UTN FACULTAD REGIONAL MENDOZA
UNIVERSIDAD TECNOLÓGICA NACIONAL

CÁTEDRA DE PROYECTO FINAL - INGENIERÍA EN ELECTRÓNICA

COMUNICADOR ALARMA DOMICILIARIA MEDIANTE LORAWAN

CADLW

PROYECTO

Versión *1.0*

22 abr 2024

INFORMACIÓN DEL PROYECTO

Autor	
Nombre Completo del integrante	Alvaro Ernesto Giunta Ferraris
Legajo	42693
e-mail	alvaro.giunta@alumnos.frm.utn.edu.ar

Tutor	Ing. Gustavo Mercado
Director	Ing. Gustavo Mercado
Jurado	Ing. Gustavo Mercado
Año Académico	2023
Responsable de la cátedra	Ing. Ana Lattuca

Empresa / Cliente / Laboratorio	Gisis S.A.
Patrocinador (Sponsor)	Gisis S.A.

1 Resumen del proyecto

1.1 Resumen

Los sistemas de seguridad hogareños monitoreados han sufrido una serie de renovaciones tecnológicas en cuanto a la tecnología disponible para realizar la comunicación de los reportes.

Estos recambios tecnológicos son impulsados por la necesidad de mantener un medio de comunicación fiable, de modo que se pueda brindar un servicio de seguridad basándose en estos.

El presente proyecto consiste en elaborar un medio de comunicación alternativo, confiable y seguro para la conexión de una estación de monitoreo remota de alarmas domiciliarias a través de una red LPWAN.

El mismo tiene un carácter de prototipo, ya que el objetivo es determinar si este tipo de redes son una solución viable ya que no se encuentran disponibles implementaciones comerciales.

En caso de obtenerse resultados satisfactorios, los resultados obtenidos servirán como base en un desarrollo e implementación a mayor escala.

1.2 Summary

Monitored home security systems have undergone a series of technological renovations in terms of the technology available for reporting communication.

These technological changes are driven by the need to maintain a reliable means of communication, so that a security service can be provided based on them.

The present project consists of developing an alternative, reliable and secure means of communication for the connection of a remote home alarm monitoring station through a LPWAN network.

It has a prototype character, since the objective is to determine if this type of networks are a viable solution since commercial implementations are not available.

If satisfactory results are obtained, the results obtained will serve as a basis for a larger scale development and implementation.

2 Palabras claves

LoRaWAN, Monitoreo de Alarma, Comunicador, LPWAN, Wireless, IoT.

3 Índice

4 Introducción

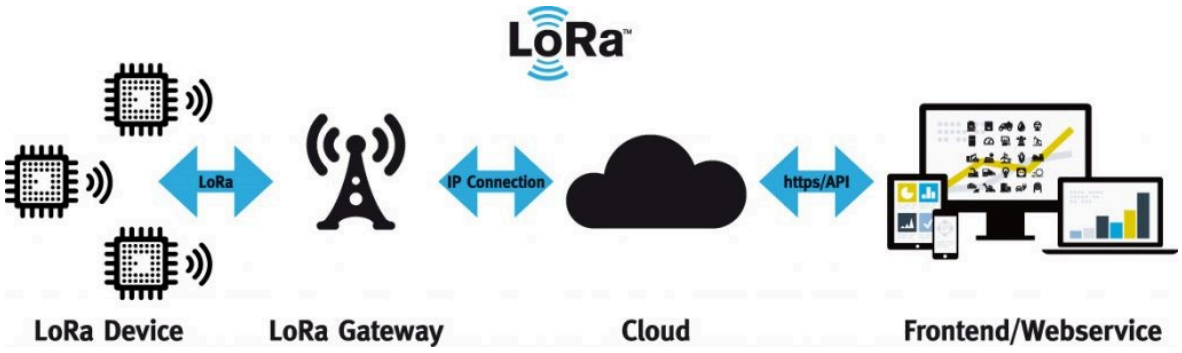
4.1 Idea y descripción del proyecto

La idea del proyecto surgió debido a las reiteradas problemáticas con los proveedores de red, tanto fijas como móviles, por motivos tan diversos como económicos, tecnológicos, de cobertura, etc.

La misma consistió en el desarrollo de un sistema de comunicación alternativo para el monitoreo remoto de alarmas domiciliarias, de modo tal de posibilitar la independencia de otros proveedores de red.

Luego de una investigación, se encontró con una novedosa tecnología denominada LPWAN (Low Power Wide Area Network) y una de sus variantes LoRaWAN.

LoRa se basa en la modulación chirp de espectro ensanchado, que tiene características de baja potencia como la modulación FSK, pero se puede utilizar para comunicaciones de largo alcance. Se puede utilizar para conectar sensores, puertas de enlace, máquinas, dispositivos, animales, personas, etc. de forma inalámbrica a la nube, operando en la banda ISM. LoRaWAN es un protocolo de red de área amplia y baja potencia (LPWAN) desarrollado por LoRa Alliance, que conecta de forma inalámbrica 'cosas' que funcionan con baterías a Internet en redes regionales, nacionales o globales, apuntando a requisitos clave de Internet de las cosas.



LoRa es la capa física, y LoRaWAN es la capa MAC, es decir, el software que se coloca en el chip para permitir la creación de redes.

La compañía desarrolladora de la tecnología es Semtech y tiene la ventaja de que muchos entusiastas comparten código y librerías de código abierto además de tener una academia para desarrolladores. Incluso existe una amplia comunidad y disponibilidad de información para ayudar a solucionar problemas.

4.1.1 Objetivo general

El objetivo general por parte de la empresa solicitante es solucionar de forma permanente las múltiples problemáticas que arrastra el mecanismo actual de reporte y comunicaciones.

Como objetivo futuro, si los resultados de este proyecto resultan satisfactorios, se buscará la implementación de este sistema en la mayoría de los abonados y clientes, llegando a instalar y mantener su propia red de comunicaciones.

4.1.2 Objetivo particular

Se buscó probar y validar un mecanismo de transmisión de los reportes de las alarmas monitoreadas.

Con este objetivo se utilizaron microcontroladores, módulos de radio, infraestructura de red y otros tipos de equipo electrónico que fueron necesarios para desarrollar un prototipo funcional del comunicador.

En particular, se realizó el trabajo sobre sistemas de alarma marca DSC, debido a los requerimientos por parte del solicitante del proyecto.

Además se tuvo que generar un mecanismo para notificar las alertas recibidas que sea compatible con el software instalado actualmente en los sistemas de la empresa solicitante.

4.2 Justificación del proyecto

4.2.1 Antecedentes del proyecto

El proyecto surge como respuesta a la necesidad específica del solicitante de migrar las comunicaciones a un método inalámbrico, de modo que se reporte el estado de alarma marca DSC.

Los sistemas de comunicaciones utilizados en este rubro han pasado por una serie de recambios generacionales, en sus orígenes se utilizaba el sistema telefónico fijo (con DTMF) para comunicar las alertas y alarmas. El avance tecnológico y las innovaciones en comunicación celular brindó la posibilidad de utilizar un sistema inalámbrico, cuyo máximo exponente se vio en la tecnología GPRS.

4.2.2 Estado actual

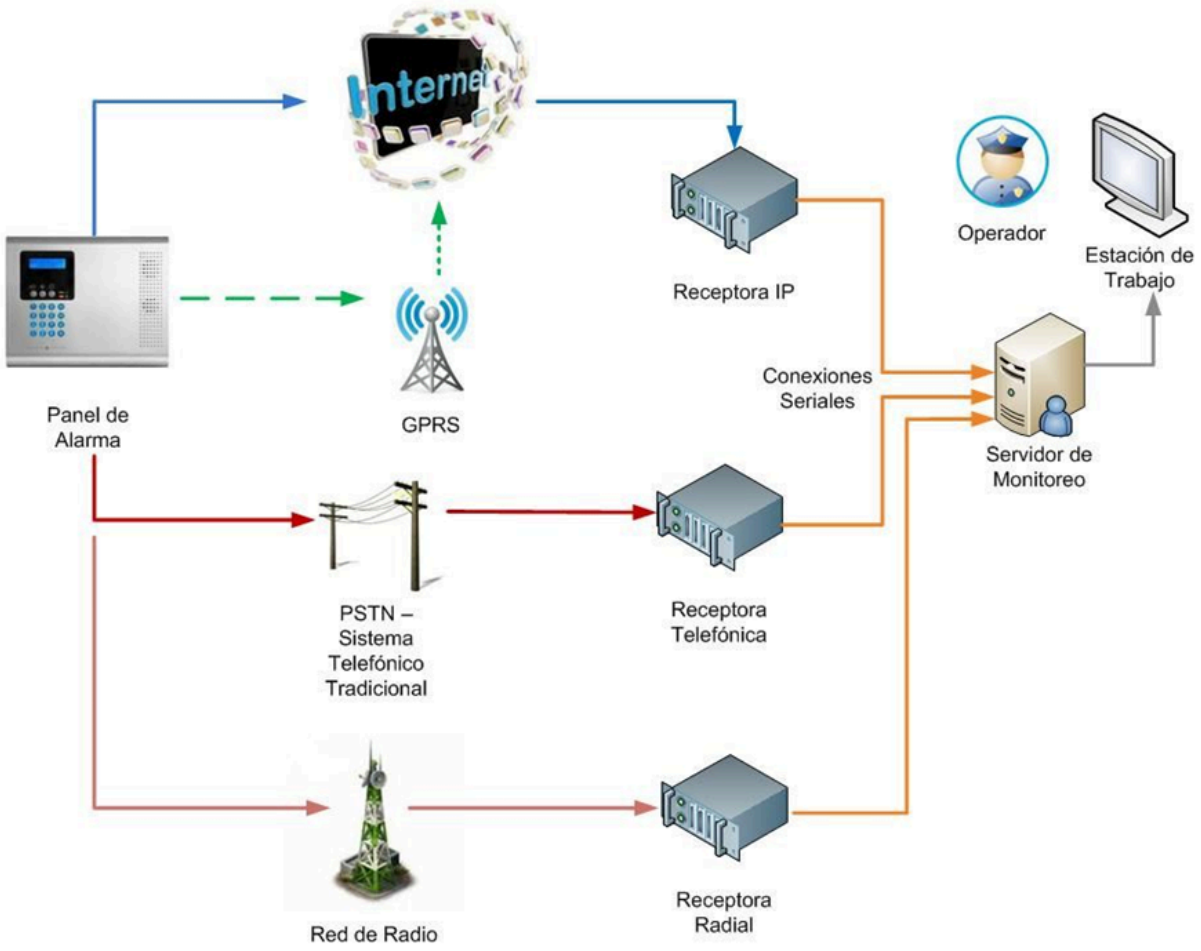
Debido a la extensa trayectoria y años en el rubro, la empresa cuenta con capacidad de recibir reportes por multiples metodos:

- Utilizando la línea telefónica
- Utilizando comunicaciones inalámbricas GPRS (2G)
- Utilizando conexiones de internet

Entre estas alternativas, las dos primeras mencionadas se encuentran en una situación crítica, pues aunque sus características son satisfactorias para esta aplicación en particular, son tecnologías antiguas que han caído en el desuso y tienen múltiples problemas de cobertura y mantenimiento.

Por otro lado, el uso de conexiones de internet resulta poco confiable en muchos lugares, debido a los reiterados cortes en el servicio producto del robo de cables y equipamiento.

Sin embargo, el uso de conexiones a internet es la tendencia del mercado mundial en cuanto al monitoreo y reporte de alertas.



4.2.3 NECESIDAD DEL NEGOCIO Y DEFINICIÓN DEL PROBLEMA

A continuación puede observarse un resumen de las características entregado por el solicitante del proyecto:

GiSIS INTEGRANDO TECNOLOGIAS

Sr. Alvaro Giunta

En función del recambio tecnológico de las telecomunicaciones y el deterioro creciente de los medios actualmente utilizados, se le solicita investigar y desarrollar un método alternativo y confiable para dar conectividad a los sistemas de seguridad que confluyen en nuestra estación de monitoreo.

El proyecto a realizar deberá cumplir con los siguientes requisitos mínimos:

1- Migrar las comunicaciones telefónicas actuales a métodos inalámbricos.

2- Obtener el estado del sistema de alarmas marca DSC ya que son las más utilizados por nuestra empresa, a fin de comunicar los reportes correspondientes.

3- Se recomienda para dichos reportes el uso de un protocolo estándar como CONTACT ID o SIA.

4- Integrar los reportes recibidos con el software de monitoreo utilizado actualmente en nuestra empresa.

5- Utilizar un vínculo radial de largo alcance y bajo consumo, de ser posible de protocolo abierto y estandarizado. Como objetivos principales debe ser seguro, encriptado y debe trabajar en frecuencias sin licenciamiento, además de garantizar el envío/recepción sin errores.

6- Debe ser Full Data, es decir debe enviar todos los reportes del sistema de alarmas. Esto incluye reportes de activación, desactivación, emergencias, supervisiones y fallas.

7- Se debe prever la posibilidad de realizar comunicación dúplex, es decir poder programar y controlar los paneles remotamente.

GiSIS bunker alarnet
Tels (261) 4325859 - 4323714
info@gisis.com.ar
www.gisis.com.ar
Av. Juan Francisco Cobos 1530
Dorrego - Guaymallén - Mendoza
(5519) Argentina

La implementación de un comunicador LoRaWAN satisface los requisitos solicitados.

4.2.4 Beneficios del proyecto

Debido a que el objetivo de este proyecto no es la comercialización, sino la investigación y análisis de viabilidad, los beneficios que se obtendrán no serán económicos, sino en pos del conocimiento.

A través de este proyecto podremos obtener un método de comunicación y monitoreo de sistemas significativamente más económico si se compara con alternativas actuales disponibles, además de la posibilidad de extrapolar los resultados obtenidos y utilizarlos en otros sistemas de requerimientos similares.

Por otro lado, se deja de lado las soluciones comerciales cerradas que imposibilitan la modificación y/o replicación. Con este sistema, al ser diseñado y desarrollado íntegramente es factible la modificación a gusto según el criterio lo crea conveniente, permitiendo una adaptabilidad muy elevada.

Lo mencionado anteriormente nos describe un sistema que tendrá múltiples beneficios futuros, ya que los conocimientos que se busca obtener en el desarrollo del mismo pueden ser aplicados en una amplia gama de ámbitos. Sumado a esto se espera el desarrollo de dispositivos económicamente viables por parte de la empresa solicitante, siendo este el objetivo principal que persigue la misma.

4.3 Alcance

El prototipo desarrollado se compone de un nodo final, el cual se encarga de determinar las alarmas y alertas que suceden y reportarlos al servidor de monitoreo. Para lograr esta notificación, los datos se transmiten de forma inalámbrica utilizando el protocolo LoRaWAN hacia una puerta de enlace (Gateway) que es la encargada de enviar la información al servidor de red. El programa de integración con el software de monitoreo se encuentra permanentemente conectado al servidor de red para obtener las alertas e introducirlas al sistema de monitoreo final.

4.3.1 Alcance

El proyecto a cumple con los siguientes requisitos:

- Migrar las comunicaciones telefónicas actuales a métodos inalámbricos.
- Obtener el estado del sistema de alarmas marca DSC a fin de comunicar los reportes correspondientes.
- Uso de un protocolo estándar CONTACT ID.
- Integra los reportes recibidos con el software de monitoreo utilizado actualmente en la empresa.
- Utiliza un vínculo radial de largo alcance y bajo consumo, de ser posible de protocolo abierto y estandarizado. Cumple las características de: ser seguro, encriptado y trabajar en frecuencias sin licenciamiento, además de garantizar el envío/recepción sin errores.
- Es Full Data, es decir envía todos los reportes del sistema de alarmas. Esto incluye reportes de activación, desactivación, emergencias, supervisiones y fallas.

4.3.2 Límites o fuera de alcance

La implementación realizada es del tipo prototipo, es decir que no se realizó la red completa sino un dispositivo terminal, que sirve de paso previo a la implementación final de la red.

La justificación de este límite es por sobre todas las cosas económica, no dispongo desde el inicio del capital necesario para la compra de los equipos necesarios para montar una red completa y dar servicio a la totalidad de los clientes.

Se busca principalmente verificar la viabilidad de la comunicación de forma fiable y segura que podría dar lugar a su implementación real,

4.3.3 Soluciones y entregables principales

La siguiente tabla muestra un listado de los entregables del proyecto (productos o servicios)

Entregables principales	Descripción del entregable
Prototipo funcional módulo DSC-LoRa	Dispositivo capaz de conectarse con la alarma y realizar envió de datos a través de la modulación LoRa
Documentación	Engloba todos los documentos requeridos por la cátedra, antes, durante y después del desarrollo

4.4 Planificación del proyecto

La planificación del proyecto está representada en las siguientes etapas:

Etapas	Duración
1. Etapa de análisis y planificación	75 horas
2. Etapa de diseño	50 horas
3. Etapa de desarrollo	180 horas
4. Etapa de pruebas	120 horas
5. Cierre de proyecto	45 horas
Duración total	570 horas

4.4.1 Cronograma

Meses	1				2				3				4				5				6				7				8				9				10				11				12			
Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Horas acumuladas	015	030	045	060	075	090	105	120	135	150	165	180	195	210	225	240	255	270	285	300	315	330	345	360	375	390	405	420	435	450	465	480	495	510	525	540	555	570	585	600	615	630	645	660	675	690	705	720
Etapa	Análisis 75 hs				Diseño 150 hs								Desarrollo 180 hs																Pruebas 120 hs								Cierre 45 hs											

4.4.2 Hitos

A continuación se muestra un listado de hitos generales del proyecto y el cronograma estimado de finalización:

- Etapa de análisis y planificación

  Dentro de esta etapa podemos identificar los siguientes hitos:

  1. Entrega de documentos relacionados a la cátedra: acta de inicio, EDT, etc, en las fechas solicitadas
  2. Definición de especificaciones y metas y estructurado general de la solución. Se entregó un pre-proyecto a fin de semestre que refleje ese contenido.
  3. El acontecimiento clave de esta etapa fue el estructurado general de la solución, que se realizó en la semana 5.

- Etapa de diseño

  Dentro de esta etapa podemos identificar los siguientes hitos:

  1. Diseño funcional y técnico del módulo, se realizó en la semana 9.
  2. Diseño de cobertura, se realizó en la semana 13.
  3. Diseño de pruebas de control y criterios de éxito, se realizó en la semana 15.

- Etapa de desarrollo

Dentro de esta etapa podemos identificar los siguientes hitos:

1. Desarrollo del hardware y las placas electrónicas relacionadas, se realizó en la semana 19.
2. Desarrollo de software necesario, se realizó en la semana 24.
3. Desarrollo de comunicaciones, se realizó en la semana 27.

- Etapa de pruebas

  Dentro de esta etapa podemos identificar los siguientes hitos:

  1. Correcto funcionamiento del hardware, se realizó en la semana 29.
  2. Correcto funcionamiento del software, se realizó en la semana 31.
  3. Correcto funcionamiento de las comunicaciones, se realizó en la semana 33.
  4. Correcto funcionamiento integral y su ajuste según especificaciones, se realizó en la semana 35.

- Etapa de cierre de proyecto

  Dentro de esta etapa podemos identificar los siguientes hitos:

  - Completar la documentación, se realizó en la semana 38.

4.5 Riesgo

			GRAVEDAD (IMPACTO)				
			MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
			1	2	3	4	5
APARICIÓN (probabilidad)	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

	Aparición (Probabilidad)	Gravedad (Impacto)		
Disponibilidad de módulos para los respectivos sistemas embebidos.	4	5	20	Riesgo muy grave
Cambios en los requisitos.	3	4	12	Riesgo importante
Plazos de entrega de proveedores.	2	5	10	Riesgo importante
Problemas de presupuesto.	1	5	5	Riesgo apreciable

Riesgo	Mitigación
Disponibilidad de módulos para los respectivos sistemas embebidos	En caso faltante de alguna tecnología seleccionada, se optará por alguna alternativa.
Plazos de entrega de proveedores.	Se buscarán proveedores alternativos.
Problemas de presupuesto	En caso de problemas de presupuesto, se recurrirá a financiación propia.
Cambios en los requisitos	Se establecerá un periodo de tiempo para reunirse con el solicitante del proyecto, y revisar requisitos.

5 Desarrollo del proyecto

5.1 Desarrollo técnico

5.1.1 Introducción

El siguiente informe es una explicación de lo investigado y realizado en el proyecto “Comunicador de alarma domiciliaria mediante LoRaWAN”, en el mismo se detalla no solo un pantallazo actual de los sistemas de alarma, sino también de comunicaciones LPWAN, luego se analizan los objetivos y características a los que el proyecto apunta satisfacer. Una vez aclarado esto, se comienza con la descripción del trabajo realizado, siguiendo un orden lógico, para luego analizar teóricamente las capacidades de cobertura y conclusiones del mismo.

Si bien el informe presentado aquí es suficiente para entender lo realizado, se recomienda la lectura previa de los archivos adjuntos (que no son incluidos en este informe por su extensión) a fin de entender la justificación en la toma de decisiones realizadas y la complejidad de análisis en cada caso. Entre estos archivos se encuentran: manual de usuario e instalación de paneles DSC, manual de usuario e instalación de comunicador DSC, manual de usuario e instalación de comunicador alternativo, estándar de protocolos de reporte y comunicación DC-09, DC-07 y Contact ID (DC-05) y paquete de especificaciones LoRaWAN de LoRa Alliance.

5.1.2 Estado actual

5.1.2.1 Sistemas de alarmas y comunicación de reportes

Los sistemas de alarmas domiciliarias tienen como objetivo la disuasión y prevención de hechos ilícitos, además de alertar y comunicar situaciones de emergencia, tanto médicas como relacionadas con incendios. Para dicho fin estos equipos incluyen una serie de características que nombraremos a continuación, con un enfoque en la marca DSC PowerSeries que será la utilizada en este proyecto.

Como características principales de los paneles podemos mencionar:

- Zonas: son los sensores que permiten identificar una posible situación de emergencia. Las zonas deben ser programadas para establecer su funcionamiento, podemos mencionar, por ejemplo, zonas con retardo de entrada, instantáneas, 24 horas, pánico, emergencia médica, etc. La cantidad de zonas depende del modelo del panel utilizado, llegando hasta un máximo de 64. Las zonas pueden ser supervisadas o no, permitiendo detectar fallas y/o intentos de sabotaje en las mismas.

- Usuarios: son las claves de acceso que permiten activar o desactivar el sistema. La cantidad de usuarios / códigos depende del modelo del panel utilizado, llegando hasta un máximo de 95. Existen 4 tipos de códigos (todos son 4 dígitos numéricos):

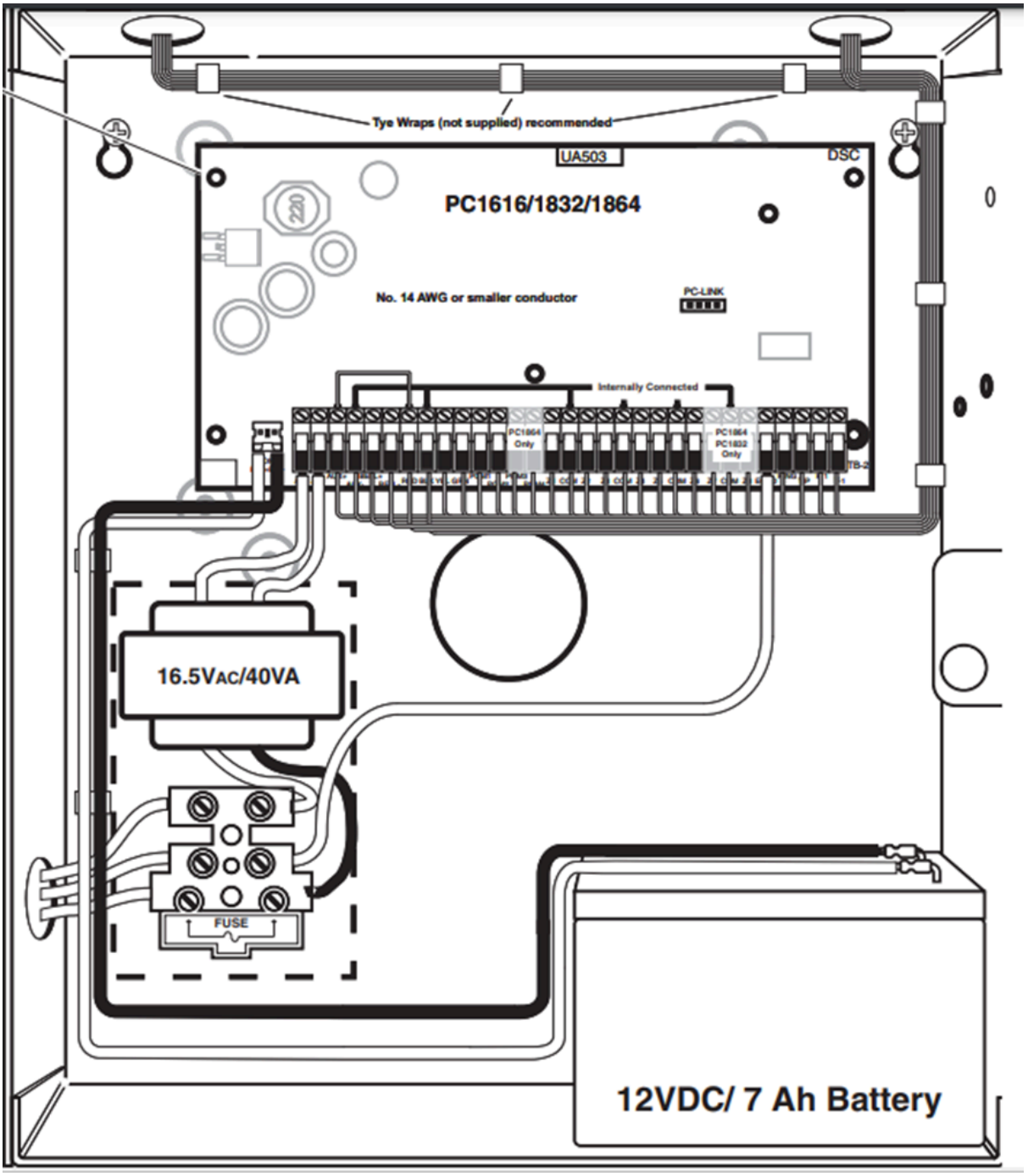
- El código maestro (código número 40) que permite acceder a la configuración del usuario, dar de alta nuevos códigos y activar/desactivar cualquier partición.
- Los códigos de asalto (típicamente el número 33) que, si bien activan/desactivan el sistema, envían además un reporte de asalto a la estación de monitoreo.
- El código de instalador que permite acceder a la configuración del sistema, pero no activar/desactivar el mismo.
- Los códigos generales, que permiten activar/desactivar una partición.

