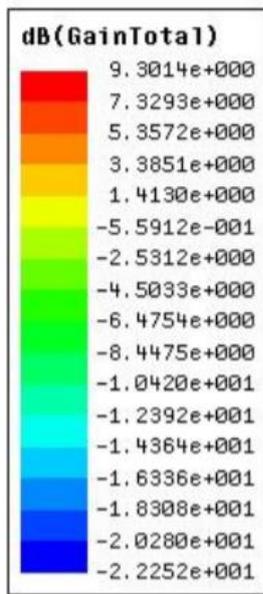


Figure 8. The radiation pattern(H side)



6.3. Anexo C. Etiqueta pasiva HYT-MT-U031b.

Características físicas

- Dimensiones 132.37mm x 22.37mm x 11 mm
- Diámetro de los orificios: 3.5mm
- Distancia entre orificios: 119mm
- Material: policarbonato

Prestaciones

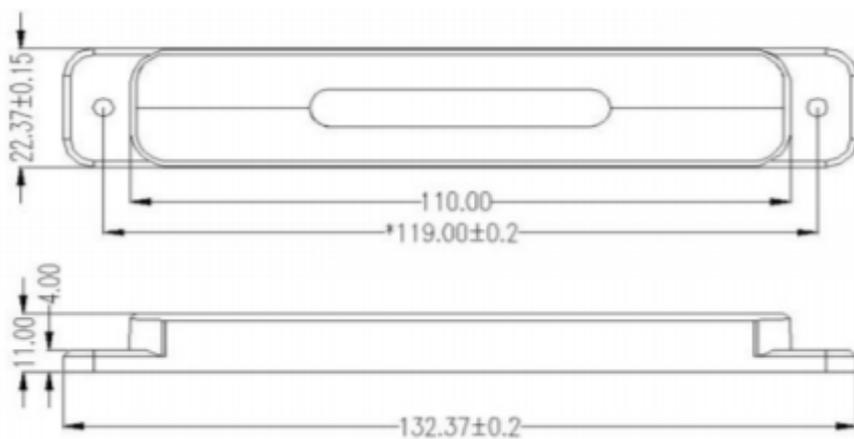
- Frecuencia: 860-960 MHz
- Protocolo: EPC Class1 Gen2, ISO 18000-6C
- Tamaño de la memoria: 512 bits.
- Distancia de lectura: < 15m
- Retención de datos: 10 años.

Características de entorno

- Temperatura de operación: -40° C - +85° C
- Temperatura de almacenamiento: -40° C - +120° C

Montaje

Magnético, atornillado, remache, colgado o adhesivo.



6.4. Anexo D. Etiqueta pasiva ALN-9662.

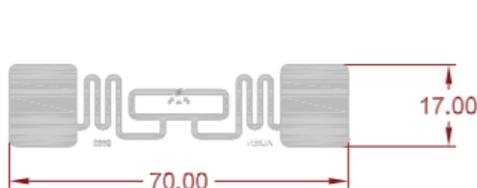


FEATURE	DESCRIPTION	BENEFIT
Squiggle tag performance in a narrower form-factor	Equivalent performance to the well-regarded Squiggle tag but in a more compact form-factor. One of Aliens best performing general-purpose tags.	Smaller form-factor, still robust, proven, and reliable
Multiple frequency optimized sensitivity	Optimized for high performance in all world regions	A worldwide performance tag

Prestaciones

- Compatible con EPC Gen 2
- Compatible con ISO/IEC 18000-6C
- Frecuencia de operación RFID UHF (860-960MHz)
- Núcleo Higgs™-3 IC con 800 bits de memoria no volátil
 - 32 bits de TID
 - 64 bits de TID Única
 - 96 bits de memoria EPC, extensible a 480 bits.
 - 512 bits de memoria de usuario.
 - 32 bits de contraseña de acceso.
 - 32 bits de “Kill password”
- Preprogramada con número de serie único e inalterable de 64 bits, ideal para autenticación
- Comandos personalizados para programación rápida

Dimensiones

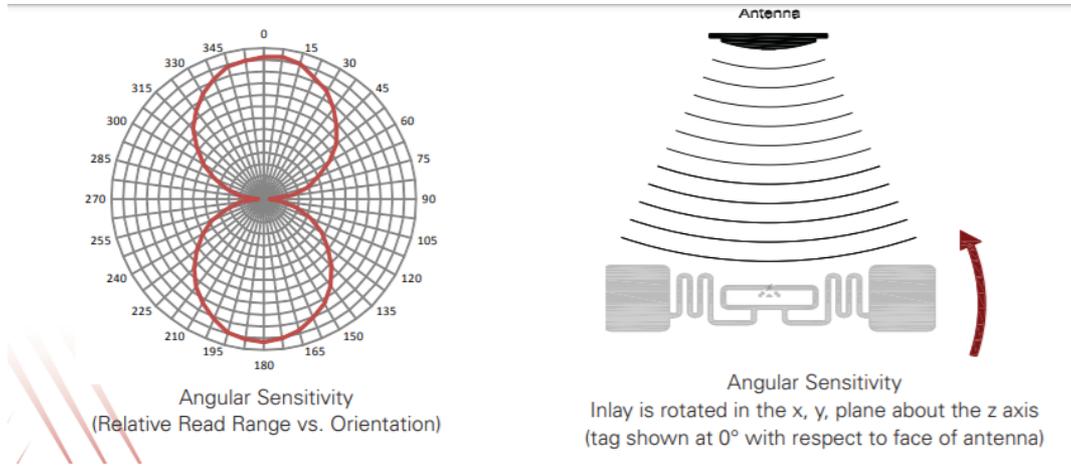


ALN-9662-FRA / FSRA
(Dry Unslit / Slit Inlay)



ALN-9662-FWRCA / FWRWA
(Clear / White Wet Inlay)

Sensibilidad angular



6.5. Anexo E. Antecedentes de RFID

Se denomina RFID (Radio Frequency IDentification) a una tecnología que se desarrolló en el ámbito militar hace 60 años. La radio frecuencia se remonta a tiempos de James Clerk Maxwell quien, en 1864, predijo la existencia de ondas electromagnéticas. A su vez, en 1888, Heinrich Hertz demostró también su existencia mediante un aparato que producía y detectaba ondas en la región UHF. Se cree que fue Nikola Tesla el primer inventor de un sistema radio, aunque no fue él quien lo llevó a la práctica, sino que fue el ingeniero Guillermo Marconi, quien en el año 1901 realizó la primera transmisión radioeléctrica transatlántica utilizando, eso sí, los diseños del propio Tesla.

Los orígenes de la tecnología RFID no están claros, ya que en parte se considera al espionaje soviético en 1945 como propulsor de dicha herramienta, inventada por Léon Theremin, una vez finalizada la Segunda Guerra Mundial. Dicha herramienta consistía en un dispositivo de escucha pasivo. Sin embargo, estos orígenes son dudosos ya que se trataba de un dispositivo de escucha encapsulado pasivo y no una etiqueta de identificación tal y como hoy la conocemos.



Figura 65. Léon Theremin, 1927.

Por otra parte, se relaciona como precursora directa de RFID a la antena IFF, establecida en 1939. Dicha antena fue utilizada por el servicio británico en la Segunda Guerra Mundial con el objetivo de distinguir entre sus propios aviones y los del enemigo. Anteriormente se necesitaba que el avión aterrizara en la base para realizar tal distinción, pero gracias a la antena IFF (Identify: Friend or Foe) se podía distinguir a una distancia de 40 kilómetros. Se instalaba una antena al fuselaje de los aviones aliados de manera que respondieran correctamente a una señal de interrogación que se les enviaba y, de tal forma, se comprobaba si el avión era aliado o no. Este sistema dio servicio desde la Segunda Guerra Mundial, aunque su uso no fue eficiente para aviones de alta velocidad o para tráfico aéreo denso. A pesar de ello, sobre dicho sistema se basó el control aéreo actual.

En 1948 se publicó “Communications by Means of Reflected Power”, de Harry Stockman. Dicho evento puede ser considerado como el nacimiento de RFID.

Los avances en radiofrecuencia y comunicaciones de radar continuaron. En la década de los 50 se efectuaron numerosos estudios orientados a la seguridad en minas de carbón, exploraciones petrolíferas e instalaciones nucleares, así como controles de acceso o sistemas antirrobo.

A finales de los años 60 comenzaron las primeras actividades comerciales a raíz de la fundación de Sensormatic y Checkpoint. Ellos desarrollaron EAS (Electronic Article Surveillance), un equipo de vigilancia anti-intrusión electrónica. Dicho equipo fue el primer desarrollo RFID y supuso el preludio de la explosión de RFID en los 70.

Finalmente, en 1973, se crearon las primeras patentes de RFID. Mario W. Cardullo obtuvo una patente para su etiqueta RFID activa con memoria degradable, y Charles Walton obtuvo la patente por su transpondedor pasivo, utilizado para abrir puertas sin llave.

El desarrollo de RFID tomó diversas direcciones durante el resto de los 70 y la década de los 80. Se implantó un sistema de seguimiento de camiones destinados a transportar material nuclear, el cual fue precursor del sistema de control de paso en peajes. Del mismo modo, se obtuvo un sistema para rastrear personas en edificios, desde hospitales a oficinas de compañías.

En el 94, el Departamento de Defensa Estadounidense comenzó a utilizar RFID para seguir el rastro de contenedores de envío, lo que le permitió reducir el número de contenedores a utilizar en un 90%.

En 2001, la firma norteamericana GAP inició un programa piloto en el cual se incluía una etiqueta en sus productos que permitía conocer su situación en todo momento. Dicha iniciativa mejoró la eficiencia de su cadena de aprovisionamiento.

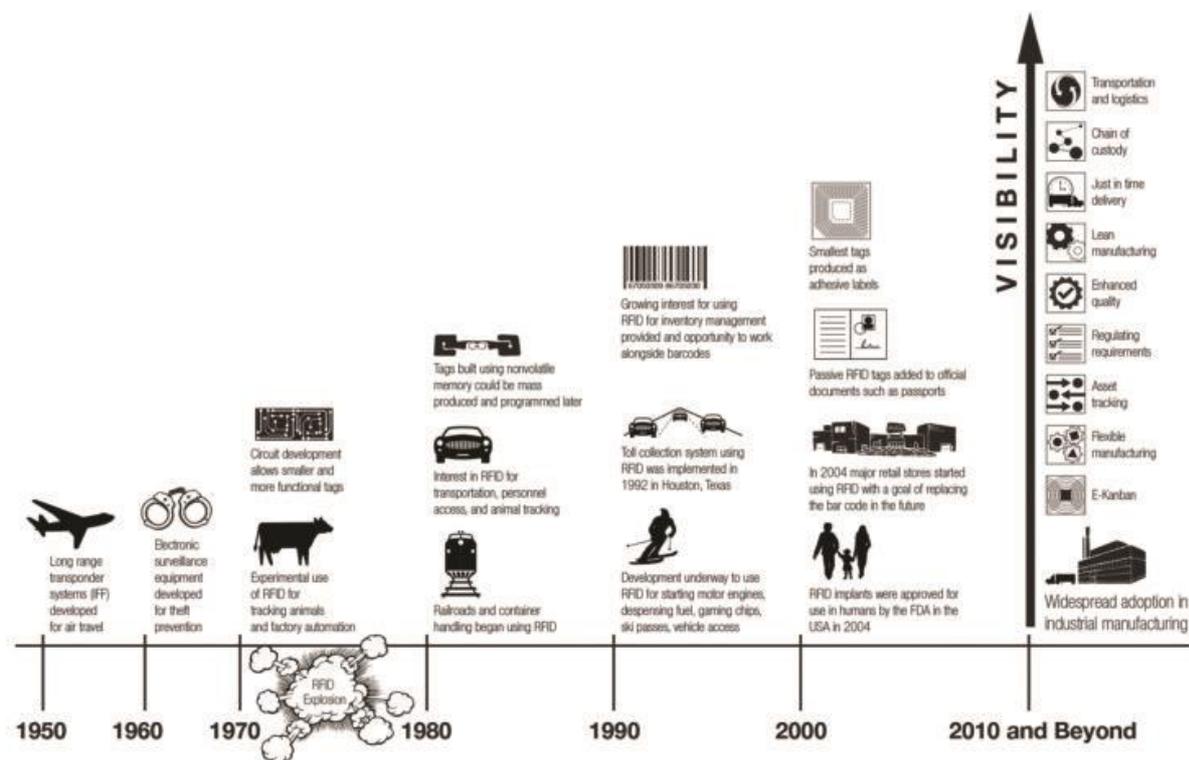


Figura 66. Historia de RFID.

Cabe destacar que, al principio, el alto costo de esta tecnología dificultó su utilización. Sin embargo, su desarrollo ha permitido automatizar y miniaturizar tanto los procesos de fabricación de RFID que actualmente se trata de una tecnología al alcance de prácticamente cualquier organización, y puede ser utilizada en un sinnfín de productos, desde contenedores de barcos hasta simples documentos.

Con la evolución de Internet y sistemas de comunicación, emerge la necesidad de conectar cualquier dispositivo de ámbito cotidiano, pero no sólo el uso doméstico se ve beneficiado (electrodomésticos, domótica...), sino el mundo empresarial tiende a adoptar también este tipo de soluciones, orientando más su aplicación a la eficiencia y optimización en vez de al confort. Es aquí donde RFID se manifiesta como una de estas tecnologías en la evolución del Internet de las cosas siendo su uso eminentemente empresarial. Actualmente, su principal uso es la identificación de objetos a distancia sin contacto y sin hilos, es decir, mediante radiofrecuencia. Un interrogador RFID realiza peticiones que unas etiquetas radiantes son capaces de recibir y responder y, como cada etiqueta tiene un código único, se podrá identificar de forma igualmente única. Asimismo, estas etiquetas pueden almacenar datos de bajo nivel, como la potencia de señal recibida por las etiquetas o la fase de dicha señal, pudiéndose realizar tareas de geolocalización. De dicha manera, este sistema podría permitir conocer la ubicación en tiempo real de todas las unidades del stock de un determinado producto en un almacén., facilitando enormemente labores que hasta el momento se realizan manualmente, como son el control de inventario o búsqueda de unidades descolocadas de un determinado elemento. [4] [1]

6.6. Anexo F. Fundamentos de RFID.

RFID son las siglas en inglés de Radio Frequency IDentification, que en español significa *Identificación por radiofrecuencia*.

El propósito fundamental de la tecnología RFID es identificar mediante un lector, sin contacto y a distancia, una tarjeta o etiqueta (tag) portada por una persona, un vehículo en movimiento o cualquier producto que se encuentra en un almacén o en una cadena de producción automatizada. [5]

El modo de funcionamiento consiste en que una etiqueta RFID que contiene generalmente datos de identificación del objeto al que se encuentra adherido, genera una señal de radiofrecuencia con dichos datos. Un lector RFID captura dicha señal, la lee y la transmite a una aplicación específica denominada “middleware”.

La comunicación se realiza entre un transmisor y un receptor, por lo que ambos llevan incorporada una antena. En la comunicación se transmite información y también energía, la cual se utiliza en el caso de las etiquetas pasivas para activar su circuitería.

Existen dos tipos de mecanismos de comunicación electromagnética, que dependerá directamente de la distancia de la comunicación y de la frecuencia que se esté empleando:

- Campo lejano: basado en campos electromagnéticos, se utiliza para comunicación de largas distancias o frecuencias altas. Es el mecanismo usado para tags UHF.
- Campo cercano: basado en campos magnéticos, se utiliza para comunicación a corta distancia o frecuencias bajas. Es el mecanismo usado para los tags HF.

La antena de las etiquetas es crítica en las comunicaciones, ya que su forma y su tamaño varían según si se utiliza campo lejano o campo próximo. En el caso de que se trate de campo lejano el tamaño de la antena ha de ser obligatoriamente la mitad de la longitud de la onda.

6.6.1. Frecuencias de Trabajo

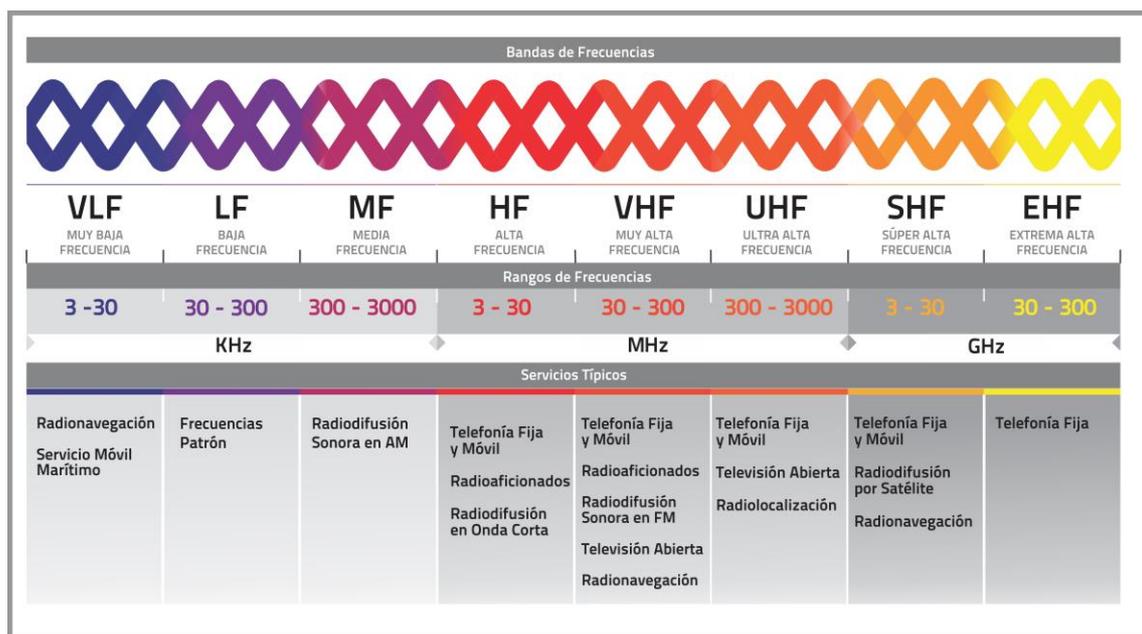


Figura 67. Banda de frecuencias.

Los sistemas RFID pueden trabajar en distintas bandas de frecuencias. [4]

- Banda LF: Podemos encontrar sistemas que trabajan de los 125-134 kHz a los 140-148,5 kHz. Tienen un alcance limitado a centímetros, la menor dentro de los sistemas RFID. Su uso más habitual es la identificación de animales o el uso para los mandos de arranque de los coches.



Figura 68. Pulsera impermeable de RFID a 125 KHz.

- Banda HF: Su banda de frecuencia de uso a nivel internacional es la de 13,56 MHz. Tiene un alcance de lectura de 1,5 metros, según el tamaño de la etiqueta. Suele emplearse en tarjetas de acceso a edificios o para etiquetas antirrobo. Éstas ofrecen una alta fiabilidad, independencia respecto a la orientación de la etiqueta, resistencia frente a interferencias eléctricas, variabilidad en el tamaño de los tags y posibilidad de aumentar el tamaño de las antenas lectoras.
- Banda UHF: Se sitúa en la banda de 868 MHz en Europa y 915 MHz en EEUU. Tiene un alcance de 5 metros, y suelen emplearse en la identificación de objetos, palés, cajas, etc. Otra de sus ventajas, aparte de su mayor rango de lectura, es su bajo coste.
- Banda de microondas: Se usan frecuencias de 2.45 GHz y 5.8 GHz. Se emplea más para los tags activos en el uso de seguimiento y trazabilidad de personas u objetos.

UHF	HF and LF
Single worldwide Gen2 standard	Multiple competing standards
20x the range and speed of HF	HF-based NFC for secure payment
Labels cost 5¢–15¢ in 2017	Labels, cards, inlays cost 50¢–\$2
The technology for item tagging	Used in access control, ticketing, payment

Figura 69. Comparativa UHF - HF & LF.

Banda frec.	LF 125 y 134.2 KHz	HF 13.56 MHz	UHF 868-915 MHz	SHF 2.45 y 5.8 GHz
Principio físico	Acoplo inductivo	Acoplo inductivo	Propagación (campo lejano)	Propagación (campo lejano)
Rango lectura	< 0.5 m	< 1 m	< 15 m	< 15 m
Coste unidad	> 1 euro	> 0.4 euro	> 0.15 euro	> 0.3 euro

Tabla 6. Prestaciones RFID según frecuencia de trabajo.

6.6.2. Componentes del Sistema

Todo Sistema RFID consta de tres partes fundamentales: [1]

6.6.2.1. Etiqueta RFID, transpondedor o Tag

6.6.2.1.1. Descripción

Una etiqueta RFID se trata de un elemento que permite almacenar y enviar información a un lector en forma de ondas de radio. Está compuesta por una antena, un microchip y el sustrato. El propósito de la antena es permitir al chip transmitir la información de identificación de la etiqueta. El chip posee una memoria interna para almacenar el número de identificación y en algunos casos datos adicionales cuya capacidad depende del modelo. El sustrato mantiene el chip y antena juntos y los protege. En su mayoría son un film de plástico.

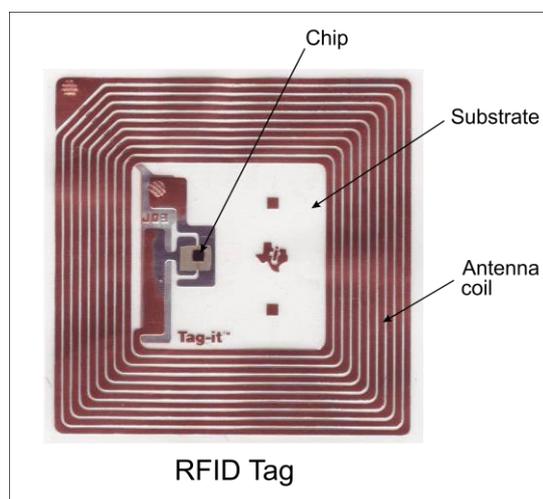


Figura 70. Antena y chip en tag RFID.

[1] No todas las etiquetas contienen chip o circuito integrado, ya que existe un tipo de etiqueta que no contiene chips, en este caso se trataría de una etiqueta RF, la cual actúa de igual modo que un interruptor, pudiendo estar apagada o encendida. Este tipo de etiqueta es muy útil, por ejemplo, en supermercados, apagándose esta etiqueta al pasar por caja, y un lector te permite abandonar el supermercado si has pagado tus productos, es decir, las etiquetas de tus productos se han apagado. Sin embargo, todas las etiquetas contienen una bobina o antena, las cuales pueden ser de múltiples formas.