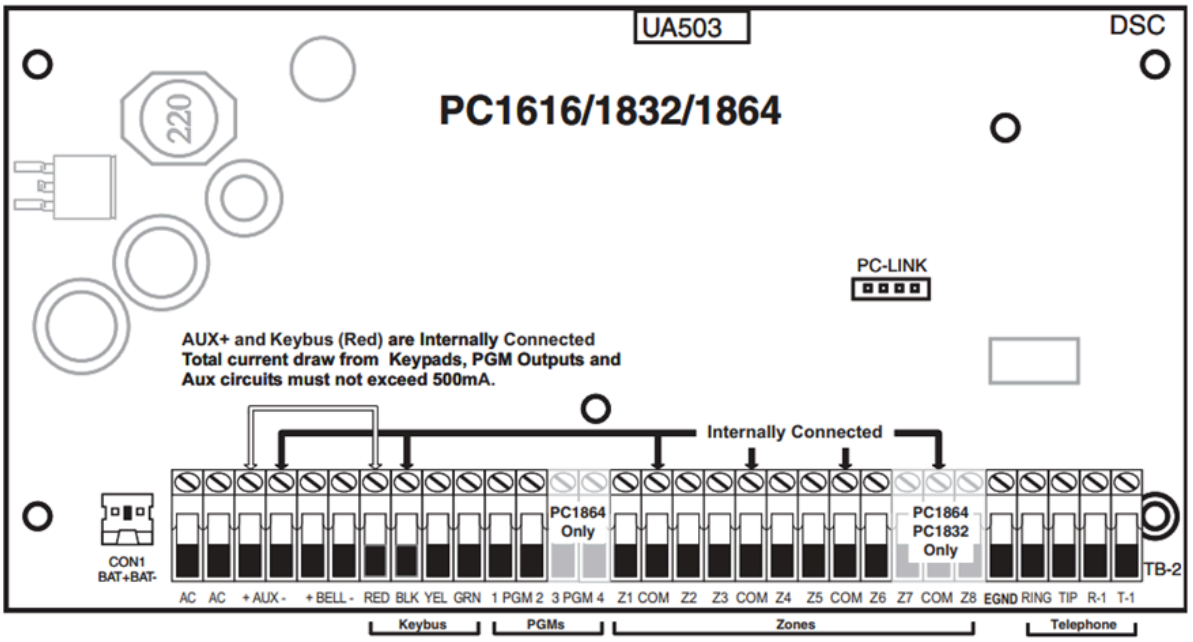
· Particiones: son sistemas de alarma independientes entre sí, pero dentro de un mismo panel. De esta forma se permite que un grupo de zonas y usuarios se asigne a una determinada partición y se pueda operar cada una de ellas independientemente. La cantidad de particiones depende del modelo del panel utilizado, llegando hasta un máximo de 8.

· Módulos: los módulos son hardware que permiten agregar funcionalidades extra al sistema. Podemos mencionar entre estos a los teclados, expansores de zonas, fuentes de alimentación, salidas programables, receptores inalámbricos, comunicador inalámbrico, entre otros. Los mismos son supervisados, por lo que en caso de falla se enviará un reporte y se mostrará una alerta en el teclado. Los módulos se conectan al panel central a través de un bus de datos de 4 hilos, que provee la alimentación necesaria para su funcionamiento (a excepción de las fuentes de alimentación).

El funcionamiento general de un sistema de alarma es ampliamente conocido, si una partición está armada (“activada”) y una o más de sus zonas fueran abiertas, el panel se dispara y activa una salida audible (bocina o sirena) y, en caso de estar configurado, envía un reporte de alerta. La condición de disparo se mantiene hasta que un usuario ingrese un código válido de desactivación. Además, en el teclado se indica el evento sucedido a través de una serie de LEDs o una pantalla LCD (según el modelo).

Cabe destacar que estos paneles son muy versátiles ya que permiten un alto nivel de programación y personalización, con más de 500 atributos diferentes (que no tiene sentido describir aquí). Puede encontrarse más información en el manual de instalación y usuario del panel.





Esquema - Panel DSC PowerSeries – Modelos PC1616/1832/1864

Los paneles permiten, además de dar alerta a través de una sirena y/o teclados, enviar reportes a una estación de monitoreo de alarmas. De esta forma una persona se encarga de analizar cada situación y dar aviso al cliente o al 911 en caso de ser necesario. Un comunicador es un dispositivo, que puede estar integrado o no al panel, y que permite el envío de reportes a través de un determinado medio.

Los sistemas de alarma tienen múltiples formas de comunicación, dependiendo de la marca y la calidad, pueden hacerlo mediante el sistema telefónico tradicional, internet (tanto GPRS como por conexiones cableadas) y sistemas de radio, aunque este es utilizado en aplicaciones muy específicas que requieran de un canal exclusivo.

En la actualidad es posible ver una gran variedad en cuanto a los medios de comunicación y los formatos utilizados, sin embargo, la gran mayoría se divide entre telefonía fija tradicional y GPRS.

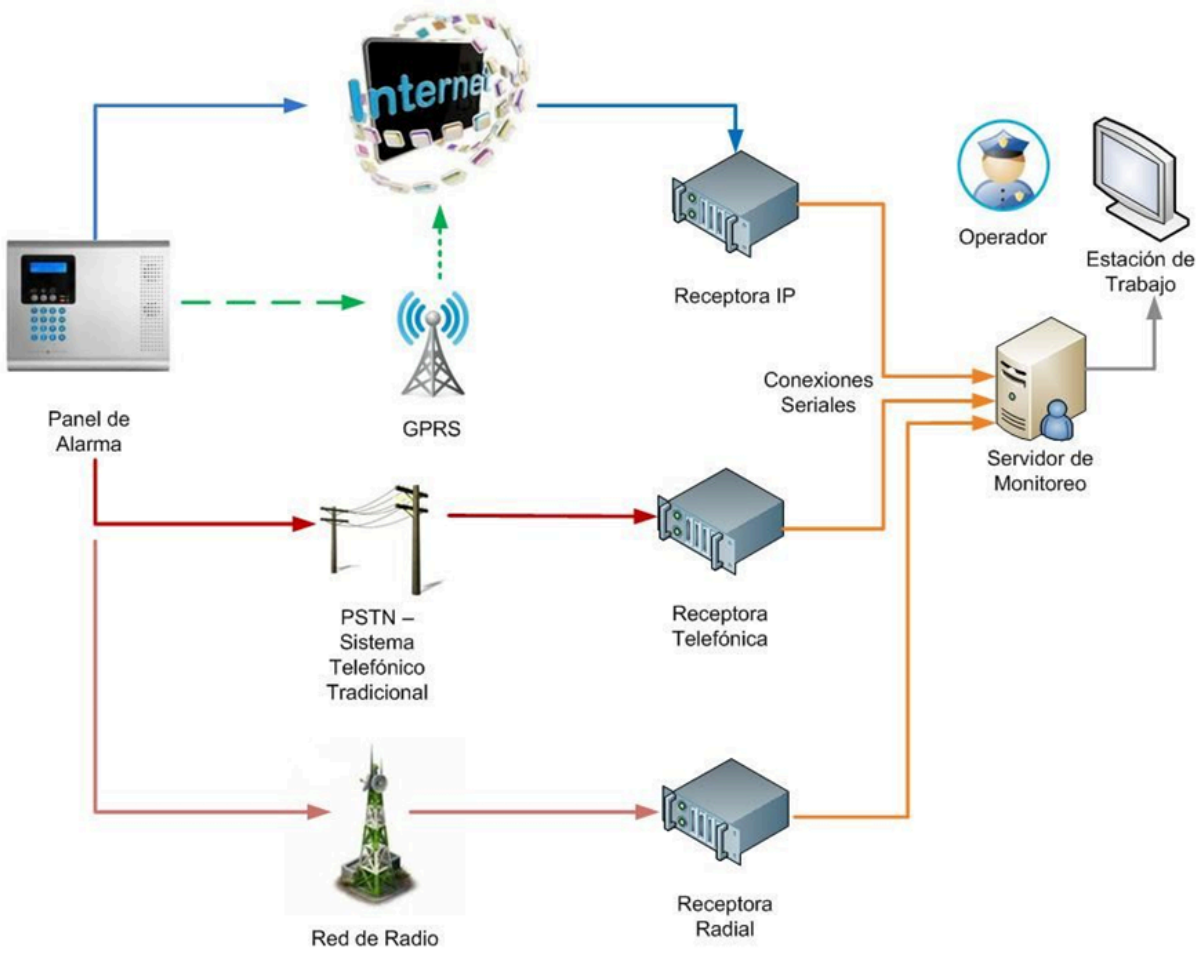
Existe una amplia oferta de comunicadores para los sistemas de alarma, ya que además de los propios de cada marca se pueden encontrar comunicadores universales (funcionan con varias marcas) aunque tienen una performance inferior.

Existen dos clases de comunicadores:

- Ø Por un lado, los comunicadores que se conectan a los buses de datos de los sistemas de alarma (Terminales KEYBUS - RED, BLK, YEL y GRN), y son generalmente fabricados por la misma marca[1][2] y tienen funcionalidades extendidas, ya que permiten realizar cambios de programación, activaciones y desactivaciones remotas, pedir el estado del sistema, etc. Tiene prestaciones superiores pero el precio es generalmente más elevado.

- Ø Por otro lado, los comunicadores que se conectan a la línea telefónica (Terminales TIP-RING del panel), son generalmente comunicadores universales y su funcionamiento se basa en hacerle creer al sistema de alarma que está conectado por teléfono cuando en realidad no lo está. Este tipo de comunicadores son más limitados, ya que solo son capaces de transmitir reportes y no aportan la posibilidad de programación, activación y desactivación remota, sin embargo, el precio suele ser inferior.

Cabe destacar que cada marca de comunicador tiene su propia receptora de señales, la cual se encarga de atender los eventos de las alarmas, confirmar su recepción y decodificarlos; para luego enviarlos a un servidor / software de monitoreo donde un operador atiende la situación de alerta. Existen además unos determinados estándares sobre el formato de la comunicación, entre los más difundidos podemos encontrar Contact ID y SIA.



Esquema – Medios de comunicación usados

5.1.2.2 REDES LPWAN

Una red de área amplia de baja potencia (red LPWAN o LPWA) es un tipo de red de área amplia de telecomunicaciones inalámbricas diseñada para permitir comunicaciones de largo alcance a una tasa de bits baja entre cosas (objetos conectados), como sensores que funcionan con una batería. La baja potencia, la baja tasa de bits y el uso previsto distinguen a este tipo de red de una WAN inalámbrica que está diseñada para conectar usuarios o empresas y transportar más datos con más energía. La velocidad de datos de LPWAN oscila entre 0,3 kbit/s y 50 kbit/s por canal.

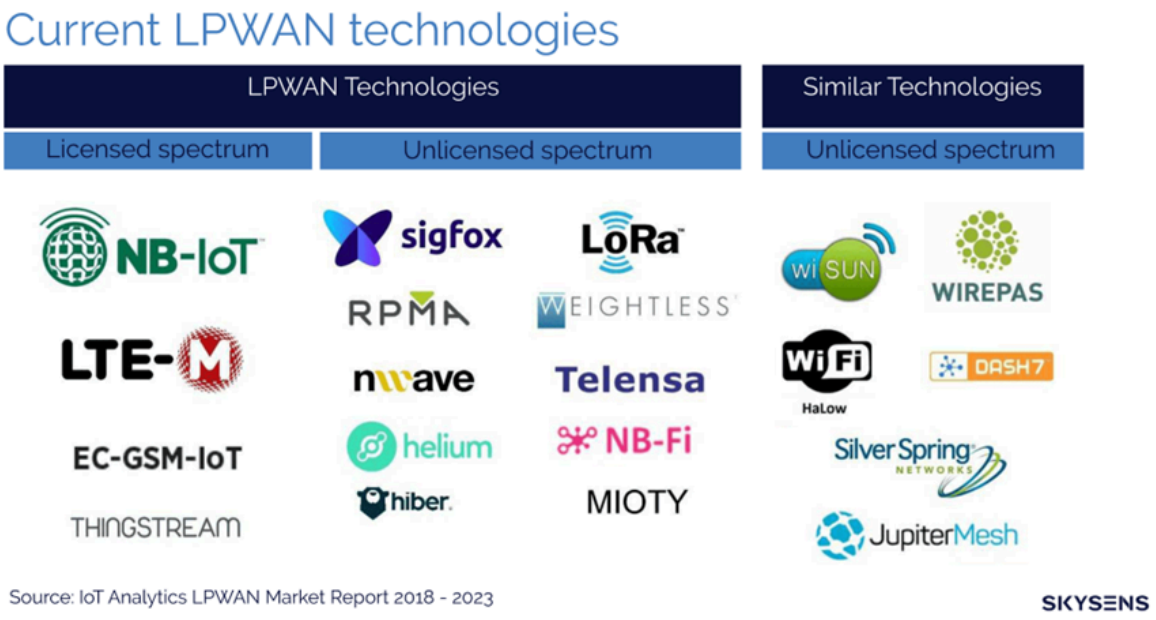
Como características principales podemos mencionar:

· Largo alcance: el alcance operativo de la tecnología LPWAN varía desde unos pocos kilómetros en áreas urbanas hasta más de 10 km en entornos rurales. También puede

permitir una comunicación de datos eficaz en ubicaciones interiores y subterráneas que antes eran inviables.

· Bajo consumo de energía: optimizados para el consumo de energía, los transceptores LPWAN pueden funcionar con baterías pequeñas y económicas hasta por 20 años.

· Bajo costo: los protocolos livianos y simplificados reducen la complejidad en el diseño de hardware y en los costos de los dispositivos. Su largo alcance combinado con una topología en estrella simplifica la infraestructura, y el uso de bandas sin licencia o con licencia reduce los costos de la red.



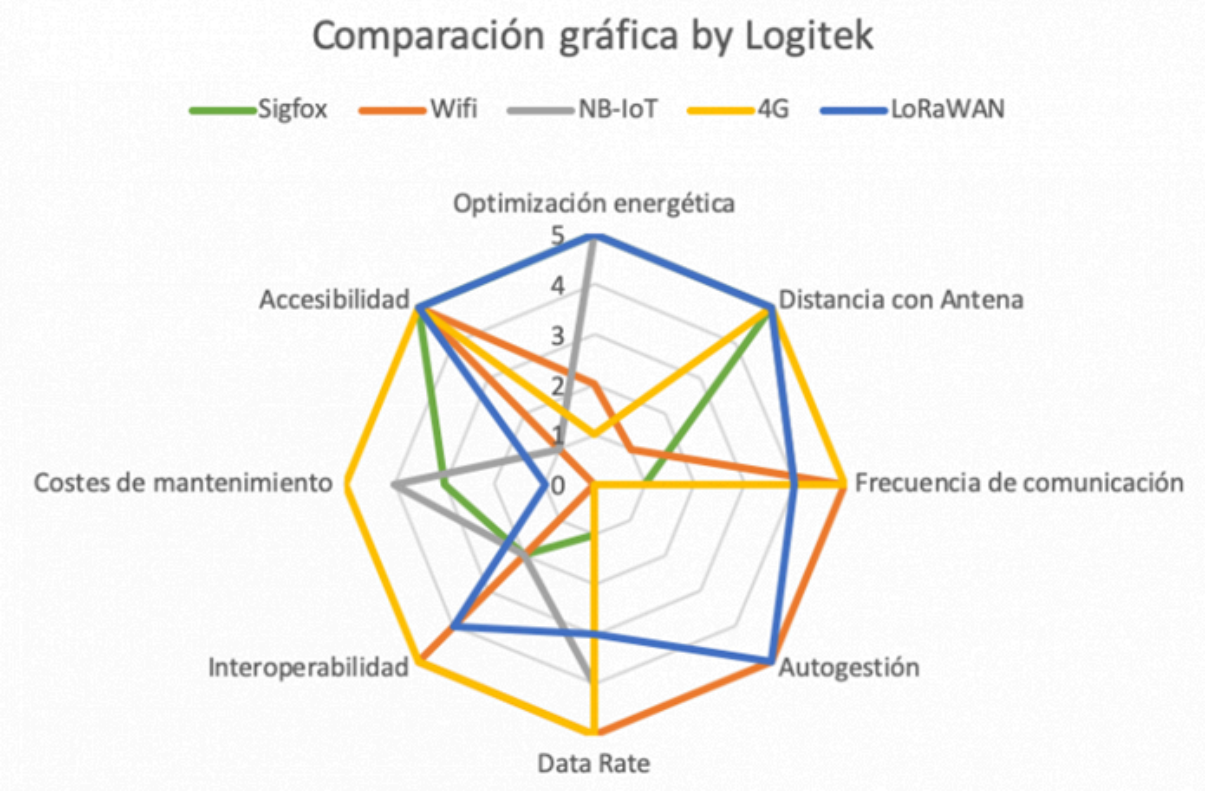
Entre las tecnologías LPWAN podemos mencionar (Apéndice A: tabla comparativa de características técnicas):

§ Sigfox: Sigfox es una tecnología LPWAN de operador, es decir, existe una compañía llamada Sigfox que se ha encargado de desplegar una infraestructura de grandes antenas da cobertura a todo el territorio. Cualquier dispositivo puede, pagando una suscripción, utilizar esta red para la transmisión de sus datos siempre que se cumplan las normas de uso establecidas por Sigfox. Como operador, ofrece no solo la red y su mantenimiento, sino que también deja disponibles en su backend (accesible vía API) los datos enviados

por los nodos. En un sistema que utilice Sigfox, los datos siempre pasan por su infraestructura.

§ LoRaWAN: LoRaWAN es un estándar desarrollado sobre la modulación radio LoRa. Si bien es cierto que puede ser una red de operador ofrecida por varias compañías en un mismo territorio, lo interesante de LoRaWAN es que, a diferencia de las demás LPWAN, permite el despliegue de redes propias autogestionadas. Este hecho abre un gran abanico de posibilidades para realizar iniciativas IoT de ámbito local para control de áreas pequeñas o medianas. Evidentemente requieren conocer un poco más técnicamente la tecnología y tener que gestionar la red, pero permite montar redes en cualquier lugar y unos costos de mantenimiento menores.

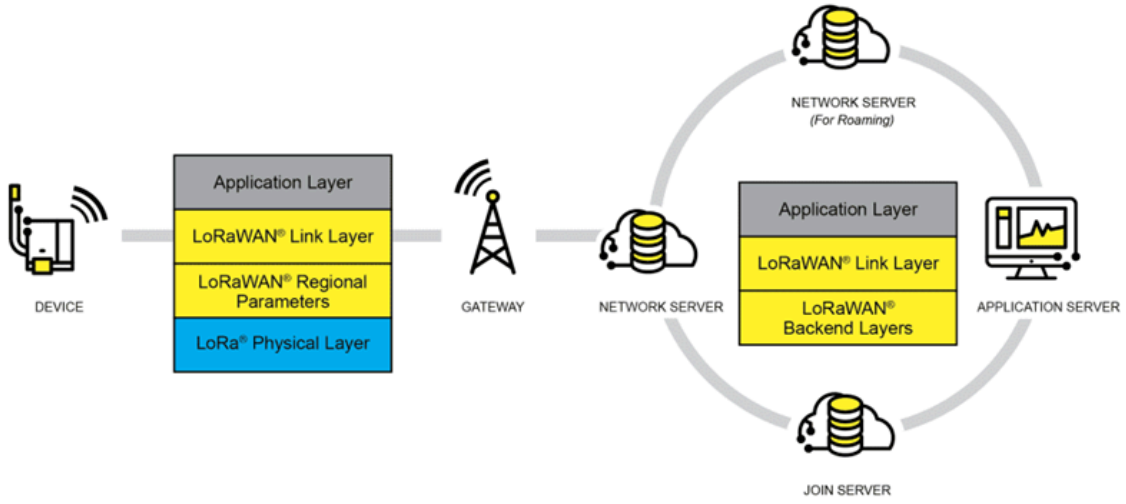
§ NB-IoT y LTE-M: son las soluciones LPWAN de operador ofrecidas por las mismas compañías de telecomunicaciones que mantienen las redes de telefonía móvil, es decir, son las tecnologías que las Telecom ofrecen al ecosistema IoT. LTE-M fue diseñada bajo el estándar LTE diseñada para soluciones que requieren bajo ancho de banda, alta vida útil de batería y movilidad (continuidad en la conexión). Tal como sucede hoy con los servicios M2M en 2G. En cambio, NB-IoT es una tecnología diseñada para soluciones estáticas, con una cantidad de transmisiones limitadas y pequeñas lo que hace que requieran un ancho de banda muy bajo soportando una latencia mayor. En este caso el foco está en que la vida útil de la batería sea muy alta. Dichas tecnologías, trabajan sobre bandas licenciadas sin riesgos de interferencias y bajo los estándares de la 3GPP.

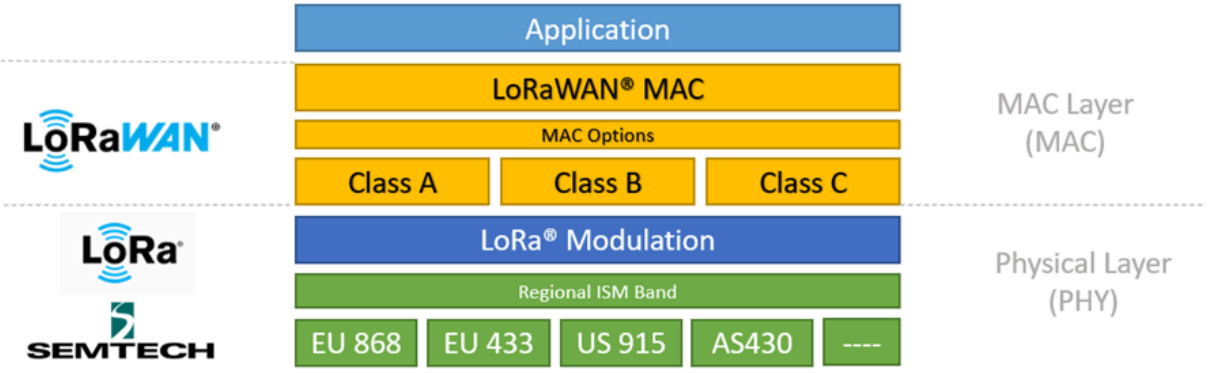


5.1.2.3 LoRaWAN

LoRa es una tecnología de modulación de RF para LPWAN. El nombre es una referencia a los enlaces de datos extremadamente largos (Long-Range) que permite. Desarrollado por Semtech en intento de estandarizar las LPWAN, LoRa logra comunicaciones de hasta 5 kilómetros en áreas urbanas y hasta 15 kilómetros en áreas rurales (Con línea de visión). Una característica clave de las soluciones basadas en LoRa son los requerimientos de energía ultra bajos, lo que permite dispositivos alimentados a batería con vida útil de hasta 10 años. Desplegada en una topología estrella, una red basada en el protocolo abierto LoRaWAN es perfecta para aplicaciones que requieran las virtudes de LoRa extendidas en un número elevado de dispositivos que recolectan pequeñas cantidades de información. La especificación LoRaWAN es un protocolo de red LPWAN diseñado para conectar de forma inalámbrica “cosas” en redes regionales, nacionales o globales. Apunta principalmente a las claves del internet de las cosas (IoT) cumpliendo con requerimientos como comunicación bidireccional, seguridad de extremo a extremo, movilidad y localización.

La arquitectura de red LoRaWAN se implementa en una topología de estrella de estrellas, en la que las puertas de enlace transmiten mensajes entre los dispositivos finales y un servidor de red central. Las puertas de enlace están conectadas al servidor de red a través de conexiones IP estándar y actúan como un puente transparente, simplemente convirtiendo paquetes de RF en paquetes de IP y viceversa. La comunicación inalámbrica aprovecha las características de largo alcance de la capa física de LoRa, lo que permite un enlace de un solo salto entre el dispositivo final y una o varias puertas de enlace. Todos los modos permiten comunicación bidireccional, y hay soporte para grupos de direccionamiento de multidifusión para hacer un uso eficiente del espectro durante tareas como actualizaciones de firmware por aire (FOTA) u otros mensajes de distribución masiva.





Si bien la especificación define la implementación técnica, no define ningún modelo comercial o tipo de implementación (pública, compartida, privada, empresarial) y, por lo tanto, ofrece a la industria la libertad de innovar y diferenciar cómo se usa. La especificación LoRaWAN es desarrollada y mantenida por LoRa Alliance, una asociación abierta de miembros colaboradores y define los parámetros de la capa física del dispositivo a la infraestructura (LoRa) y el protocolo (LoRaWAN) y, por lo tanto, proporciona una interoperabilidad perfecta entre los fabricantes.