Los tags pueden ser clasificados atendiendo a diversas características; como tipo de memoria, capacidad de

almacenamiento, origen de la fuente de alimentación... Por ejemplo, sus clasificaciones más generales son:

- La cantidad de datos que puede almacenar: Puede variar desde un simple bit, los bits suficientes para almacenar un Código Electrónico de Producto, o miles de bits. Normalmente las etiquetas con alta capacidad de almacenamiento son activas.
- El tipo de energía: Las etiquetas RFID de bajo coste normalmente son pasivas, lo que significa que usan la energía emitida por el lector para encender su microchip. Sin embargo, las etiquetas activas disponen de su propia fuente de alimentación interna, y es por ello por lo que pueden transmitir a largas distancias.
- La frecuencia de operación: Frecuentemente las bandas de frecuencia para los sistemas RFID son 135 KHz, 13.56 MHz, 915 MHz y 2.45 GHz. Estas frecuencias las pone el gobierno, quien controla el espectro electromagnético en cada región.
- El algoritmo de anticolidión usado: Las colisiones de radio frecuencia ocurren cuando muchas etiquetas responden simultáneamente a una petición de un lector. Sus señales pueden interferir en las de las otras, provocando que el lector no pueda identificar a las etiquetas.

Gracias a que existen tantas clasificaciones podremos elegir el mejor tipo de etiqueta RFID para cada una de las aplicaciones. Dependiendo del entorno en el que van a ser utilizadas, las etiquetas pueden tomar diversas formas y tamaños. Existe la posibilidad de encapsulación en diferentes tipos de material, y normalmente éste suele ser PVC para obtener una mayor durabilidad, sobre todo en aplicaciones de ciclo cerrado, donde se tienen que reutilizar, o ambientes hostiles. También se pueden insertar en tarjetas de plástico o láminas de papel. Por último, hay que destacar el encapsulado en cristal o cerámica, especialmente idóneos para entornos corrosivos.

Existen también algunas características que puede modificar el comportamiento de una etiqueta:

- Adherir el tag: Cualquier etiqueta debe tener un mecanismo que permita adherirla al objeto o persona al cual va a ir asignado.
- Lectura de la etiqueta: Cualquier tipo de etiqueta debe poner comunicar información mediante radiofrecuencia, para que pueda ser leída por el lector.
- Kill/Disable: El lector puede enviar un comando a una etiqueta para que deje de funcionar permanentemente. No todos los tags poseen esta funcionalidad.
- De una única escritura: A muchas etiquetas se les introduce su identificación en el propio proceso de fabricación, siendo por lo tanto imposible para el usuario cambiar o configurar este valor.
- De muchas escrituras: Algunas etiquetas RFID, etiquetas de lectura/escritura, tienen la posibilidad de poder escribir y rescribir información en ellas tantas veces como se desee.
- Anticolisión: Permite a las etiquetas conocer cuándo debe transmitir para no entorpecer o molestar a otras lecturas, ya que cuando hay muchos tags próximos a un lector, éste podría verse dificultado para comunicarse con ellos a la vez.
- Seguridad: Algunas etiquetas permiten cifrar la información en la comunicación. Algunos de ellos también permiten responder únicamente a lectores que les proporcionan una contraseña o password secreto.
- Estándares: Las etiquetas pueden cumplir uno o más estándares, permitiendo por lo tanto comunicarse con los lectores que los cumplen o son compatibles con ellos.

6.6.2.1.2. Clasificación según alimentación

Sin embargo, la clasificación más importante que se puede realizar es atendiendo al origen de la energía, batería interna o fuente de alimentación.

- Etiquetas Pasivas: No se requiere fuente de alimentación interna, ya que toda la energía se recoge del campo electromagnético creado por el lector, el cual basta para excitar el circuito integrado y generar una respuesta.

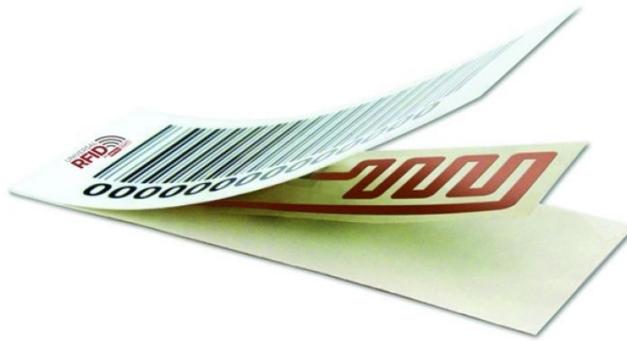


Figura 71. Tag pasivo.

La dinámica es la siguiente; [6] La antena crea un campo electromagnético que es recibido por la antena del tag, creándose una diferencia de potencial en las bornas de la antena tag y, por tanto, una corriente. Esta corriente es rectificadora por un diodo y filtrada usando un condensador de almacenamiento para crear una tensión más o menos constante, que será la que alimente el circuito lógico y la memoria del tag. La memoria pasiva es no volátil ya que el tag está normalmente apagado. Un circuito similar de rectificación, usando un condensador más pequeño para permitir que la tensión varíe en la escala de tiempos del lector, se utiliza para demodular la información del lector. Esta técnica se conoce como “detección de envolvente”. Finalmente, un transistor a modo de switch conmuta la corriente; en ON la antena está a tierra y la corriente fluye por ella, En OFF la antena queda al aire, sin corriente que la recorra.

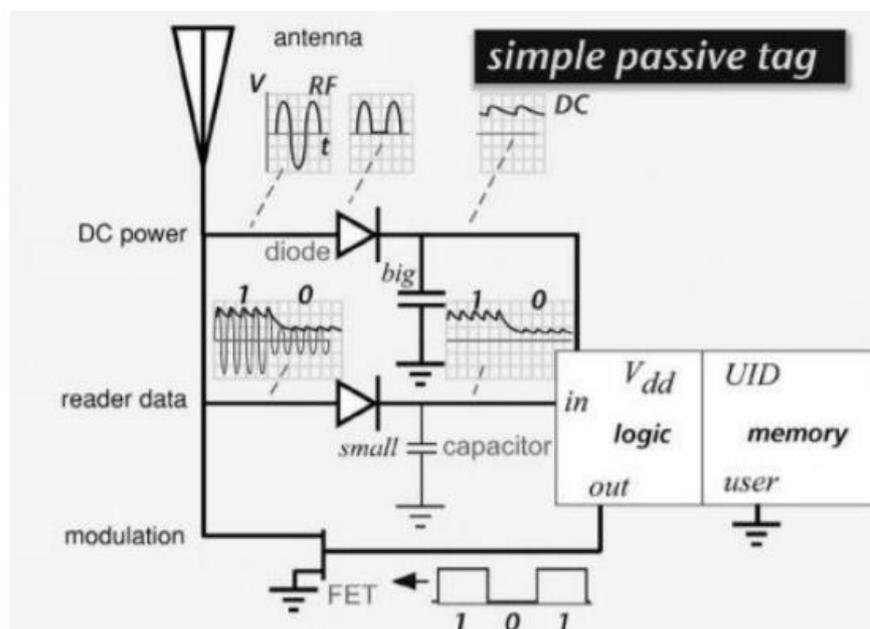


Figura 72. Esquemático de un tag RFID pasivo.

[7] De dicha manera, se genera una señal de respuesta, conocida como *Backscatter signal*. Como se ha comentado antes, se va generando una corriente en la antena, producto de la conmutación de estados del transistor entre ON y OFF. Esta corriente no es distinta de la corriente inicial que se produjo por la onda electromagnética recibida por la antena y empezó todo el proceso detallado anteriormente. Esta corriente, por tanto, origina una radiación en la antena y, por tanto, una señal de respuesta en la misma frecuencia. Esto es posible gracias al principio de reciprocidad³, un principio de la teoría electromagnética válido la mayor parte de las veces en el mundo ordinario. En este caso, este principio afirma que una estructura que puede recibir una onda también puede transmitirla.

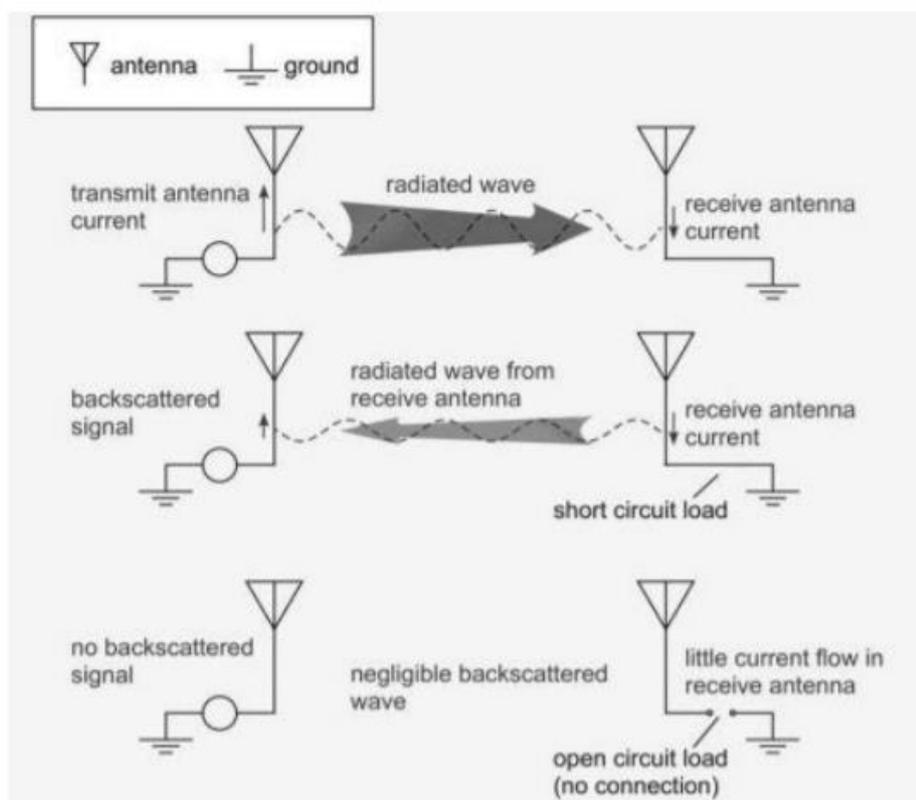


Figura 73. Simplificación del “Backscatter Signaling”.

En otras palabras, el transistor modula la señal de respuesta en función de la señal procedente del micro de la etiqueta. Nótese que la señal que llega al transistor es una señal en banda base⁴ a frecuencia de kHz como mucho,

³ [31] Es un teorema muy usado en análisis de circuitos. El teorema de reciprocidad cuenta con dos enunciados que en términos generales nos dice:

“En cualquier red bilateral real pasiva, si la fuente de tensión simple V_x en la rama x produce la respuesta en corriente I_y en la rama y , entonces la eliminación de la fuente de tensión en la rama x y su inserción en la rama y produciría la respuesta en corriente I_x .”

⁴ [32] El término banda base se refiere a la banda de frecuencias producida por un transductor, tal como un micrófono, un manipulador telegráfico u otro dispositivo generador de señales que no es necesario adaptarlo al medio por el que se va a transmitir.

Banda base es la señal de una sola transmisión en un canal, banda ancha significa que lleva más de una señal y cada una de ellas se transmite en diferentes canales, hasta su número máximo de canal.

En los sistemas de transmisión, la banda base es generalmente utilizada para modular una portadora. Durante el proceso de demodulación se reconstruye la señal banda base original. Por ello, podemos decir que la banda base describe el estado de la señal antes de la modulación y de la multiplexación y después de la demultiplexación y demodulación.

Las frecuencias de banda base se caracterizan por ser generalmente mucho más bajas que las resultantes cuando éstas se utilizan para modular una portadora o subportadora.

aunque la señal reflejada al lector debe estar a MHz. El uso de un enlace mediante backscatter significa que el circuito de modulación por switching en la etiqueta solo necesita operar a frecuencias modestas comparables a la información, no la frecuencia de la portadora, ahorrando coste y potencia.

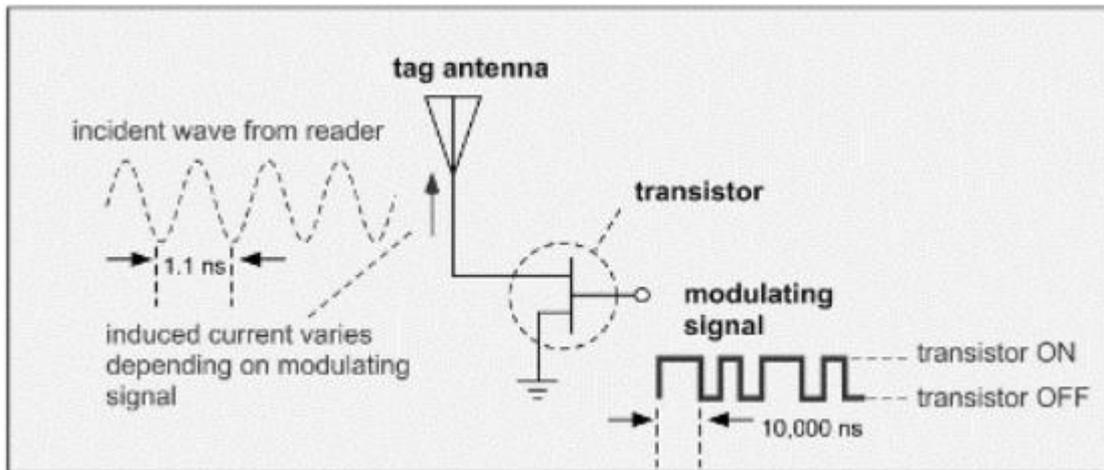


Figura 74. Backscatter modulado usando un transistor como switch.

Es fundamental que, para establecer un enlace de esta manera, el lector transmita una señal. En muchos sistemas de radio, el transmisor se apaga cuando el receptor está tratando de recibir la señal. Este esquema se denomina *semi-duplex*, distinto del *full-duplex*, donde transmisor y receptor trabajan de forma simultánea.

Las etiquetas RFID pasivas son las etiquetas más económicas disponibles en el mercado, sin embargo, tienen como inconveniente que el rango de comunicación es menor que en las etiquetas activas o semiactivas.

Esta característica es uno de los principales factores que determinan el coste y el tiempo de vida de la etiqueta o tag. Las etiquetas con batería son más caras, pero este incremento de coste se contrarresta con las ventajas que éstas ofrecen. Las etiquetas RFID activas, es decir, las etiquetas que disponen de batería interna tienen una distancia de lectura mucho mayor que las pasivas, además a éstas se les pueden añadir otras funcionalidades como pueden ser sensores de temperatura, velocidad o movimiento, entre otras.

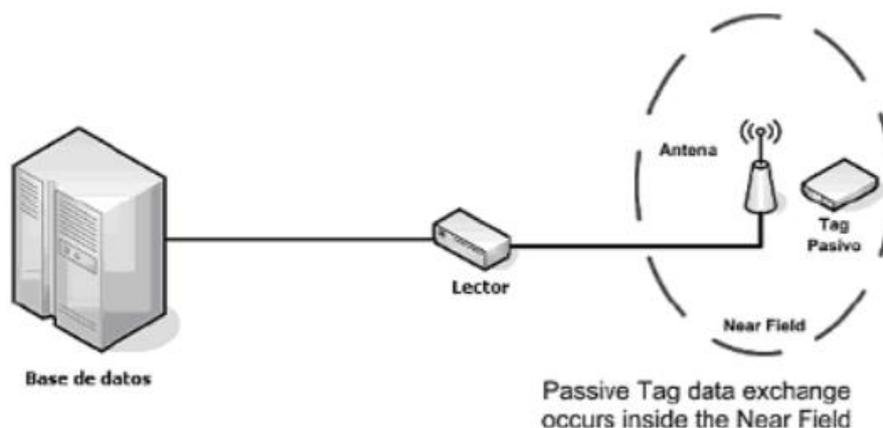


Figura 75. Procesado de etiquetas pasivas.

- **Etiquetas Activas:** [1] Disponen de una propia batería para el suministro de energía, la cual utilizan para dar corriente a sus circuitos integrados y para propagar la señal al lector, es por ello permiten una mayor cobertura de difusión. Normalmente tienen una mayor capacidad de almacenamiento de información, más allá de un simple código de identificación, debido a que disponen de más energía que permite enviar más información. También pueden llevar incorporados sensores adicionales a la propia memoria

como sensores de temperatura, de velocidad, de movimiento, etc., los que permiten almacenar o controlar datos vitales en algunas aplicaciones, como puede ser por ejemplo en productos perecederos.

Gracias a la fuente de energía interna son capaces de transmitir señales más potentes que las de las etiquetas pasivas, convirtiéndoles por ello en sistemas más eficientes para entornos difíciles para la radiofrecuencia como por ejemplo el agua o el metal. Estas etiquetas son mucho más fiables, es decir, tienen menos errores que las pasivas debido a que éstas tienen capacidad de establecer sesiones con el lector.

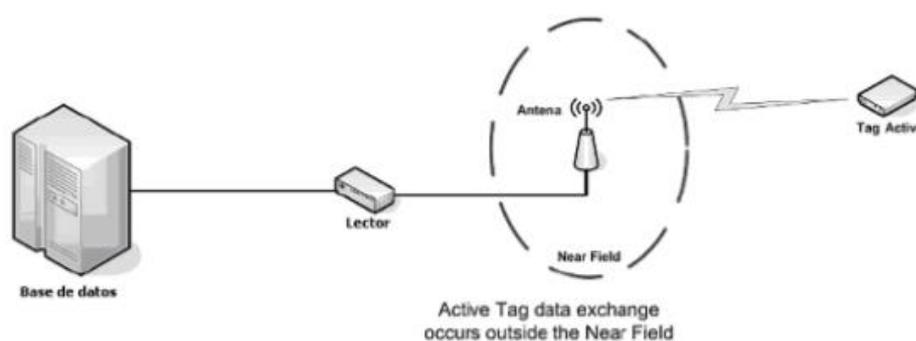


Figura 76. Procesado de etiquetas activas.

Estas etiquetas RFID activas son las más caras del mercado, suelen ser de mayor tamaño sobre todo si incluyen sensores, y por lo general su vida útil es mucho más corta, tan corta como sea la vida útil de su fuente de alimentación. Hablando en números, tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años.



Figura 77. Tags activos.

- **Etiquetas Semi-Activas o Semi-Pasivas:** [1] Estas etiquetas utilizan una batería para activar la circuitería del chip, como las etiquetas RFID activas, pero la energía para generar la comunicación con el lector es la que recoge de las ondas de radio de éste, como las etiquetas RFID pasivas, es por ello que son llamadas Semi-Activas o Semi-Pasivas. Debido a que utilizan una batería, éstas son más grandes y más caras que las etiquetas pasivas y más baratas y más pequeñas que las activas, sin embargo, consiguen mejores rangos de comunicación en comparación con las pasivas por la misma razón que las etiquetas activas. Del mismo modo, algunas de estas etiquetas llevan integrados sensores de temperatura, o movimiento para proporcionar mayores funcionalidades. Este tipo de etiquetas tienen una fiabilidad comparable a la de las etiquetas RFID activas a la vez que pueden mantener el rango operativo de una

etiqueta RFID pasiva, además su tiempo de vida suele ser mayor que la de las etiquetas activas.

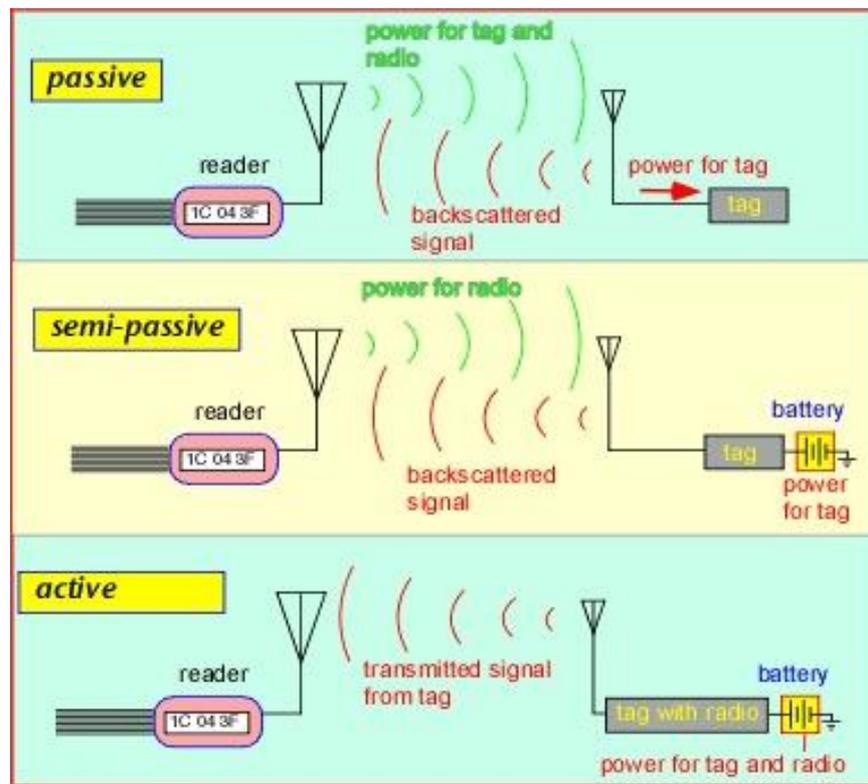


Figura 78. Comparativa de tags pasivos, semi-pasivos y activos.

6.6.2.1.3. Parámetros que intervienen en el comportamiento de la etiqueta

[1] Existen una serie de parámetros que intervienen en el comportamiento de la etiqueta dependiendo de la frecuencia que se utilice. Estos efectos son provocados por diferentes materiales, los cuales afectan a las señales de radiofrecuencia.

Absorción

Algunos materiales absorben la energía propagada en las ondas de radio, provocando que haya menos potencia disponible para que la etiqueta RFID pueda devolver la señal, es decir, responder al lector. Cuando una onda de radio tropieza con un obstáculo, parte de su energía es absorbida por éste y se convierte en otro tipo de energía, mientras que otra parte se atenúa y sigue propagándose.

La atenuación ocurre cuando la energía de una señal de radio se reduce en el momento de la transmisión. La atenuación aumenta a medida que aumenta la frecuencia o aumenta la distancia. Cuando una señal choca con un obstáculo, la atenuación producida depende directamente del tipo de material del que esté constituido el obstáculo. En este caso, los materiales líquidos son los que provocan absorción, tanto el agua, como el jabón o los medicamentos. Éstos absorben las ondas de radio y reducen la energía transmitida por el lector que es captada por la etiqueta, provocándose por ello una reducción de la fuerza de la señal.

No obstante, no todos los materiales líquidos provocan absorción, ya que el agua se comporta de una manera muy distinta al aceite. Algún ejemplo del grado de atenuación de los distintos materiales se puede observar en la tabla de a continuación.

Material	Grado de atenuación	Ejemplo
Aire	Ninguno	Lectura de tag RFID al aire libre.
Plástico	Bajo	Lectura de tag RFID de un objeto a través de su envoltorio de plástico.
Vidrio	Bajo	Lectura de tag RFID de un objeto encerrado detrás de una vidriera, como puede ser en una joyería.
Agua	Medio	Lectura de tag RFID en un ambiente húmedo.
Seres Vivos	Medio	Lectura de tag RFID incluida en una mascota o un ser humano.
Ladrillos	Media	Lectura de tag RFID a través de una pared de ladrillo.
Metal	Muy Alto	Lectura de tag RFID incluida en el interior de un armario metálico.

Tabla 7. Grado de atenuación según material.

Reflexión

En algunas ocasiones, los materiales del entorno de la etiqueta RFID puede reflejar o refractar la onda, lo que provocaría que la etiqueta recibiera además de la onda principal enviada por el lector, ondas reflejadas que son diferentes a la onda principal. Cuando una onda de radio choca contra un obstáculo, parte o la totalidad de la onda se refleja y se observa una pérdida de la intensidad.

Una onda de radio es susceptible de propagarse en varias direcciones. Una señal de origen, después de haberse reflejado varias veces, puede llegar a un mismo punto destino después de tomar muchas rutas diferentes. La diferencia temporal en la propagación entre dos señales que toman diferentes rutas puede provocar que flujos de datos que se reciban se superpongan entre sí, produciendo una interferencia que se incrementa a medida que aumenta la velocidad de transmisión.

La reflexión es provocada principalmente por materiales metálicos, éstos provocan que la energía que proviene del lector no pueda ser absorbida en su totalidad por la etiqueta, que puede provocar una desintonización de la antena.

Efectos dieléctricos

La concentración de campo magnético cerca de un material dieléctrico se puede multiplicar, provocando por ello una desintonización de la antena de la etiqueta.

Efectos de propagaciones complejas

Estos efectos se producen debido a dos fenómenos físicos, las ondas diferentes a la directa, y los múltiples caminos causados por las ondas estacionarias que pueden cancelar la onda directa.

Interferencia

[8] La interferencia es un fenómeno en el que dos o más ondas se superponen para formar una onda resultante de mayor, menor o igual amplitud. El efecto de interferencia puede ser observado en todos los tipos de onda, como ondas de luz, radio, sonido, entre otros.

En la superposición de ondas con la misma frecuencia el resultado depende de la cantidad y de la diferencia de fase. Si sumamos dos ondas, la onda resultante tendrá la misma frecuencia y, en el caso de que la fase sea $0, 2\pi$, etc, la amplitud será el doble.

Este tipo de interferencias da lugar a patrones de interferencia, ya que, dependiendo de la fase, la interferencia será destructiva (las ondas se encuentran desfasadas 180 grados o π radianes) o constructiva (desfase de 0 grados/radianes).

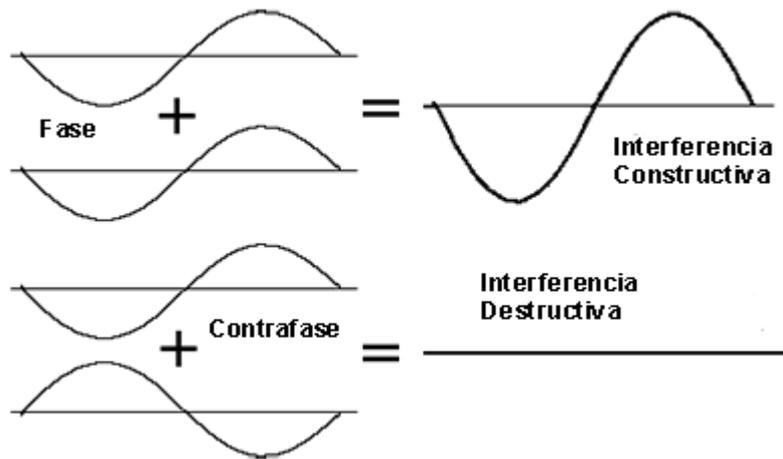


Figura 79. Interferencia.

En RFID, la interferencia ocurre cuando una antena recibe señales de la misma frecuencia desde dos o más fuentes. Debido a lo cual la tarea del lector se ve dificultada al tener que diferenciar entre señales que compiten entre ellas y llevan a una alta tasa de errores bit, y bajas tasas de datos. Sin embargo, la interferencia mutua⁵ es producida por lecturas exitosas provenientes de etiquetas de zonas de lectura muy cercanas.

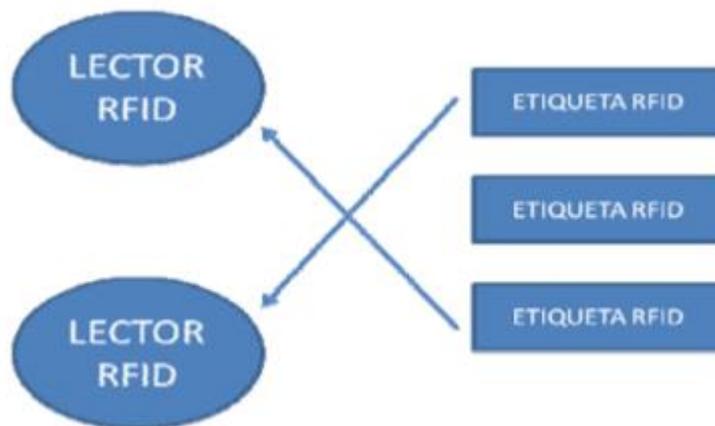


Figura 80. Interferencia mutua.

En los Estados Unidos, para evitar las colisiones que se producen por la interferencia entre dispositivos que comparten el mismo espectro de frecuencia, los reglamentos de la Comisión Federal de Comunicaciones (FCC), obligan a la utilización de una técnica llamada **salto de frecuencia**. **Mediante esta técnica, los dispositivos deben saltar de canal en canal en forma pseudo-aleatoria para reducir la probabilidad de transmitir en la misma frecuencia utilizada por otro dispositivo para recibir señales.**

Para evitar las colisiones, en Europa, el Instituto Europeo de Estándares de Telecomunicaciones (ETSI), encargado de regular la tecnología RFID, ordena un ciclo de tareas del 10% en la banda RFID Europea, es decir, el transmisor de un lector individual no puede estar activo más de un 10% del tiempo. Lo cual provoca problemas en las principales aplicaciones de esta tecnología. Posteriormente, el ETSI propuso técnicas de frecuencia ágil que utilizan el protocolo ‘escuchar antes de hablar’, mediante el cual un receptor debe escuchar un canal dado antes de utilizarlo para transmitir. La agilidad de frecuencias se convierte en una mejora importante comparada con el ciclo de tareas, dando como resultado un uso mucho más eficiente de la banda RFID en toda Europa.

Aunque las interferencias debidas a otros sistemas de lectores son estadísticamente improbables, las señales espurias, armónicas, de frecuencias más bajas transmitidas en una mayor potencia pueden tener un impacto de

⁵ Se produce cuando las etiquetas RFID son detectadas por dos o más lectores responsables de monitorear áreas físicas distintas. Esto provoca confusión cuando los datos deben relacionarse. Esta interferencia es causada por excesiva intensidad de la señal, una mala sintonización de las antenas de interrogación y una mala configuración del lector. Esta situación es inaceptable y el sistema debe diseñarse para eliminar este problema.

importancia que podría provocar la desensibilización del receptor y la distorsión intermodulación. Por ello, es aconsejable la realización de un análisis espectral en la localización de RFID para detectar posibles fuentes de interferencia.

La interferencia entre lectores es improbable, pero no elimina la necesidad de comprender el entorno desde la perspectiva del diseño RFID. La culpa de la mayoría de estos problemas, de interferencia del lector y de interferencia mutua, son debidos a la falta de información e inmadurez de la tecnología, ya que a través de una mayor comprensión de los principios físicos de RFID se puede realizar una instalación RFID con confianza.

Los lectores RFID ofrecen la posibilidad de ser programados con diferentes niveles de flexibilidad, también conocido como sintonizabilidad. Mejorando la sintonizabilidad de los lectores y seleccionando la infraestructura adecuada para cada aplicación es posible minimizar la interferencia mutua en los sistemas RFID, para ello se utilizarán, entre otras, las siguientes herramientas:

- La configuración del lector: La potencia de salida del lector determina la distancia a la que se podrá leer una etiqueta. La mayoría de los lectores presentan la posibilidad de ajustar esta potencia de salida, lo que permite modular el campo emitido por las antenas del lector y así evitar que interfiera con los sistemas adyacentes.
- La infraestructura física: Si se requiere una señal muy intensa y la sintonización del lector y los parámetros de configuración de la antena no pueden eliminar el ruido causado por la interferencia mutua, puede ser necesario instalar infraestructura física que aisle los sistemas de lectores adyacentes. Un método posible sería la instalación de una pantalla conductora entre ambos lectores, o si la frecuencia es UHF con un filtro de malla es suficiente para detener el campo eléctrico y aislar el sistema.
- Activación del lector: Este método es más costoso, consiste en utilizar un activador en el lector, de modo que cuando se detecte algún movimiento éste se active por un lapso de tiempo y los datos de las etiquetas son capturados. De este modo se elimina la radiación innecesaria del entorno interrumpiendo la intensidad del campo cuando ya no es necesaria.

6.6.2.1.4. Capacidad

[1] La capacidad de una etiqueta RFID se refiere a la cantidad de información que es capaz de almacenar el chip o memoria interna que ésta lleva incluido. La capacidad de las memorias aumenta de manera directa al aumento del precio de las etiquetas, es decir, normalmente a mayor capacidad de almacenamiento mayor precio de las etiquetas.

Existen etiquetas de diversa capacidad, las capacidades más utilizadas en la actualidad las podemos clasificar de la siguiente manera:

- Un bit de información: Este tipo de etiquetas son las utilizadas como medida de seguridad en las tiendas, es decir, la etiqueta RFID está a '1' cuando el producto no se ha pagado, y se pone a '0' al pasar por la línea de caja. En realidad, estas etiquetas RFID no disponen de chip interno, si no que si la etiqueta RFID esta activa representa un '1' y si se desactiva representa un '0'.

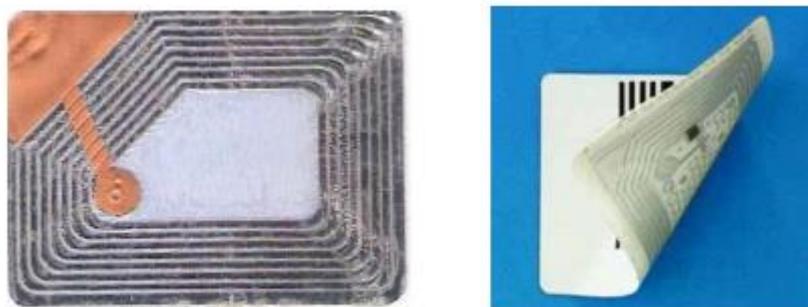


Figura 81. Etiquetas RFID sin memoria interna (izquierda), y con memoria interna (punto negro en imagen a la derecha).

- 64 bits de información: Estas memorias de 64 Bits de información fueron las descritas en la primera versión de la EPCglobal. Estas memorias que permitían albergar un código de hasta 64 bits de información, ayudaba a mantener el bajo precio de los chips inicialmente, sin embargo, el tiempo proporcionó la cantidad suficiente de EPCs como para que resultara necesario el desarrollo de una segunda versión para satisfacer las necesidades actuales.
- 96 bits de información: Las memorias que contienen 96 bits de capacidad son las desarrolladas para poder albergar el Electronic Product Code en su versión de 96 bits. Esta versión es la más extendida, y fueron elegidos los 96 bits con el deseo de asegurar que todos los objetos tengan un EPC único en una versión que mantenga el bajo coste. Estas etiquetas RFID pertenecen a la Generación 1 de la EPCglobal, la cual soportaba hasta 96 bits de información.
- 256 bits de información: Estas memorias son las albergadas en la Generación 2 de la EPCglobal y aportan un EPC de 256 bits de información, es decir, disponen de la suficiente capacidad de memoria como para albergar un código de 256 bits. Es la tercera versión del EPC existente, última versión hasta la actualidad.
- Más de 256 Bits de información: Estas memorias además de poder albergar Códigos Electrónicos de Producto de hasta 256 bits de información, según la Gen II de la EPCglobal, permiten almacenar más información relativa al producto que podría resultar de importancia, como podría ser el peso, la fecha de caducidad, o simplemente para almacenar las medidas tomadas a través de los sensores que pueden llevar las etiquetas RFID, como la presión, temperatura, humedad, etc. Este tipo de memorias, como era de esperar, son las de mayor coste actualmente en el mercado.

6.6.2.1.5. Tipos de memoria

[1] Hay que tener presente que el chip o circuito integrado de las etiquetas tiene un elevado impacto en el comportamiento de ésta.

El chip recoge la energía de radio frecuencia enviada por el lector y la convierte en alimentación eléctrica para la etiqueta, que utilizará para activar la circuitería interna del chip, almacenar la información enviada por el lector en la memoria o recuperar la información, que haya sido solicitada por el lector, de la memoria interna de la etiqueta y posteriormente modular la señal de respuesta al lector.

Los parámetros que intervienen en el consumo son:

- Capacidad de memoria del chip: La prioridad en el diseño de las etiquetas RFID es el coste. Este motivo es el responsable de que los niveles de capacidad de los chips que se integran en las etiquetas RFID sean mínimos. En éste se almacena el número serializado de identificación para guardar el resto de parámetros asociados a este producto en una base de datos potente y sobre la cual se puedan llevar a cabo medidas de seguridad. A tamaños más elevados de capacidad, se necesitan mayores consumos de potencia para poder leer y codificar la información almacenada en la etiqueta. Sin embargo, en algunas ocasiones interesa almacenar en la etiqueta más información que un simple número serializado.
- Eficiencia de su circuito: El chip recibe energía de la antena de la etiqueta en forma de corriente oscilatoria a una frecuencia determinada, que dependerá del tipo de etiqueta. Esta corriente debe ser rectificadora y convertida en consonancia a una frecuencia determinada. Éstos hacen que la precisión de los componentes del chip tenga una elevada importancia en la eficiencia en este proceso de conversión.
- Impedancia entre la antena y el chip: Si la conexión entre el chip y la antena no tiene impedancia correcta, provoca que no toda la energía que llega se aproveche, debido a un efecto de rebote o reflexión en este punto que haría que una cierta cantidad de esta energía rebotará y volviese. Estos casos los podemos encontrar en las etiquetas con procesos de fabricación muy pobres, que prima el muy bajo coste sobre el bajo coste con calidad. La mejor forma de saber estas características es consultando estudios o preguntando a vendedores especializados.

Cada fabricante realiza su propio diseño de chips, y emplea procesos de fabricación diferentes. Esto permite a

cada fabricante optimizar cada uno de estos parámetros y por esta razón existen diferencias en el comportamiento de las etiquetas, dependiendo de ésta y de su fabricante.

Las memorias se pueden clasificar atendiendo a si su memoria es de sólo lectura o además se puede escribir en ellas:

- Sólo lectura: el código de identificación que contiene es único y es personalizado durante la fabricación de la etiqueta. Cuando ésta se fabrica y sólo entonces, se escribe en su memoria un código de identificación para el producto, el cual no se puede modificar durante el tiempo de vida de la etiqueta. Éste consiste en un código serializado y único. Éstas suelen tener una capacidad de almacenamiento muy baja, ya que únicamente se necesitan unos bits para almacenar un código identificador.
- De lectura y escritura: la información de identificación puede ser modificada por el lector. La información podría ser almacenada en el proceso de fabricación del chip, pero ésta puede ser modificada con el lector, pudiendo además de almacenar más información en la etiqueta, modificarse el código de identificación almacenado. Este tipo de memorias suelen tener una capacidad de almacenamiento mayor que para las memorias de sólo lectura, ya que normalmente se utilizan para incluir más información importante sobre el producto.
- Anticolisión: se trata de etiquetas especiales que permiten que un lector identifique varias etiquetas de manera simultánea. Siendo este tipo de etiquetas muy útiles para leer de una vez todos los productos que hay almacenados en un estante en un almacén, por ejemplo.

Todas las etiquetas RFID disponen de un código de identificación del producto, denominado EPCN, siglas de Electronic Product Code Network, que identifica unívocamente a un producto. Además, si la capacidad lo permite y la memoria es de lectura/escritura, éstos pueden almacenar más información que un mero código de identificación.

6.6.2.1.6. Antena

[1] Las formas y los tamaños de las antenas son múltiples y variados:

- Etiquetas de alta frecuencia: el diseño de las antenas es menos complejo, ya que consiste en una bobina de material conductor. En este caso el tamaño y la longitud son dos factores muy importantes ya que impactan directamente con la distancia de lectura, la cual está siempre limitada por el tipo de acoplamiento.
- Etiquetas de ultra alta frecuencia: Las antenas de las etiquetas son dipolos y esto abre la posibilidad a una gran multitud de diseños, los cuales siempre van orientados a un objetivo o un equilibrio entre varios objetivos, que normalmente suelen ser el rendimiento, distancia de lectura, eficiencia en la transferencia de energía y el coste. El patrón de radiación de las antenas clásicas tipo dipolo es omnidireccional.

El diseño estándar de un dipolo consiste en dos planos simétricos de longitud $\frac{1}{4}$ de la longitud de la onda. El dipolo dual se crea para mejorar la sensibilidad de la etiqueta a la orientación. De este modo se consigue que cuando un dipolo está orientado incorrectamente, el otro está correctamente, garantizando que siempre encontremos una orientación correcta. El dipolo conocido como doblado, proporciona un mayor ancho de banda, comportándose por tanto similarmente a una banda de frecuencias mayor. En este caso la longitud de los planos es $\frac{1}{2}$ de la longitud de la onda.

Cada fabricante tiene más de diez modelos de etiquetas, cada uno de éstos con unas características apropiadas para el objetivo que pretendan cubrir.

Las antenas de las etiquetas RFID tienen el diseño basado en varios factores, los cuales determinan su forma y tamaño, según el objetivo de la aplicación. De ahí que existan antenas con forma rectangular, cuadrada, redonda...etc.

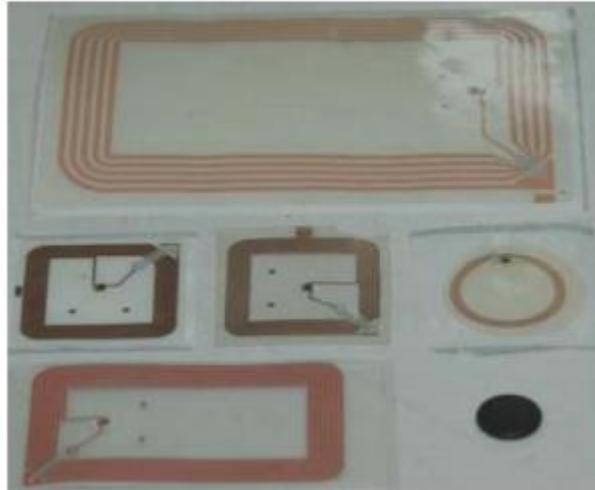


Figura 82. Forma de las antenas RFID.

Los factores más importantes relacionados con el diseño son los que se enumeran a continuación:

1. Distancia de lectura
2. Sensibilidad a la orientación (Ángulo de apertura).
3. Densidad de la potencia radiada.
4. Ganancia, en relación al haz patrón.
5. Características del entorno (metal, líquido, madera...).
6. Polarización de la onda emitida.
7. Especificaciones concretas del objeto a etiquetar.

6.6.2.1.7. Electronic Product Code

[1] Hoy en día los códigos de barras se han integrado de tal forma que ya que la mayoría de productos son identificados mediante ellos. Éstos están constituidos por un código universal de producto, conocido como UPC (Universal Product Code).

Se trata de una forma diferente de codificar números y letras usando una combinación de barras y espacios en diferentes medidas. El código UPC representa la clave para acceder a un registro de alguna base de datos en donde realmente reside la información, es decir, los símbolos no contienen información sobre el objeto, el precio... sino la clave para acceder a esa información. En cambio, **con la tecnología RFID se puede almacenar algún tipo de información además de la clave dependiendo de la capacidad de la etiqueta RFID.**

El UPC sirve para identificar 10.000.000.000 productos diferentes. El UPC se compone de 12 números que identifican el código de la empresa, el código del producto y un dígito de control.



Figura 83. UPC.

- El primer dígito se corresponde con un 1 o un 7, es el llamado número del sistema. El 1 o 7 indica que el producto tiene un tamaño y peso determinado y no un peso variable.
- Los cinco dígitos siguientes (18908) se corresponde con el código de la empresa, esta clave de cinco dígitos es única para cada fabricante y la asigna un organismo rector para evitar códigos duplicados.
- Los cinco dígitos siguientes (14447) se corresponde con el código del producto que el fabricante asigna a cada uno de sus productos.
- Y el último dígito (3) se trata del dígito de control. Para calcular el dígito de control se multiplica cada número por 1 o por 3 dependiendo de su posición. Si se trata de una posición par se multiplica por 1, y si se trata de una posición impar por 3, posteriormente se suman los resultados de las multiplicaciones y se le restan al valor de la decena superior.

El UPC es la simbología más utilizada en el comercio de Estados Unidos, sin embargo, la versión propia del UPC en Europa es el EAN (European Article Number). Es un estándar internacional de aceptación mundial. Identifica a los productos indicando el país, la empresa, y el código del producto con una clave única internacional. El EAN-13 es la versión más extendida del sistema EAN y consta de un código de 13 cifras en las que sus tres primeros dígitos identifican el país, los seis siguientes la empresa productora, los tres números posteriores al artículo y finalmente un dígito verificador, que da seguridad al sistema.

En RFID, sin embargo, los datos incluidos en la etiqueta pueden estar en muchos formatos, siempre y cuando el lector y la etiqueta estén de acuerdo en ello. Los formatos principalmente dependen del fabricante, pero los estándares ya están surgiendo.

El EPC (Electronic Product Code) ha sido denominado ‘la próxima generación de códigos de barras’ y por ello se considera el relevo del UPC. En el libro blanco ‘**The Networked Physical World, Proposal for Engineering the Next Generation of Computing, Commerce and Automatic Identification**’, desarrollado en 2001 por Sanjay Sarma, David Brock y Kevin Ashton se propone por primera vez un sistema de código electrónico de producto. Éste consiste en un esquema de codificación que fue desarrollado por el Auto-ID Labs, sucesora de Auto-ID Center, que permite identificar todos los artículos de una manera única e inequívoca en la cadena de suministro, a diferencia del UPC que sólo identifica clases de objetos o categorías genéricas de productos. En lugar de estar impreso sobre papel como ocurre hoy con el sistema de código de barras, este número se inserta dentro de una etiqueta electrónica que puede ser detectada mediante ondas de radio. Esta serie de bits sirven para identificar la empresa fabricante, categoría del producto, y el número del producto.