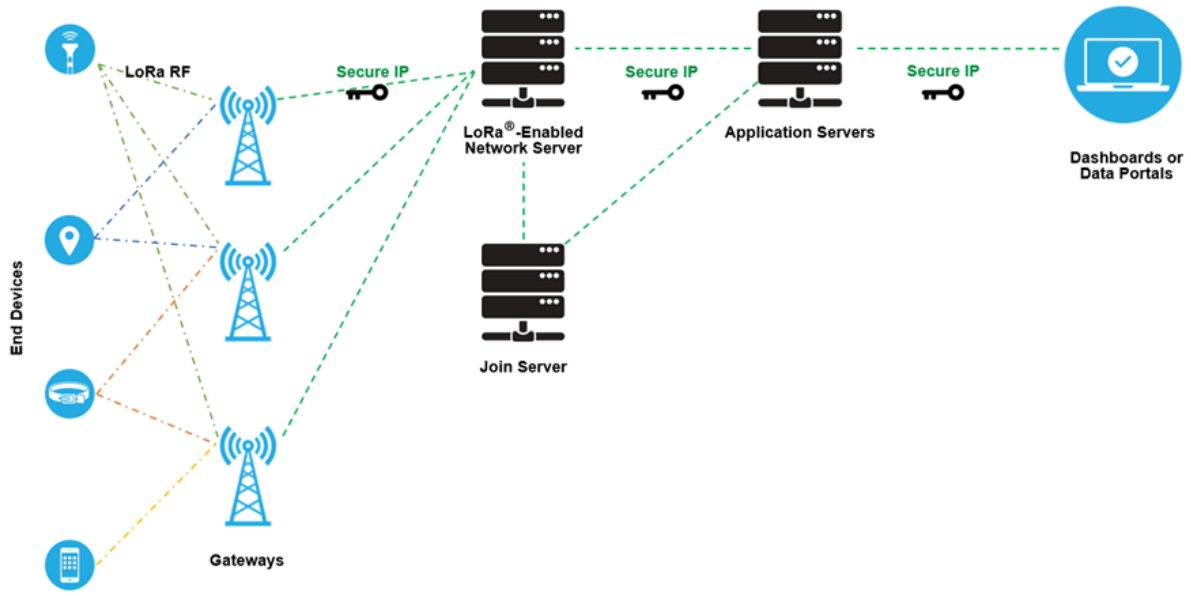
5.1.2.3.1 Elementos de la red

Podemos resumir los elementos de una red LoRaWAN en los siguientes ítems:

- Dispositivos finales
- Puertas de enlace
- Servidor de red

· Servidor de aplicación

· Servidor de unión



Un dispositivo final (end device) habilitado para LoRaWAN es un sensor o un actuador que está conectado de forma inalámbrica a una red LoRaWAN a través de puertas de enlace de radio que utilizan la modulación LoRa RF.

En la mayoría de las aplicaciones, un dispositivo final es un sensor autónomo, a menudo alimentado por batería, que digitaliza las condiciones físicas y los eventos ambientales. Los casos de uso típicos para un actuador incluye: alumbrado público, cerraduras inalámbricas, cierre de válvula de agua, prevención de fugas, entre otros.

Cuando se fabrican los dispositivos basados en LoRa se les asignan varios identificadores únicos. Estos identificadores se utilizan para activar y administrar de forma segura el dispositivo, para garantizar el transporte seguro de paquetes a través de una red pública o privada y para enviar datos cifrados a la nube.

Una puerta de enlace (Gateway) LoRaWAN recibe mensajes de RF modulados LoRa desde cualquier dispositivo final en la distancia de audición y reenvía estos mensajes de datos al servidor de red LoRaWAN (LNS), que está conectado a través de una red troncal IP. No existe una asociación fija entre un dispositivo final y una puerta de enlace específica. En cambio, el mismo sensor puede ser atendido por múltiples puertas de enlace en el área. Con LoRaWAN, cada paquete de enlace ascendente enviado por el dispositivo final será recibido por todas las puertas de enlace a su alcance, como se ilustra en la figura. Esta disposición reduce significativamente la tasa de errores de paquetes (ya que las posibilidades de que al menos una puerta de enlace reciba el mensaje son muy altas), reduce significativamente la sobrecarga de la batería para sensores móviles/nómadas y permite la geolocalización de bajo costo (suponiendo que las puertas de enlace en cuestión tengan capacidad de geolocalización).

El tráfico IP desde una puerta de enlace al servidor de la red se puede reenviar a través de Wi-Fi, Ethernet cableado o mediante una conexión celular. Las puertas de enlace LoRaWAN funcionan completamente en la capa física y, en esencia, no son más que reenviadores de mensajes de radio LoRa. Solo verifican la integridad de los datos de cada mensaje LoRa RF entrante. Si la integridad no está intacta, es decir, si el CRC es incorrecto, el mensaje se eliminará. Si es correcto, la puerta de enlace lo reenviará al LNS, junto con algunos metadatos que incluyen el nivel RSSI de recepción del mensaje, así como una marca de tiempo opcional. Para los enlaces descendentes de LoRaWAN, una puerta de enlace ejecuta las solicitudes de transmisión provenientes del LNS sin ninguna interpretación de la carga útil. Dado que varias puertas de enlace pueden recibir el mismo mensaje LoRa RF desde un único dispositivo final, el LNS realiza la deduplicación de datos y elimina todas las copias.

El servidor de red LoRaWAN (LNS) administra toda la red, controla dinámicamente los parámetros de la red para adaptar el sistema a las condiciones cambiantes y establece conexiones AES seguras de 128 bits para el transporte de datos de extremo a extremo (desde el dispositivo final LoRaWAN a la aplicación de los usuarios finales en la nube), así como para el control del tráfico que fluye desde el dispositivo final LoRaWAN al LNS (y viceversa). El servidor de red garantiza la autenticidad de todos los sensores de la red y la integridad de todos los mensajes. Al mismo tiempo, el servidor de red no puede ver ni acceder a los datos de la aplicación.

En general, todos los servidores de red LoRaWAN comparten las siguientes características:

- Comprobación de la dirección del dispositivo
- Autenticación de tramas y gestión de contadores de tramas
- Acuses de recibo de mensajes recibidos
- Adaptación de tasas de datos mediante el protocolo ADR
- Respondiendo a todas las solicitudes de capa MAC provenientes del dispositivo,
- Reenvío de cargas útiles de aplicaciones de enlace ascendente a los servidores de aplicaciones apropiados
- Puesta en cola de cargas útiles de enlace descendente provenientes de cualquier servidor de aplicaciones a cualquier dispositivo conectado a la red
- Reenvío de mensajes de solicitud de unión y aceptación de unión entre los dispositivos y el servidor de unión.

Los servidores de aplicaciones son responsables de manejar, gestionar e interpretar de forma segura los datos de las aplicaciones de los sensores. También generan todas las cargas útiles de enlace descendente de la capa de aplicación a los dispositivos finales conectados.

El servidor de unión administra el proceso de activación por aire para que los dispositivos finales se agreguen a la red.

El servidor de unión contiene la información necesaria para procesar tramas de solicitud de unión de enlace ascendente y generar tramas de aceptación de unión de enlace descendente. Señala al servidor de red qué servidor de aplicaciones debe conectarse al dispositivo final y realiza las derivaciones de clave de cifrado de sesión de red y aplicación. Comunica la clave de sesión de red del dispositivo al servidor de red y la clave de sesión de la aplicación al servidor de aplicaciones correspondiente.

Para ello, el servidor de unión debe contener la siguiente información para cada dispositivo final bajo su control:

· DevEUI (identificador único de serie del dispositivo final)

· AppKey (clave de cifrado de la aplicación)

· NwkKey (clave de cifrado de red)

· Identificador del servidor de aplicaciones

· Perfil de servicio del dispositivo final

5.1.2.3.2 CLASES LORAWAN

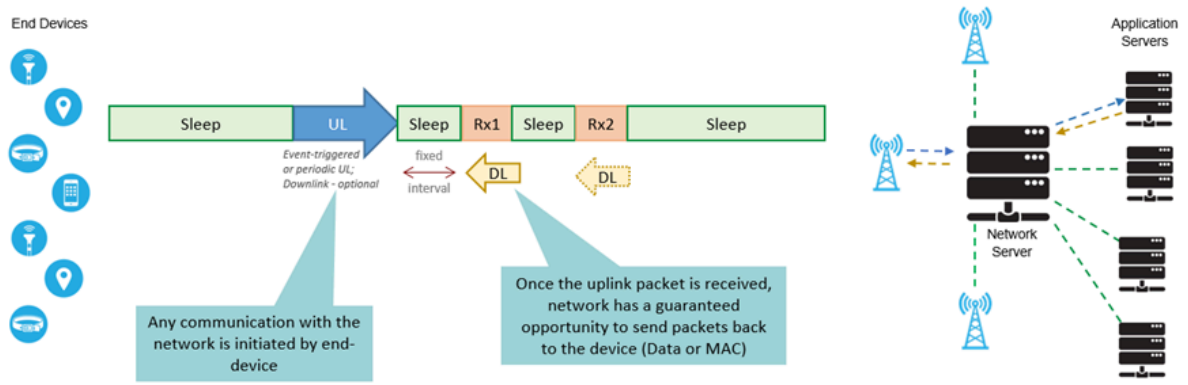
LoRaWAN tiene tres clases diferentes de dispositivos de punto final para abordar las diferentes necesidades reflejadas en la amplia gama de aplicaciones:

· Clase A: (dispositivos finales bidireccionales de menor potencia)

La clase predeterminada que debe ser compatible con todos los dispositivos finales de LoRaWAN, la comunicación de clase A siempre la inicia el dispositivo final y es totalmente asíncrona. Cada transmisión de enlace ascendente se puede enviar en cualquier momento y va seguida de dos breves ventanas de enlace descendente, lo que brinda la oportunidad de comunicación bidireccional o comandos de control de red si es necesario. Este es un tipo de protocolo ALOHA.

El dispositivo final puede entrar en el modo de suspensión de bajo consumo durante el tiempo definido por su propia aplicación: no hay requisitos de red para activaciones periódicas. Esto convierte a la clase A en el modo de funcionamiento de menor consumo de energía, al mismo tiempo que permite la comunicación de enlace ascendente en cualquier momento.

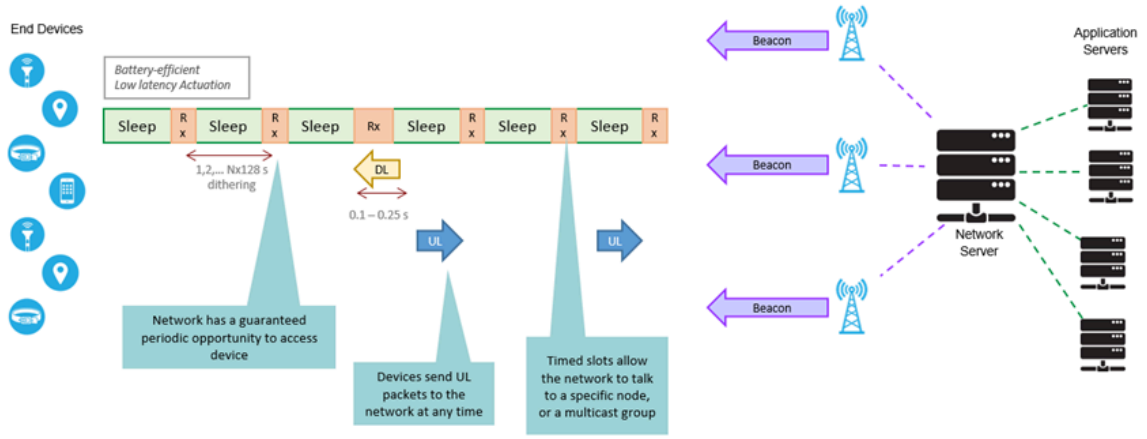
Debido a que la comunicación de enlace descendente siempre debe seguir una transmisión de enlace ascendente con un cronograma definido por la aplicación del dispositivo final, la comunicación de enlace descendente debe almacenarse en el servidor de red hasta el próximo evento de enlace ascendente.



There is no fixed association between an end device and a gateway. An uplink packet will be processed by all gateways within range and forwarded to the Network Server

· Clase B: (dispositivos finales bidireccionales con latencia de enlace descendente determinista)

Además de las ventanas de recepción iniciadas de clase A, los dispositivos de clase B se sincronizan con la red mediante balizas periódicas y abren 'ranuras de ping' de enlace descendente en horarios programados. Esto proporciona a la red la capacidad de enviar comunicaciones de enlace descendente con una latencia determinista, pero a expensas de un consumo de energía adicional en el dispositivo final. La latencia es programable hasta 128 segundos para adaptarse a diferentes aplicaciones, y el consumo de energía adicional es lo suficientemente bajo como para seguir siendo válido para aplicaciones alimentadas por batería.



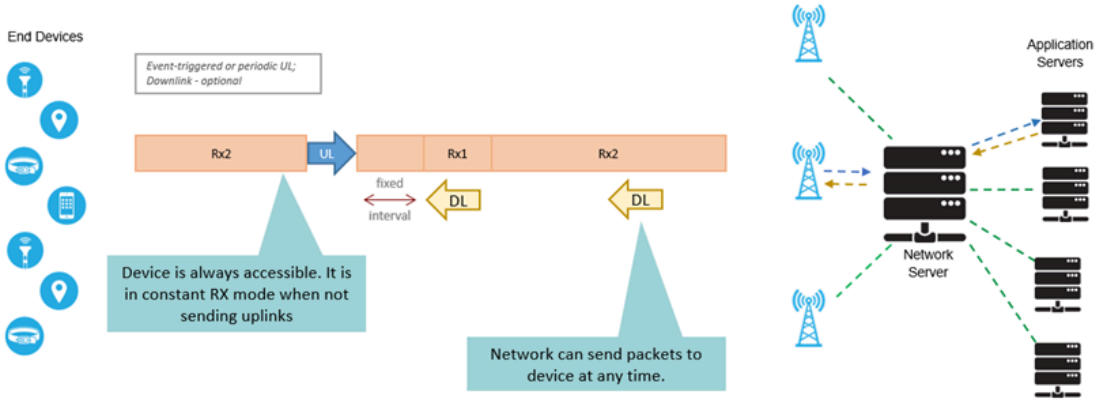
There is no fixed association between an end device and a gateway. An uplink packet will be processed by all gateways within range and forwarded to the Network Server

· Clase C: (latencia más baja, dispositivos finales bidireccionales)

Además de la estructura de clase A de enlace ascendente seguida de dos ventanas de enlace descendente, la clase C reduce aún más la latencia en el enlace descendente al mantener el receptor del dispositivo final abierto en todo momento en que el dispositivo no está transmitiendo (semidúplex). En base a esto, el servidor de red puede iniciar una transmisión de enlace descendente en cualquier momento

suponiendo que el receptor del dispositivo final esté abierto, por lo que no hay latencia. El compromiso es el consumo de energía del receptor (hasta 50 mW), por lo que la clase C es adecuada para aplicaciones en las que se dispone de energía continua.

Para los dispositivos alimentados por batería, es posible el cambio de modo temporal entre las clases A y C, y es útil para tareas intermitentes, como actualizaciones inalámbricas de firmware.



Además del salto de frecuencia, todos los paquetes de comunicación entre los dispositivos finales y las puertas de enlace también incluyen una configuración de 'Velocidad de datos' (DR) variable. La selección de DR permite un equilibrio dinámico entre el rango de comunicación y la duración del mensaje. Debido a la tecnología de espectro ensanchado, las comunicaciones con diferentes DR no interfieren entre sí y crean un conjunto de canales virtuales de 'código' que aumentan la capacidad de la puerta de enlace. Para maximizar la duración de la batería de los dispositivos finales y la capacidad general de la red, el servidor de red LoRaWAN administra la configuración de DR y la potencia de salida de RF para cada dispositivo final de forma individual mediante un esquema de tasa de datos adaptable (ADR). Las velocidades en baudios de LoRaWAN oscilan entre 0,3 kbps y 50 kbps.

5.1.2.3.3 SEGURIDAD

La seguridad es una preocupación principal para cualquier implementación masiva de IoT y la especificación LoRaWAN define dos capas de criptografía:

- Una clave de sesión de red única de 128 bits compartida entre el dispositivo final y el servidor de red

- Una clave de sesión de aplicación única de 128 bits (AppSKey) compartida de extremo a extremo en el nivel de la aplicación

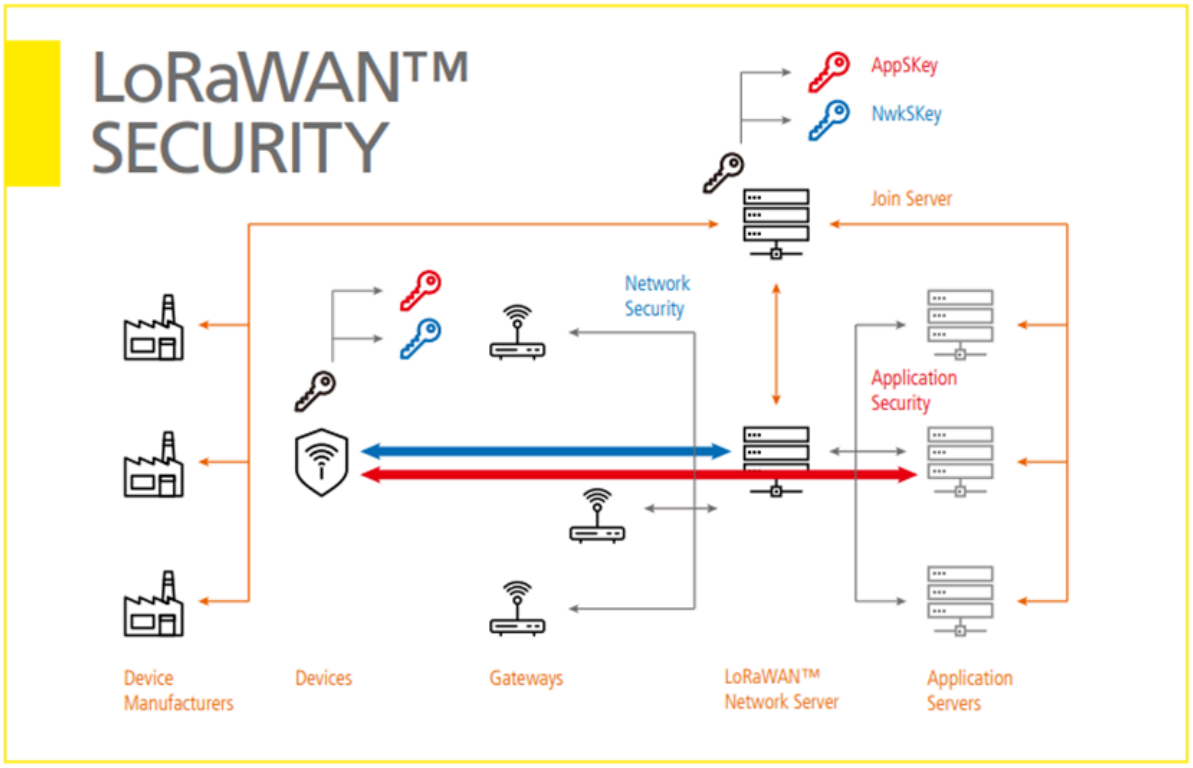
Los algoritmos AES se utilizan para proporcionar autenticación e integridad de paquetes al servidor de red y cifrado de extremo a extremo al servidor de aplicaciones. Al proporcionar

estos dos niveles, es posible implementar redes compartidas 'multi-inquilino' sin que el operador de la red tenga visibilidad de los datos de carga útil de los usuarios.

Las claves se pueden activar por personalización (ABP) en la línea de producción o durante la puesta en marcha, o se pueden activar por aire (OTAA) en el campo. OTAA permite que los dispositivos se vuelvan a registrar si es necesario.

Over-the-Air Activation (OTAA)	Activation by Personalization (ABP)
• Device manufacturers autonomously generate essential provisioning parameters • Secure keys (session-long and derived) can be renewed regularly • Devices can store multiple “identities” to dynamically and securely switch networks and operators during its lifetime • High-grade, tamper-proof security options are available	• A simplified (less secure) commissioning process • IDs and Keys are personalized at fabrication • Devices become immediately functional upon powering up; the Join procedure is skipped • Devices are tied to a specific network/service; the NetID is a portion of the device network address

La figura ilustra la seguridad de las transmisiones de paquetes de datos. El tráfico de control entre el dispositivo final y el servidor de red está protegido con una clave de sesión de red AES de 128 bits (NwkSKey). El tráfico de datos que viaja entre el dispositivo final y el servidor de aplicaciones está protegido con una clave de sesión de aplicación de 128 bits (AppSKey). Este método garantiza que ni la puerta de enlace ni el servidor de red puedan leer los datos del usuario.



El procedimiento de unión de un dispositivo consta de los siguientes pasos:

1. Comenzaremos con las claves de seguridad, las claves root individuales se almacenan de forma segura en los dispositivos finales y las claves coincidentes se almacenan de forma segura en el servidor de unión.

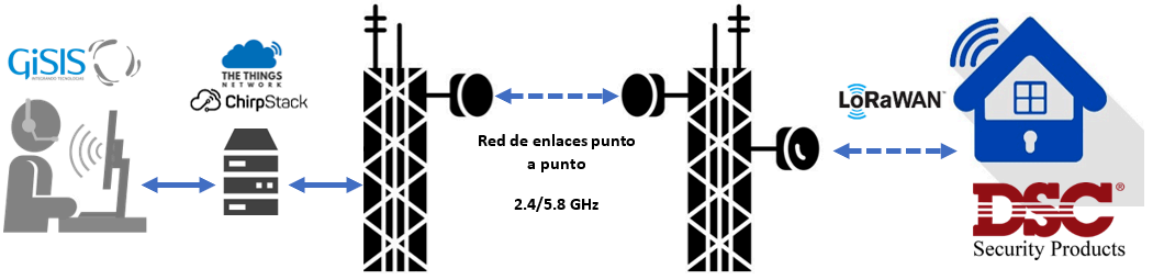
2. El dispositivo final envía un mensaje de solicitud de unión al servidor de unión.

3. Una vez que el servidor de unión autentica el dispositivo que solicita unirse a la red, devuelve un mensaje de aceptación de unión al dispositivo.

4. A continuación, el dispositivo final obtiene claves de sesión localmente, en función de DevEUI, Join EUI, DevNonce, claves root y campos en los mensajes de solicitud de unión y aceptación de unión. Por su parte, el servidor de unión también obtiene claves de sesión de los ID de serie, claves root y campos en solicitudes de unión y mensajes de aceptación de unión. Finalmente, el servidor de unión comparte claves de sesión con servidores de red y de aplicaciones.

5.1.3 Descripción del proyecto

A partir de los objetivos generales planteados, podemos diagramar la estructura general que se pretende implementar y para la cual este proyecto servirá de prueba de concepto, lo que se ve reflejado a continuación:



Con lo cual es necesaria la implementación y/o configuración de los siguientes elementos:

1. Nodo final: el nodo final es el dispositivo que se conecta directamente al panel de la alarma. Cumple las siguientes tareas:
    a. Obtención de estado de la alarma
    b. Reporte de eventos
2. Puerta de enlace
3. Servidor: el servidor será el encargado de gestionar todo el sistema. Cumple las siguientes tareas:
    a. Servidor de red LoRaWAN
    b. Programa de integración con software de monitoreo

5.1.3.1 Establecimiento de la comunicación

Teniendo en cuenta los requerimientos y la estructura general planteada, y para que este proyecto sirva como validador de la implementación a futuro, es necesario implementar un “banco de pruebas” que permita saber si el funcionamiento es viable.

Con esto en mente se implementará el servidor en un equipo local cuyas especificaciones satisfagan las condiciones mínimas para el funcionamiento del mismo (aunque no sea suficiente para una puesta en producción, donde se deban atender a múltiples clientes y se necesite almacenar mayor cantidad de datos), por otro lado, la red de enlaces punto a punto de la figura anterior, si bien está instalada y en funcionamiento, resulta sumamente incómoda para el trabajo diario por lo cual toda la red que permite la conexión entre el Gateway y el servidor será realizada con un router administrable. Además, el proyecto consta de la construcción de un único nodo final funcional.

Todas las modificaciones al esquema tienen como principal objetivo la reducción de costos y tiempos, a fin de acelerar la obtención de resultados.

5.1.3.1.1 Servidor de red

El hardware provisto por la empresa es un servidor HP ProLiant ML 110 G4 cuyas especificaciones técnicas se detallan a continuación

- Procesador: Intel Pentium 2.80 GHz
- Memoria RAM instalada: 512 MB
- Almacenamiento interno: 2x 160 GB RAID 1
- Conectividad: Gigabit Ethernet 100 Mbit/s

Al mismo se le instaló el sistema operativo Ubuntu server 16.04 que luego fue actualizado a la versión 18.04 y se le definieron los parámetros necesarios para su funcionamiento en red, se activó el firewall y se cargaron los usuarios con sus contraseñas correspondientes. Además, se configuró un servidor openSSH y las claves correspondientes para permitir un trabajo cómodo de forma remota.

Una vez instalado el OS y verificado su correcto funcionamiento, se procedió a la instalación del servidor de red LoRaWAN. En la investigación surgieron las siguientes alternativas:

- Servidor de red Chirpstack
- Servidor de red The Things Stack (TTS)

La principal diferencia entre ambas alternativas resulta ser la licencia, mientras que Chirpstack es un desarrollo totalmente open-source, The Things Stack pertenece a The Things Network una empresa dedicada a ofrecer como servicio software para servidores de

red LoRaWAN (entre otras cosas). Sin embargo, ofrecen una versión llamada community edition, la cual permite su uso sin necesidad de pago, pero con características reducidas. Por otro lado, los requerimientos de hardware de TTS son más exigentes que los de Chirpstack, y considerando el servidor en el que se instalará es un aspecto importante a tener en cuenta, estos son los motivos que terminaron decantando en el uso de Chirpstack.

Las propias páginas de Chirpstack y TTS proveen sus guías de instalación, en particular, Chirpstack brinda 3 posibilidades: usando los binarios pre-compilados, contenedores Docker y a través de repositorios Deb; debido a que estamos trabajando sobre Ubuntu server, se utilizó la instalación por los repositorios.

El software requiere para funcionar las siguientes dependencias: mosquitto[4] (un bróker MQTT), Redis (almacén de datos en memoria) y una base de datos (en este caso se utiliza PostgreSQL). Como observación general, todas las dependencias utilizadas son open-source y no es necesario el pago de ninguna licencia para su uso. El propio instructivo de instalación indica cómo generar la base de datos, con su correspondiente configuración y generación de usuarios y contraseñas. Como extra a lo que el instructivo indica, se configuró usuarios y contraseñas tanto en Redis como en mosquitto.