El objetivo de este sistema EPC es volver la cadena de valor cada vez más eficiente e incrementar la visibilidad de los objetos que se mueven por ella, todo esto se puede lograr a través de la Red de EPC, la cual está conformada por las etiquetas, el hardware, el software y EPCIS. EPCIS o Servicios de Información de EPC consiste en un servicio de información de EPC que permite intercambiar información vía Internet con los socios comerciales acerca del movimiento de los productos, garantizando así la visibilidad de los mismos y facilitando por ello la toma de decisiones que impacten en la eficacia hacia los clientes y consumidores.

El EPC es usado por la EPCglobal como el formato de identificación general (GID-96). El EPC nació como respuesta a los sectores profesionales para facilitarles la identificación de objetos, sin embargo, este código electrónico debía contemplar un requisito, debía ser aplicable a nivel global, algo que solo podría conseguirse si la tecnología seguía un estándar mundial. Es por ello por lo que se creó el organismo EPCglobal, constituido por el EAN y el Uniform Code Council o GS-1, para comercializar la tecnología EPC, la cual fue originalmente desarrollada por Auto-ID.



Figura 84. EPC.

Debajo del estándar GID-96, todos los EPC están divididos en partes:

- 8 bits, consiste en un campo de cabecera usado para garantizar la singularidad de un código EPC.
- 28 bits General Manager Number, este número identifica la compañía o la organización.
- 24 bits Object Class, consiste en la clase del producto, es decir, clasifica a los productos en grupos.
- 36 bits Serial Number, el número de serie es único para cada objeto individual.

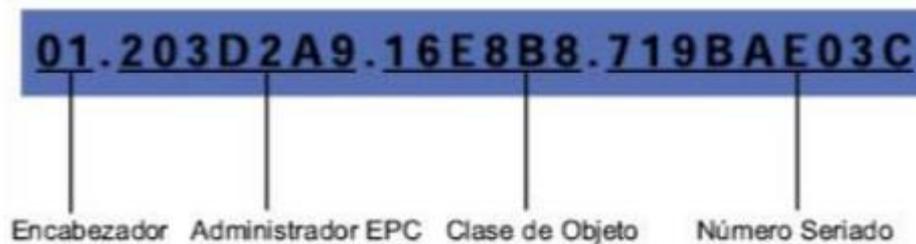


Figura 85. Campos del estándar GID-96.

La integración de un UPC en un EPC se realiza de una manera muy sencilla:

- El número de la compañía del UPC pasaría de igual manera a formar parte del número de la compañía del EPC.
- El código del producto del UPC, pasaría a formar parte de la clase del producto del EPC.
- El número de serie del EPC sería el correspondiente al objeto concreto que se quiera identificar.

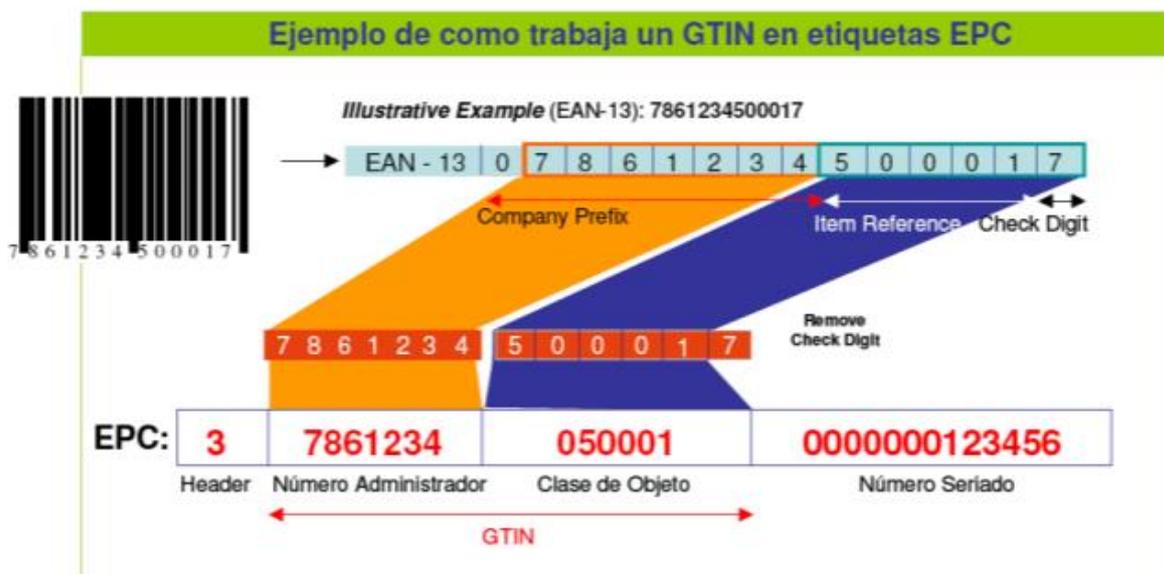


Figura 86. Integración de un UPC en un EPC.

El EPC de cada producto concreto es almacenado en un servidor de nombres que funciona a través de Internet denominado ONS (Object Name Service) desarrollado por el EPCglobal.

A este servidor ONS pueden acceder las empresas autorizadas a buscar información sobre un producto concreto. El sistema envía el código EPC a través de Internet a una base de datos Object Name Service, ONS, que funciona igual que los DNS de Internet, pero en lugar de identificar una dirección, identifica un producto, es decir, en vez

de realizar una traducción de nombre de dominio en una dirección IP o viceversa, realiza una traducción de un código EPC en un producto u objeto en concreto y viceversa. El servidor ONS iguala el número EPC a la dirección del servidor donde está guardada la información del producto.

El sistema EPC lo forman el Código electrónico del producto (EPC), las etiquetas, los lectores... Todo este sistema forma el denominado IoT, en el cual gracias a los EPC los objetos son identificados como objetos únicos e inequívocos.



Figura 87. La pila EPC.

El Servidor ONS utiliza el lenguaje PML (Physical Markup Language) también conocido como Product Markup Language (Lenguaje de marcado físico) o (Lenguaje de marcado de productos) respectivamente. El sistema ONS conecta el EPC con su archivo asociado en PML de forma automática, de manera que al introducir un determinado EPC, este servicio remite el archivo PML.

El lenguaje PML es el utilizado para describir objetos físicos, el cual está basado en el lenguaje XML, e incluye esquemas que permiten la definición de todas las características de un producto u objeto. Este lenguaje consiste en un lenguaje estándar para representar y distribuir información sobre los objetos, permitiendo la estandarización de la interfaz entre la infraestructura RFID y otros sistemas de información. El lenguaje PML no pretende sustituir a los actuales lenguajes utilizados para las transacciones comerciales o cualquier otra aplicación XML, sino que resulta ser un complemento a estos para definir la red EPC. La formación de este lenguaje, así como las correspondientes herramientas software, ha sido uno de los aspectos más difíciles de la Internet of Things.

El proceso se inicia con la lectura de una etiqueta RFID, mediante la aplicación de un campo magnético, del EPC incluido en el chip de la etiqueta. El lector obtiene el EPC y se lo comunica al middleware o subsistema gestor. El cual, una vez recibida la información, busca en la base de datos del servidor local el archivo PML asociado a ese código de producto. En el caso de encontrar el producto, el proceso termina. Si no es así, el middleware remite el EPC al servidor ONS, el cual emitirá una petición de localización de dicho PML. Una vez recibida la petición, la respuesta se da en forma de dirección IP. Cuando el middleware obtiene la dirección IP de respuesta, éste conecta con el servidor PML que le facilitará el archivo PML correspondiente, paso con el cual el proceso finaliza.

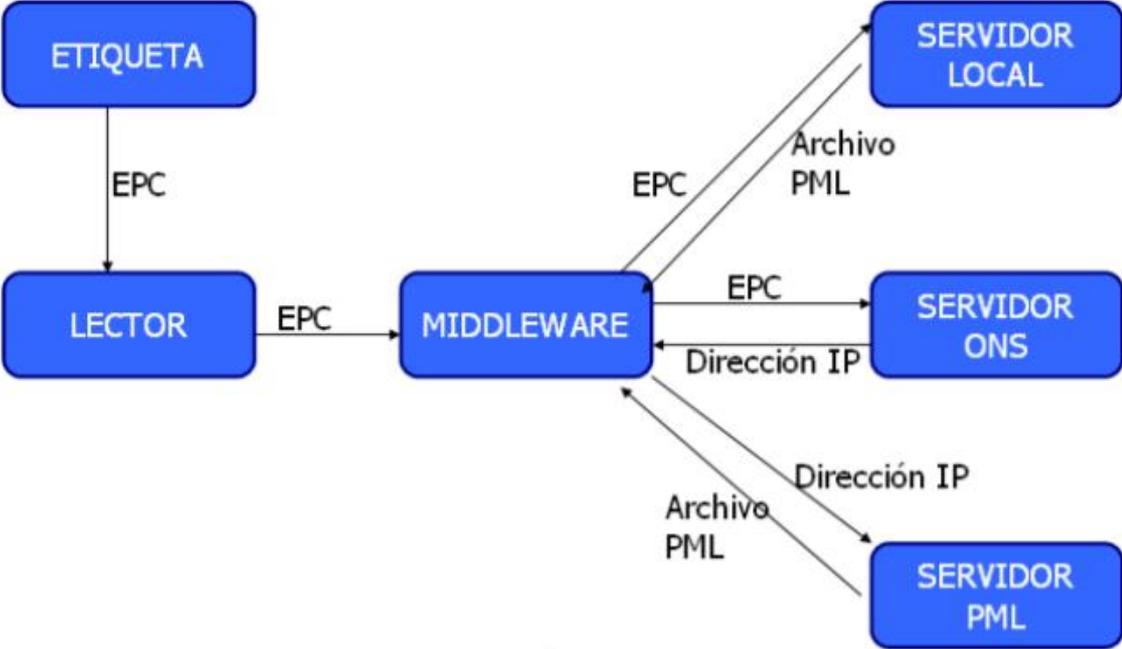


Figura 88. Estructura de la tecnología RFID.

6.6.2.2. Lector de RFID o Transceptor⁶

6.6.2.2.1. Descripción

[1] Se compone de una antena, un transceptor y un decodificador. El lector envía señales al entorno, cuando éste capta una señal de una etiqueta, extrae la información y se la pasa al subsistema de procesamiento de datos. Estas señales podrían transmitir energía en el caso de que se trate de leer una etiqueta pasiva.

Algunos lectores llevan además integrado un módulo programador que les permite escribir información en las etiquetas, si éstas permiten la escritura.

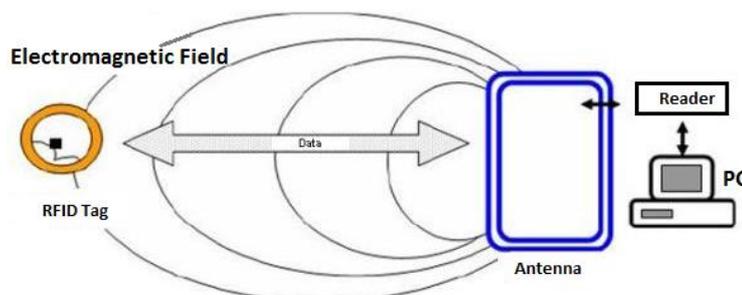


Figura 89. Antena RFID interactuando con un Tag.

Los lectores pueden operar manualmente o de forma automática. Lo normal es que operen de manera automática, para lo cual utilizan algoritmos de anticollisión para poder leer múltiples etiquetas, y de manera simultánea, existentes en el campo de lectura.

Las operaciones básicas que puede llevar a cabo un lector RFID:

- **Lectura Fija de etiquetas:** Un lector puede configurarse para que realice de manera constante lecturas fijas. A medida que las etiquetas responden a las emisiones del lector estas lecturas son incluidas en una lista de etiquetas en la memoria del lector. Sin alguna de éstas no responde, será eliminada de la lista acumulada en la memoria.
- **Modo Directo/Interactivo:** Este tipo de lectores responde a comandos proporcionados por las aplicaciones de gestión almacenadas en servidores. El servidor puede indicar al lector que reúna una lista de etiquetas dentro del rango de lectura o que busque una etiqueta específica dentro del rango. “En ambos casos el lector comienza por recoger una lista. Una vez completado el comando instruido por el servidor, el lector espera hasta recibir el siguiente comando.” (RFID Magazine, 2001).

[9] En un sistema RFID pasivo, el transmisor del lector permanece emitiendo una portadora continua durante el tiempo que el receptor del lector está escuchando la señal del tag. Los lectores RFID usan componentes específicos como circuladores⁷ o acopladores para permitir que solo las señales reflejadas lleguen al receptor, que de otra forma podría estar saturado por la enorme señal transmitida. Sin embargo, en un sistema de una única antena, la señal transmitida desde el lector rebota en su propia antena hacia el receptor, y la onda transmitida desde la antena rebota en cualquier objeto cercano, incluyendo la antena de la etiqueta que se está tratando de encontrar.

⁶ Un transceptor es un dispositivo que cuenta con un transmisor y un receptor que comparten parte de la circuitería o se encuentran dentro de la misma caja. En este caso, el transceptor RFID hace referencia al circuito integrado que gestiona el envío y recepción de señales.

⁷ [34] Se llama circulador a un dispositivo de microondas con tres puertas, numeradas 1, 2 y 3. Toda la energía que incide por la puerta 1 se transmite a la puerta 2; la incidente por la puerta 2 pasa a la 3 y la incidente por la puerta 3, sale por la 1. La transmisión en sentido inverso no se produce.

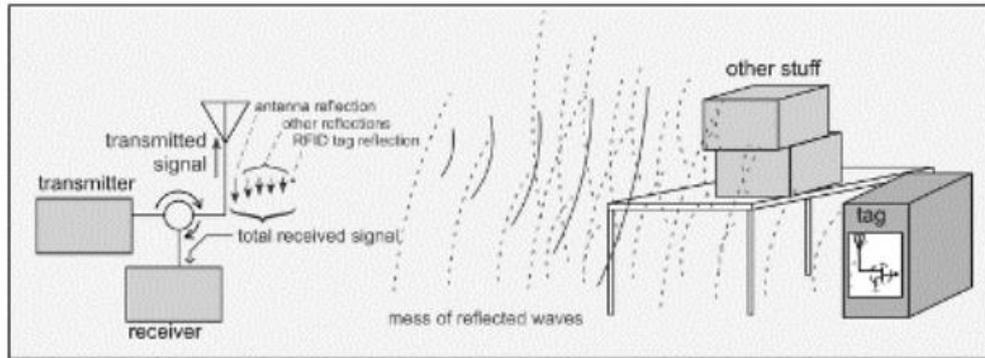


Figura 90. Transmisión y recepción de señales del lector RFID.

En el caso de emplearse dos antenas (una para transmitir y otra para recibir), hay parte de la potencia de la señal que se acopla directamente de una a otra, de igual forma que las antes mencionadas reflexiones con el entorno. La señal total en el receptor es el vector suma de todas estas contribuciones, de las cuales la mayoría son mucho más grandes que la señal deseada, con amplitudes y fases propias, la mayoría impredecibles *a priori*. Por tanto, el efecto de una variación en la carga de la antena del tag (siendo la carga, en este caso, la modulación ejercida por el transistor en el circuito de la etiqueta) es completamente impredecible e incontrolable en la señal del receptor.

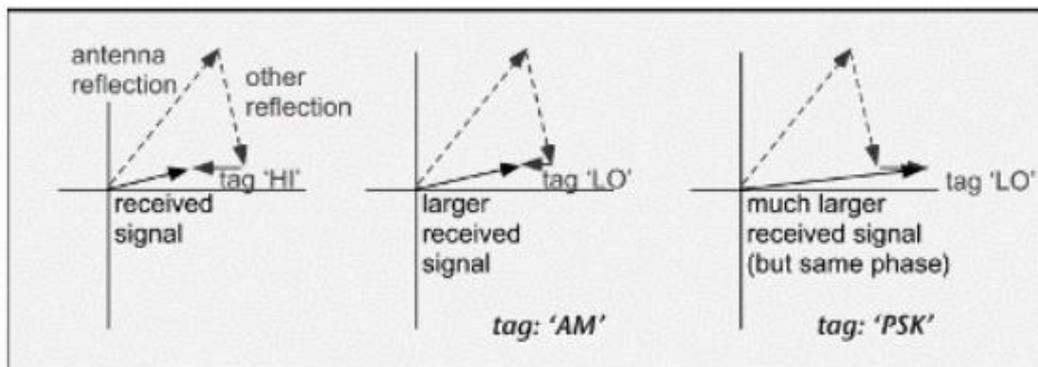


Figura 91. La señal recibida no está correlada con la señal de la etiqueta.

En la figura anterior, se muestra el caso donde las variaciones en la amplitud (HI cuando llega con amplitud grande, y LO cuando llega con amplitud pequeña) de la señal procedente del tag originan que la señal recibida incremente su magnitud sin variar su fase (Figura 38, caso AM). Las variaciones en la fase de la señal de la etiqueta sin variar el tamaño de la señal reflejada pueden alterar la amplitud de la señal del lector (Figura 38, caso PSK).

Lo único que puede afirmarse con seguridad es que una variación en el estado de la antena del tag origina una variación en la fase o amplitud de la señal que llega al receptor del lector.

[10] Volviendo al caso de única antena en un sistema pasivo, la señal que el lector envía al entorno tiene tres funciones fundamentales:

- Aportar la suficiente energía a la etiqueta para su funcionamiento.
- Establecer una señal de reloj sincronizada en la etiqueta.
- Servir de portadora para la señal de información de respuesta de la etiqueta.

El lector RFID lanza lecturas al entorno mediante modulaciones ASK (DSB-ASK, SSB-ASK y PR-ASK), y codifica sus comandos con PIE.

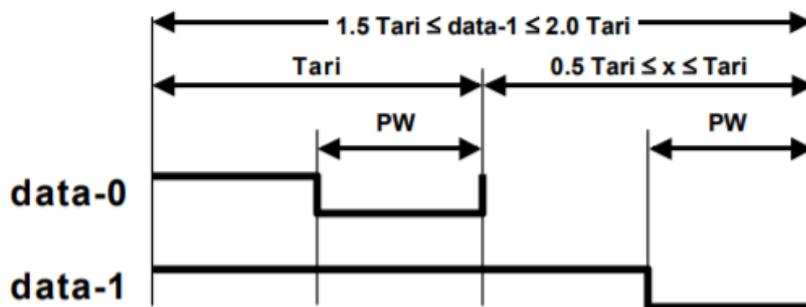
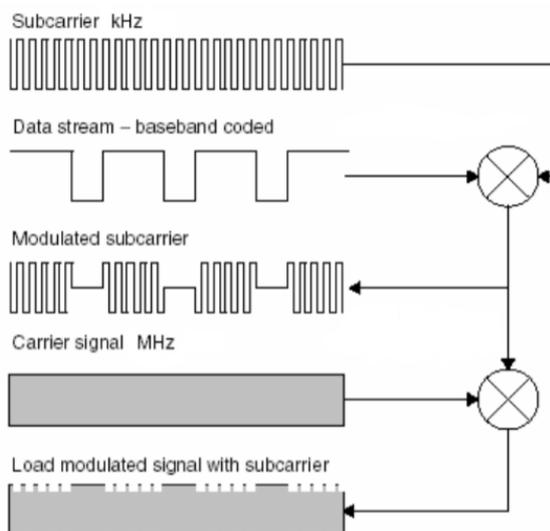


Figura 92. Codificación PIE. Se define $Tari$ como el intervalo de tiempo de referencia para la señalización entre lector y tag, y es la duración de $data-0$, comprendida entre $6.25 \mu\text{seg}$ y $25 \mu\text{seg}$.

En función del parámetro $Tari$ (Type A Reference Interval) se obtendrán unas tasas de datos diferentes:

- $Tari = 25 \mu\text{seg}$
 - 40 kbps de máxima
 - 27 kbps de media
- $Tari = 12.5 \mu\text{seg}$
 - 80 kbps de máxima
 - 53 kbps de media
- $Tari = 6.25 \mu\text{seg}$
 - 160 kbps de máxima
 - 107 kbps de media

La antena de la etiqueta recibe la señal del lector, y se realiza el backscattering. La señal que devuelve está modulada en PSK o ASK, aunque también emplea variaciones de la FSK. Particularmente, modulaciones de subportadora. Se denomina así porque la etiqueta genera en su circuitería una portadora propia modulada con la señal de información (la cual denominaremos subportadora modulada). Esta subportadora modulada, modula por backscattering la portadora que envía el lector, obteniéndose la señal de respuesta.



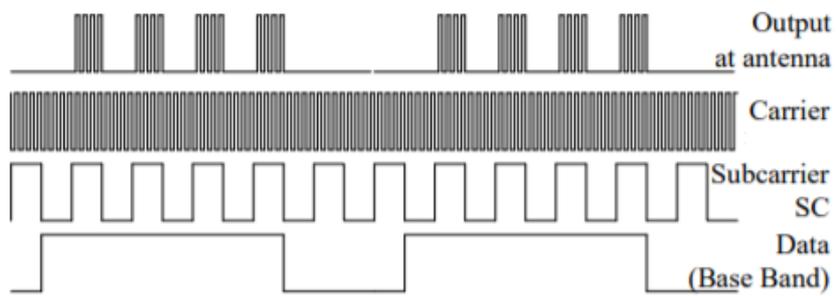


Figura 93. Ejemplos de modulación de subportadora.

[11] Las codificaciones que más emplea la etiqueta es la FM0 o la Miller. Ambas se parecen, con la diferencia de que la FM0 invierte la fase de cada símbolo⁸ y la Miller invierte la fase entre 0's. La Miller admite más símbolos ($M=2, 4, 8$).

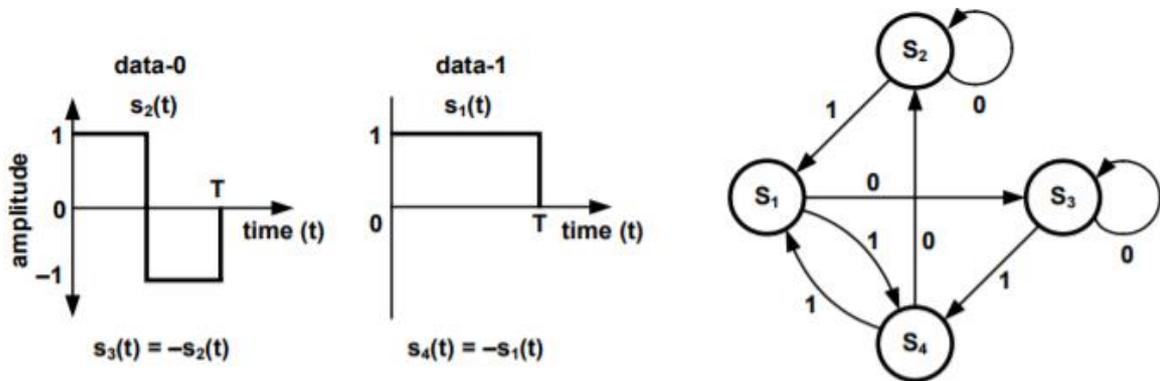
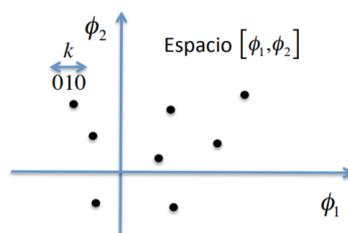


Figura 94. Símbolos FM0 y máquina de estado finito.

8

Símbolo: un grupo de k bits, donde $k = \log_2 M$ y M es el numero de símbolos.



Ejemplo de constelación
 $M = 8$
 $k = \log_2 M = 3$
 (cada punto => un símbolo)

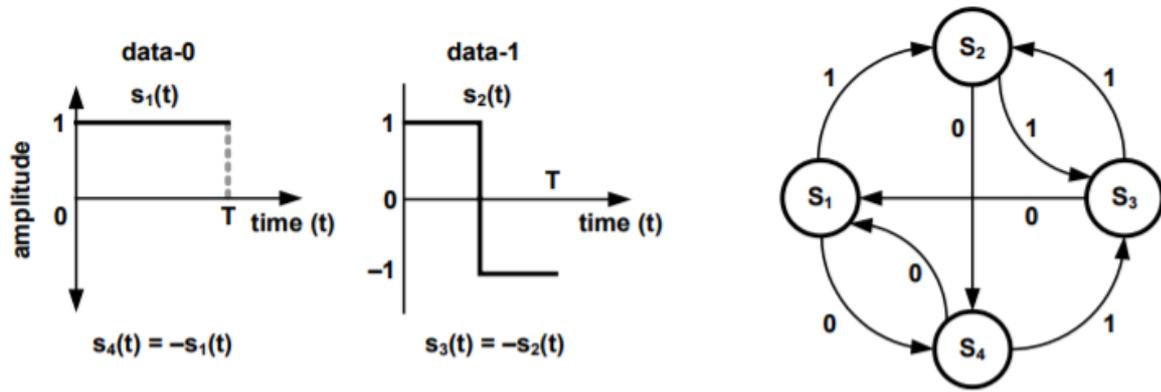


Figura 95. Símbolos Miller y máquina de estado finito.

En función de codificación que emplee la etiqueta se obtendrán unas tasas de datos:

- FM0: entre 40 y 640 kbps
- Miller (M=2): entre 20 y 320 kbps
- Miller (M=4): entre 10 y 160 kbps
- Miller (M=8): entre 5 y 80 kbps

Los valores típicos obtenidos de forma experimental oscilan entre 60 y 70 kbps usando Miller con M=4.

No solo se emplean FM0 y Miller, existen más tipos de codificaciones en la etiqueta.

SIGNAL	WAVEFORM	DESCRIPTION
Data	1 0 1 1 0 0 0 1 1 0 1 0	Digital Data
Bit Rate CLK		Clock Signal
NRZ L (Direct)		Non-Return to Zero - Level '1' is represented by logic high level. '0' is represented by logic low level.
Biphase L (Manchester)		Biphase - Level (Split Phase) A level change occurs at middle of every bit clock period. '1' is represented by a high to low level change at midclock. '0' is represented by a low to high level change at midclock.
Differential Biphase S		Differential Biphase - Space A level change occurs at middle of every bit clock period. '1' is represented by a change in level at start of clock. '0' is represented by no change in level at start of clock.

Figura 96. Otros tipos de codificación RFID.

Existen una serie de consideraciones que ayudan a elegir cual es el lector más apropiado para cada aplicación.

Estas consideraciones se enumeran a continuación:

- Frecuencia operativa: La frecuencia de operación ha de encajar con los requerimientos de las etiquetas que se desean leer.
- Multi-protocolo: Una característica deseable de los lectores es que éstos permitan la lectura de etiquetas RFID bajo distintos protocolos. Ya que las diferentes etiquetas RFID podrían tener protocolos distintos.
- Codificación: si se desea utilizar el lector para escribir información en una etiqueta de lectura/escritura será necesaria la capacidad de configuración y codificación del comando.
- Adaptación a la normativa local: la potencia de salida es diferente en Estados Unidos y en Europa, de igual modo que las frecuencias.
- Memoria: Para la gestión de las listas de etiquetas almacenadas en el lector, a mayor memoria mayor será la cantidad posible de etiquetas que se almacenan en la lista del lector.
- Capacidad de red: capacidad para interconectar lectores entre sí.
- Potencia: La potencia de operación de los lectores.
- Configurable y actualizable: Capaz de incluir las nuevas versiones para no quedar obsoleto.
- Antena: se adapta a varias condiciones utilizando un auto sintonizador dinámico. Puede aceptar múltiples antenas para varias aplicaciones.
- Interfaces de control: Input/output digital y circuitos de control para sincronización con otros componentes en una línea automatizada.
- Actualizaciones: A medida que los estándares y la tecnología evolucionan, los lectores necesitarán un firmware actualizable para no tener que realizar continuamente compras de nuevos equipos.
- Radio de lectura: El lector, especialmente las antenas del lector, al igual que las etiquetas tiene un elevado impacto en el comportamiento de la solución RFID, ya que va a permitir un mayor o menor radio de lectura. De esta forma, será necesario escoger un lector apropiado para cada tipo de aplicación, dependiendo de la distancia a la que se encuentren el lector y las etiquetas.
- Firmware: El firmware del lector puede determinar también el comportamiento. Dos lectores pueden cumplir los mismos estándares y sin embargo no tener el mismo comportamiento, ya que éstos podrían hacer lo mismo de diferentes maneras.



Figura 97. Lector RFID.

Para cada aplicación se ha tener en cuenta el rendimiento que se requiere, así como el número y tipos de conectores que necesitamos para el correcto funcionamiento. Analizando todas las variantes se podrá elegir para cada caso concreto el mejor lector con el objetivo de encontrar la solución idónea en funcionamiento y coste.

6.6.2.3. Subsistema de procesamiento de datos o Middleware

Proporciona los medios de proceso y almacenamiento de datos. Se trata del software que reside en un servidor entre el lector y las aplicaciones empresariales. Filtra datos y permite pasar sólo la información útil hacia dichas aplicaciones. Algunos también pueden gestionar la red de lectores.

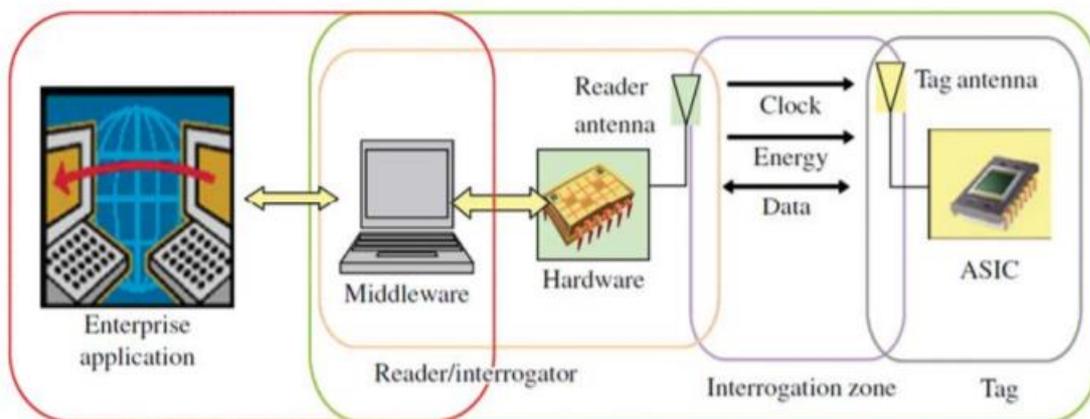


Figura 98. Arquitectura típica de un sistema RFID genérico.

[1] “En el mundo de la tecnología RFID muchas veces el middleware es el gran desconocido porque constantemente se habla de lectores y de etiquetas RFID, pero no hay que olvidar que la gestión de la información captada por dichos elementos es igual o incluso más importante”. (RFID Magazine, 2001).

El middleware consiste en un subsistema de gestión que reside entre la infraestructura de la tecnología RFID y las aplicaciones empresariales, de manera que sus funciones abarcan muchos aspectos, entre las cuales cabe destacar la gestión de los lectores, el filtrado de los datos y el control de la infraestructura.

La mayoría de las empresas realizan ensayos con lectores y tipos de etiquetas RFID para seleccionar cuales son los mejores para optimizar la lectura o el mejor emplazamiento de las etiquetas en sus productos. Sin embargo, éstas dedican muy poco tiempo a analizar el sistema que permitirá la codificación de las etiquetas, la recolección de información que los lectores envían, y la gestión de toda la infraestructura física, lectores y etiquetas, del sistema. **Se debe tener en cuenta que la capa física de esta tecnología no aporta un valor real si no se sabe cómo actuar con la información recogida del sistema RFID.**

Las funciones básicas del middleware son la gestión a nivel de control y configuración toda la red de hardware de lectores y etiquetas, recolectar y filtrar datos de las lecturas, y traspasar éstos de manera eficiente a los sistemas de gestión.

El middleware no es necesario en todos los proyectos, sino que éste sólo es importante dentro de los marcos de trabajo en los que se deba interactuar entre el mundo físico que forma la infraestructura RFID y el mundo lógico de la información.

En la arquitectura del middleware se pueden diferenciar dos grandes bloques, el primer bloque denominado Edge Server consiste en la infraestructura que está situada a nivel local. A este bloque se conectan los dispositivos RFID. El segundo bloque, designado Enterprise Server se situará donde la entidad centraliza sus aplicaciones, en el centro de datos. Los múltiples Edge Servers existentes se conectarán al Enterprise Server, quién será el encargado de trasladar la información a las aplicaciones empresariales a través de un bus o de una conexión directa.

El funcionamiento del middleware consiste en el siguiente, el lector lee la etiqueta RFID, y dicha información la envía al Edge Server, éste verifica y filtra los datos, por si esta lectura fuera una lectura fantasma o una lectura duplicada. En el caso de que todo sea correcto, éste genera un evento que se traspasa al Enterprise Server quien registrará los datos en una base de datos. Si por este dato se tuviera que generar alguna acción con otra aplicación,

el Enterprise Server será el encargado de comunicar y transferir la información necesaria para la realización del proceso. Cuando una aplicación empresarial realiza una petición de información, el Enterprise Server es el encargado de responder con los datos correctos a ésta.

6.7. Anexo G. Estándares y regularizaciones RFID

[12] Existe una gran variedad de organizaciones que han determinado estándares para RFID según intereses, aplicaciones y la determinación de la globalización. Entre las más destacadas encontramos la ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), ASTM (American Society for Testing and Materials), o EPC Global (Asociación entre EAN International y GS1 Uniform Code Council).

También existen algunos sectores industriales que han establecido guías, bien por su inexistencia o bien para su mejor adaptación a sus realidades particulares. Algunos ejemplos de estas industrias los encontraríamos en la FSTC (Financial Services Technology Consortium), CompTIA (Computer Technology Industry Association), la IATA (International Air Transport Association), EMV Contactless (Europay, Mastercard y Visa), organizaciones gubernamentales, etc.

Así pues, los estándares y regulaciones establecidos para la RFID hasta la fecha son:

1. **ISO 14223:** Estándar que especifica la estructura del código de radiofrecuencia (RF) para transponders usados en animales. Esta norma es una extensión de los otros estándares ISO 11784 y ISO 11785.
2. **ISO 14443:** Estándar relacionado con las tarjetas de identificación electrónicas, en especial tarjetas de proximidad. El sistema RFID utiliza un lector con microcontrolador incrustado y una antena que opera a una frecuencia de 13,56 MHz. El lector genera a su alrededor un campo electromagnético de modo que, al acercarse una tarjeta al campo, ésta se alimenta eléctricamente de esta energía inducida y puede establecerse la comunicación lector-tarjeta.

El estándar ISO 14443 consta de cuatro partes:

- **ISO 14443-1:2008 Part 1:** Especifica las características físicas.
- **ISO 14443-2:2010 Part 2:** Especifica la potencia RF y el interfaz de señal.
- **ISO 14443-3:2011 Part 3:** Especifica las funciones de inicialización y anticolidión entre chips.
- **ISO 14443-4:2008 Part 4:** Especifica el protocolo de transmisión.

Se describen dos tipos de tarjetas; tipo A y tipo B, cuya principal diferencia (ambos se comunican vía radio a 13,56 MHz) se refiere al método de modulación, esquemas de código y procedimientos del protocolo de inicialización. Sin embargo, ambos tipos utilizan el mismo protocolo de transmisión descrito en la parte 4 (bloque de datos, tiempo de respuesta y multi-activación).

La tarjeta Calypso, del Consorcio de Transportes Europeo, cumple con la norma ISO/IEC 14443 parte 1, 2, 3 y 4 de tipo B.

Las tarjetas Mifare, de NXP, cumplen con las partes 1, 2 y 3 de tipo A de la especificación ISO/IEC 14443.

La tarjeta inteligente FeliCa, de Sony, se basa en los estándares de NFC-F.

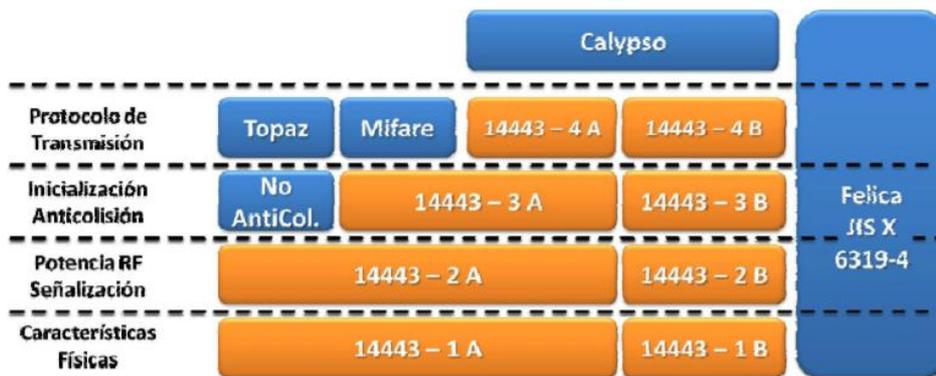


Figura 99. ISO/IEC 14443.

3. **ISO 15692:** Protocolo de los datos usados en el intercambio de información en los sistemas RFID para la gestión de ítems, operando con el proceso de datos y la presentación en el tag RFID, así como el procesamiento inicial de los datos capturados desde transponder.
4. **ISO 15693:** Estándar basado también en la frecuencia de 13,56 MHz (HF) y es conocido como el estándar para las tarjetas de vecindad (vicinity cards). La diferencia principal es la distancia de lectura/escritura que este estándar regula llegando a alcanzar 1,5 metros de distancia. Una de las claves de esta mayor distancia respecto a las tarjetas de proximidad (ISO 14443) es el necesario campo magnético que requieren para su activación, siendo de 0,15 a 5 mA (1,5 a 7,5 mA para las ISO 14443).
5. **ISO 180000:** Estándar que describe las diferentes tecnologías y/o frecuencias para la gestión a nivel de ítem. Las diferentes partes de este estándar describen el interfaz de comunicación vía aire de estas distintas frecuencias para establecer los distintos comportamientos físicos. Las distintas partes son:
 - Parte 1: referencia a la arquitectura y definición de los parámetros a estandarizar.
 - Parte 2: parámetros establecidos para la interfaz de comunicación vía aire bajo los 135 KHz.
 - Parte 3: parámetros establecidos para la interfaz de comunicación vía aire bajo los 13,56 MHz.
 - Parte 4: parámetros establecidos para la interfaz de comunicación vía aire bajo los 2,45 GHz.
 - Parte 6: parámetros establecidos para la interfaz de comunicación vía aire entre 860 MHz y 960 MHz.
 - Parte 7: parámetros establecidos para la interfaz de comunicación activo vía aire bajo los 433 MHz.
6. **ISO 18092:** Estándar que describe el intercambio de información sin contacto entre sistemas, conocido también como NFC (Near Field Communication - interfaz y protocolo NFCIP-1), usando dispositivos de acoplamiento inductivo operando a la frecuencia de 13,56 MHz. [13] También define

los **modos de comunicación activo y pasivo**⁹ de la interfaz y el protocolo de comunicación de campo cercano (NFCIP-1). Esta norma específica, en particular, esquemas de modulación, codificaciones, velocidades de transferencia y formato de trama de la interfaz RF, así como esquemas de inicialización y condiciones requeridas para el control de colisión de datos durante la inicialización. Además, esta norma define un protocolo de transporte que incluye la activación del protocolo y los métodos de intercambio de datos.

Esta norma también se conoce como la ECMA-340, exactamente con su 3ª edición de junio de 2013. La ECMA-356 “NFCIP-1 – RF Interface Test Methods” y ECMA-362 “NFCIP-1 – Protocol Test Methods” especifican test para ECMA-340.

La ECMA-373 especifica la interfaz de dos hilos entre un transceptor y un “front-end”¹⁰.

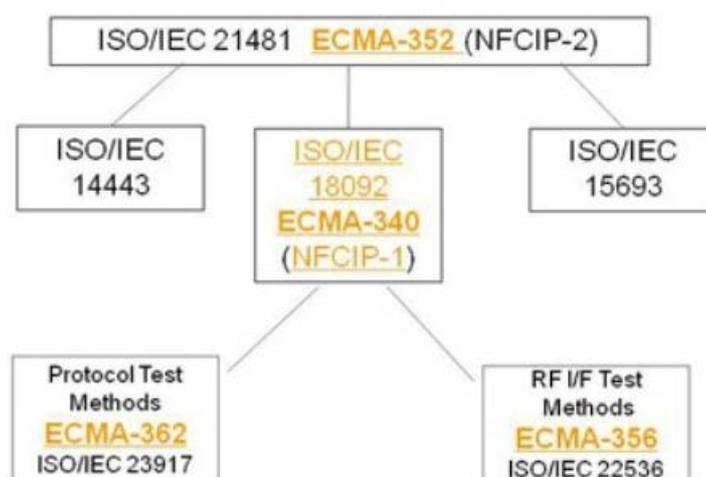


Figura 100. Convenio de protocolo NFC.

Diferencia entre ISO 14443 – ISO 18092

[14] ISO/IEC 18092 (NFCIP-1) está basado en ISO/IEC 14443 pero tiene una diferencia crítica. Utiliza un protocolo de comando distinto para reemplazar la Parte 4 del ISO/IEC 14443. Incluye, además, dos modos de comunicación; activo y pasivo,¹¹ lo que permite a un dispositivo NFC comunicarse con otros equipos NFC en un modo “peer-to-peer”, así como con ISO/IEC 18092 basado en etiquetas NFC.

Dentro de los modos activo y pasivo, existen tres modos de operación definidos en ISO/IEC 18092:

- **Lectura/Escritura:** En este modo el teléfono NFC puede leer o escribir datos de cualquier etiqueta compatible con el formato de datos NFC.
- **Peer-to-Peer:** Dos dispositivos habilitados para NFC pueden intercambiar datos a través de algún tipo de protocolo binario personalizado.
- **Card-Emulation:** Mientras que los teléfonos NFC pueden actuar como lectores cuando interactúan con otros tags, en este modo el teléfono también puede actuar como una etiqueta para otros lectores (terminales POS¹²).

⁹ Descritos en el apartado 2.2. RFID y NFC.

¹⁰ Parte de una web que conecta e interactúa con los usuarios que la visitan.

¹¹ Descritos en el apartado 2.2. RFID y NFC.

¹² Point of Sale, en castellano Terminal Punto de Venta (TPV).

Específicamente, el Foro NFC establece que en el modo de emulación de tarjeta (Card-Emulation), los teléfonos habilitados para NFC pueden admitir los requisitos de la aplicación de pago EMV de tarjeta sin contacto especificados en EMV CCPS v2.0 e incorporados por American Express ExpressPay 2.0, MasterCard PayPass 2.0 y Visa payWave 2.1.1.

Por lo tanto, si el dispositivo NFC funciona con las especificaciones de ISO/IEC 18092 en modo de emulación de tarjeta, debe ser interoperable con un lector/grabador (terminal POS) que funcione con las especificaciones de ISO/IEC 14443.

Sin embargo, ISO/IEC 18092 también define un modo de igual a igual (Peer-to-Peer) en el que dos dispositivos pueden intercambiar datos (es decir, una tarjeta que actúa como lector). No existe tal equivalente actual definido en ISO/IEC 14443 y, por lo tanto, estos dispositivos NFC no serían interoperables con los dispositivos que operan bajo ISO/IEC 14443.

Por lo tanto, si planea operar en modo Peer-to-Peer, por ejemplo, implementando su propio protocolo de intercambio de datos binarios a través de NFC, es posible que deba usar un dispositivo/conjunto de chips compatible con ISO 18092.

7. **ISO 18185:** Estándar que define el protocolo de comunicación de los sellos electrónicos para los contenedores de transporte de mercancías (sistema de identificación del estado del sello, indicador de batería del sello, identificador único del sello incluyendo el ID del fabricante y tipo de sello).
8. **ISO 21481:** Sistemas de intercambio de información y telecomunicaciones entre sistemas, Near Field Communications interface y protocolo - 2 (NFCIP-2).
9. **ISO 28560-2:** Especifica el estándar de grabación y el patrón de datos para las aplicaciones RFID en bibliotecas. Está basado en el estándar ISO 15962.
10. **ASTM D7434:** Estandariza los métodos de test para determinar el rendimiento de los transponders pasivos de radiofrecuencia RFID en cargas paletizadas o unificadas.
11. **ASTM D7435:** Estandariza los métodos de test para determinar el rendimiento de los transponders pasivos de radiofrecuencia RFID en contenedores cargados.
12. **EPC UHF class1 Gen2:** Estandariza los chips RFID pasivos su EPC (Electronic Product Code) en la identificación de los ítems en la cadena de suministro a nivel mundial. Se detallará más adelante al final de esta sección.
13. **EMV Contactless:** Especificaciones para los sistemas de pago que define la arquitectura y requisitos generales, puntos de partida, especificaciones del kernel y el protocolo de comunicaciones contactless. Se basa en la ISO 7816 y la ISO 14443
Para finalizar, cabe señalar las regulaciones que cada país o región establece, así en nuestro ámbito de aplicación, nos regimos por las normativas europeas ETSI (European Telecommunications Standards Institute):
14. **EN 300 220-1 V2.4.1 (2012-01):** Características técnicas y métodos de medida para los equipos de radio de corto alcance (entre las frecuencias de 25 MHz y 1000 MHz) con una potencia de emisión hasta 500 mW.
15. **ETSI EN 302 208-1 V1.4.1 (2011-07):** Características técnicas y métodos de medida para los equipos de radio (entre las frecuencias de 865 MHz y 868 MHz) con una potencia de emisión hasta 2 W.