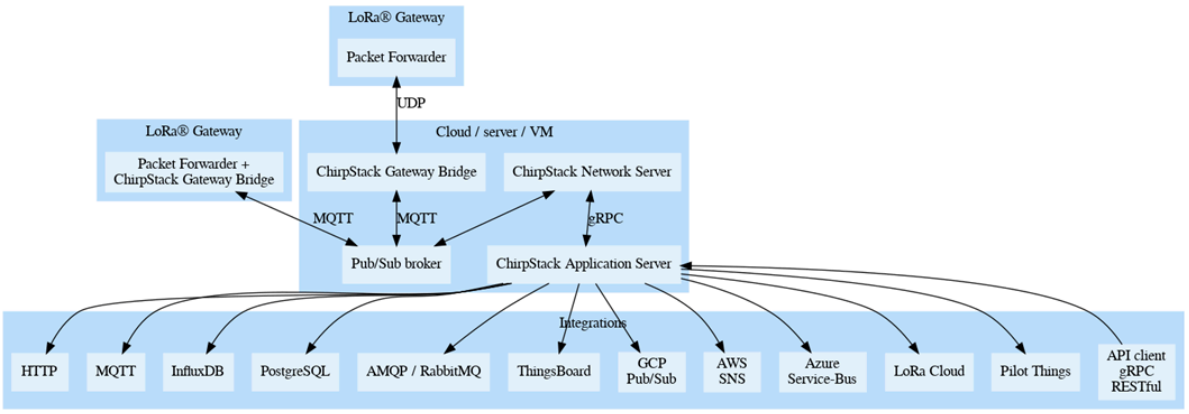
Una vez que se tienen todas las dependencias instaladas y se puede verificar su correcto funcionamiento, se procede con la instalación del servidor de red. Para esto, se agregan los repositorios y se hace uso de apt para instalarlos. Es necesario instalar los siguientes componentes:

- chirp stack-gateway-bridge: es un servicio que convierte los protocolos de paquetes reenviados LoRa en un formato común de datos de Chirp Stack (JSON o Protobuf).

- chirp stack-network-server: es una implementación de LoRaWAN Network Server de código abierto. La responsabilidad del componente del servidor de red es por un lado la deduplicación de las tramas LoRaWAN recibidas por las puertas de enlace, y por el otro, haciendo uso de las tramas recopiladas, se manejan autenticación, LoRaWAN capa mac, comunicación con el servidor de aplicaciones Chirp Stack y programación de tramas de enlace descendente

- chirp stack-application-server: Es responsable de la parte del "inventario" de dispositivos de una infraestructura LoRaWAN, el manejo de la solicitud de unión y el manejo y cifrado de las cargas útiles de la aplicación. Ofrece una interfaz web donde se pueden administrar usuarios, organizaciones, aplicaciones y dispositivos. Para la integración con servicios externos, ofrece gRPC y API RESTful. Los datos del dispositivo se pueden enviar y/o recibir a través de MQTT, HTTP y se pueden escribir directamente en InfluxDB.

La configuración de estos se hace a través de archivos TOML y se puede encontrar un ejemplo completo en la propia página de cada uno. En estos archivos, además de cargar los usuarios y contraseñas generados anteriormente, se configura la región (En este caso AU 915), frecuencias, canales y otros parámetros propios de la red.

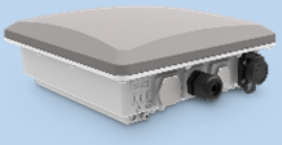


Una vez que se tienen todos los componentes del servidor en correcto funcionamiento, podemos empezar la configuración del sistema.

El servidor de aplicaciones Chirp Stack puede conectarse a una o varias instancias del servidor de red. Los usuarios administradores globales pueden agregar nuevos servidores de red a la instalación del servidor de aplicaciones. El primer paso a seguir es cargar el servidor de red, para lo cual debemos saber la dirección IP y el puerto configurado. Además, deberemos crear un perfil de servicio y una organización. La organización es una entidad que permite asignar usuarios, dispositivos y nodos de forma que sean invisibles para otras organizaciones. Los perfiles de servicio pueden ser vistos como “contratos” con una organización, dando lugar a una serie de flexibilidades en cuanto a implementaciones. Una vez que tenemos estas entidades creadas y configuradas, podemos crear usuarios y contraseñas para permitir acceso a otras personas.

5.1.3.1.2 Puerta de enlace

La puerta de enlace o Gateway es el elemento encargado de funcionar de puente entre el servidor de red y los dispositivos finales. Para lograr tal fin, existen múltiples alternativas comerciales disponibles por lo que la tarea principal consta de una investigación de alternativas y la selección de una de estas.

Nombre	Mikrotik wAP LR9 kit (R11e-LR9)	MultiTech Conduit AP MTCAP-LAP3-915	RAK WisGate Edge Pro RAK 7289
Imagen			

Links	https://mikrotik.com/product/wap_lr9_kit https://mikrotik.com/product/r11e_lr9	https://www.multitech.com/models/92507565LF s://www.multitech.com uments/publications/d sheets/86002238.pdf	https://store.rakwirele om/products/wisgate-e pro-rak7289 https://docs.rakwireles m/Product-Categories/ Gate/RAK7289/Datashe
Características	· Gateway de exterior · Interfaz WLAN de 2,4 GHz y puerto Ethernet para usar como back-end · Antena interna +2dBi (kit antena externa opcional +6.5 dBi) · Opera en la frecuencia de 902-928 MHz · Sistema operativo RouterOS · Certificado IP 20 · Alimentación PoE	· Gateway de interior · Ethernet 10/100 BaseT para back-end IP · Certificado para Australia 915 MHz · 4G-LTE Categoría 1 · Antenas: Modelos-001A Sin conectores de antenas; Modelos-041A LoRa: SMA hembra. · Software mPower	· Admite hasta 16 canales LoRa · Backhaul múltiple con conectividad Ethernet, Wi-Fi y celular · Certificado IP67/NEMA-6 · Alimentación Poe · GPS · Sin posibilidad de antena interna · Software OpenWRT
Precio	U$S 169	U$S 453	U$S 372

La selección terminó decantándose por el Gateway Mikrotik debido a que estaba disponible para su compra en el país, su precio era el más conveniente y la empresa solicitante tiene experiencia trabajando con productos de la marca. Se compró también el kit de antena de +6.5 dBi.

La configuración del Gateway se realiza mediante acceso web o puede utilizarse el software WinBox. La misma consiste en cargar la dirección IP y el puerto del servidor de red que ya está en funcionamiento, además de configurar los canales y la norma que se desea utilizar (AU 915).

Las características de la radio, el equipo y la antena son:

R11e-LR8/R11e-LR9 specifications

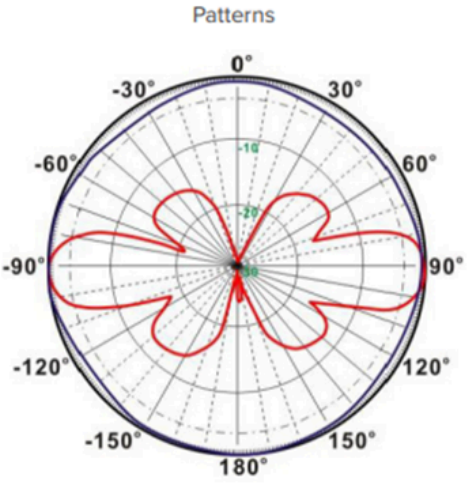
Product code	R11e-LR8	R11e-LR9
Interface	Mini-PCIe	
Supported class	A and C	
Frequency	863-870 MHz (EU863-870, RU864-870, IN865-867)	902-928 MHz (AU915-928, US902-928, AS923, KR920-923)
RF Output power	863-870 MHz 14 dBm	902-928 MHz 23 dBm
Receive max sensitivity	-137 dB @ SF12	
Range	Up to 15 km in rural environment and up to 2 km in urban environment when using MikroTik LoRa® 6.5 dBi antenna kit	
Operating ambient temperature	-40°C .. +70°C	
Max power consumption	2 W	

wAP LR8/LR9 kit specifications

Product code	RBwAPR-2nD&R11e-LR8	RBwAPR-2nD&R11e-LR9
CPU	QCA9531 650 MHz	
Size of RAM	64 MB	
10/100 Ethernet ports	1	
Wireless	Built-in 2.4 GHz 802.11b/g/n, dual-chain	
Antenna gain	2 dBi	
PoE in	Yes	
Supported input voltage	9 V - 30 V (Passive PoE)	
Dimensions	185 x 85 x 30 mm	
Operating ambient temperature	-40°C .. +60°C	
Operating system	RouterOS, License level 4	
Max power consumption	7 W	

Antenna kit for LoRa® specifications

Product code	TOF-0809-7V-S1
Frequency	824 - 960 MHz
Gain	6.5 dBi
Horizontal beamwidth	360°
Vertical beamwidth	30°
Nominal impedance	50 Ω
Lightning protection	DC ground
Connector	SMA female
Weight	0.6 kg
Dimensions	Ø 25 x 950 mm
Mast diameter	Ø 30 - 50 mm



Una vez que se tiene conectada la puerta de enlace y se chequea la conectividad con el servidor, debe cargarse el mismo en el servidor de red. Para lograr esto se deben cumplir 2 etapas, primero se debe crear un perfil relacionado al modelo. Se deben configurar los canales a utilizar y coincidir con lo configurado anteriormente en el software del dispositivo.

Una vez que se tiene este perfil, se crea una instancia de este que permite su uso. Se necesita conocer el ID único del Gateway para cargarlo en el sistema, el mismo puede encontrarse fácilmente en el propio software de MikroTik. Además, se pueden configurar las coordenadas del mismo para luego mostrar su ubicación en un mapa.

El perfil de la puerta de enlace puede ser generado de forma global, de modo que todas las organizaciones sean capaces de utilizar dicho perfil, o puede ser generado por una organización (si tiene los permisos para hacerlo). Lo mismo sucede con la instancia de cada Gateway en particular.

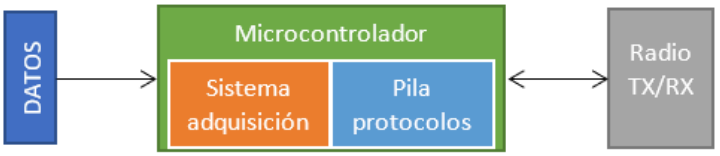
Una vez creado, dentro del perfil del Gateway es posible ver un Log de las tramas enviadas.

5.1.3.1.3 Dispositivos finales

La elección del hardware del dispositivo final está sumamente ligada a la aplicación en la que va a ser utilizado. Es necesario por ello conocer no solo el sistema de adquisición de datos (que será discutido en el próximo capítulo) sino también el sistema de transmisión y recepción. En cuanto al primer tema mencionado, las exigencias no son elevadas, pues se trata de un bus de datos de 2 hilos bidireccional con reloj de 1000 Hz, de modo que un microcontrolador de gama baja es capaz de manejarlo sin mayores inconvenientes (por ejemplo, un ATMEGA 328 – Arduino UNO). Por otro lado, el sistema de comunicaciones se compone de dos partes: una radio que tenga la capacidad de transmitir siguiendo el estándar LoRa PHY y una pila de protocolos que sea capaz de manejar dicha radio. Con esto en mente podemos encontrar tres tipos de soluciones en el mercado:

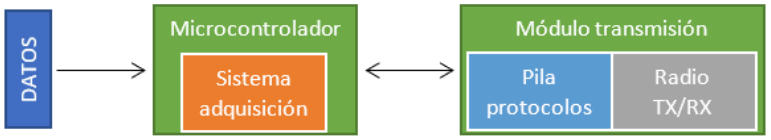
· Sistemas en los que se anexa una radio, por lo que tanto la pila de protocolos como la adquisición de datos conviven en un mismo microcontrolador.

Esta arquitectura tiene la ventaja de permitir un control personalizable en cuanto al flujo de trabajo interno, sin embargo, requiere de un microprocesador más potente puesto que debe realizar múltiples tareas con tiempos de acción limitados. Además, requiere la compra de al menos dos "subsistemas" por separado, con las complicaciones económicas y logísticas que ello implica. Se necesita mantener la pila de protocolos actualizada, por lo que es necesario un entendimiento más profundo de la misma.



· Sistemas en los que se anexa un módulo LoRaWAN, por lo que el sistema de adquisición de datos envía órdenes de control a un microcontrolador secundario que maneja los protocolos de comunicación.

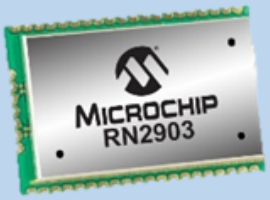
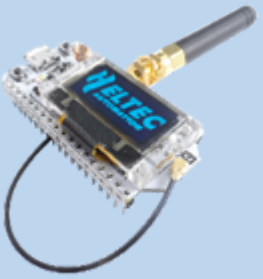
Esta arquitectura libera significativamente la carga del microcontrolador principal, pero se pierde la flexibilidad en cuanto al control de la pila de protocolos. Además, requiere la compra de al menos dos "subsistemas" por separado, con las complicaciones económicas y logísticas que ello implica. Como ventaja, el mantenimiento de la pila de protocolos corre por parte del fabricante del módulo, por lo que los conocimientos de este no deben ser excesivamente profundos



· Sistemas de desarrollo, funciona de forma muy similar al primero, pero con la diferencia que la radio se incluye incorporada en la propia placa.

Al igual que en el primer caso, se permite un control personalizado del flujo de trabajo del microcontrolador, a su vez que requiere que sea más potente para poder cumplir con las exigencias de tiempos, sin embargo, al tratarse de una placa de desarrollo, el fabricante de esta indirectamente realiza la selección pensando en su utilización futura, por lo que podemos centrar nuestra atención en las capacidades de adquisición (que en este caso no son significativamente exigentes). Esta arquitectura tiene una ventaja, generalmente el fabricante provee múltiples recursos de hardware y software lo que permite acelerar los tiempos de desarrollo. Uno de los recursos típicos es la propia pila de protocolos, por lo que su mantenimiento corre a cargo del fabricante.

A partir de esto podemos analizar algunas alternativas:

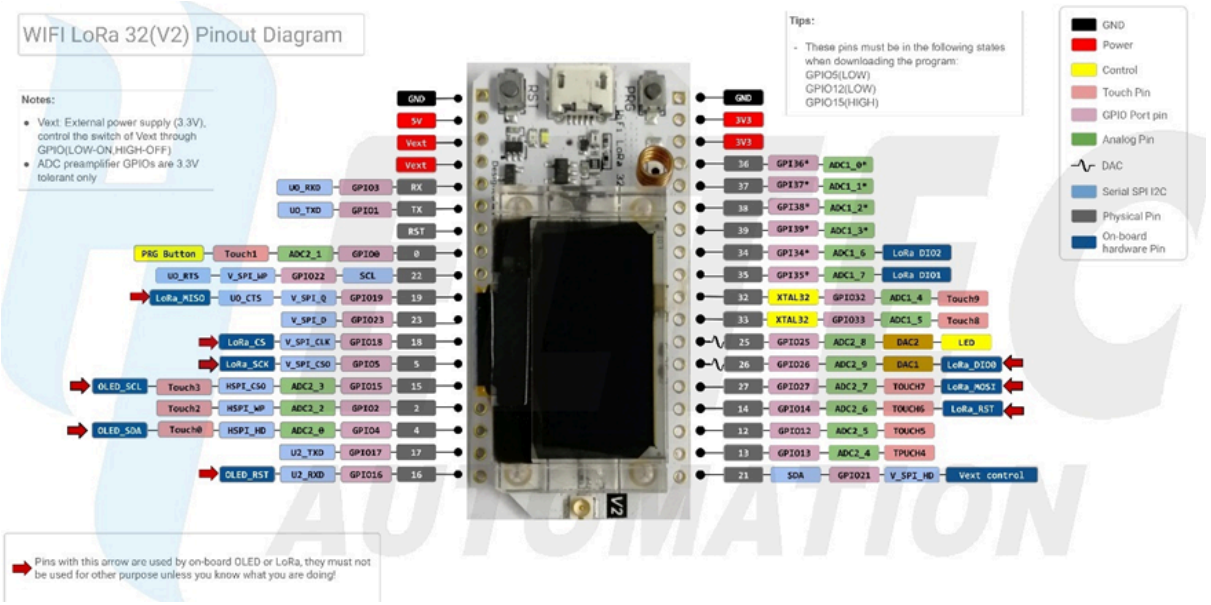
Nombre	RAK RAK 3172	Microchip RN2903	915 MHZ RN2903 LORA INOLOGY MOTE	Heltec - WiFi LoRa 32
Imagen				
Tipo	Modulo de transmision	Modulo de transmision	Sistema de desarrollo	Sistema de desarrollo
Links	https://store.rakwireless. isduo-lpwan-module-rak3	https://www.microchip.c ct/RN2903	https://www.microchip.c ppment-tool/DM164139	https://heltec.org/project wifi-lora-32/

Caracterísi	· Basado en CCU6 · Cumplimiento nes LoRaWAN 1.0.3 · Supported bands: 70, IN865, EU868, AU915, KR920, RU864, and /4 · LoRaWAN activación P · Comunicaciones LoRa nt (P2P) · Set de comandos AT terfaz UART · ARM Cortex-M4 · Memoria flash con tes · RAM 64 kbytes · Consumo de 1.69 µA ep · Voltaje de n: 2.0 V ~ 3.6 V · Posibilidad de X · Basado en Semtech	· Stack protocolo en placa · Interfaz de comandos ante UART · Alta sensibilidad de hasta -146 dBm · Potencia de n: Ajustable hasta +18.5 · Cumplimiento de iones LoRaWAN de clase A · PIC18LF46K22 interno rrollo de programa de · 14 pines GPIO	· Conector SMA 915 · Conector Mini USB · Microprocesador 0 8-bit · Programación ICSP · Display LCD · Switches S1 & S2 ción del menú) · Sensor de luz · Termistor lineal activo · Regulador LDO · 4 LEDs · (2) Packs baterías · Switch para n por baterías · Conectores para imentación alternativa	· Microprocesador: l-core 32-bit MCU + ULP · Chip LoRa Semtech 278 · Interfaz micro USB, e voltaje, protección ESD y circuito · Interfaz de batería anejo de batería integrado · Conexión WiFi, LoRa y ntena 2.4 GHz integrada y X para LoRa. · Display OLED 128*64 · Chip CP2102 USB a e para programación y · Provee protocolo ESP N en librería. · Potencia de salida RF
Precio	U$S 6	U$S 17.36	U$S 91.29	U$S 18.20

Como se observa, la mayoría de las opciones comerciales están basadas en la solución original realizada por Semtech, quien también posee la patente de la modulación LoRa. La línea de radios es la SX12xx y se puede comprar directamente desde tiendas digitales. Sin

embargo, es poco conveniente ya que al ser solamente una radio es necesario implementar todo el Stack en un UC externo y armar una placa para el conexionado (Típicamente SPI).

Teniendo en cuenta los precios y la implementación de tipo prototipo, se buscó la opción más económica que permita a su vez un desarrollo sencillo, por esto se eligió el uso del sistema de desarrollo Heltec LoRa32 ya que tiene un microcontrolador ESP32 con el cual ya se trabajó anteriormente y el costo es significativamente menor a otras alternativas. A continuación, puede verse el diagrama de pines disponibles.



Una vez establecido el hardware podemos avanzar en el software necesario, como ya se mencionó es necesario implementar una pila o stack de protocolos que permita la comunicación; entre las alternativas para lograr esto se analizaron las siguientes opciones:

· LoRaMac-Node: Implementación de referencia y documentación de un nodo LoRa, provisto por Semtech, es el punto de inicio de muchas otras implementaciones. Sin embargo, tiene compatibilidad con poco hardware y se requiere portarlo para utilizarlo en ESP32. La gran ventaja es que al ser mantenida por la empresa madre de la tecnología, soporta todas las funcionalidades y versiones del protocolo.

· LMIC: LoRaMacInC es una implementación realizada por IBM que actualmente se encuentra descontinuada, sin embargo, MCCI realizó un fork del mismo y mantiene un stack propio. Si bien está orientado para ser utilizado en el entorno de Arduino, utilizarlo en ESP32 no representa un reto significativo debido al soporte sobre este IDE.

· Heltec ESP32_LORAWAN: Es la librería que ofrece el desarrollador del entorno de desarrollo para utilizar con la placa, que consta de una adaptación de la implementación de referencia para funcionar en un microcontrolador ESP32. Requiere una licencia única para funcionar asociada con la propia placa de desarrollo. Tiene la desventaja de no estar completamente actualizada ni funcional (cumple el protocolo V1.0.2 clases A y C).

Luego de una serie de testeos sobre las librerías, se llegó a la conclusión de que la librería LMIC resulta ser la mejor opción en cuanto a flexibilidad de configuración de parámetros, al mismo tiempo que no dificulta demasiado su uso.

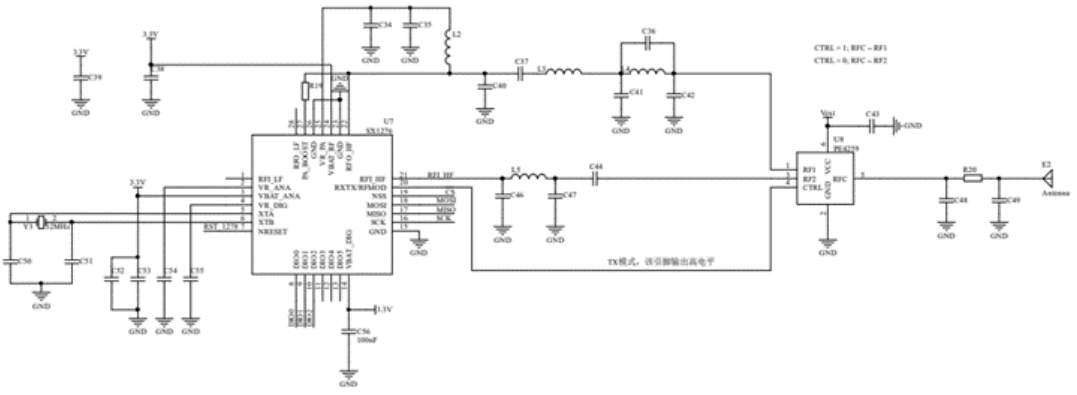
A partir de aquí es necesario elegir el entorno de desarrollo que se va a utilizar. Para esto se analizaron 3 opciones: el entorno de desarrollo de ESP, el entorno de desarrollo de Arduino y el uso de PlatformIO. PlatformIO es una herramienta profesional multiplataforma, multiarquitectura y marco múltiple para ingenieros de sistemas embebidos. Si bien su uso puede requerir una curva de aprendizaje mayor que las otras opciones, se elige esta alternativa debido a la altísima compatibilidad con distintos dispositivos y librerías, sumado a la capacidad de personalizar todo el proyecto a gusto propio. Además, puede funcionar como una extensión para Visual Studio Code, el editor de código fuente de Microsoft. El mismo cuenta con un abundante ecosistema de extensiones y funcionalidades, logrando de esta forma un entorno de desarrollo completo y cómodo. El mismo es de uso gratuito (Licencia MIT) y funciona en Windows, Linux y MAC.

Como últimas características importantes a destacar, ya que son útiles para las estimaciones y cálculos de cobertura, detallaremos las capacidades de RF con las que cuenta el hardware seleccionado. Debido a que se utiliza el chip SX1276 de Semtech, obtendremos algunas de las características de su hoja de datos:

- Potencia de transmisión: +20 dBm – 100 mW / +14dBm amplificador de alta eficiencia
- Sensibilidad: -148 dBm (dependiente de parámetros LoRa PHY)
- Rango dinámico RSSI: 127 dB
- IIP3: -11dBm
- Conector IPEX -1
- Antena: +0.9 dBm (No especificado, es la antena más común y barata disponible – peor caso)

Esquemático de RF.

SX1276



5.1.3.2 Obtencion de estado

La obtención del estado del sistema de alarma es uno de los objetivos principales del proyecto. Cabe recordar que la correcta obtención del estado no es únicamente una cuestión cualitativa, para que el estado sea válido, debe ser obtenido en el momento que ocurre un evento. Con esto en mente podemos pensar una serie de métodos mediante el cual es posible lograr la obtención de estos.

La primera alternativa es el uso de la comunicación telefónica ya integrada, la idea principal es simular un sistema telefónico para que la alarma haga la llamada y transmita el evento como si lo hiciese contra la estación de monitoreo solo que en su lugar se colocará un dispositivo que transforma la señal de teléfono en LoRaWAN para recién allí enviar el evento.

Esta alternativa tiene sus ventajas y desventajas, por un lado, el sistema de alarmas garantiza que los eventos serán transmitidos por la línea utilizando protocolos estándar por lo que el comunicador puede ser utilizado de forma universal (al menos en teoría), además la configuración relacionada puede ser realizada directamente utilizando las opciones del sistema de alarma y es (a priori) la solución técnicamente más sencilla. Por otro lado, obtener el estado de esta forma anula completamente el cumplir con el pedido de prever la posibilidad de realizar comunicación dúplex (programar y activar la alarma remotamente), por otro lado, la simulación de una línea requiere el uso de bobinas de alta reactancia en audiofrecuencias (típicamente 4 Hy) las cuales encarecen significativamente el costo total.

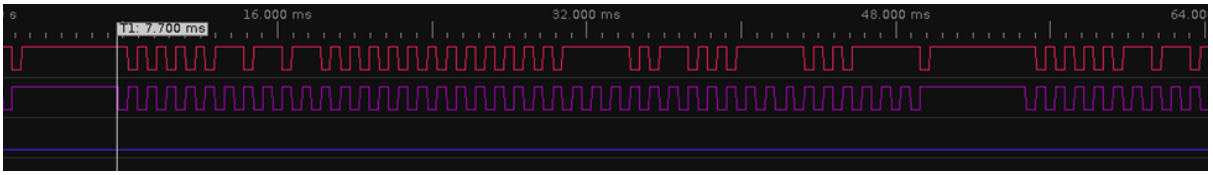
La segunda alternativa es realizar una conexión directa al panel de la alarma a través del bus de datos. La idea principal es establecer un dispositivo que actúe como sniffer del bus, de modo que cuando se detecte un evento se genere una comunicación.

Al igual que el caso anterior, esta alternativa tiene ventajas y desventajas, por un lado, garantiza cumplir con el pedido de prever la posibilidad de activar y programar la alarma remotamente (ya que en este mismo bus se conectan otros dispositivos como teclados y comunicadores). Requiere un trabajo más intensivo en cuanto a programación, pero el circuito electrónico es simple y en consecuencia su costo es menor. Como desventaja, el protocolo utilizado en el bus no sigue un estándar ni se encuentra publicado, sino todo lo contrario; es una comunicación propietaria por lo que utilizarlo requiere realizar ingeniería inversa y/o apoyarse en otros desarrollos extraoficiales. Además, será necesario verificar (una vez que se tenga un dispositivo funcional) la validez temporal de los eventos obtenidos, si bien es de suponer que observando el bus de comunicaciones interno el estado aparecerá al menos en simultáneo con la comunicación telefónica, en ningún momento el fabricante lo garantiza.