6.7.1. EPC Class 1 Gen 2

[4] Las siglas EPC vienen de Electronic Product Code, que es un código único destinado a la identificación inequívoca de un objeto, persona, etc. y que está contenido en las etiquetas RFID.

Surge de la necesidad de distinguir los productos unitarios de una misma especie. Este código es universal y está compuesto por 24 dígitos, de los cuales, los 9 últimos están destinados a la identificación del objeto. Además, este código puede almacenar otras propiedades como la fecha de fabricación, fabricante, tamaño, fecha de caducidad, etc.

La EPCglobal es la organización que lidera de manera global el desarrollo de los estándares del EPC soportado por los sistemas RFID. Fue fundada en 2003 como sucesora de la organización perteneciente al MIT (Massachusetts Institute of Technology) Auto-ID Center. Los estándares EPC pueden ser de cuatro clases:

- **Clase 0:** etiquetas que se pueden programar sólo una vez, pero se pueden leer muchas veces (WORM – Write Once Read Many). La programación se realiza en el proceso de fabricación. Esta clase también es conocida como Class 1 Generation 1.
- **Clase 1:** son etiquetas pasivas con una memoria no volátil. Dependiendo del tipo, pueden ser WORM, es decir, solo se puede programar una vez, pero leer muchas veces, o pueden ser WMRM (Write Many Read Many), es decir, se pueden leer y escribir muchas veces.
- **Clase 2:** tienen características similares a las etiquetas de clase 1 Gen2, pero además añaden algunas funcionalidades como el uso extendido de memoria, control de acceso por autenticación, etc.
- **Clase 3:** aún no está definida, pero incorporará características para etiquetas semipasivas usando la banda UHF.
- **Clase 4:** son etiquetas activas que pueden comunicarse tanto con lectores como con otras etiquetas.

La EPC Class 1 Generation 2 se comenzó a definir en octubre del año 2002 por parte de la Auto-ID Center y finalizada en diciembre de 2004 por la EPCglobal, a quién fueron traspasados todos los procesos de desarrollo de los estándares tras su fundación. Sus propósitos fueron los de mejorar las características de la generación 1, añadiendo nuevas funcionalidades y perfeccionamiento, además de anticipando posibles aplicaciones futuras, establecer una única especificación en la banda UHF o realizar un desarrollo global dirigido a los reguladores de las diversas regiones mundiales.

En cuanto a las principales características de la EPC Class 1 Generation 2 podemos citar las siguientes:

- Los interrogadores pueden transmitir utilizando tres tipos de modulación:
 - DBS-ASK¹³ (Double-Sideband Amplitude Shift Keying)

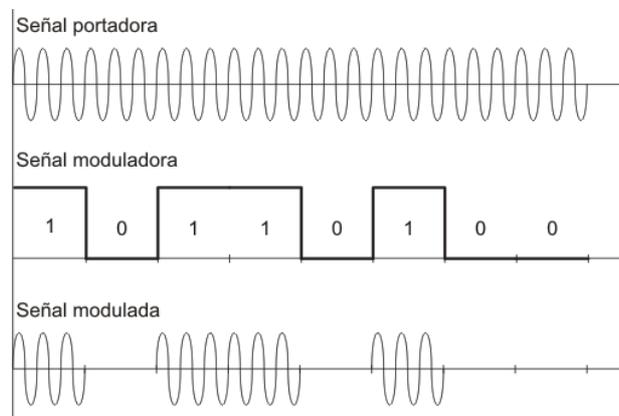
¹³ [33] ASK es una modulación de amplitud donde la señal moduladora (datos) es digital. Los dos valores binarios (0 y 1) se representan con dos amplitudes diferentes y es usual que una de las dos amplitudes sea cero; es decir uno de los dígitos binarios se representa mediante la presencia de la portadora a amplitud constante, y el otro dígito se representa mediante la ausencia de la señal portadora, en este caso la frecuencia y la fase se mantiene constante.

La modulación en ASK no es otra cosa que una variante de la modulación en AM que se adapta perfectamente a las condiciones de los sistemas digitales, además de que les permite trabajar sobre una sola frecuencia de transmisión en vez de tener que lidiar con pulsos cuadrados que contienen componentes en todas las frecuencias del espectro.

- SSB-ASK (SingleSideband Amplitude Shift Keying)
- PR-ASK (Phase-Reversal Amplitude Shift Keying)

Utilizando un formato PIE (Pulse-Interval Encoding), que consiste en un formato de representación en el que para representar un “1” lógico utiliza un pulso largo transmitido de manera ininterrumpida, seguido de un pulso corto sin transmitir, mientras que para un “0” lógico utiliza un pulso corto transmitido de manera ininterrumpida, seguido de un pulso corto sin transmitir.

- Los sistemas RFID podrán comunicarse utilizando frecuencias comprendidas entre 860 y 960 MHz. La elección de la frecuencia a utilizar por parte del interrogador dependerá de la normativa regional, así como del entorno radioeléctrico local.
- Dense-Interrogator channelized signaling: el estándar de la EPC Class 1 Generation 2 incorpora un método que soporta múltiples lectores minimizando la interferencia entre ellos. Permite tres modos de operación: single reader mode para un solo lector, multiple reader mode para múltiples lectores y dense reader mode para un entorno con alta densidad de lectores.
- En el entorno de un solo lector, este transmite y espera la respuesta de la etiqueta sin transmitir temporalmente. En los entornos densos o de múltiples lectores, la transmisión y la respuesta se separan en diferentes canales frecuenciales. Al variar la regulación europea con respecto a la normativa americana, el ancho de banda dedicado no es el mismo en los dos territorios. Mientras los sistemas europeos dispondrán de 10 canales en la banda UHF dedicada a RFID, los sistemas americanos disponen de 50 canales. Además, como en proporción, los lectores transmiten mucha más energía que las etiquetas (unos seis órdenes de magnitud), existe la posibilidad de introducir una máscara de rebaja en la transmisión de los lectores, que atenúe la energía en los canales adyacentes.
- Mayores velocidades de transmisión: mientras la Gen1 utilizaba velocidades entre 70 y 149 kbps, la Gen2 permite velocidades entre 80 y 640 kbps.
- El EPC de las etiquetas de la Gen2 es de 256 bits, mientras que en la generación anterior era de 96 bits.



Su recuperación también resulta ser más sencilla, dado que sólo depende de sincronizar la frecuencia de las señales sinusoidales que sirven de portadoras y regeneradoras dependiendo si se hallan en el modulador o el demodulador.

El ASK por sí sólo, a pesar de todas estas consideraciones, no es uno de los métodos más utilizados debido a que para cada frecuencia es necesario realizar un circuito independiente, además de que sólo puede transmitirse un solo bit al mismo tiempo en una determinada frecuencia. Otro de los inconvenientes es que los múltiplos de una frecuencia fundamental son inutilizables y que este tipo de sistemas son susceptibles al ruido.

Mejoras que ofrece Gen2

[1] El aporte más importante que proporciona la Gen2 es el de tener un único protocolo global, ya que la primera generación tenía dos, para la clase 1 y la clase 0.

Las mejoras de Gen2 frente a sus generaciones antecesoras son:

- **Velocidad o transmisión de datos:** Con la generación 2 hay una velocidad máxima de 640 kbps, mientras que en la generación 1 teníamos 80 kbps en la clase 0 y 140 kbps en la clase 1. Por lo que la generación 2 tiene una velocidad ocho veces mayor que su antecesora la generación 1. Esta mejora supone un gran avance para las empresas porque al incrementar la velocidad se incrementan las etiquetas leídas por segundo, reduciendo por ello los tiempos empleados en la lectura.
- **Capacidad de lectura:** Gracias a este factor de mejora la capacidad de lectura también se ve incrementada. La Gen2 permite escribir 16 bits cada 20 milisegundos. Este parámetro, la velocidad de escritura, también es importante para la velocidad de los procesos. En condiciones ideales se calcula que con la Gen2 podríamos leer unas 1.700 etiquetas/segundo en Estados Unidos y unas 600 etiquetas/segundo en Europa, ya que existen más restricciones en cuanto a potencia y ancho de banda. Gracias a estas velocidades, las empresas, podrían identificar objetos situados en una cinta transportadora con velocidades máximas de 200 metros por minutos, aunque este dato se vería afectado dependiendo del entorno de trabajo, ya que factores como el número de etiquetas que pasan simultáneamente lo afectaría.
- **Comando Select:** La generación 2 ofrece una nueva funcionalidad, gracias a la cual se permite la posibilidad de que el lector seleccione a partir del comando 'SELECT'. Gracias al cual y mediante un filtro de búsqueda por diferentes bits, como pueden ser el EPC, ID, la memoria de usuario, etc., se conseguirían leer una serie de etiquetas en concreto. Mediante esta posibilidad se ve incrementada la eficiencia de lectura y se reduce la información a procesar por el sistema lector, o middleware. Además, esta generación soporta varios comandos 'SELECT' para operaciones más complejas.
- **Modos de operación:** Las transmisiones entre los lectores y las etiquetas RFID se gestionan en tiempo o espectro de frecuencias, para evitar las interferencias entre lecturas. La generación 2 dispone de tres modos de operar: single reader mode (un solo lector), multiple reader mode (múltiples lectores) y dense reader mode (con alta densidad de lectores). Gracias a estos tres modos se minimizan las interferencias entre los lectores y así se evitan colisiones. Estos parámetros serán distintos dependiendo de las regulaciones locales, ya que el ancho de banda en Europa es de 2 MHz y en América 26 MHz. En el modo single reader, primero transmite el lector y espera la respuesta de la etiqueta, ambas comunicaciones se realizan de manera separada temporalmente. En cambio, en modo múltiple o denso la pregunta y la respuesta se separan en diferentes canales de frecuencia.
- **Fiabilidad:** En la mayoría de las aplicaciones, no se requiere altas velocidades de lectura, sin embargo, es más importante estar seguros de que todas las etiquetas RFID han sido identificadas correctamente. La generación 2 utiliza diversas técnicas para reducir las lecturas falsas. La primera, cuando un lector envía un comando QUERY, la etiqueta RFID responde con un retraso máximo de 4 ms, si el retraso fuese mayor se ignoraría la respuesta. Si por el contrario responde dentro del tiempo establecido, se inicia el diálogo. La etiqueta envía primero un preámbulo (una onda única que no varía). Si el lector ve y valida el preámbulo, entonces lee las ondas radio para transformarlo a bits de datos. El lector verifica que los bits formen una estructura de código EPC válido. Además, esta generación, ha sido diseñada de forma que la etiqueta es capaz de enviarle al lector cuantos bits le envía, de este modo el lector compara este dato con los bits que realmente ha recibido. Si ambos coinciden se comprueba el CRC (Cyclic Redundancy Check), de 16 bits de tamaño (también usado en la Clase 1 Gen 1), para asegurar que se había recibido al completo y sin ningún bit corrupto.
- **Mayor Robustez:** Una nueva característica de la Gen2 es una mayor robustez al contar las etiquetas con el algoritmo Q Algorithm y simetría AB. El "Q algorithm" permite identificar muchas etiquetas rápidamente de manera precisa. La simetría AB evita los problemas de poner las etiquetas en modo 'sleep' y 'wake up'. El algoritmo Q, que permite a la etiqueta generar un

número aleatorio, proporciona al lector la posibilidad de distinguir dos etiquetas con el mismo EPC, lo que provocaba confusión en el lector cuando se leían etiquetas con el mismo EPC. Por otra parte, la simetría AB mejora el sistema para contar las etiquetas, ya que evita confusiones cuando intervienen más de un lector. La generación 2 no utiliza los modos ‘sleep’ y ‘wake up’, para ello utiliza dos estados que consisten en un flag A y B. De esta forma se elimina la problemática de poner a las etiquetas en ‘sleep’ y se garantiza que el lector sepa a cada lectura cuáles son nuevas etiquetas y cuales ya estaban.

- Sesiones: En la generación 1 cuando un lector lee una etiqueta, pone a ésta en modo ‘sleep’, así cuando se quiere hacer otro inventario se hace un ‘wake up’ de ella. Este modo de trabajo provoca que no pueda haber inventarios simultáneos sin interferirse. Sin embargo, la generación 2 se anticipa a situaciones donde hay varios lectores simultáneamente que quieren realizar inventarios, comunicándose con una misma etiqueta, de este modo se permite a los lectores contar en paralelo objetos sin interferirse entre ellos. Hay 4 sesiones lógicas (S0, S1, S2 y S3) con simetría AB para cada sesión, que evitan que entre ellas no se puedan interferir. El sistema RFID se puede configurar para que los lectores utilicen la sesión según el tipo, así podríamos determinar que los lectores fijos utilizarán la S0, los de las carretillas la S1 y los móviles la S2.
- El protocolo de Gen1 permite enviar el comando ‘Kill’ para desactivar la etiqueta permanentemente, para proteger la privacidad, para realizar esta desactivación se necesita que el lector envíe 8 bits de código para que la etiqueta responda y realice el proceso. Estos 8 bits sólo permiten 256 números únicos. El protocolo de la generación 2 tiene un password de 32 bits, usado para el código ‘Kill’ al igual que para bloquear y desbloquear los campos de la memoria de la etiqueta. Esto significa más de 4 billones de posibles opciones, que garantizan que sólo con el permiso del propietario de la etiqueta se pueda modificar la información contenida en su memoria.

En la tecnología RFID, al ser una tecnología de evolución, existe un miedo a que el camino en el que se invierte se quede obsoleto. Para evitar esta obsolescencia los lectores son capaces de leer cualquier generación y además son actualizables.

	Gen2 Clase 1	Gen1 Clase 1
EPC	96/256 Bits	64/96 Bits
Velocidad	80/640 Kbps	70/140 Kbps
Ratio de lectura	EU ETSI – 460 Etiquetas/Segundo US FCC - 880 Etiquetas/segundo Adaptable según el ruido del entorno de trabajo.	EU ETSI – 115 Etiquetas/segundo US FCC – 230 Etiquetas/segundo
Ratio de escritura	5 Etiquetas/segundo	3 Etiquetas/segundo
Frecuencia	860 - 960 MHz	860 – 930 MHz
Inventario	Protocolo Q y simetría AB	Modo binario ‘Sleep’ y ‘wake up’
Verificación	16 Bits CRC	16 Bits CRC
Modos del lector	US FCC Frequency Hopping (salto de frecuencias). EU ETSI - Escuchar después de hablar. Canales de frecuencia y 4 sesiones. 3 modos de trabajo del lector segundo el entorno.	US FCC Frequency Hopping (salto de frecuencia) EU ETSI – Escuchar después de hablar.
Seguridad	32 bits bloqueo y ‘kill’.	8 Bits de ‘kill’.
Expansión	Anticipa clase 2 y 3. Memoria de usuario ilimitada según el tipo de etiqueta.	Por sobre de 96 bits.

Tabla 8. Comparativa Gen2 – Gen1.

6.8. Anexo H. RFID y Código de barras óptico

El código de barras óptico se registró por primera vez en octubre de 1952, en EEUU, con objeto de identificar vagones de ferrocarril. Se comenzó a utilizar comercialmente en 1966 y alcanzó su éxito en 1980. [15]

El primer uso industrial que se le dio fue en 1981, cuando el departamento de defensa estadounidense marcó todos los productos militares que se vendían. Dicho sistema se denomina LOGMARS, siendo aún utilizado hoy día. [16]

Básicamente, un código de barras consiste en la representación de un conjunto de líneas paralelas con distinto grosor y espaciado que en su conjunto tienen una determinada información, y que es único para cada producto. Actualmente, el código de barras más utilizado a nivel mundial es el EAN 13 (*European Article Number*), constituido por 13 dígitos y con capacidad de información de 43 bits. [17] La capacidad de codificación del código de barras se limita por la difracción de la luz a través de los bordes de las líneas, la sensibilidad del lector y la distancia de lectura. La difracción restringe el ancho de línea mínimo detectable, así como la separación entre dos líneas adyacentes. De este modo, aumentar la longitud del código de barras es la única forma de aumentar su capacidad de información. Este aspecto se considera una de las principales limitaciones que presenta esta tecnología.



Figura 101. Estructuras de códigos de barras: (a) unidimensional con codificación EAN 13 y (b) bidimensional (QR)

Durante los últimos 25 años el código de barras ha sido el principal medio de identificación automática de productos en la cadena de abastecimiento. Su dominio en el mercado se debe, en parte, a su bajo coste de producción; menos de un céntimo de euro por unidad, y a su baja probabilidad de error; una entre dos millones. Sin embargo, RFID es una tecnología que ha tenido un gran crecimiento en los últimos años. De hecho, se piensa que puede sustituir al código de barras, pero, por el momento, no reemplaza a ninguna de las otras tecnologías de auto identificación existentes, ya que cada una tiene sus propias ventajas e inconvenientes. [18]

A pesar de ello, la tecnología RFID se ha visto como la sucesora del código de barras, ya que ofrece diferentes ventajas sobre esta tecnología. A continuación, se destacan algunas de ellas. [19]

Método de lectura

El lector óptico del código de barras requiere de una verificación visual directa. El lector indica cuándo obtiene una buena lectura dentro de su rango, y una mala lectura es inmediatamente asociada con una etiqueta y un ítem específicos.

[20] Los códigos de barras se leen pasando un pequeño punto de luz sobre el símbolo del código de barras impreso. Solo se ve una fina línea roja emitida desde el escáner láser. Pero lo que pasa es que las barras oscuras absorben la fuente de luz del escáner y la misma se refleja en los espacios luminosos. Un dispositivo del escáner toma la luz reflejada y la convierte en una señal eléctrica. El láser del escáner (fuente de luz) comienza a leer el código de barras en un espacio blanco (la zona fija) antes de la primera barra y continúa pasando hasta la última línea, para finalizar en el espacio blanco que sigue a ésta. Debido a que el código no se puede leer si se pasa el escáner fuera de la zona del símbolo, las alturas de las barras se eligen de manera tal de permitir que la zona de lectura se mantenga dentro del área del código de barras. Mientras más larga sea la información para codificar,

más largo será el código de barras necesario. A medida que la longitud se incrementa, también lo hace la altura de las barras y los espacios a leer.

La lectura RFID, por el contrario, no requiere de línea de visión directa para obtener la información de la etiqueta. La señal de radio es capaz de viajar a través de la mayoría de los materiales, lo cual resulta muy ventajoso en aplicaciones donde la información debe ser obtenida a partir de ítems que tengan una orientación heterogénea.

El lector RFID es capaz de distinguir una etiqueta individual a pesar de que múltiples etiquetas se encuentren dentro de su rango de lectura. No obstante, dicha discriminación de etiquetas no resuelve la ubicación física absoluta de un ítem que sí ofrece el código de barras cuando el objetivo es un punto específico.

Características	Código de barras	RFID
Capacidad / Identificación	Espacio limitado / Estandarizada	Mayor cantidad de información / Unívoca por producto
Actualización Lectura	Sólo una lectura cada vez	Lectura / escritura simultánea
Tipo de lectura	Sólo en superficie	A través de diversos materiales
Flexibilidad	Requiere línea de visión para lectura	No requiere línea de visión para lectura
Precisión / Durabilidad	Requiere intervención humana / Puede estropearse fácilmente	100 % automático / Soporta ambientes agresivos

Tabla 9. Comparativa RFID – Código de barras óptico

Velocidad de lectura

Las etiquetas RFID se pueden leer, teóricamente, 1000 veces por segundo o más rápidamente que las etiquetas de código de barras. Esto resulta muy práctico en aplicaciones de recepción de mercaderías en grandes volúmenes, donde se necesita leer un elevado número de ítems.

Durabilidad

Las etiquetas RFID pueden ser insertadas en sustratos de plástico, u otros materiales, para mayor protección. La naturaleza de las mismas les permite perdurar más que las del código de barras, aunque ambas dependen del adhesivo que las mantiene intactas y pegadas a un ítem.

Sin embargo, existe una gran vulnerabilidad con la etiqueta RFID. Un corte que dañe el punto de unión entre el chip y la antena inutilizaría dicha etiqueta, mientras que el código de barras apenas resultaría degradado.

Almacenamiento de datos

El código UPC identifica la clasificación de un ítem genérico, mientras que EPC permite identificar un ítem de forma completamente individual mediante un número de serie asignado. Los tags RFID más costosos pueden almacenar varios kilobytes de memoria.

Dicho incremento en la capacidad de almacenamiento ofrece la posibilidad de crear una base de datos de información portátil, permitiendo el rastreo de un gran número de productos con datos como el tiempo en tránsito, su ubicación en el centro de distribución o la fecha de vencimiento del ítem.

Flexibilidad de información

Los tags RFID son capaces de realizar operaciones de lectura y escritura, lo que permite la actualización de información en tiempo real de un ítem.

Seguridad

Algunos tags RFID pueden soportar la combinación de palabras clave que pueden hacerlas ilegibles para sistemas de lectura que no usen las claves de acceso del código EPC.

Coste

La tecnología RFID es menos cara que los códigos de barras. Aunque un código de barras apenas tiene coste, requiere de una persona que lo escanee, lo que resulta un trabajo costoso. Por el contrario, la lectura RFID no requiere de intervención humana.

Prestaciones

RFID es mucho más preciso que los códigos de barras. Un operario humano puede llegar a perder u olvidar algunos ítems en el proceso de escaneo, mientras que RFID consigue ratios de escaneo generalmente mucho más altos. Puede no llegar al 100% de lecturas correctas, pero se acerca más a ello que el código de barras.

Además, los tags pasivos UHF pueden ser leídos a distancias de hasta 10 metros, cuando los códigos de barras se pueden leer a 30 cm.

	Códigos de barras ópticos	RFID
Tamaño	Muy pequeños	Medio
Rango de lectura	Varios centímetros	Hasta 15 m (pasivos)
Capacidad de almacenaje	43 bits (código EAN 13)	96 bits EPC Class1 Gen2
Lectura simultanea	No	Si
Reprogramable	No	Si
Fácil de copiar	Si	No
Posición lector/etiqueta	Necesita visión directa	No necesita visión directa
Coste	< 0.01 euros	≈ 0.15 euros

Tabla 10. Prestaciones RFID – Códigos de barras ópticos.

Los códigos de barras continúan siendo una gran tecnología, barata y al alcance de todo el mundo. Probablemente el código de barras seguirá siendo una buena opción para muchos, pero es evidente que la tecnología RFID cuenta con unas características y ventajas que la hacen única. [21] Lo importante, a la hora de decidir qué tecnología usar, es responder a las siguientes preguntas:

- ¿Es fundamental en mi negocio tener información asociada a cada producto?
- Con RFID, ¿puedo automatizar más mis procesos?
- ¿Puedo solucionar “cuellos de botella” con RFID?
- ¿Existen errores recurrentes en la producción, expedición o cualquier problema interno?
- ¿Qué coste supondría implementar RFID en mi negocio? ¿Lo implementaría en todo mi negocio, o sólo en una parte? ¿Habrá ahorros de personal? ¿En cuánto tiempo puedo amortizar el sistema RFID adquirido?

6.9. Anexo I. RFID y NFC

Se denomina NFC (*Near Field Communication*) a una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. [22] Fue aprobada en 2003 como estándar ISO/IEC y en 2008 se empezó a combinar con Bluetooth en algunos periféricos. Los estándares de NFC cubren protocolos de comunicación y formatos de intercambio de datos, y están basados en ISO 14433¹⁴ y FeliCa. Los estándares incluyen ISO/IEC 18092¹⁵ (NFCIP-1) y los definidos por el Foro NFC, fundado en 2004 por Nokia, Philips y Sony.

NFC es una plataforma abierta pensada desde el inicio para teléfonos y dispositivos móviles. Se comunica mediante inducción en un campo magnético, en donde dos antenas de espiral son colocadas dentro de sus respectivos campos cercanos. Trabaja en la banda de los 13,56 MHz, por lo que no requiere ninguna licencia de uso.

Soporta dos modos de funcionamiento, al igual que todos los dispositivos del estándar NFCIP-1:

- Activo: ambos equipos con chip NFC generan un campo electromagnético e intercambian datos.
- Pasivo: solo un dispositivo genera el campo electromagnético y el otro aprovecha la modulación de la carga para poder transferir los datos. El iniciador de la comunicación es el encargado de generar dicho campo.

El protocolo NFCIP-1 puede funcionar a 106, 212, 424 u 848 kbits/s, por lo que su enfoque, más que para la transmisión de grandes datos, es para comunicación instantánea; identificación y validación de equipos/personas.

Su principal fortaleza es la velocidad de comunicación, que es casi instantánea sin necesidad de emparejamiento previo. También ofrece un uso transparente a los usuarios, y los equipos con esta tecnología con capaces de enviar y recibir información al mismo tiempo. Por el contrario, su alcance es muy reducido, pues se mueve en un rango máximo de 20 cm. [23]

Respecto a la seguridad, ya que estamos ante una comunicación por radiofrecuencia, la lectura de nuestra transmisión es una posibilidad que siempre existe. Sin embargo, con NFC se cuenta con la ventaja de la poca distancia a la que se opera. A pesar de ello, no se puede descartar la copia de códigos de nuestro chip para uso fraudulento, además de la modificación o inserción de errores en nuestro chip.

Sus aplicaciones más comunes, dentro de aquellas en las que se precisa un intercambio de datos de forma inalámbrica, son: [23]

- Identificación: el acceso a lugares donde se precisa una identificación se podría realizar acercando el teléfono móvil o tarjeta NFC a un dispositivo de lectura. Los abonos de autobús serían un ejemplo muy gráfico.
- Recogida/intercambio de datos: Google es el principal protagonista de este uso. Combinando etiquetas RFID, tareas como la marcar la ubicación, recibir información de un evento o establecimiento resultan inmediatas.
- Sincronización instantánea de dispositivos: Las etiquetas NFC son pequeña pegatinas que pueden ser ubicadas en varios sitios y configurarlas para que al pasar el móvil sobre ellas realicen configuraciones automáticas.
- Pago con el teléfono móvil: La comodidad de uso y que el gasto pueda estar asociado a una cuenta de banco son prestaciones que pueden situar a esta tecnología como método de pago del futuro.

¹⁴ ISO 14443 es un estándar internacional relacionado con las tarjetas de identificación electrónicas. Consultar apartado 2.3. Estándares y regularizaciones RFID.

¹⁵ ISO 18092 es el estándar a partir del cual deriva NFC. Consultar apartado 2.3. Estándares y regularizaciones RFID.



Figura 102. Sistema de pago mediante NFC.

En la actualidad, la mayor parte de marcas y sistemas operativos de smartphones, como Android, BlackBerry, Apple, Symbian OS, J2ME, Bada o MeeGo incorporan NFC.

Centrándonos más en RFID y sus diferencias con NFC, hay que especificar que RFID se denomina a la tecnología en sí, la forma por la cual podemos conectar o identificar varios dispositivos de manera inalámbrica. NFC, sin embargo, no es más que una parte dentro de la tecnología RFID, un subconjunto dentro de la misma. Funciona a la misma frecuencia de 13,56 MHz, pero tiene sus particularidades propias, como el límite de alcance, restringido a unos 20 cm por motivos de seguridad. Supongamos que se pudiera pagar con el móvil a 3 metros de distancia. Podría suponer un problema en la medida que alguien sentado en la mesa de al lado pudiera recibir tal información y clonarla. NFC evita dicho inconveniente con apenas unos centímetros de margen. [24]

Respecto al uso, RFID está muy extendido en la industria logística y a la identificación de productos. NFC, por el contrario, si está orientado al uso diario de los consumidores, como móviles y tarjetas bancarias. También permite compartir información de contactos, identificarnos con tarjetas, controles de acceso, etc. Siempre procesos habituales en los consumidores.

6.10. Anexo J. Redes IoT

[25] Para 2020, más de 50 mil millones de dispositivos estarán conectados a través de comunicaciones de radio. De acuerdo al rápido crecimiento del “Internet de las cosas”, las redes de área amplia y baja potencia se han convertido en tecnologías de comunicación a larga distancia imperantes en el mercado.

Esta llamada “Internet de las cosas”, o IoT, hace referencia a la interconexión e intercambio de datos entre dispositivos. Actualmente, con el mencionado explosivo crecimiento de tecnologías IoT, un creciente número de aplicaciones prácticas pueden ser encontradas en diversos campos incluyendo la seguridad, seguimiento de activos, agricultura, ciudades inteligentes o casas inteligentes. Dichas aplicaciones requieren especificaciones tales como baja tasa de datos, bajo consumo, largo alcance y rentabilidad.

Las comúnmente usadas tecnologías de corto alcance (Bluetooth, ZigBee...) no están adaptadas para escenarios que requieren un largo alcance de transmisión, y las soluciones aplicadas a comunicaciones móviles (2G,3G,4G) pueden soportar una amplia cobertura, pero consumen demasiada energía. Es por esto, que tales requerimientos para soportar IoT han conducido a nuevas tecnologías inalámbricas; las LPWAN.

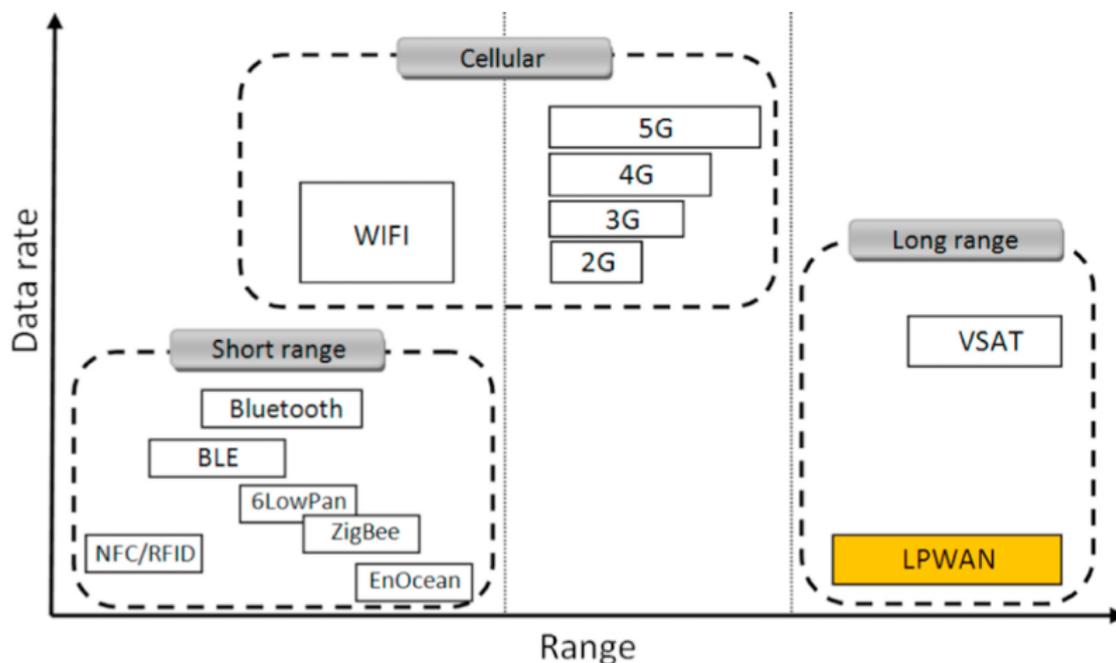


Figura 103. LPWAN, en comparación a otras tecnologías inalámbricas.

[26] LPWAN (Low Power Wide Area Network), conocido también como LPWA o LPN, es un protocolo de transporte inalámbrico de datos que hoy en día se entiende como uno de los protocolos básicos para la implementación de IoT.

Para tener una idea de la relevancia de LPWAN se puede considerar la predicción que realiza *statista.com* de un aumento constante de la cantidad de dispositivos LPWAN conectados alrededor del mundo, esperando que esta cantidad llegue a rondar los 3.500 millones de dispositivos para 2021.

Por supuesto debemos aceptar que los estándares definitivos para IoT todavía están por definirse, de hecho, los protocolos se encuentran en pleno desarrollo y existen varios proyectos que pretenden definir estándares.

Sin embargo, en la mayoría de literatura aparece LPWAN como una opción válida de protocolo de transporte para ciertas necesidades de IoT.

Son tres las características técnicas de LPWAN que lo hacen coincidir con los requerimientos de IoT. Estas son:

- El alcance geográfico: LPWAN está diseñado para el transporte inalámbrico de datos entre dispositivos separados por distancias en el rango de kilómetros y no de metros.
- La cantidad de data transmitida: La idea de LPWAN es regular el transporte puntual de pequeñas

cantidades de datos.

- El bajo consumo eléctrico: El protocolo se fundamenta en el uso de dispositivos cuyas baterías permiten una duración de años en lugar de semanas y meses.

Estas características además diferencian a LPWAN de otras tecnologías inalámbricas como Wi-Fi, Bluetooth, 3GPP¹⁶ y Zigbee.

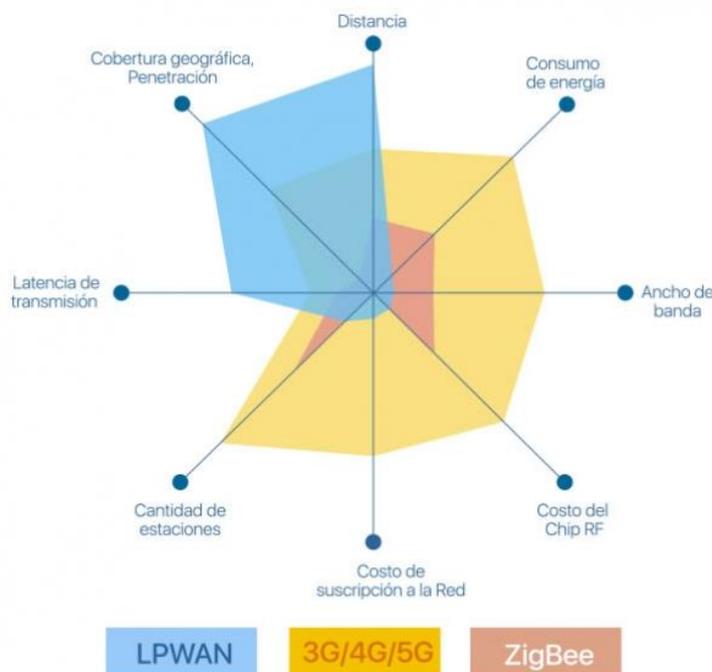


Figura 104. Comparativa LPWAN – 3G/4G/5G – ZigBee.

La tecnología LPWAN cubre casi que en exclusiva las necesidades de aquellas aplicaciones que requieren transferir de forma inalámbrica pequeñas cantidades de datos, pocas veces al día y a través de largas distancias.

Por lo regular, se asocia las redes LPWAN con redes de sensores y dispositivos distanciados geográficamente, que solo requieren o pueden transmitir poca información sobre su estado.

Los diferentes productos que implementan LPWAN trabajan en Europa en la banda ISM (Industrial, Scientific and Medical), la cual representa un espectro que internacionalmente se reserva al uso no comercial asociado con la industria, la ciencia y los servicios médicos. Esta banda es importante porque este grupo de frecuencias pueden ser utilizadas sin el pago por concepto de licencia, siempre y cuando se respeten las restricciones en los niveles de potencia transmitidas.

Esto representa otra diferencia de LPWAN y las tecnologías celulares, por ejemplo, en las cuales es necesario pagar por el derecho a transmitir en una frecuencia específica.

Para LPWAN existe una diferencia en la frecuencia utilizada dependiendo de la región en la cual se encuentre; en Europa se utiliza la franja entre 867 y 869 MHz, en Estados Unidos se utiliza la franja entre 902 y 928 MHz

¹⁶ [35] El 3GPP (3rd Generation Partnership Project: Proyecto Asociación de Tercera Generación) es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como miembros organizativos.

El objetivo inicial del 3GPP era asentar las especificaciones de un sistema global de comunicaciones de tercera generación 3G para teléfonos móviles basándose en las especificaciones del sistema evolucionado GSM (Global System for Mobile Communications: sistema global de telecomunicaciones móviles) dentro del marco del proyecto internacional de telecomunicaciones móviles 2000 de la ITU (Unión Internacional de Telecomunicaciones).

y en Asia depende del país. En el caso de Japón se utiliza la franja entre 920 y 925 MHz.

El uso de diferentes frecuencias implica que los dispositivos de hardware pueden utilizarse en diferentes países, pero requieren un ajuste en software para poder trabajar en una frecuencia particular.

Las desventajas que se pueden señalar son las siguientes:

- La baja velocidad de transmisión no permite manejar grandes volúmenes de datos, por lo que elementos como fotos y videos quedan descartados. Como ya se mencionó LPWAN permite la creación de redes de sensores y dispositivos; sin embargo, hay que decir que incluso en estas redes los volúmenes de datos de telemetría que pueden transportar no pueden ser muy grandes, lo que descarta elementos muy complejos o de los cuales se requiere mucha información.
- Existen reportes de problemas de atenuación de las señales cuando la red LPWAN incluye dispositivos ubicados en edificios o separados por elementos físicos, funcionando de forma más eficiente en espacios abiertos con líneas de vista aseguradas.
- La conectividad entre los dispositivos y su aplicación o servidor no es constante y puede ser unidireccional; del dispositivo a un elemento de captura, lo cual dificulta actividades como el control de movimiento de objetos en tiempo real. Aunque hay que decir que la mayoría de las implementaciones de LPWAN permiten comunicaciones bidireccionales. Otro elemento con el que las implementaciones de LPWAN tienen que batallar es la fiabilidad de las transmisiones. Es por ello que se introducen diferentes procesos de encriptación y autenticación para resolver esta deficiencia del protocolo.

Existen varias implementaciones del protocolo LPWAN. Hay diferencias entre cada una de ellas en cuanto a los esquemas de modulación, el alcance geográfico, la cantidad de datos transmitidos y a sus capacidades de encriptación y autenticación.

A continuación, se van a detallar las tres implementaciones LPWAN líderes que compiten por el despliegue IoT a gran escala.

6.10.1. LoRaWAN

[27] Lo primero que hay que aclarar es que LoRa y LoRaWAN no son lo mismo, LoRa es el tipo de modulación en radiofrecuencia patentado por Semtech y que entre sus principales ventajas se encuentra:

- Alta tolerancia a las interferencias.
- Alta sensibilidad para recibir datos (-168 dB).
- Basado en modulación chirp¹⁷.
- Bajo Consumo (hasta 10 años con una batería).
- Largo alcance 10 a 20km.
- Baja transferencia de datos (hasta 255 bytes).
- Conexión punto a punto.
- Frecuencias de trabajo: 915 MHz América, 868 MHz Europa, 433 MHz Asia.

Todo esto hace a la tecnología ideal para conexiones a grandes distancias y para redes de IoT que se pueden utilizar en ciudades inteligentes, lugares con poca cobertura celular o redes privadas de sensores o actuadores, por eso es que nace LoRaWAN.

LoRaWAN es un protocolo de red que usa la tecnología LoRa para comunicar y administrar dispositivos LoRa, se compone de dos partes principalmente: gateways y nodos, los primeros son los encargados de recibir y enviar información a los nodos y los segundos, son los dispositivos finales que envían y reciben información hacia el

¹⁷ [39] Un sistema de frecuencia modulada pulsada o chirping es un sistema de espectro ensanchado en el que la portadora de radiofrecuencia se modula con un periodo fijo y una secuencia de ciclo de trabajo fija. Al principio de cada pulso transmitido, la frecuencia de la portadora se modula en frecuencia, causando un ensanchado adicional de la portadora. El patrón de la modulación en frecuencia dependerá de la función de ensanchado que se elija. En algunos sistemas, la función de ensanchado es un barrido en frecuencia modulada lineal, barriendo las frecuencias hacia arriba o hacia abajo. La portadora se convierte en analógica.

gateway.

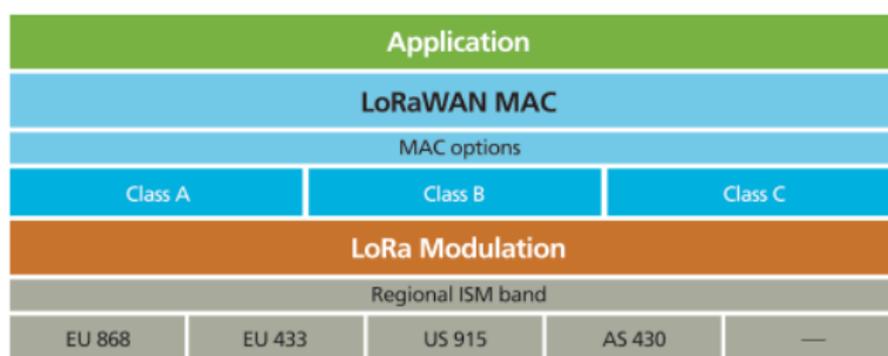


Figura 105. Arquitectura LoRaWAN.

Las principales características de LoRaWAN son:

- Topología estrella.
- Alcance de 10 a 15 km en línea de vista.
- Encriptación AES 128.
- Soporte para 3 clases de nodos.
- Administración de dispositivos.
- Redes públicas y privadas.
- Bajo consumo y largo alcance.
- Baja transferencia de datos (hasta 242 bytes).

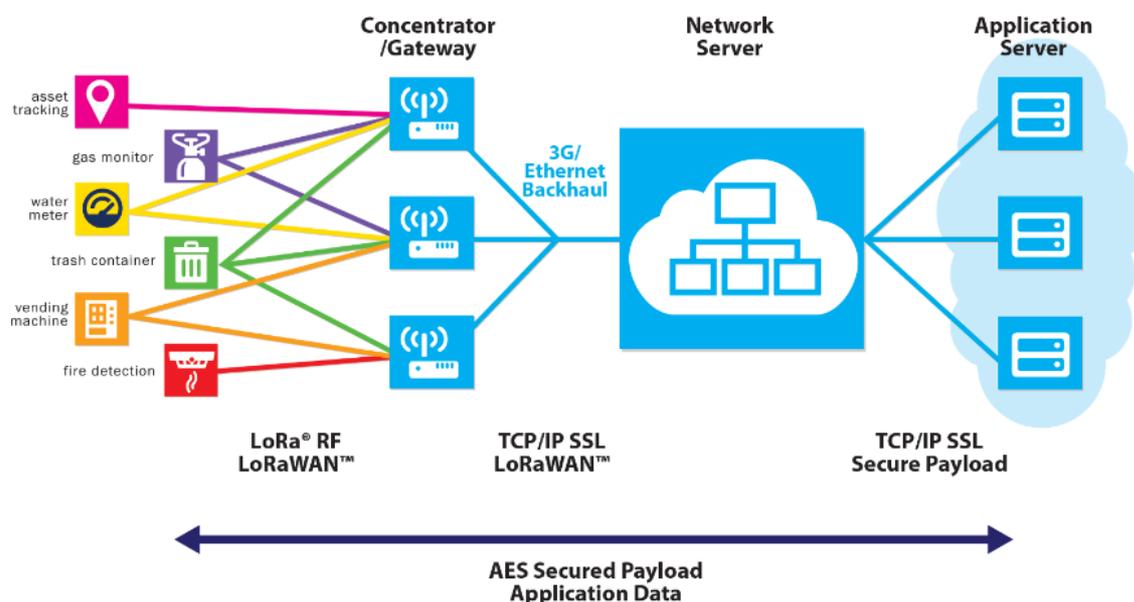


Figura 106. Estructura de la red LoRaWAN.

En resumen, LoRa termina siendo una tecnología muy flexible para solucionar diversos y variados problemas, gracias a sus topologías de conexión P2P, mesh y redes LoRaWAN privadas o públicas. Gracias a su largo alcance y bajo consumo esto la hace una tecnología barata y fácil de implementar.

6.10.2. SigFox

[28] SigFox es una compañía francesa fundada en 2009 que proporciona el servicio de red de cobertura amplia de bajo consumo (LPWAN), es inalámbrica y fue creada para que funcione e interactúe con dispositivos de bajo consumo energético, tales como sensores que funcionan con pilas convencionales, con tasas de transferencias de datos de hasta 12 bytes.

La red funciona con la tecnología de transmisión UNB¹⁸, y consiste en emplear canales estrechos del espectro para alcanzar grandes distancias con un requerimiento mínimo de energía.