Teniendo en cuenta las ventajas y desventajas mencionadas, los requisitos y expectativas establecidas se decidió que inicialmente se optará por la conexión por bus de datos y se intentará validar este método. En caso de no cumplir las expectativas o no ser viable técnicamente, se optará por utilizar la conexión telefónica.

5.1.3.2.1 Conexión por bus de datos

El bus de datos del sistema de alarmas tiene 4 hilos, los cuales son fácilmente identificables mediante un osciloscopio o analizador lógico. Estos son RED, BLACK, GREEN y YELLOW; los hilos red y black son de alimentación y masa respectivamente, existiendo una diferencia de tensión 12.2 V entre las mismas que puede ser aprovechado como fuente de energía para todo el sistema, por otro lado, los hilos green y yellow son de datos y reloj respectivamente, y será de donde se obtendrán los bits que deben ser decodificados para obtener los estados. Todas las señales son de 12.2 V por lo que es posible que se necesite realizar adaptaciones de tensión para poder leer datos desde un microprocesador.



A partir de un análisis con un osciloscopio y un analizador lógico se pueden determinar lo siguiente:

- El reloj (clock) funciona a 1KHz
- Para marcar la separación entre dos mensajes, el reloj se mantiene en alto durante al menos 5 milisegundos (5 ciclos)
- La base central actúa como maestro y el resto de los dispositivos como esclavos. Los datos son enviados bidireccionalmente entre maestro y esclavo al mismo tiempo, en los flancos de reloj ascendentes el maestro está habilitado para escribir y en los flancos de reloj descendentes lo hacen los esclavos
- Los datos enviados por el maestro son principalmente de la forma:
    - Comando (8 bits)
    - Relleno (paridad ¿?) (1 bit)
    - Datos (x * 8 bits)
    - Suma de comprobación (8 bits) - Su aparición depende del comando
- La suma de comprobación es una simple suma de los otros bytes.
- Los esclavos responden desde el bit 9 en adelante.
- Un esclavo parece solo tener un drenaje abierto en la línea de DATOS, si no se envía nada, se leerá como un 1 lógico.

Teniendo en cuenta esto, se puede realizar el primer intento de leer el bus de datos desde el microcontrolador. Se necesita adaptar los niveles lógicos para poder ser leídos, en principio un simple divisor resistivo es suficiente para realizar esta tarea. Además, es necesario usar

una entrada de interrupciones para detectar cambios de nivel lógico en el reloj y un timer, debido a que cuando escribe un esclavo generalmente no lo hace perfectamente sincrónico con el cambio del reloj y es conveniente leer en el medio del pulso.

Luego de una intensa investigación damos con un proyecto destinado a la conexión de un microcontrolador con el bus de datos KeyBus. Si bien el mismo no logra decodificar por completo el contenido de los mensajes, es un gran paso en su objetivo. Está destinado principalmente a lograr un teclado funcional, por lo que la obtención de los eventos es secundaria; debido a esto, se hace uso de la interfaz capaz de captar datos y ordenarlos y del significado de la información decodificada, más que de las variables y estados que la librería ofrece.

Luego de observar el comportamiento del bus de datos por periodos prolongados, se puede observar que existe un sistema de notificaciones en el bus de datos, el mismo genera una notificación cada vez que un evento es detectado utilizando los comandos 0xA5 y/o 0xEB (dependiendo de la versión del sistema). Estos comandos se producen en sincronismo con la comunicación mediante línea telefónica fija y su contenido coincide plenamente con lo recibido en el sistema de monitoreo.

El contenido de los mensajes de las notificaciones es el siguiente:

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8
Command [0xA5] System status messages Partitions 1-2	Stop bit	Bit 0-3: year digit 2 Bit 4-7: Year digit 1	Bit 0-1: Day digit part 1 Bit 2-5: Month Bit 6-7: Partition	Bit 0-4: Hour bit 5-7: Day digit part 2	bit 0-1: Selects set of status commands 5 bit 2-7: Minute	Status	Unknown	CRC

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10
Command [0xA5] System status messages Partitions 1-8	Stop bit	Partition	Bit 0-3: year digit 2 Bit 4-7: Year digit 1	Bit 0-1: Day digit part 1 Bit 2-5: Month Bit 6-7: Unknown	Bit 0-4: Hour bit 5-7: Day digit part 2	bit 0-1: Unknown 5 bit 2-7: Minute	Selects set of status commands	Status	Unknown	CRC

En estos comandos nos interesan 3 items principales: los bits de partición, los bits de selección de set y los bits de estado. Los bits de partición indican a qué partición pertenece el evento o si se trata de un evento local. Existen (al menos) 11 sets de estados, dentro de los cuales pueden existir hasta $2^8 = 64$ estados distintos; de esta forma podemos imaginarnos a cada set como una tabla de estados y a cada estado como una entrada de esa tabla, luego cuando un comando de mensajes es leído utilizamos la tabla que indica el campo de set y el estado como un índice dentro de esta tabla. El listado con los eventos decodificados, su set correspondiente y el código de transmisión utilizado puede encontrarse entre los apéndices.

Una vez que identificamos un evento que necesita ser transmitido podemos pasar a generar un reporte.

5.1.3.2.2 Formato Contact ID

El protocolo Contact ID fue diseñado específicamente para la transmisión de eventos de alarmas domiciliarias a una estación de monitoreo utilizando como medio una línea telefónica. Para esto se hace uso de técnicas de DTMF a fin de transmitir datos por un medio diseñado para sonido, además de establecer la correspondencia entre pares de frecuencias y dígitos, establece una serie de señalizaciones para indicar distintos estados (handshake, kiss off, etc). Estos parámetros no son significativos por lo que no ahondaremos más en el tema.

Sobre estos parámetros funciona un formato de mensajes, el cual indica una conformación a seguir al momento de transmitir el evento, es el siguiente:

ACCT MT QXYZ GG CCC S

Donde:

- ACCT: Es el número de cuenta
- MT: Es el tipo de mensaje, para Contact ID corresponde 18
- Q: Es el calificador del evento, que aporta información específica al mismo
    - 1 para nuevo evento o apertura
    - 3 para restauración o cierre
    - 6 para evento ya comunicado, pero aún presente
- XYZ: Es el Código de evento
- GG: Es el grupo o partición, se utiliza 00 para no dar una partición específica
- CCC: Es el número de zona o de usuario, se utiliza 000 para no dar una zona o usuario específicos
- S: Suma de comprobación tal que al realizar la suma de todos los dígitos del mensaje y dividirlos por 15 el resto de 0.

El estándar establece también una serie de códigos de evento (XYZ) y su respectivo significado, en base a esto es que se estableció los códigos a utilizar que se encuentran detallados en el apéndice. Deja además espacio para agregar códigos personalizables en caso de ser necesario.

Cabe destacar que el estándar establece como válidos a los dígitos 0 – 9 y B – F, quedando excluido del uso el dígito A (10), puesto que el dígito 0 tiene en realidad el valor 10 y ese es su valor correspondiente al momento de calcular el checksum.

Es un formato muy sencillo, pero a su vez completo, además de ser ampliamente utilizado en múltiples equipos del sector; razón por la cual se decidió adoptar su uso para este proyecto pensando en la compatibilidad futura con un sistema de monitoreo.

Puede encontrarse una tabla con todos los eventos generados en el anexo 3, allí se especifica tanto el código de evento como los calificadores posibles.

5.1.3.2.3 Reporte de eventos y funcionamiento general

El funcionamiento general del sistema es tal que se mantienen en paralelo dos tareas principales, por un lado, la pila de protocolos LoRaWAN y por el otro el sistema de adquisición. La pila de protocolos se configura para trabajar en Clase A con un tiempo de polling de 5 segundos (se configuran todas las claves y parámetros necesarios para funcionar con la red ya establecida), esto quiere decir que cada 5 segundos se transmitirá un mensaje en caso de estar disponible.

El sistema de adquisición hace uso de un timer, un pin de interrupciones y una memoria fifo (implementada dentro de la memoria interna del microcontrolador). El uso del timer y la interrupción es para la obtención de datos en crudo del bus, pues una vez detectado un cambio de estado en el pin de interrupción se establece un timer para leer exactamente en el medio del pulso de datos (250 uSeg después) y obtener así la cadena de bits correspondiente al mensaje. Además, si no se detecta una interrupción en un periodo de tiempo mayor a 5 ciclos de reloj se interpreta que la cadena ha finalizado y se pasa esa información al sistema decodificador. El sistema decodificador establece si la cadena recibida es un comando de notificación y si lo fuese, se genera a partir del set de estados y el estado en sí, el código contact ID correspondiente, además de la partición. Estos datos son ordenados y almacenados en la memoria fifo a la espera de que la pila LoRaWAN los pida para enviarlos.

De forma externa, la pila de protocolos tiene pocas interacciones con el sistema de adquisición, la interfaz le permite indicarle 4 eventos: conexión establecida, conexión perdida, pedido de mensaje para enviar y mensaje enviado con éxito. En un funcionamiento normal, la pila de protocolos estará permanentemente pidiendo mensajes para transmitir, pero solo transmitirá cuando exista un mensaje disponible, una vez que se confirma que el mensaje se transmitió exitosamente se notifica al sistema de adquisición para que elimine el mismo de la fila. Por otro lado, si por algún motivo se perdiera la conexión, la pila de protocolos informa al sistema de adquisición y pasa al estado de reconexión. (Durante este tiempo el sistema de adquisición acumula mensajes en la memoria fifo en caso de quedarse sin espacio, elimina los mensajes más viejos para hacer lugar a los nuevos). En caso de reconectarse, se da aviso al sistema de adquisición y el mismo primero genera un mensaje de reconexión y a partir de allí comienza a enviar todos los mensajes que tenga en fila, una vez se vacíe la memoria el funcionamiento vuelve a ser el normal. Situación similar ocurre en caso de reinicio o inicio por primera vez del microcontrolador, en este caso se genera un mensaje de restablecimiento del comunicador antes de empezar a transmitir con normalidad.

Para facilitar la validación y manejo de los mensajes en el otro extremo, se modifica ligeramente el formato CID, en lugar de enviar todos los dígitos seguidos se hace uso de un separador que no se encuentra entre los dígitos disponibles y que no se computa en el checksum, simplemente sirve para marcar los distintos campos dentro de la cadena enviada.

5.1.3.3 Integración con software de monitoreo

5.1.3.3.1 Extracción de datos

Una vez que se tienen los mensajes en el servidor LoRaWAN necesitamos un método para extraer los mismos. El servidor de aplicación permite conectarse y realizar esta acción de diversas formas, en este caso y por simplicidad, utilizaremos la integración por protocolo MQTT.

MQTT es un protocolo de comunicación M2M (machine-to-machine) de tipo message queue, es un servicio de mensajería push con patrón publicador/suscriptor (pub-sub). En este tipo de infraestructuras los clientes se conectan con un servidor central denominado broke. Para filtrar los mensajes que son enviados a cada cliente los mensajes se disponen en topics organizados jerárquicamente. Un cliente puede publicar un mensaje en un determinado topic. Otros clientes pueden suscribirse a este topic, y el broker le hará llegar los mensajes suscritos.

Los clientes inician una conexión TCP/IP con el broker, el cual mantiene un registro de los clientes conectados. Esta conexión se mantiene abierta hasta que el cliente la finaliza. Por defecto, MQTT emplea el puerto 1883 y el 8883 cuando funciona sobre TLS.

MQTT dispone de un mecanismo de calidad del servicio o QoS, entendido como la forma de gestionar la robustez del envío de mensajes al cliente ante fallos (por ejemplo, de conectividad). MQTT tiene tres niveles QoS posibles:

- QoS 0 unacknowledged (at most one): El mensaje se envía una única vez. En caso de fallo por lo que puede que alguno no se entregue.
- QoS 1 acknowledged (at least one): El mensaje se envía hasta que se garantiza la entrega. En caso de fallo, el suscriptor puede recibir algún mensaje duplicado.
- QoS 2 assured (exactly one). Se garantiza que cada mensaje se entrega al suscriptor, y únicamente una vez.

Usar un nivel u otro depende de las características y necesidades de fiabilidad de nuestro sistema. Lógicamente, un nivel de QoS superior requiere un mayor intercambio mayor de mensajes de verificación con el cliente y, por tanto, mayor carga al sistema.

La seguridad siempre debe ser un factor importante que considerar en cualquier sistema de comunicación M2M. El protocolo MQTT dispone de distintas medidas de seguridad que podemos adoptar para proteger las comunicaciones. Esto incluye transporte SSL/TLS y autenticación por usuario y contraseña o mediante certificado. Sin embargo, hay que tener en cuenta que muchos de los dispositivos IoT disponen de escasa capacidad, por lo que el SSL/TLS puede suponer una carga de proceso importante.

La integración requiere entonces que nos suscribamos a un topic específico, para que el broker nos envíe toda la información que nos es útil. El esquema de los topics es el siguiente:

```
application/[ApplicationID]/device/[DevEUI]/event/[EventType]
```

Nuestro objetivo es recibir todos los eventos, de todos los dispositivos relacionados con la aplicación creada, por lo que el topic al cual debemos suscribirnos es:

```
application/ID/device/+/event/#
```

Para suscribirnos debemos utilizar un usuario y contraseña que previamente deberá ser cargada en el broker. Para realizar esta tarea utilizaremos un programa escrito en Python, el cual se encuentra corriendo de forma permanente en el mismo servidor donde se encuentra Chirpstak. Una vez que somos capaces de obtener los mensajes, se realiza una separación y validación y, si no se encuentra ningún error, está listo para ser ingresado en el software de monitoreo.

5.1.3.3.2 Inyección de datos

El software de monitoreo permite la adición y configuración de recibidoras, de modo tal que se pueden agregar distintos modelos y todas terminan siendo integradas en un mismo software. Una de las recibidoras es la llamada SIA IP, esta recibidora en lugar de integrarse con un equipo funciona como una recibidora de software, siguiendo el estándar SIA-DC-09, pensado para la comunicación de eventos sobre IP.

El objetivo de este estándar es detallar el protocolo y los detalles relacionados para informar eventos desde el equipo de las instalaciones a una estación central utilizando el protocolo de Internet (IP) para transmitir el contenido del evento. Es importante distinguir que, si bien este método de notificación utiliza el protocolo de interfaz de receptor a computadora SIA como base, está diseñado para el transporte de eventos desde instalaciones protegidas a una estación central, posiblemente utilizando la Internet pública.

Este estándar está destinado a los fabricantes de paneles de control y receptores de estaciones centrales para garantizar la compatibilidad del equipo, así como a todas las partes afectadas. El cumplimiento de esta norma es voluntario.

Una vez configurada esta recibidora para recibir en un determinado puerto UDP, podemos comenzar a enviarle mensajes siguiendo el formato correspondiente. El formato del protocolo SIA-DC-09 es compatible con el formato Contact ID, por lo que dentro del mensaje se especifica este formato y luego es posible enviar los campos tal y como especifica CID.

El funcionamiento general del sistema de integración es el siguiente: se escucha de forma permanente el topic MQTT a la espera de eventos, cuando un evento llega es validado y, si pasa la prueba, se lo introduce en un mensaje que es enviado a la recibidora de software. Por otro lado, se realiza un envío periódico de mensajes a la recibidora, a modo de test, de forma tal que sea factible detectar que el sistema de integración se mantiene funcionando.

Además, la integración fue configurada como un servicio en systemd (gestor de daemons de Linux) de modo tal que arranca en conjunto con el sistema operativo y hace uso del watchdog que provee el mismo, permitiendo reiniciarse si ocurriese algún error durante la ejecución.

El programa de integración cuenta además con las siguientes características:

- Sistema de configuración por archivo toml, con validación de configuración previo a arranque

- Sistema de generación de archivos de logs de eventos, con diferenciación de tipo de eventos según su naturaleza (críticos, error, información) con permanencia configurable. Replicado en el sistema de logs de systemd: journalctl.

Por otro lado, el software de monitoreo asocia el número de cuenta que contiene cada mensaje recibido con una cuenta específica y decodifica el CID siguiendo la misma tabla utilizada para su codificación, por lo que en cada cuenta aparece un listado de eventos ocurridos de modo tal que un operador pueda leerlos fácilmente.

5.1.4 Análisis de resultados

5.1.4.1 Etapa de pruebas

Una vez se obtuvo un prototipo funcional, se propone la realización de una prueba para ver la confiabilidad y estabilidad de este. La misma consiste en configurar el sistema de alarma para que envíe un reporte de testeo cada 10 minutos, se configura también el software de monitoreo para generar una alerta cada vez que la señal no se recibe en tiempo y forma. La prueba se realizó durante 44 días corridos (desde el 16/7/22 al 29/8/22) arrojando los siguientes resultados.

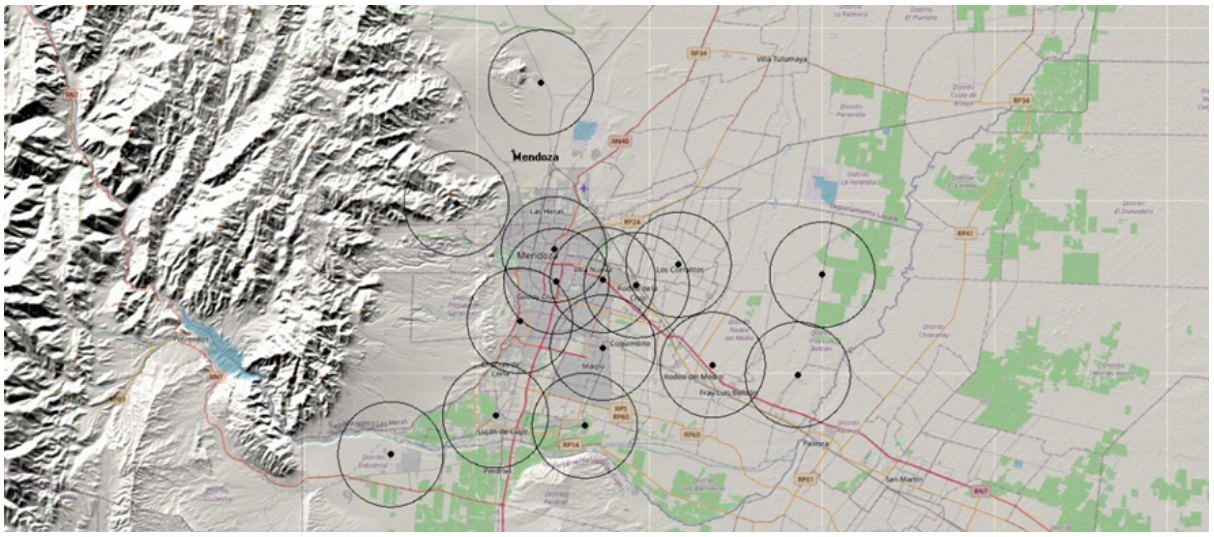
Resultado de prueba estabilidad	
Duración de la prueba	44 días (63360 minutos)
Intervalo mensaje de testeo	10 minutos
Reportes de testeo esperados	6336 mensajes
Alerta software falta de testeo	65 veces
Porcentaje falla	1,03%
Comunicaciones exitosas	98,97%

Con los resultados obtenidos podemos afirmar que el prototipo es estable en su funcionamiento y logra transmitir eventos con una alta confiabilidad.

5.1.4.2 CÁLCULO DE COBERTURA

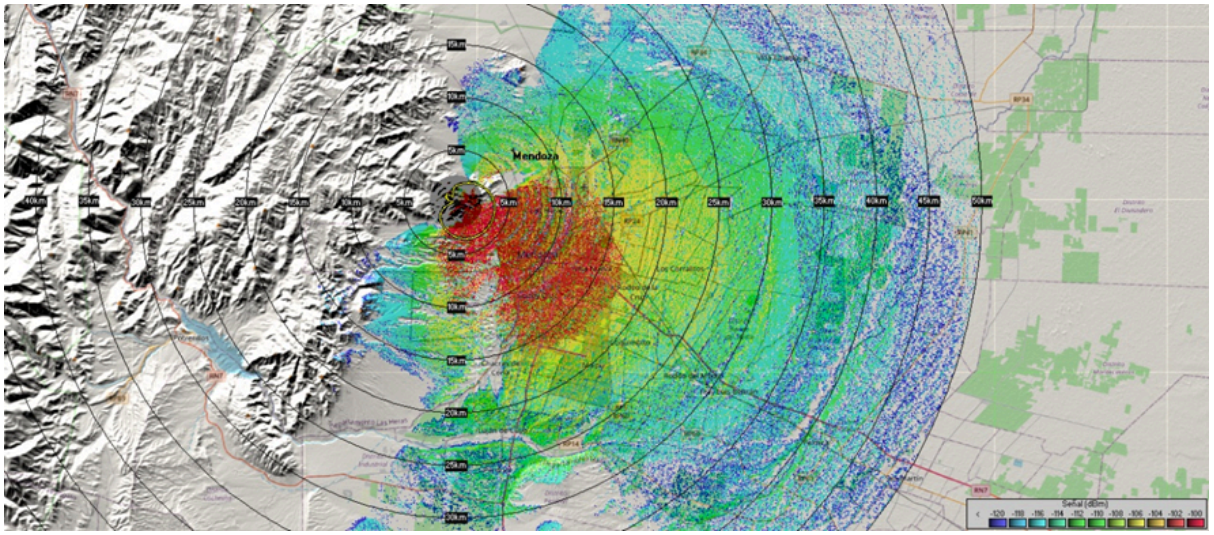
Para la simulación del cálculo de cobertura se hizo uso del software RadioMobile, el cual está destinado para este fin y es de licencia gratuita. Se utilizó como base la guía conferencia de TTN para Radio Planning con las modificaciones adecuadas. En cuanto a los sitios, se basó su ubicación en puntos en los que la empresa solicitante ya cuenta conectividad y disponibilidad de antenas, los mismos se detallan a continuación:

Nodo	Coordenadas	Altura	Torre
Cerro arco	-32.84483622223687, -68.92758139823286	1.511,30	18
Dorrego	-32.91139114957135, -68.82563599796457	772,00	30
Guaymallén	-32.88425735144635, -68.82802339623015	736,00	24
Villanueva	-32.91032670298284, -68.77830893645358	729,00	24
Rodeo de la Cruz	-32.914800115779066, -68.74396651421614	703,00	30
Rodeo del Medio	-32.98296718365088, -68.66639257214413	695,00	30
Los Corralitos	-32.89722301429389, -68.7010960794481	657,00	24
Las Margaritas Norte	-32.90581702266007, -68.55459191359344	643,00	24
Las Margaritas sur	-32.9913396024352, -68.5794445518717	665,00	30
Capdeville	-32.741534129902924, -68.84138239623222	754,00	30
Godoy Cruz Oeste	-32.94522478607956, -68.86288542386312	866,00	18
Maipú	-32.96817243866873, -68.7783049035805	792,00	30
Parque Industrial Luján	-33.05941343351444, -68.99457036961206	1.094,00	30
Drumond	-33.02613358494945, -68.88771219707708	958,00	30
Cruz de Piedra	-33.03489266188749, -68.79669616226899	867,00	60



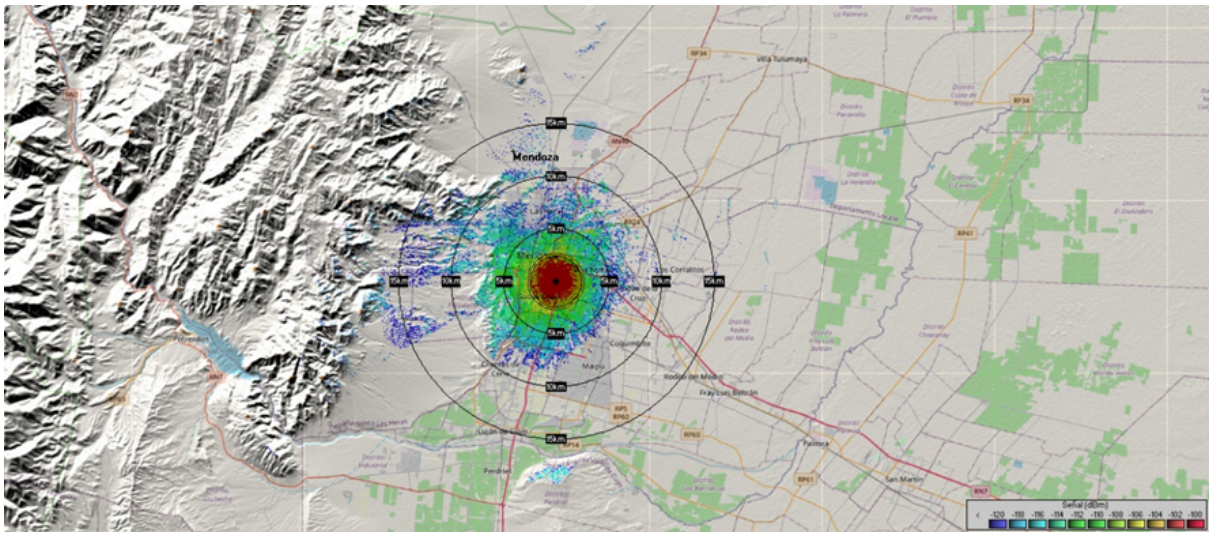
Todas las simulaciones realizadas a continuación utilizan los datos previamente mencionados en este informe, sin embargo, con el objetivo de lograr que la simulación se aproxime más a la realidad se disminuyó en 10 dB la sensibilidad de los dispositivos (esto debido a que el software solo tiene en consideración la forma del terreno pero no la presencia de edificios u otros obstáculos similares)

En el Sitio Cerro Arco, se simuló utilizando una antena direccional tipo panel de 10 dBi para evitar radiar en direcciones innecesarias, el resultado obtenido es el siguiente:

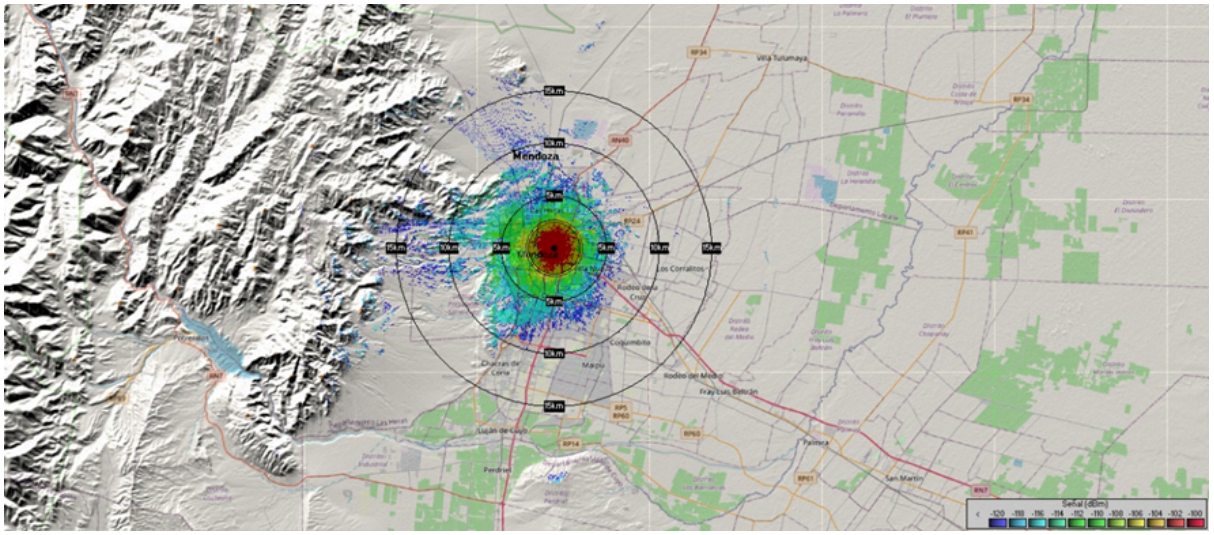


En el resto de los sitios, se simuló utilizando la antena omnidireccional correspondiente al Gateway Mikrotik, con 6,5 dBi de ganancia. Los resultados obtenidos son los siguientes:

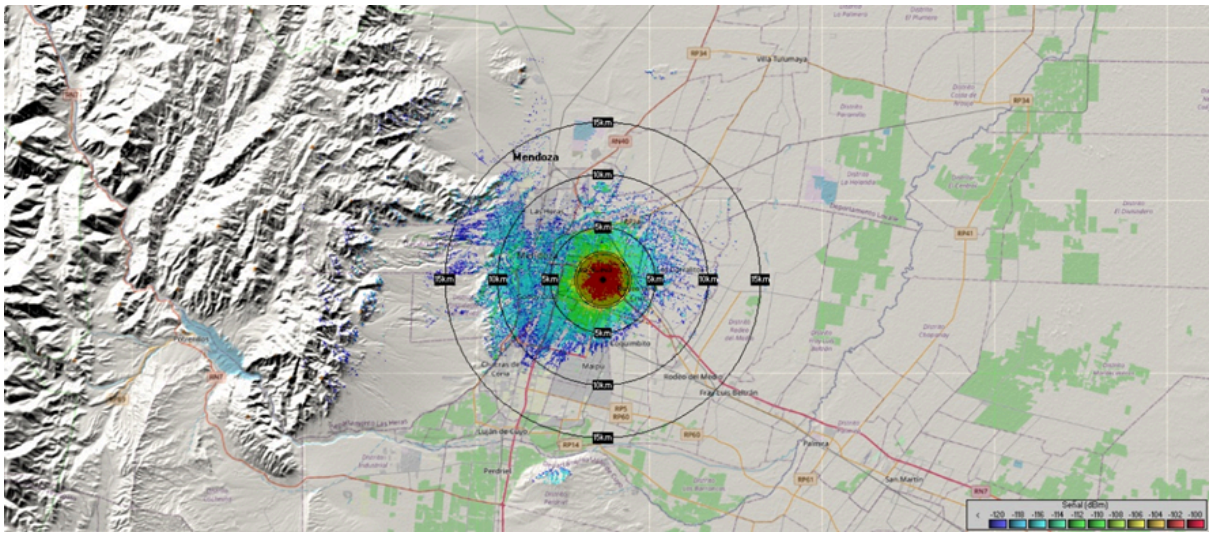
Sitio Dorrego:



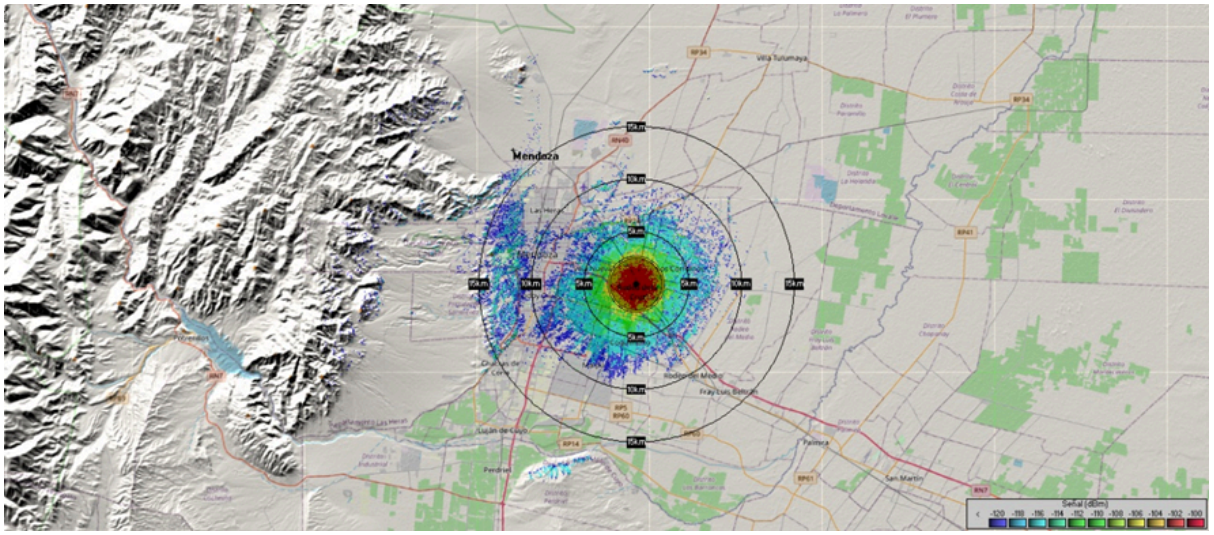
Sitio Guaymallén:



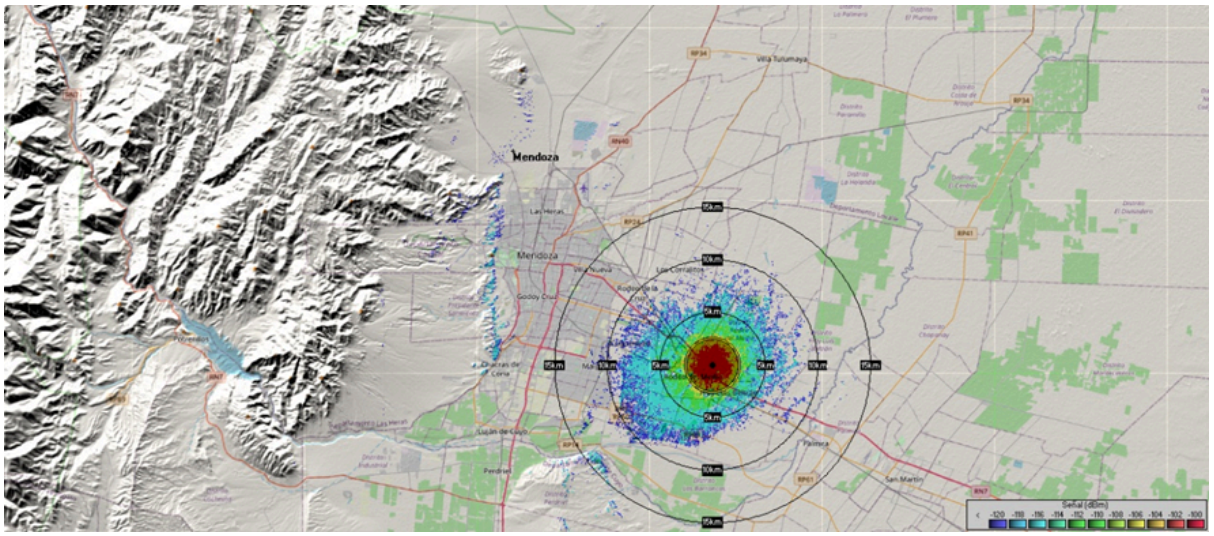
Sitio Villanueva:



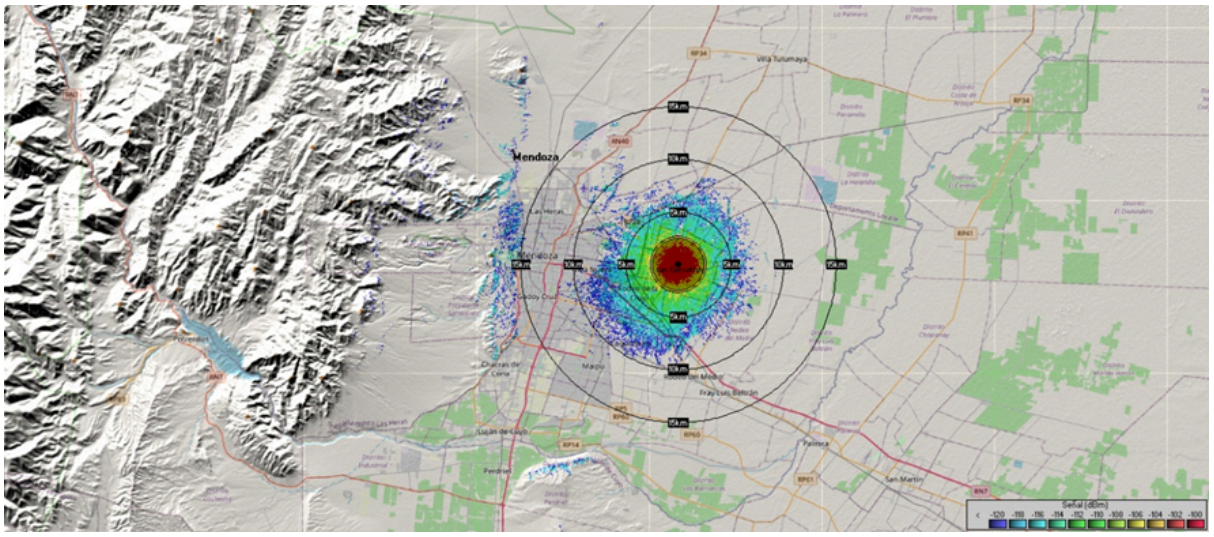
Sitio Rodeo de la Cruz:



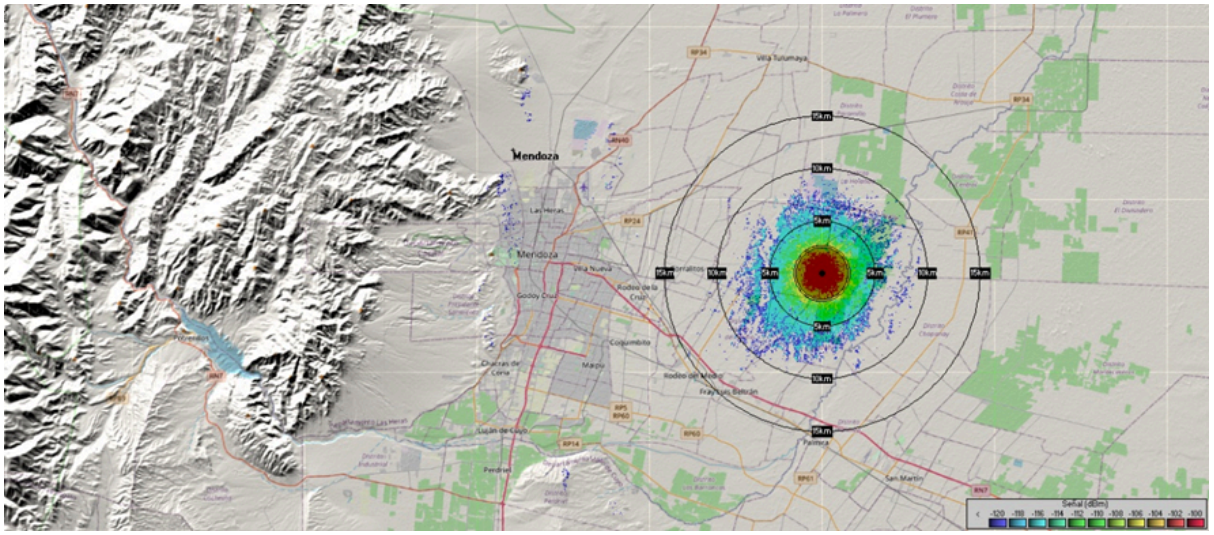
Sitio Rodeo del Medio:



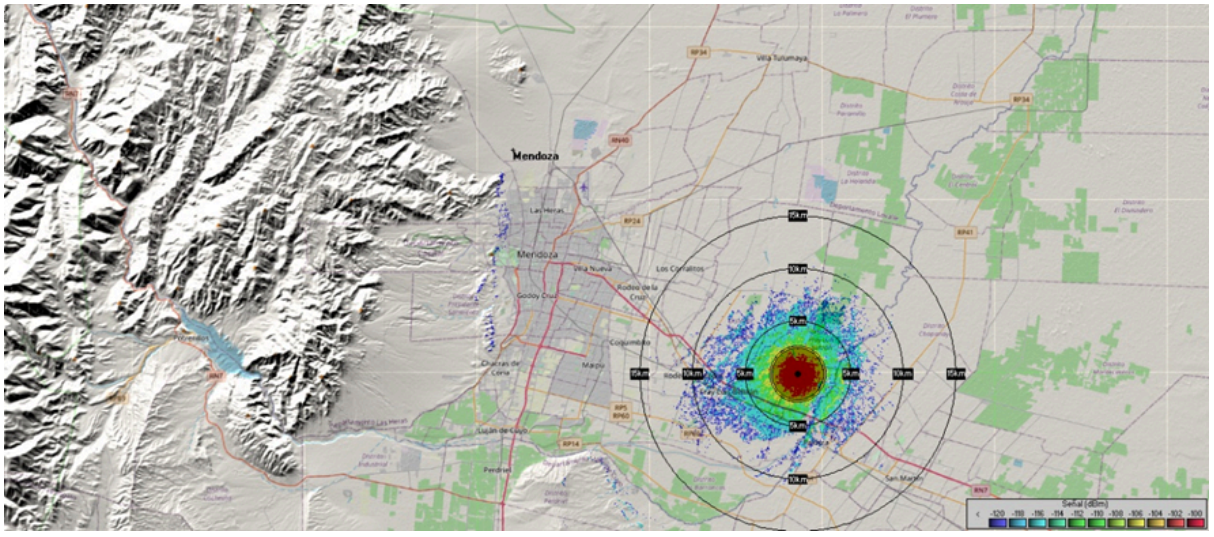
Sitio Los Corralitos:



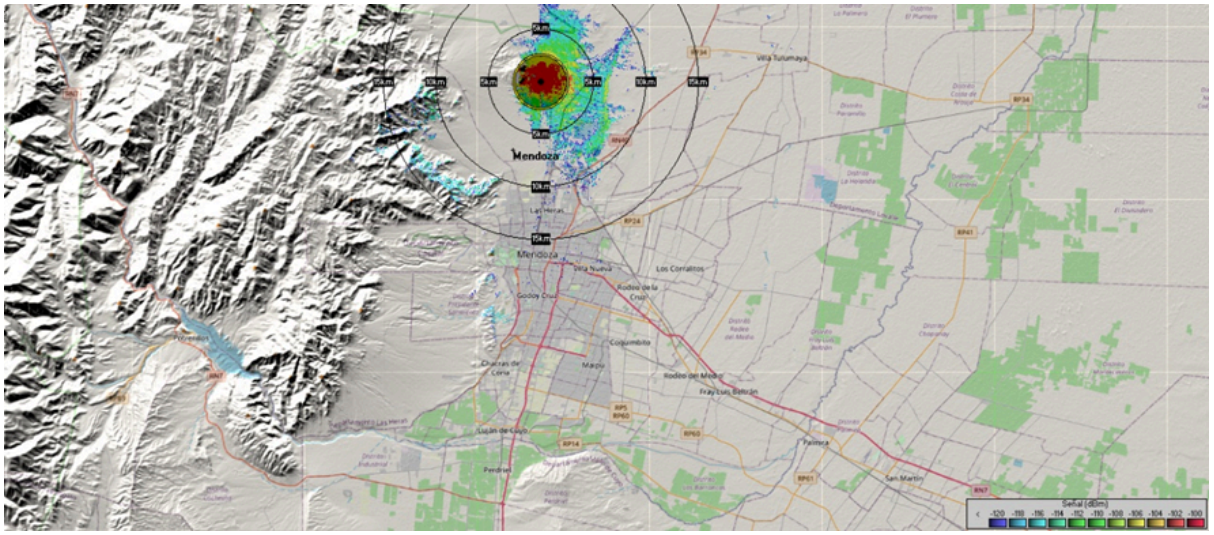
Sitio Las Margaritas Norte:



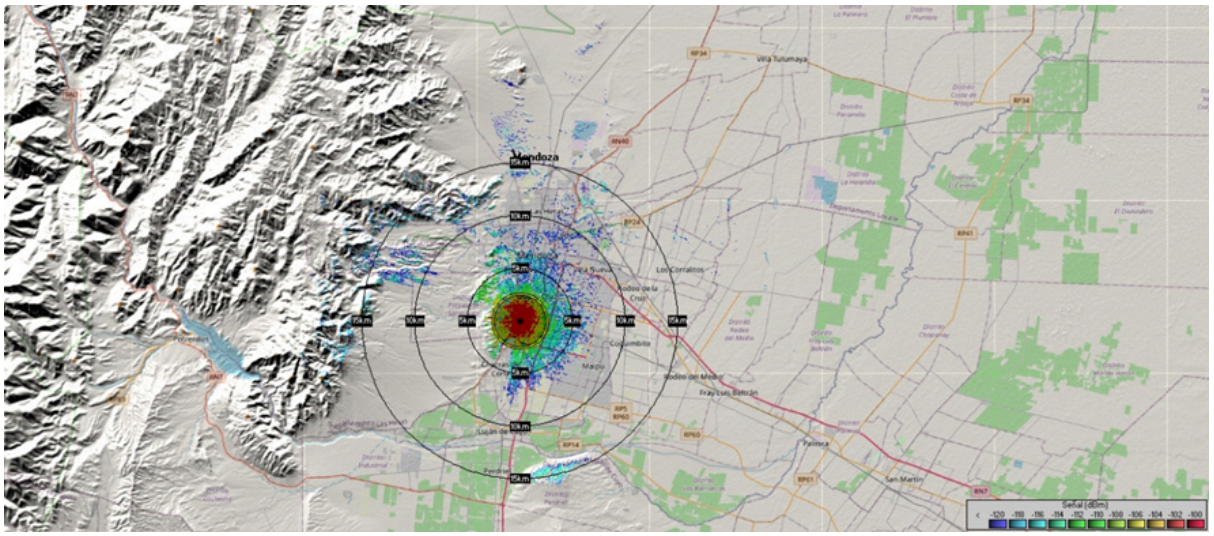
Sitio Las Margaritas Sur:



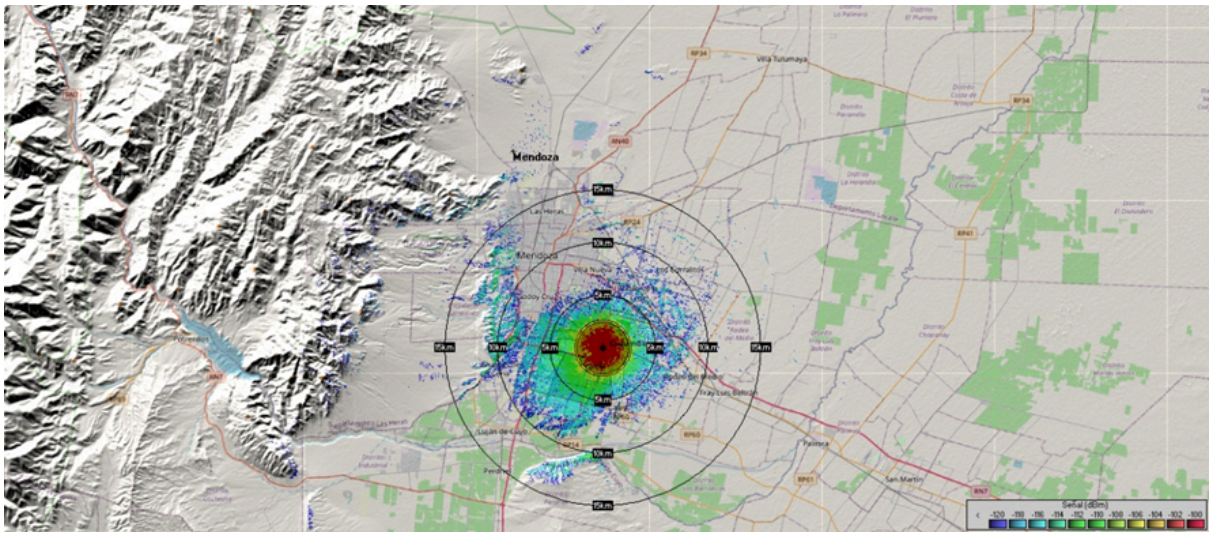
Sitio Capdeville:



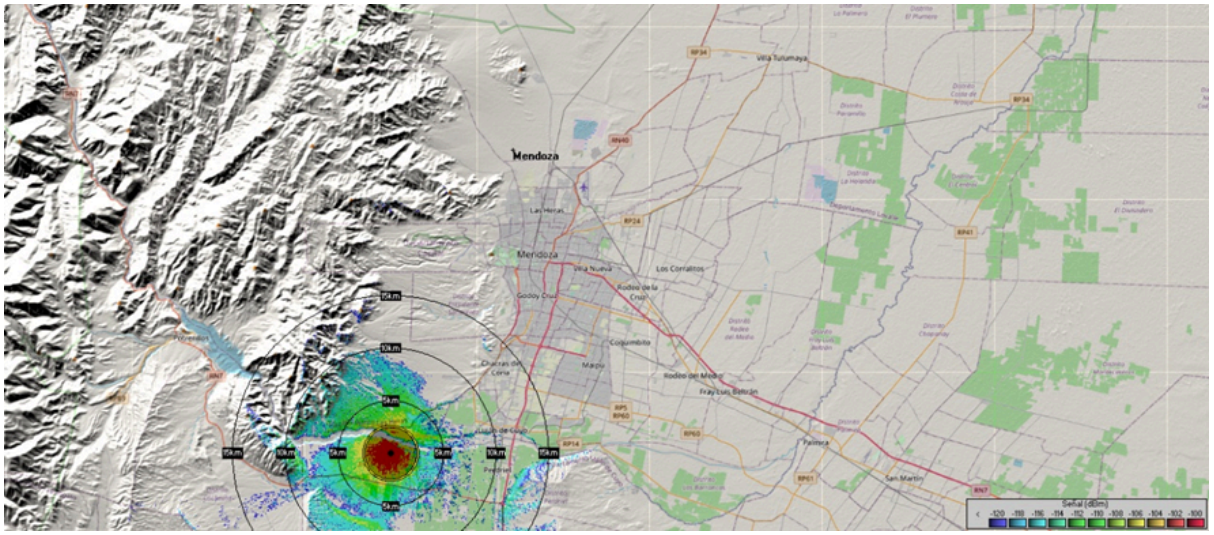
Sitio Godoy Cruz Oeste:



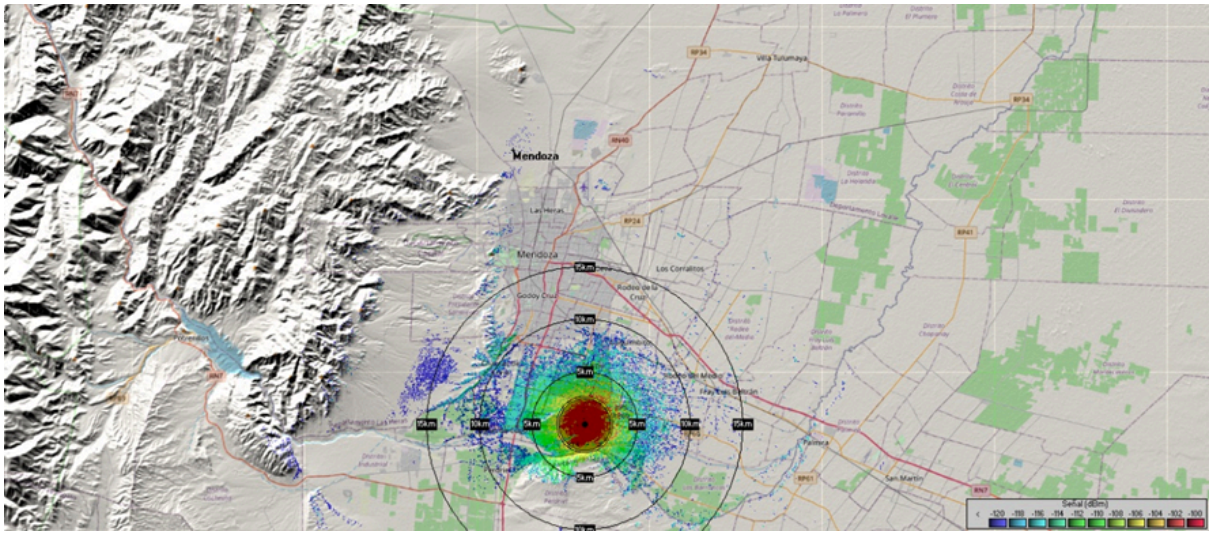
Sitio Maipú:



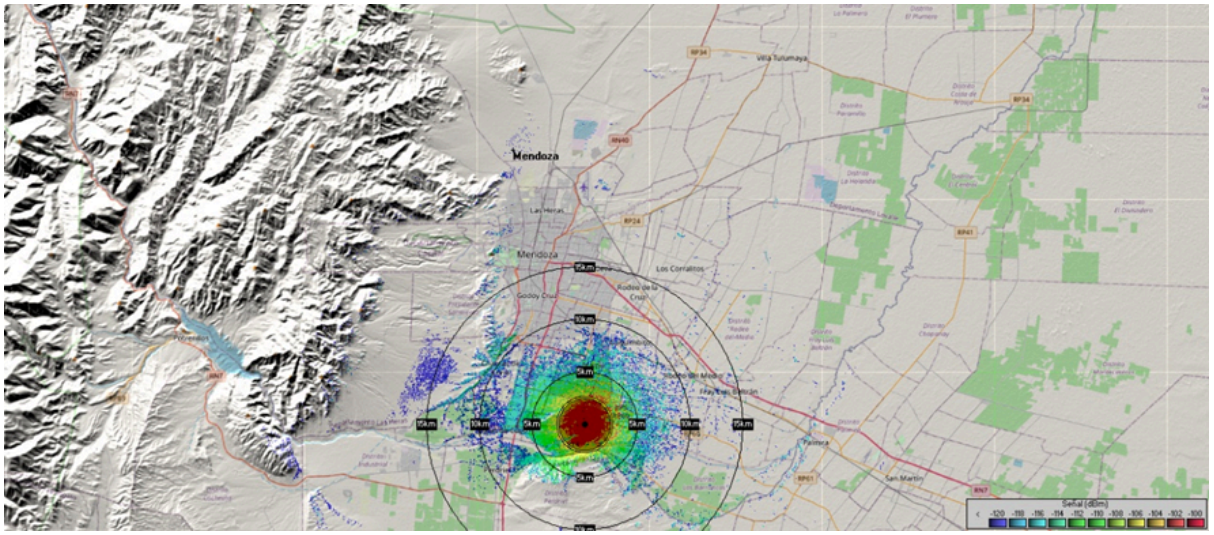
Sitio Parque industrial Luján:



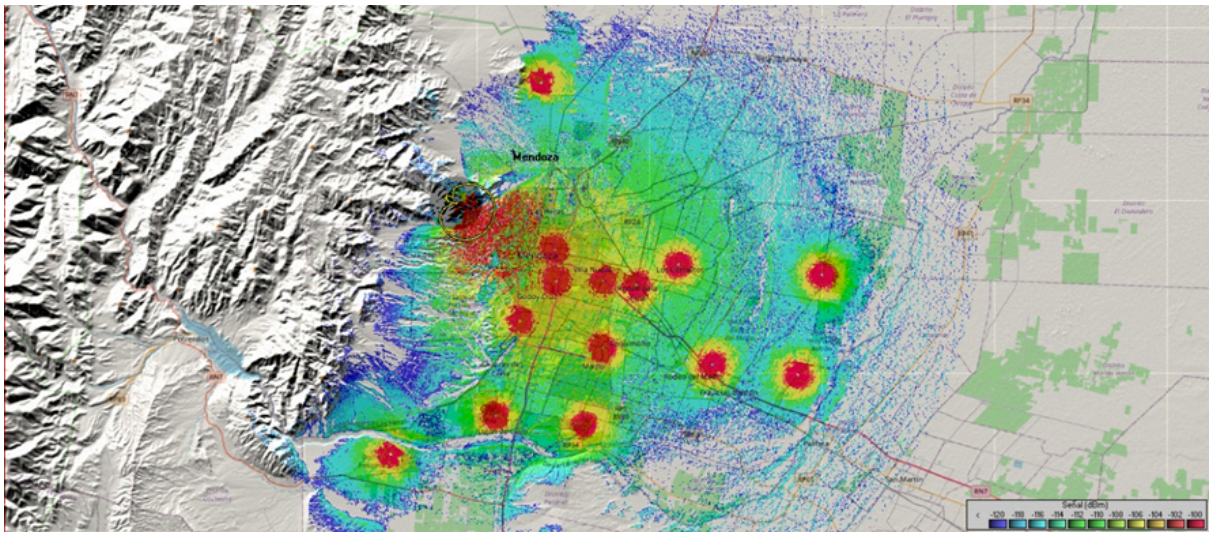
Sitio Drumond:



Sitio Cruz de piedra:

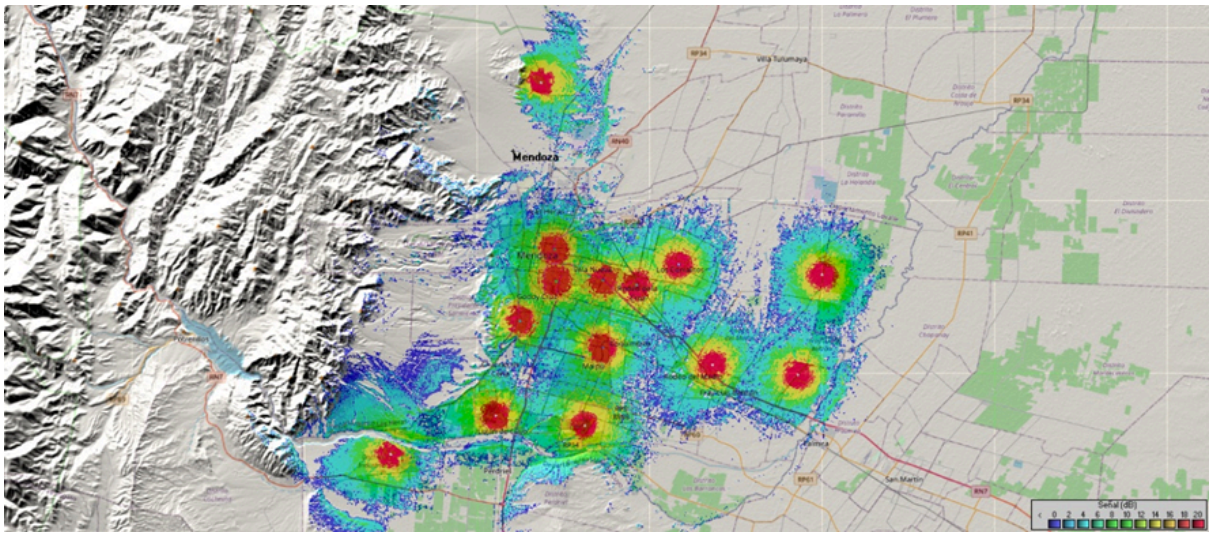


Una vez que tenemos una idea de la capacidad de cobertura de cada sitio en particular, pasamos a simular el comportamiento en conjunto de varios sitios. Si pusiéramos en funcionamiento todos los sitios en simultáneo el mapa de cobertura se vería así:



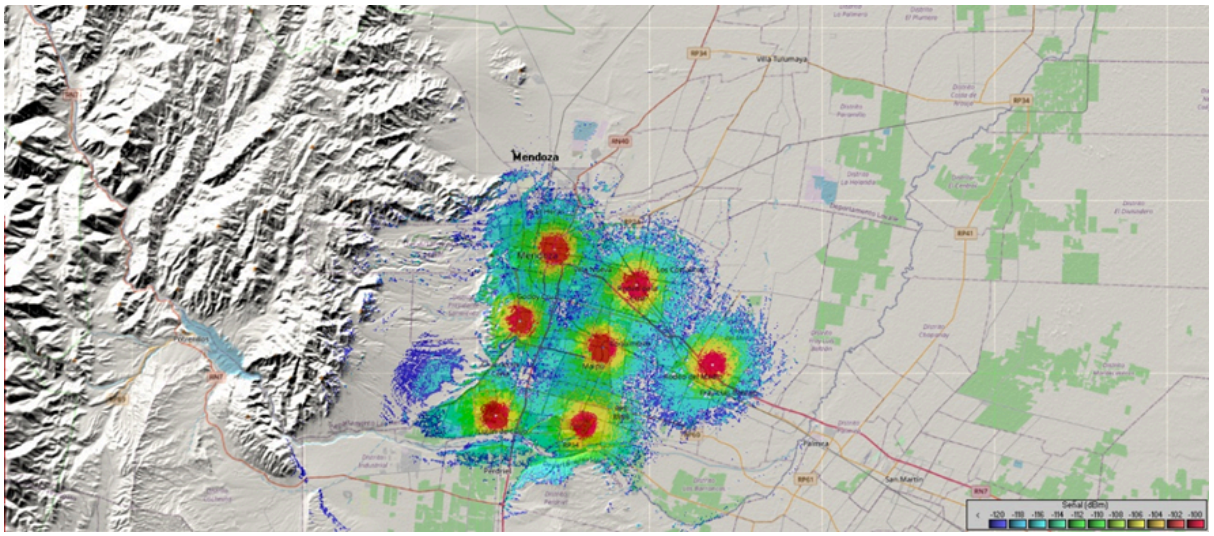
Podemos observar que se cubre por completo la ciudad de Mendoza y alrededores con buena señal

Sin embargo, gran parte del aporte de cobertura lo realiza el sitio del Cerro Arco, si no consideramos el mismo el mapa se vería así:

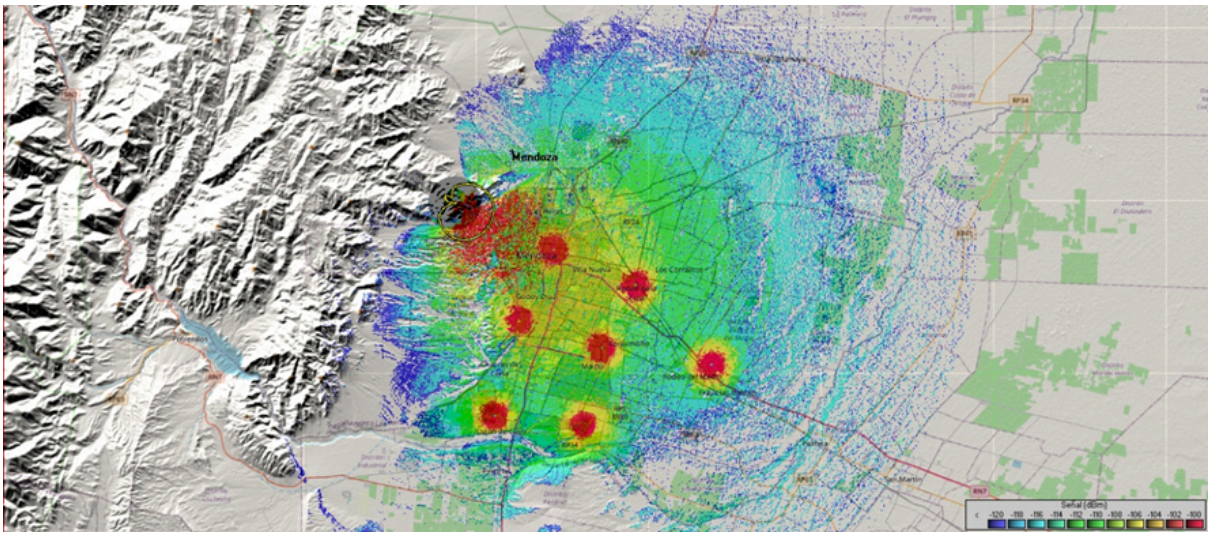


Podemos ver que se mantiene la buena cobertura en lugares altamente poblados, pero existen zonas de características rurales que dejamos de cubrir.

Por otro lado, considerando que existen algunos lugares donde los sitios se encuentran cercanos entre sí, podemos realizar una selección, obteniendo el siguiente mapa:



Y si a la selección realizada le sumamos el sitio del Cerro Arco, se obtiene el siguiente mapa:



De estas simulaciones se desprende que para lograr una buena cobertura es necesaria la puesta en marcha de alrededor de 8 sitios

Las imágenes mostradas se dejan como archivo adjunto, las mismas pueden ser visualizadas utilizando Google Earth o similar.

5.1.5 Anexos

5.1.5.1 Anexo 1: Comparativa redes LPWAN

Global standard used	Frequency bands	Channel width	Range	Maximum end node transmit power	Packet size	Data rate (uplink/downlink)	Topology	End node roaming allowed
DASH7 Alliance Protocol 1.x	433/868/915 MHz ISM/SRD	25 kHz or 200 kHz	0–5 km	433 MHz: +10dBm 868/915 MHz: +27dBm	max. 256 bytes/packet	9.6 kbit/s, 55.55 kbit/s or 166.667 kbit/s / 9.6 kbit/s, 55.55 kbit/s or 166.667 kbit/s	Node-to-node, Star, Tree	Yes
IEEE P802.11ah (low power Wi-Fi)	Unlicensed Sub-1 GHz bands (excluding TV whitespace)	1/2/4/8/16 MHz	Up to 1 km (outdoor)	Dependent on Regional Regulations (from 1	Up to 7,991 Bytes (w/o Aggregation), up	150 kbit/s ~ 346.666Mbit/s/150kbit/s ~ 346.666Mbit/s	Star, Tree	Allowed by other 802.11 amendments

				mW to 1 W)	to 65,535 Bytes (with Aggregation)			(like 802.11r)
Ingenu RPMA	2.4 GHz ISM	1 MHz (40 channels available)	>500 km LoS	to 20 dBm	6B–10 kB	AP aggregates to 624 kbit/s per Sector (Assumes 8 channel Access Point)/AP aggregates to 156 kbit/s per Sector (Assumes 8 channel Access Point)	Typically Star. Tree supported with an RPMA extender	Yes
LTE-Cat M	Cellular	1.4 MHz	2.5–5 km	100 mW	~100-~1000 bytes typical	~200 kbit/s/~200 kbit/s	Star	Yes
LoRaWAN	433/868/780/915 MHz ISM	EU: 8x125kHz, US 64x125kHz/8x125kHz, Modulation: Chirp Spread Spectrum	2–5km (urban), 15km (rural), 702 km LoS tested,[3] 1500 km Link Budget[4]	EU:<+14 dBm, US:<+27 dBm	User defined	EU: 300 bit/s to 50 kbit/s/300 bit/s to 50 kbit/s, US:900 bit/s-100kbit/s/900bit/s-100kbit/s	Star on Star	Yes
nWave	Sub-1 GHz ISM	Ultra narrow band	10 km (urban), 20–30 km (rural)	25–100 mW	12 byte header, 2-20 byte payload	100 bit/s/-	Star	Yes

SigFox	868/902 MHz ISM	Ultra narrow band	30–50 km (rural), 3–10 km (urban), 1000 km LoS	10µW to 100 mW	12 bytes (payload)	100 bit/s to 140 messages/day/ max. 4 messages of 8 bytes/day	Star	Yes
Weightless-W	400-800 MHz (TV whitespace)	5 MHz	5 km (urban)	17 dBm	10 byte min.	1 kbit/s to 10 Mbit/s/1 kbit/s to 10 Mbit/s	Star	Yes
Weightless-N	Sub-1 GHz ISM	Ultra narrow band (200 Hz)	3 km (urban)	17 dBm	Up to 20 bytes	100 bit/s/-	Star	Yes
Weightless-P	Sub-1 GHz ISM	12.5 kHz	2 km (urban)	17 dBm	10 byte min.	200 bit/s to 100 kbit/s/200 bit/s to 100 kbit/s	Star	Yes

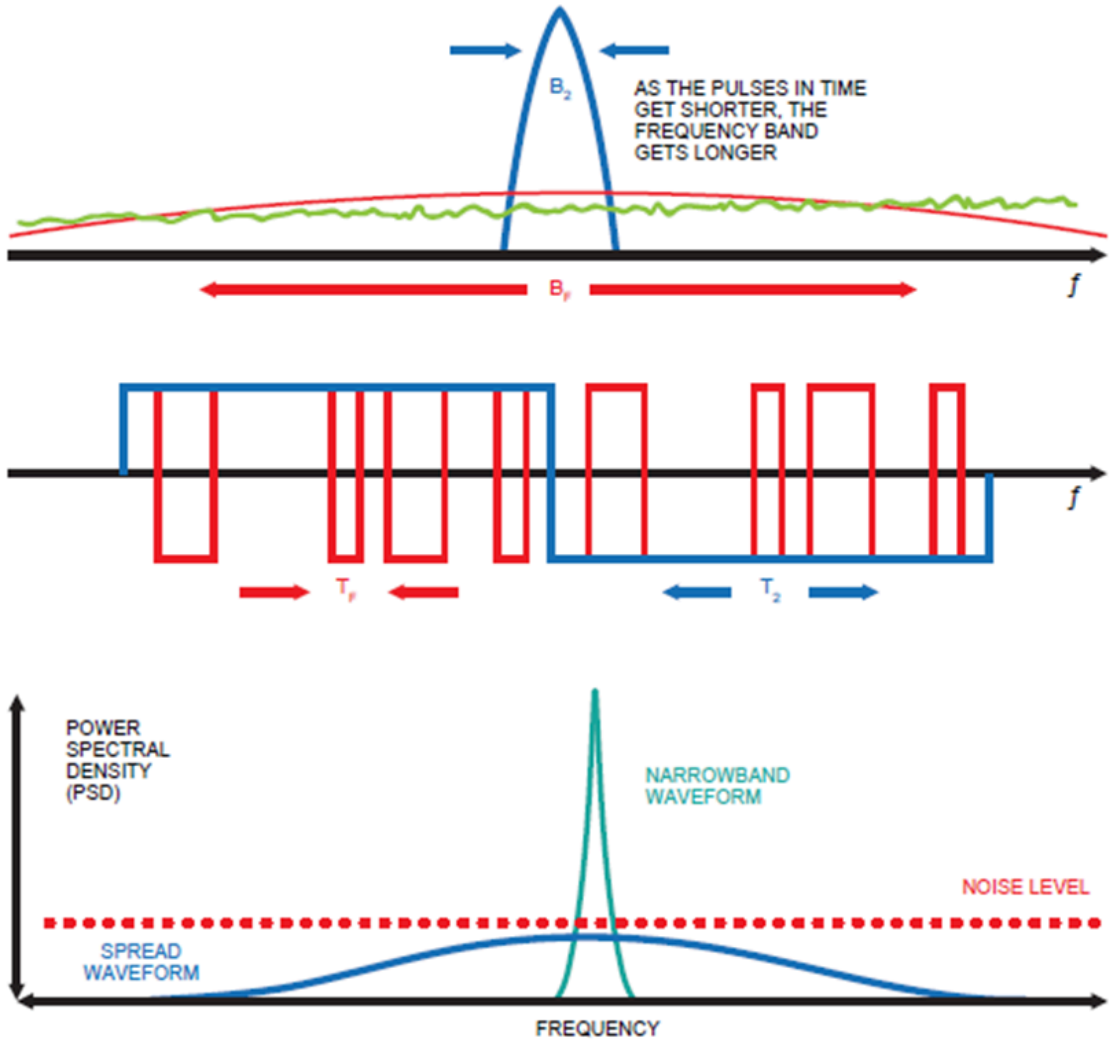
5.1.5.2 Anexo 2: LoRa PHY Modulación de radio - LoRa

Una técnica patentada de modulación de espectro ensanchado derivada de la tecnología Chirp Spread Spectrum (CSS) ofrece un compromiso entre sensibilidad y velocidad de datos, mientras opera en un canal de ancho de banda fijo de 125 KHz o 500 KHz (enlace ascendente), y 500 KHz (enlace descendente). Además, LoRa utiliza factores de dispersión ortogonales (orthogonal spreading factors – OVSF), esto permite que la red conserve la duración de la batería de los nodos finales conectados al realizar optimizaciones adaptativas de los niveles de potencia y las velocidades de datos de un nodo final individual. Por ejemplo, un dispositivo final ubicado cerca de una puerta de enlace debe transmitir datos con un factor de dispersión bajo, ya que el riesgo de desconectar el enlace es bajo. Sin embargo, un dispositivo final ubicado a varios kilómetros de una puerta de enlace necesitará transmitir con un factor de dispersión mucho más alto. Este factor de dispersión más alto proporciona una mayor ganancia de procesamiento, y una mayor sensibilidad de recepción, sin embargo, la velocidad de la comunicación será necesariamente menor.

LoRa es una implementación de capa puramente física (PHY) o de "bits", según lo define el modelo de red de siete capas de OSI. En lugar de cableado, el aire se utiliza como medio para transportar ondas de radio LoRa desde un Transmisor de RF en un dispositivo IoT a un receptor de RF en una puerta de enlace y viceversa.

** No existe una relación uno a uno entre los dispositivos basados en LoRa y las puertas de enlace en una red LoRaWAN; los mensajes enviados hacia y desde los dispositivos finales viajan a través de todas las puertas de enlace dentro del alcance. La deduplicación es manejada por el servidor de red.*

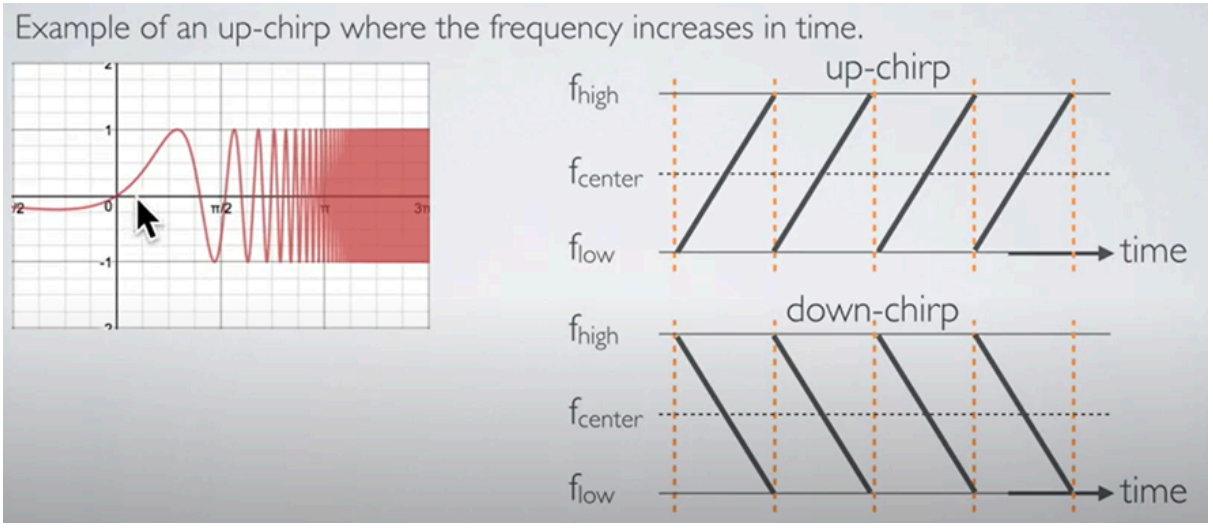
En un sistema tradicional o de espectro ensanchado de secuencia directa (DSSS), la fase portadora de la señal del transmisor cambia de acuerdo con una secuencia de código. Al multiplicar la señal de datos con un patrón de bits predefinido a una velocidad mucho mayor, también conocido como código de expansión (spreading code o secuencia de chip), se crea una señal "más rápida" que tiene componentes de frecuencia más alta que la señal de datos original. Esto significa que el ancho de banda de la señal se extiende más allá del ancho de banda de la señal original. En la terminología de RF, los bits de la secuencia de código se denominan chips (para distinguir entre los bits más largos, no codificados, de la señal de datos original). Cuando la señal transmitida llega al receptor de RF, se multiplica por una copia idéntica del código de dispersión utilizado en el transmisor de RF, lo que da como resultado una réplica de la señal de datos original.