El funcionamiento de esta red es muy similar a las redes de telefonía celular debido a que esta red funciona a partir de la colocación de varias estaciones receptoras y transmisoras; la diferencia entre las estaciones SigFox y las de telefonía celular es en que los dispositivos y sensores que estén conectados a la red SigFox no están sujetas a una sola estación base específica, es decir, cualquier estación puede recibir la información y transmitirla hacia la nube.

La banda pública empleada para el intercambio de mensajes en SigFox es en 200 kHz y en la que cada mensaje tiene un ancho de 100 Hz y puede ser transmitido a una de tasa desde 100 bits hasta 600 bits. Estas tasas varían de acuerdo al país en donde se encuentre.

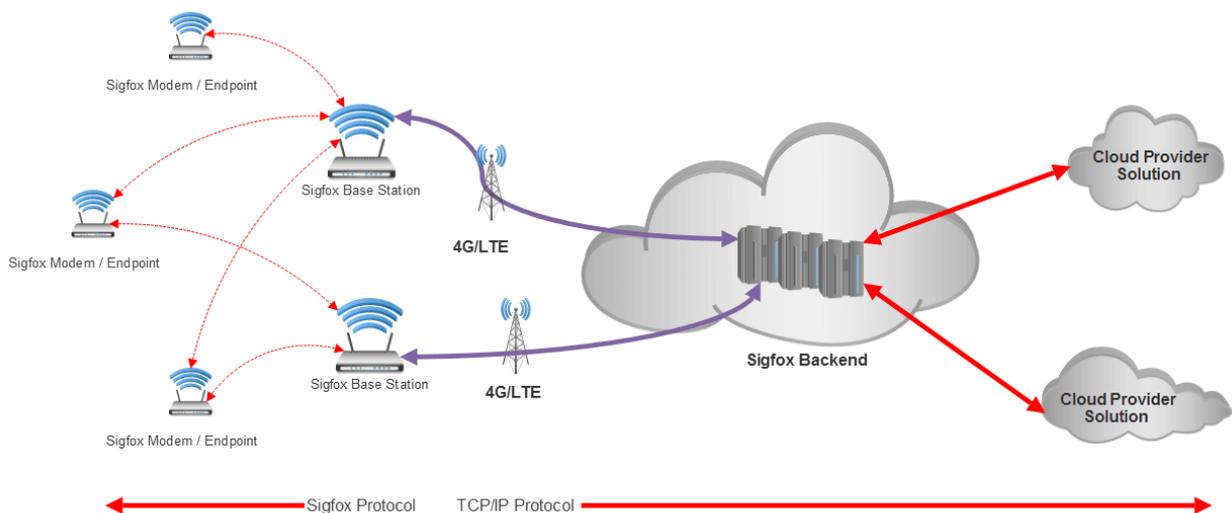


Figura 107. Arquitectura SigFox.

La seguridad es muy importante en esta red por lo que cada dispositivo debe tener asignado un código de identificación, cuenta con protocolos de encriptamiento VPN y emplea al final el protocolo *https*.

Los servicios principales con los que cuenta esta red son:

- Sistema de mensajería.
- Servicio de nube y manejo de datos.
- Servicios de geolocalización y rastreo.

Dado que su red es única y como se mencionó anteriormente, tiene el atributo de ser como una red de telefonía celular, una red con una amplia cobertura en casi cualquier lugar en la que se pueden enviar y recibir mensajes más el atributo de internet, específicamente en el IoT, en la que se puede enviar, recibir y procesar datos.

SigFox puede hacer uso de otras formas de comunicación como complemento y viceversa porque es compatible con Bluetooth, GPS, las redes 2G, 3G y 4G y WiFi. Debido a la versatilidad y flexibilidad de esta red, las empresas (micro, pequeñas, medianas y grandes) hacen uso de esta red.

¹⁸ La tecnología Ultra Narrow Band está diseñada para funcionar con bajas velocidades de transferencias de 10 a 1000 bits por segundo.

6.10.3. Narrow Band

[29] Narrowband (NB) es la primera tecnología centrada en conectar a Internet objetos cotidianos que requieren pequeñas cantidades de datos en períodos de tiempo largos. Es una de las distintas tecnologías competidoras (SigFox, LoRaWan...) que se denominan, generalmente, LPWAN. Es un estándar desarrollado por 3GPP para permitir una amplia gama de dispositivos y servicios móviles.

[30] NB se enfoca específicamente en la cobertura interior, bajo coste, larga duración de la batería y alta densidad de conexión. NB utiliza un subconjunto del estándar LTE¹⁹, pero limita el ancho de banda a una única banda estrecha de 200 kHz. Utiliza modulación OFDM para enlaces descendentes y SC-FDMA para enlaces ascendentes.

Compatible con todos los principales fabricantes de equipos móviles, NB puede coexistir con redes móviles 2G, 3G y 4G. También se beneficia de todas las características de seguridad y privacidad de las redes móviles, como la compatibilidad con la confidencialidad de la identidad del usuario, la autenticación de la entidad, la confidencialidad, la integridad de los datos y la identificación de equipos móviles.

Esta tecnología ha sido desarrollada para permitir comunicaciones eficientes y una alta durabilidad de la batería, para dispositivos distribuidos masivamente. Utiliza la ya existente red móvil para conectar todos esos objetos. NB está diseñado para ampliar el futuro de la conectividad IoT de una manera más segura y fiable. Es ideal para dispositivos que generan un tráfico de datos no muy alto y tienen un ciclo de vida largo.

Las ventajas de usar NB son:

- Bajo consumo de energía.
- Conectividad fiable, ratificada por el 3GPP (estándar global en el espectro autorizado).
- Menor coste por componente.
- Despliegue simplificado en la arquitectura de red móvil existente.
- Seguridad garantizada por doble autenticación y una interfaz fuertemente encriptada.
- Permite un gran número de dispositivos conectados.
- Mayor alcance en interiores y exteriores.
- Transferencia de información optimizada.
- Permite más de 100.000 conexiones por celular.

¹⁹ [36] LTE (Long Term Evolution) es una tecnología de transmisión de datos de banda ancha inalámbrica que está principalmente diseñada para poder dar soporte al constante acceso de teléfonos móviles y de dispositivos portátiles a internet.

Podríamos resumir diciendo que LTE es la tecnología utilizada en los teléfonos móviles o celulares de cuarta generación, los llamados teléfonos 4G, para la bajada y subida de datos desde internet. Realmente los 4G usan LTE Advanced, la misma tecnología, pero más avanzada.

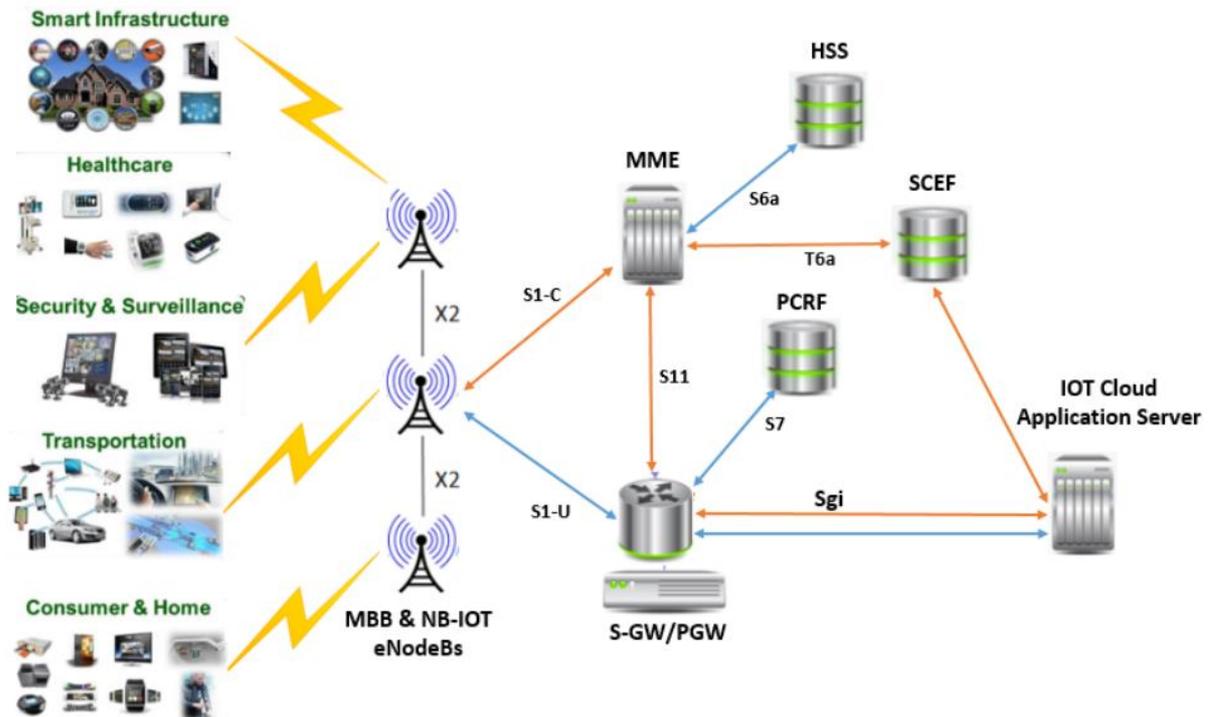


Figura 108. Arquitectura NB.

6.10.4. Comparativa LoRaWAN/SigFox/NB

Se deben considerar muchos factores al elegir la tecnología LPWAN adecuada para una aplicación de IoT, incluida la calidad del servicio, la duración de la batería, la latencia, la escalabilidad, la longitud de la carga útil, la cobertura, el alcance, la implementación y el coste.

Calidad de servicio (QoS)

SigFox y LoRa emplean espectros sin licencia y protocolos de comunicación asíncrona. Pueden solucionar problemas de interferencia, multitrayecto y desvanecimiento. Sin embargo, no pueden ofrecer la misma calidad de servicio que ofrece NB. Éste emplea un espectro con licencia y un protocolo síncrono basado en LTE, que son los óptimos para QoS.

Debido a la QoS y la compensación de costes, NB se prefiere para aplicaciones que requieren una calidad de servicio garantizada, mientras que las aplicaciones que no tienen esta restricción deben elegir LoRa o Sigfox.

Duración de la batería y latencia

En Sigfox, LoRa y NB, los dispositivos finales están en modo de reposo (sleep mode) la mayor parte del tiempo fuera de la operación, lo que reduce la cantidad de energía consumida, es decir, la vida útil prolongada de los dispositivos finales. Sin embargo, el dispositivo final NB consume energía adicional debido a la comunicación síncrona y el manejo de la QoS, y sus modos de acceso OFDM/FDMA requieren más corriente de pico. Este consumo de energía adicional reduce la vida útil del dispositivo final NB en comparación con Sigfox y LoRa.

Sin embargo, NB ofrece la ventaja de una baja latencia. A diferencia de Sigfox, LoRa proporciona la clase C para manejar también la latencia bidireccional baja a expensas de un mayor consumo de energía. Por lo tanto, para las aplicaciones que son insensibles a la latencia y que no tienen una gran cantidad de datos para enviar, Sigfox y LoRa de clase A son las mejores opciones. Para las aplicaciones que requieren baja latencia, NB y LoRa clase C son las mejores opciones.

LoRA	NB-IoT
Older (2015)	Newer (2017)
Unlicensed spectrum	Licensed frequency bands
Lower cost per device (but gateway needed)	Higher cost per device (but no gateway needed)
Longer battery life	Shorter battery life
High latency / less frequent data transfer	Low latency / more frequent data transfer
7 to 10 mile range	11 to 13 mile range
Better rural/remote performance	Better urban/dense performance
Lower data rates	Higher data rates (10x LoRa's rates)

Tabla 11. Comparativa LoRa - NB.

	Sigfox	LoRaWAN	NB-IoT
Modulation	BPSK	CSS	QPSK
Frequency	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Licensed LTE frequency bands
Bandwidth	100 Hz	250 kHz and 125 kHz	200 kHz
Maximum data rate	100 bps	50 kbps	200 kbps
Bidirectional	Limited / Half-duplex	Yes / Half-duplex	Yes / Half-duplex
Maximum messages/day	140 (UL), 4 (DL)	Unlimited	Unlimited
Maximum payload length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Interference immunity	Very high	Very high	Low
Authentication & encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Adaptive data rate	No	Yes	No
Handover	End-devices do not join a single base station	End-devices do not join a single base station	End-devices join a single base station
Localization	Yes (RSSI)	Yes (TDOA)	No (under specification)
Allow private network	No	Yes	No
Standardization	Sigfox company is collaborating with ETSI on the standardization of Sigfox-based network	LoRa-Alliance	3GPP

Tabla 12. Detalles técnicos de tecnologías LPWAN.

Escalabilidad y longitud de carga útil

El soporte de la gran cantidad de dispositivos es una de las características clave de Sigfox, LoRa y NB. Estas tecnologías funcionan bien con la creciente cantidad y densidad de dispositivos conectados. Se consideran varias técnicas para hacer frente a esta característica de escalabilidad, como la explotación eficiente de la diversidad en un canal, así como en el tiempo y el espacio. Sin embargo, NB ofrece la ventaja de una escalabilidad muy alta que Sigfox y LoRa. NB permite una conectividad de hasta 100K dispositivos finales por celda en comparación con 50K por celda para Sigfox y LoRa

Sin embargo, NB también ofrece la ventaja de la longitud de carga útil máxima. NB permite la transmisión de datos de hasta 1600 bytes. LoRa permite enviar un máximo de 243 bytes de datos. Por el contrario, Sigfox propone la longitud de carga útil más baja de 12 bytes, lo que limita su utilización en varias aplicaciones de IoT que necesitan enviar grandes tamaños de datos.

Cobertura y alcance de la red

La mayor ventaja de utilización de Sigfox es que una ciudad base puede cubrir una ciudad entera (es decir, un rango > 40 km). En Bélgica, un país con una superficie total de aproximadamente 30 500 km², el despliegue de la red Sigfox cubre todo el país con solo siete estaciones base.

Por el contrario, LoRa tiene un rango inferior (es decir, rango < 20 km) que requiere solo tres estaciones base para cubrir una ciudad entera como Barcelona. NB tiene el rango más bajo y las capacidades de cobertura (es decir, rango < 10 km). Se enfoca principalmente en la clase de dispositivos que se instalan en lugares alejados del alcance típico de las redes celulares. Además, el despliegue de NB se limita a las estaciones base LTE. Por lo tanto, no es adecuado para regiones rurales o suburbanas que no se benefician de la cobertura de LTE.

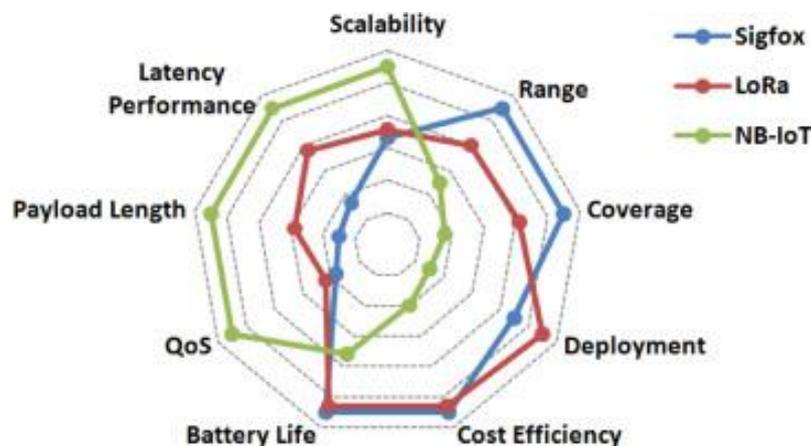


Figura 109. Ventajas de NB, LoRa y SigFox de cara a IoT.

Modelo de despliegue

Las especificaciones NB se publicaron en junio de 2016; por lo tanto, se necesitará tiempo adicional antes de que se establezca su red. Sin embargo, los ecosistemas de Sigfox y LoRa están maduros y ahora están bajo comercialización en varios países y ciudades. LoRa tiene la ventaja que le permite implementarse actualmente en 42 países frente a 31 países para Sigfox. Sin embargo, las implementaciones mundiales de LoRa y Sigfox todavía están en desarrollo.

Además, una ventaja significativa del ecosistema LoRa es su flexibilidad. A diferencia de Sigfox y NB, LoRa ofrece despliegue de red local, es decir, LAN que usa la puerta de enlace LoRa, así como la operación de red pública a través de estaciones base. En el campo industrial, se podría usar un modelo operativo híbrido para implementar una red local LoRa en áreas de fábrica y usa la red pública LoRa para cubrir las áreas externas.

Coste

Se deben considerar varios aspectos de coste, como el coste de espectro (licencia), el coste de despliegue/red y el coste del dispositivo. Atendiendo a la Tabla 6, es evidente que Sigfox y LoRa son más rentables en comparación con NB.

	Costo del espectro	Costo de despliegue	Costo del dispositivo final
Sigfox	Gratis	> 4000 € / estación base	<2 €
LoRa	Gratis	> 100 € / pasarela > 1000 € / estación base	3-5 €
NB-IoT	> 500 M € / MHz	> 15 000 € / estación base	> 20 €

Tabla 13. Diferentes costes de LoRa, NB y SigFox.

En conclusión, cada tecnología tendrá su lugar en el mercado de IoT. Sigfox y LoRa servirán como el dispositivo de menor coste, con un rango muy largo (alta cobertura), un tráfico de información pequeño y una vida útil muy larga de la batería. A diferencia de Sigfox, LoRa también servirá para el despliegue de la red local y la comunicación fiable cuando los dispositivos se mueven a altas velocidades. Por el contrario, NB servirá a los mercados de IoT de mayor valor que están dispuestos a pagar por una latencia muy baja y una alta calidad de servicio.

A pesar de las pruebas de las compañías de telefonía celular, la falta de implementaciones comerciales de NB deja abiertas las preguntas sobre la vida útil real de la batería y el rendimiento que puede alcanzar esta tecnología en condiciones reales. Finalmente, se espera que la comunicación móvil inalámbrica de 5ª generación (5G) proporcione los medios para permitir un mundo completamente conectado de personas y dispositivos para el año 2020, lo que llevaría a una solución global de LPWAN para aplicaciones de IoT.

REFERENCIAS

- [1] E. G. Carrasco, Estado del Arte en Tecnologías RFID, Madrid, 2009.
- [2] «<https://www.nxtiot.io/index.php/2018/11/29/lpwan-la-tecnologia-de-comunicacion-iot-de-mas-rapido-crecimiento/>,» [En línea].
- [3] «https://www.xatakamovil.com/conectividad/que-redes-lpwa-gran-canal-paralelo-al-5g-para-dispositivos-conectados,» [En línea].
- [4] S. D. Molinera, Sistema de localización mediante tecnología RFID, 2016.
- [5] «<https://www.by.com.es/blog/que-es-rfid/>,» [En línea].
- [6] M. M. Z. Tanim, How does passive RFID works, briefly explained, 2016.
- [7] «https://www.eetimes.com/document.asp?doc_id=1276306,» [En línea].
- [8] «<https://es.wikipedia.org/wiki/Interferencia>,» [En línea].
- [9] «https://www.eetimes.com/document.asp?doc_id=1276306&page_number=2,» [En línea].
- [10] «<http://ftp.it.murdoch.edu.au/units/ICT219/Papers%20for%20transfer/Passive%20RFID%20Basics.pdf>,» [En línea].
- [11] «https://www.gs1.org/sites/default/files/docs/epc/uhfclg2_2_0_0_standard_20131101.pdf,» [En línea].
- [12] «<https://www.fqingenieria.com/es/conocimiento/estandares-y-regularizaciones-para-rfid-36>,» [En línea].
- [13] «<https://www.ecma-international.org/publications/standards/Ecma-340.htm>,» [En línea].
- [14] «<https://bitexperts.com/Question/Detail/3360/difference-between-iso-14443-and-iso-18092-i-e-rfid-vs-nfc>,» [En línea].
- [15] «https://es.wikipedia.org/wiki/C%C3%B3digo_de_barras#Historia,» [En línea].
- [16] «<http://www.codigosdebarraonline.com/historia-codigo-de-barras>,» [En línea].
- [17] C. H. Prieto, Nuevas Estrategias para el Diseño de Sistemas Chipless-RFID y Aplicaciones, 2018.
- [18] «<https://www.evaluandoerp.com/comparacion-tecnologias-rfid-codigo-barras/>,» [En línea].
- [19] «<http://www.rfidpoint.com/que-es-rfid/rfid-vs-codigo-de-barras/>,» [En línea].
- [20] «https://es.wikipedia.org/wiki/Lector_de_c%C3%B3digo_de_barras#C%C3%B3mo_se_leen_los_c%C3%B3digos_de_barras,» [En línea].

- [21] «<https://www.fqingenieria.com/es/conocimiento/ventajas-de-la-tecnologia-rfid-versus-el-codigo-de-barras-82>,» [En línea].
- [22] «https://es.wikipedia.org/wiki/Near_field_communication,» [En línea].
- [23] «<https://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve>,» [En línea].
- [24] «https://www.redeszone.net/2019/03/31/diferencias-nfc-rfid/?utm_source=related_posts&utm_medium=widget,» [En línea].
- [25] «<https://www.sciencedirect.com/science/article/pii/S2405959517302953>,» [En línea].
- [26] «<https://pandorafms.com/blog/es/que-es-lpwan/>,» [En línea].
- [27] «<https://medium.com/beelan/haciendo-iot-con-lora-cap%C3%ADtulo-1-qu%C3%A9-es-lora-y-lorawan-8c08d44208e8>,» [En línea].
- [28] «<https://blog.330ohms.com/2017/05/11/que-es-sigfox-y-como-funciona/>,» [En línea].
- [29] «<https://accent-systems.com/es/nb-iot/>,» [En línea].
- [30] «https://en.wikipedia.org/wiki/Narrowband_IoT,» [En línea].
- [31] «https://es.wikipedia.org/wiki/Teorema_de_reciprocidad,» [En línea].
- [32] «https://es.wikipedia.org/wiki/Banda_base,» [En línea].
- [33] «https://www.ecured.cu/Modulaci%C3%B3n_ASK,» [En línea].
- [34] «<https://es.wikipedia.org/wiki/Circulador>,» [En línea].
- [35] «<https://es.wikipedia.org/wiki/3GPP>,» [En línea].
- [36] «<https://www.areatecnologia.com/tecnologia/lte.html>,» [En línea].
- [37] «<https://es.wikipedia.org/wiki/VSWR>,» [En línea].
- [38] «https://es.wikipedia.org/wiki/Universal_Asynchronous_Receiver-Transmitter,» [En línea].
- [39] «https://es.wikipedia.org/wiki/Frecuencia_modulada_pulsada,» [En línea].