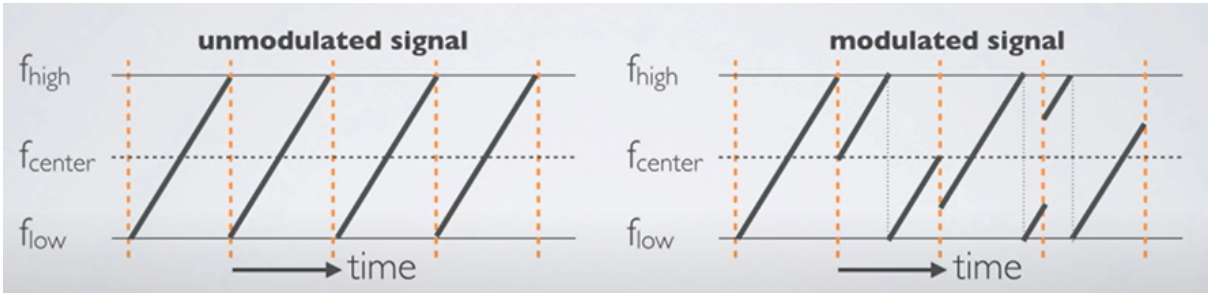


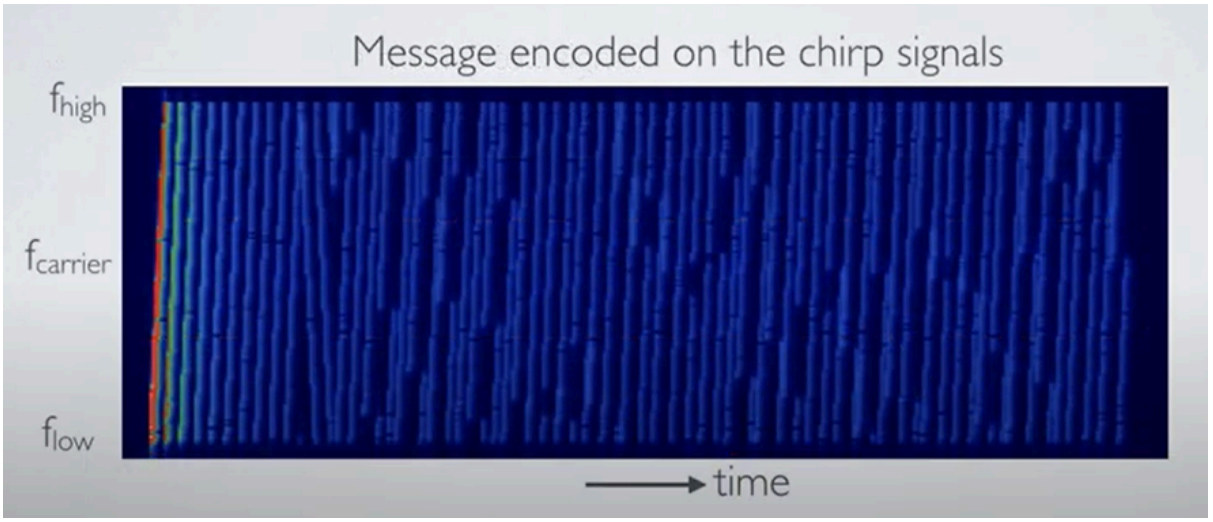
La relación Log10 de la tasa de chip de la secuencia de código y la tasa de bits de la señal de datos se denomina ganancia de procesamiento (Gp). Esta ganancia es lo que permite que el receptor recupere la señal de datos original, incluso si el canal tiene una relación señal-ruido

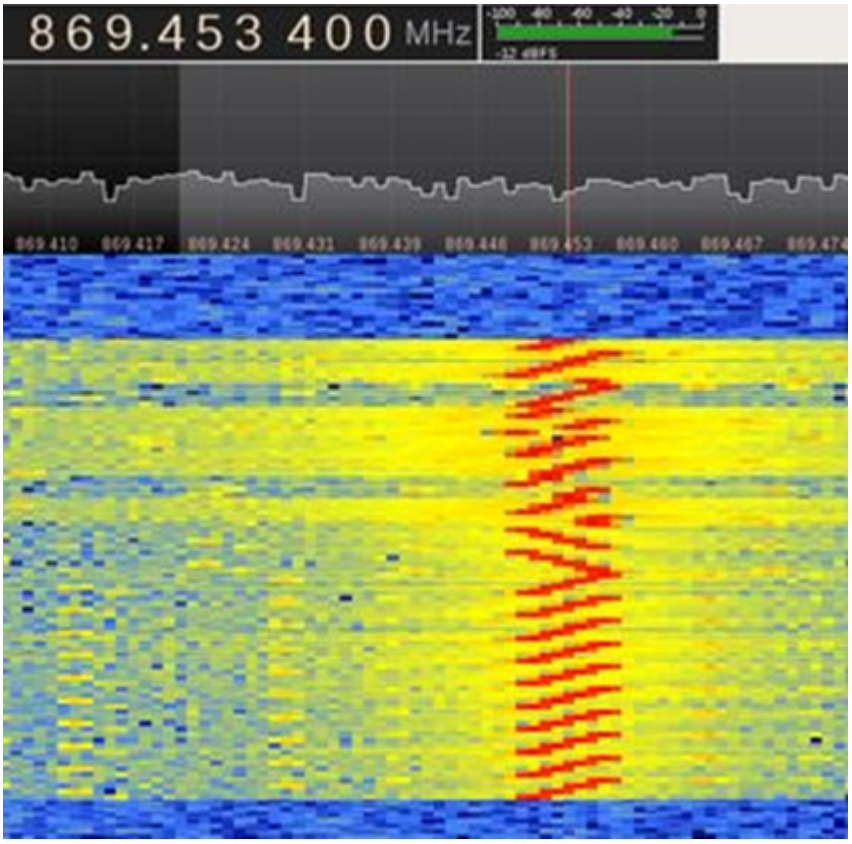
(SNR) negativa. LoRa tiene un Gp superior en comparación con la modulación por cambio de frecuencia (FSK), lo que permite un nivel de potencia de salida del transmisor reducido mientras se mantiene la misma velocidad de datos de la señal y un presupuesto de enlace similar.

Una de las desventajas de un sistema DSSS es el hecho de que requiere un reloj de referencia de alta precisión (y costoso). La tecnología LoRa Chirp Spread Spectrum (CSS) ofrece una alternativa DSSS de bajo costo y bajo consumo de energía, pero robusta, que no requiere un reloj de referencia de alta precisión. En la modulación LoRa, la dispersión del espectro de la señal se logra generando una señal de chirrido (chirp) que varía contínuamente en frecuencia, como puede verse a continuación.

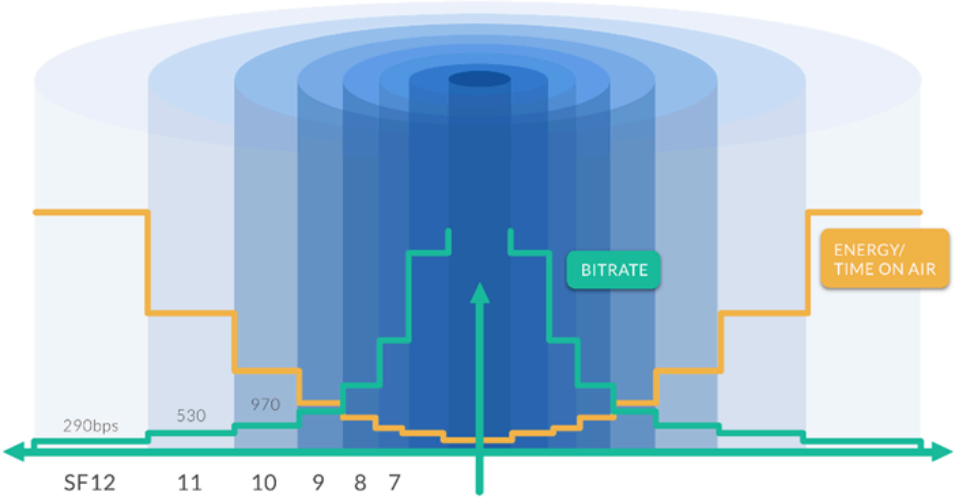








2D simulation (flat environment)



5.1.5.3 Anexo 3: Estados decodificados y códigos CID usados

La siguiente tabla detalla los eventos capaces de ser decodificados al ser leídos desde el bus de datos del sistema, incluyendo el set de estados al que pertenecen. En caso de haber un estado que necesite ser transmitido, se indica en la tercer columna la información del código CID generado:

- si se transmite evento (E), restauración (R) o ambos (ER)
- se indica el código de evento utilizado luego del guión
- en caso de existir, se muestra el número de usuario o zona correspondiente

Set de estados	Estado decodificado	Código de transmisión
Set 0x00	Zones in alarm / restore (zones 1 - 32)	[ER-130/zone #]
	Duress alarm	[E-121]
	Disarmed with alarm memory	[E-458]
	Recent closing alarm	[E-459]
	Zone expander supervisory alarm / restore	[ER-143]
	Keypad Fire alarm / restore	[ER-110]
	Keypad Aux (medical) alarm / restore	[ER-100]
	Keypad panic alarm / restore	[ER-120]
	PGM2 input alarm / restore	[ER-130/zone 99]
	Zone tamper / restore (zones 1 - 32)	[ER-383/zone #]
	Keypad lockout	[E-461/zone 99]
	Armed / disarmed with access codes (codes 1-34, 40-42)	[ER-401/code #]
	Armed partial	[E-456]
	Armed / disarmed special	[ER-400/code 0]
	Auto-arm cancelled	[E-455]
	Panel battery trouble / restore	[ER-302]
	Panel AC power trouble / restore	[ER-301]
	Panel bell trouble / restore	[ER-321]
	Panel fire zone trouble / restore	[ER-373/zone 99]

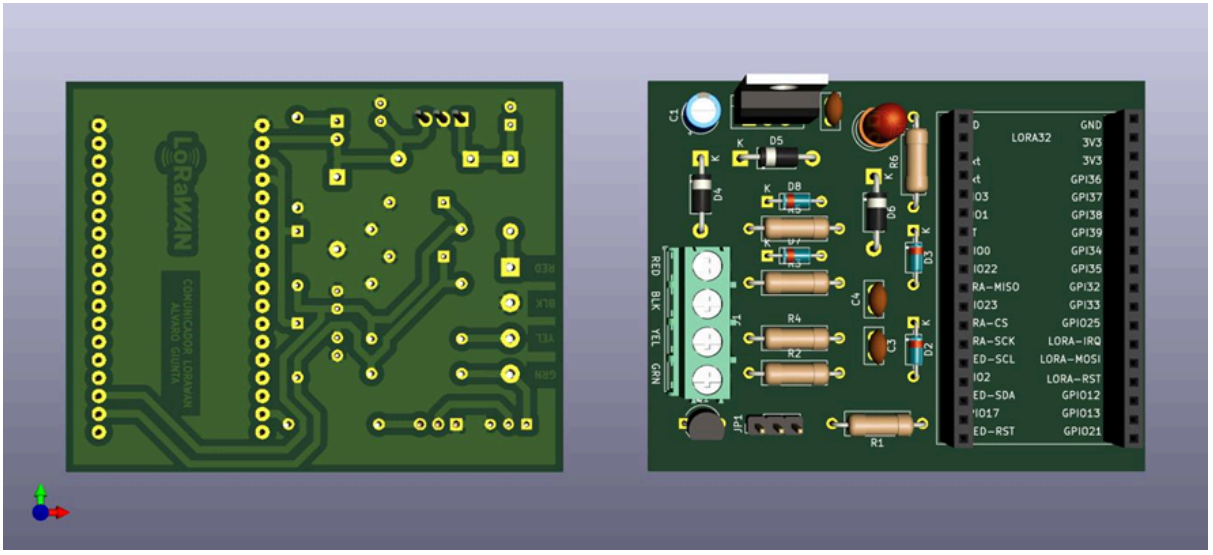
	Panel aux supply trouble / restore	[ER-312]
	Telephone line trouble / restore	[ER-350]
	Phone 1 fail to connect	[E-351]
	Phone 2 fail to connect	[E-352]
	Event buffer threshold 75% full since last DLS upload	
	DLS lead-in	
	DLS lead-out	
	Periodic test transmission	[E-602]
Set 0x01	Cross zone alarm	[E-139]
	Delinquency alarm	[E-654]
	Late to close	[E-404]
	Access codes used (codes 33-34, 40-42)	
	Downloading forced answer	
	Armed: Auto-arm	[E-403]
	Zone battery low / restored (zones 1-32)	[ER-384/zone #]
	Zone fault / restored (zones 1-32)	[ER-380/zone #]
	Exit installer programming	[R-430]
	Enter installer programming	[E-429]
	Walk test begin / end	[ER-607]
	Zones bypassed (zones 1-32)	[E-570/zone #]
	Command output 4	
	Exit fault pre-alert	
	Armed: Entry delay	

	DownLook remote trigger	
Set 0x02	Quick exit	
	Keybus fault / restore	[ER-315]
	Zone bypass (*1)	
	Command output (*7)	
	Cold start	[E-308]
	Warm start	[E-305]
	Panel factory default	[E-317]
	Swinger shutdown	
	Armed / disarmed: keySwitch	[ER-409]
	Armed Keypad away	[R-400]
	Armed Quick-arm	[R-408]
	Activate stay/away zones	
	Armed: stay	[R-441]
	Armed: away	
	Armed: no entry delay	
	Access codes (*1) 1-34, 40-42	
	Access codes (*5) 40-42	
	Access codes 1-34, 40-42	
	Access codes (*6) 40-42	
	Keypad restored / trouble: Slots 1-8	[ER-701/#1-8]
	Zone expander restored: 1-6	[R-704/#1-6]
	Zone expander trouble: 1	[E-704/#1]

Set 0x03	Zone expander trouble 2-6	[E-704/#2-6]
	Zone expander trouble / restored (7)	[ER-704/#7]
	Zone expander tamper / tamper restored (7)	[ER-714/#7]
	RF Module: Supervisory trouble / restore	[ER-702]
	Power Supply Module: Supervisory trouble / restore	[ER-703]
	Keypad tamper / tamper restored (Slots 1-8)	[ER-711/#1-8]
	Power supply module tamper / tamper restored	[ER-713]
	PGM low power module tamper / tamper restored	[ER-715]
	Power Supply module battery trouble / restore	[ER-338]
	Power supply module aux supply trouble / restore	[ER-337]
	Power supply module output 1 trouble / restore	[ER-343]
Set 0x04	Periodic test with trouble	[E-608]
	Exit fault	[E-457]
	Alarm cancelled	[E-406]
	Zones in alarm / restore (Zones 33 - 64)	[ER-130/zone #]
	Zones tamper / restore (Zones 33 - 64)	[ER-383/zone #]
Set 0x05	Armed / disarmed by access code (Codes 35-39, 43-95)	[ER-401/code #]
Set 0x14	TLink com fault	
	TLink network fault	
	TLink receiver trouble	
	TLink receiver restored	
Set 0x16	Trouble acknowledged	

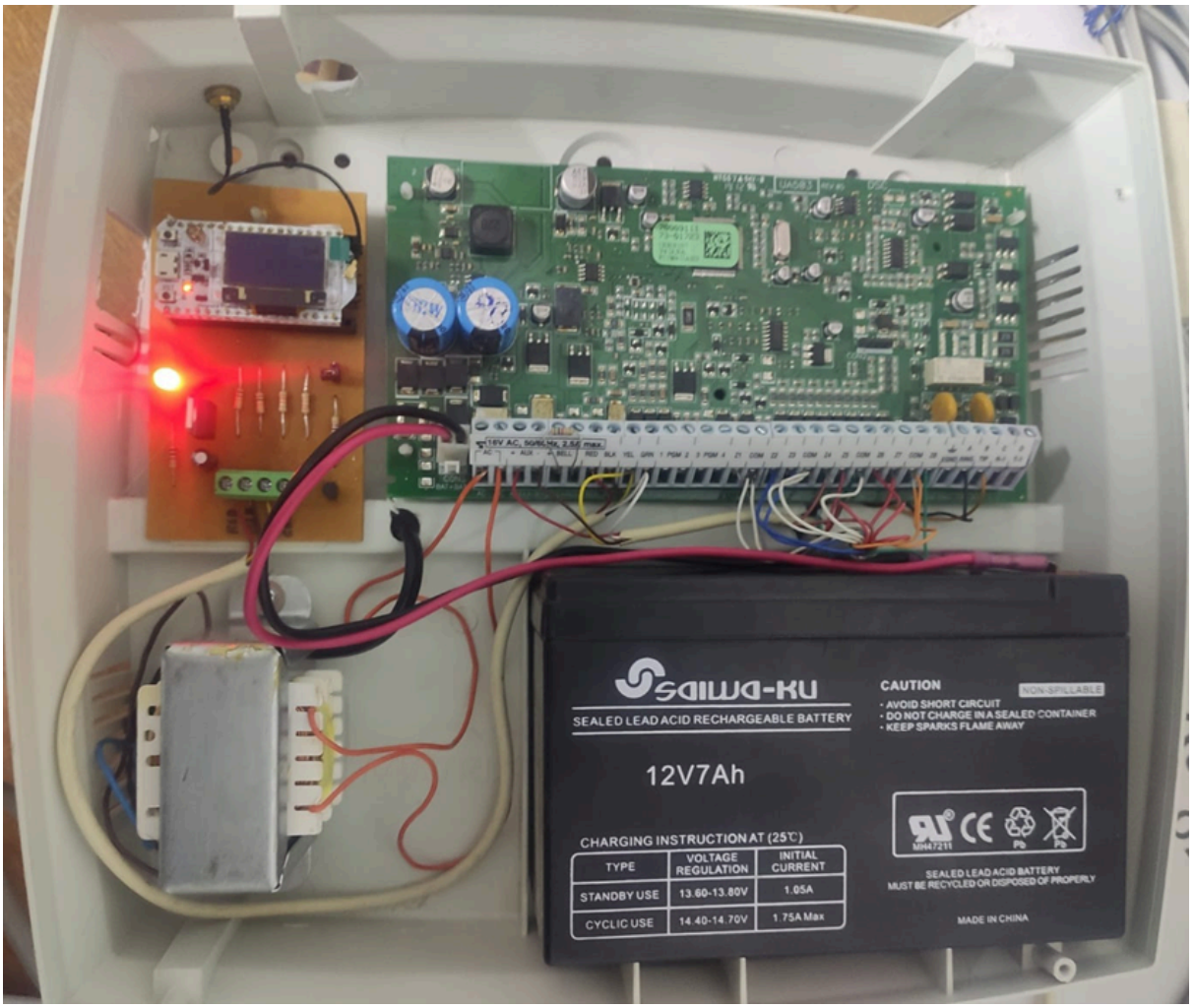
	RF delinquency trouble / restore	
Set 0x17	Access codes (*1) (codes 35-39, 43-95)	
	Access codes (*2) (codes 35-39, 43-95)	
	Access codes (*3) (codes 35-39, 43-95)	
Set 0x18	Access codes (*7) (codes 35-39, 43-95)	
	Access codes (*5) (codes 35-39, 43-95)	
	Access codes (*6) (codes 35-39, 43-95)	
Set 0x1B	System reset transmission	

5.1.5.4 Anexo 4: PCB y Galería imágenes




LINUX SEVER


routerboard
MikroTik



5.2 Factibilidad Económica

Para el cálculo de la factibilidad económica, se tuvieron los siguientes supuestos:

- Se considerará un horizonte de evaluación de 5 años
- El producto estará compuesto por un comunicador
- El precio de venta del producto es de 65 USD
- Dentro de los costos fijos se consideran los servicios básicos (Luz, Agua, etc.) y alquiler. Todo lo referido a marketing, ventas, etc. es realizado por la persona a cargo del proyecto
- Se cobrará el 100% del precio del producto al realizar la compra
- Se produce una cantidad limitada de equipos a principio de año, que serán vendidos en el transcurso del mismo.
- Para el cálculo se toma una tasa de interés del 12%

5.2.1 Aproximación al valor actual neto

5.2.1.1 Valor actual neto nulo

El flujo de caja para asegurar la subsistencia del proyecto se ve reflejado en el siguiente cuadro:

Flujo de caja	0	1	2	3	4	5
Unidades vendidas		100	26	25	25	25
Ingreso		U$D 6.560,00	U$D 1.705,60	U$D 1.640,0(	U$D 1.640,00	U$D 1.640,00
Precio unitario		U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60
Costos fijos						
Total costos fijos		U$D 840,00	U$D 840,00	U$D 840,00	U$D 840,00	U$D 840,00
Costos variables						
Costo de venta del producto		U$D 45,60	U$D 45,60	U$D 45,60	U$D 45,60	U$D 45,60
Herramientas e instrumentos	U$D 200,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00
Equipos electrónicos	U$D 200,00	U$D 0,00	U$D 0,00	U$D 200,00	U$D 0,00	U$D 0,00
Costos totales		U$D 885,60	U$D 885,60	U$D 1.085,6(	U$D 885,60	U$D 885,60
Depreciación herramientas		U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67
Utilidad antes de impuestos		U$D 4.727,73	-U$D 126,67	-U$D 392,27	-U$D 192,27	-U$D 192,27
Impuesto a las ganancias (30%)		U$D 1.418,32	-U$D 38,00	-U$D 117,68	-U$D 57,68	-U$D 57,68
Utilidad después de impuestos		U$D 3.309,41	-U$D 88,67	-U$D 274,59	-U$D 134,59	-U$D 134,59
Depreciación herramientas		U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67
Inversión inicial						
Herramientas y equipos electrónicos	-U$D 400,00					
Capital de trabajo	-U$D 5.556,00					
Recuperación capital de trabajo						U$D 5.556,00
Valor de desecho						U$D 0,00
Flujo del proyecto	**-U$D 5.956,00**	**U$D 3.416,08**	**U$D 18,00**	**-U$D 167,92**	**-U$D 27,92**	**U$D 5.528,08**

Tasa de interés	12%
VAN	**U$D 107,94**
TIR	**13%**

Para el cálculo de VAN = 0, el precio de venta del producto fue de 65 USD para cada año. La cantidad de ventas realizadas para cada año fue de 100 productos en el primer año y 25 los años subsiguientes.

El capital de trabajo para asegurar la subsistencia del proyecto se ve reflejado en el siguiente cuadro:

INGRESO MENSUAL AÑO UNO		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Precio de venta		U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60
Unidades vendidas		0	10	10	10	10	10	10	8	8	8	8	8
Total de ventas		U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
Realización del cobro													
Cobro al momento de la compra	100%	U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
Ingreso total		U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
PRODUCCIÓN													
Stock		100	90	80	70	60	50	40	32	24	16	8	0
Ventas		0	10	10	10	10	10	10	8	8	8	8	8
Producción Mensual		100	0	0	0	0	0	0	0	0	0	0	0
EGRESOS													
Costos Fijos		U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00
Costos de Fabricación		U$D 4.560,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00
Egreso total		U$D 4.630,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00
CAPITAL DE TRABAJO													
Ingresos		U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
Egresos		U$D 4.630,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00
Acumulado		-U$D 4.630,0	-U$D 4.044,0	-U$D 3.458,0	-U$D 2.872,0	-U$D 2.286,0	-U$D 1.700,0	-U$D 1.114,0	-U$D 659,20	-U$D 204,40	U$D 250,40	U$D 705,20	U$D 1.160,0
Máximo Acumulado		-U$D 4.630,0											

CAPITAL DE TRABAJO SIN MARGEN		U$D 4.630,00
CONSIDERACION MARGEN	20,00%	U$D 5.556,00

5.2.1.2 Valor actual neto optimista

Para el cálculo de VAN optimista, el supuesto de ventas se basa en el caudal actual de clientes con el que cuenta la empresa solicitante, y su capacidad de implementación progresiva.

Por otro lado, se presupone que la problemática de conectividad afectará de igual forma a otras empresas del sector, por lo que se visualiza en ellos otros potenciales clientes. De esta forma, cuando la empresa solicitante haya reemplazado todos sus comunicadores actuales por los desarrollados aquí, se presupone la implementación (que podría solaparse) por parte de otras empresas del rubro, lo cual lleva a mantener el flujo de ventas inicial.

El capital de trabajo según lo mencionado anteriormente se ve reflejado en el siguiente cuadro:

Flujo de caja	0	1	2	3	4	5
Unidades vendidas		100	100	100	110	120
Ingreso		U$D 6.560,00	U$D 6.560,00	U$D 6.560,0(	U$D 7.216,00	U$D 7.872,00
Precio unitario		U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60
Costos fijos						
Total costos fijos		U$D 840,00	U$D 840,00	U$D 840,00	U$D 840,00	U$D 840,00
Costos variables						
Costo de venta del producto		U$D 45,60	U$D 45,60	U$D 45,60	U$D 45,60	U$D 45,60
Herramientas e instrumentos	U$D 200,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00
Equipos electrónicos	U$D 200,00	U$D 0,00	U$D 0,00	U$D 200,00	U$D 0,00	U$D 0,00
Costos totales		U$D 885,60	U$D 885,60	U$D 1.085,6(	U$D 885,60	U$D 885,60
Depreciación herramientas		U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67
Utilidad antes de impuestos		U$D 4.727,73	U$D 4.727,73	U$D 4.527,7	U$D 5.383,73	U$D 6.039,73
Impuesto a las ganancias (30%)		U$D 1.418,32	U$D 1.418,32	U$D 1.358,3	U$D 1.615,12	U$D 1.811,92
Utilidad después de impuestos		U$D 3.309,41	U$D 3.309,41	U$D 3.169,4	U$D 3.768,61	U$D 4.227,81
Depreciación herramientas		U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67	U$D 106,67
Inversión inicial						
Herramientas y equipos electrónicos	-U$D 400,00					
Capital de trabajo	-U$D 5.556,00					
Recuperación capital de trabajo						U$D 5.556,00
Valor de desecho						U$D 0,00
Flujo del proyecto	**-U$D 5.956,00**	**U$D 3.416,08**	**U$D 3.416,08**	**U$D 3.276,0**	**U$D 3.875,28**	**U$D 9.890,48**

Tasa de interés	12%
VAN	**U$D 10.224,13**

El flujo de caja según lo mencionado anteriormente se ve reflejado en el siguiente cuadro:

INGRESO MENSUAL AÑO UNO		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Precio de venta		U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60	U$D 65,60
Unidades vendidas		0	10	10	10	10	10	10	8	8	8	8	8
Total de ventas		U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
Realización del cobro													
Cobro al momento de la compra	100%	U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
Ingreso total		**U$D 0,00**	**U$D 656,00**	**U$D 656,00**	**U$D 656,00**	**U$D 656,00**	**U$D 656,00**	**U$D 656,00**	**U$D 524,80**	**U$D 524,80**	**U$D 524,80**	**U$D 524,80**	**U$D 524,80**
PRODUCCIÓN													
Stock		100	90	80	70	60	50	40	32	24	16	8	0
Ventas		0	10	10	10	10	10	10	8	8	8	8	8
Producción Mensual		100	0	0	0	0	0	0	0	0	0	0	0
EGRESOS													
Costos Fijos		U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00
Costos de Fabricación		U$D 4.560,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00	U$D 0,00
Egreso total		**U$D 4.630,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**	**U$D 70,00**
CAPITAL DE TRABAJO													
Ingresos		U$D 0,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 656,00	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80	U$D 524,80
Egresos		U$D 4.630,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00	U$D 70,00
Acumulado		-U$D 4.630,0(	-U$D 4.044,0(	-U$D 3.458,(	-U$D 2.872,(	-U$D 2.286,(	-U$D 1.700,(	-U$D 1.114,(	-U$D 659,20	-U$D 204,40	U$D 250,40	U$D 705,20	U$D 1.160,0(
Máximo Acumulado		**-U$D 4.630,0(**											

CAPITAL DE TRABAJO SIN MARGEN		**U$D 4.630,00**
CONSIDERACION MARGEN	**20,00%**	**U$D 5.556,00**

5.2.2 Tasa interna de retorno

La tasa interna de retorno (TIR) obtenida al considerar el caso optimista resulta:

TIR	**58%**

5.2.3 Payback o plazo de recuperación

El plazo de recuperación (Payback) obtenido al considerar el caso optimista resulta:

PRI			
PERIODO	FLUJO	ACUMULADO	NETO
0	-U$D 5.956		
1	U$D 3.416	U$D 3.416	-U$D 2.540
2	U$D 3.416	U$D 6.832	U$D 876
3	U$D 3.276	U$D 10.108	U$D 4.152
4	U$D 3.875	U$D 13.984	U$D 8.028
5	U$D 9.890	U$D 23.874	U$D 17.918
PRI		**1,73 años**	

5.2.4 Productos y servicios de otros fabricantes

Si bien existen en el mercado algunas alternativas, las mismas no son una competencia directa ya que no utilizan tecnologías LPWAN. Entre estas se encuentran:

- Comunicador inalambrico DSC:

El 3G2060 es un comunicador de alarma celular 3G inalámbrico. Se conecta a un panel de control DSC PowerSeries PC1864/1832/1616 y permite además del envío de reportes, la programación remota. Precio de compra U$S 395 + IVA.

- Comunicador inalámbrico NT-com: El comunicador inalambrico NT-com ofrece varias versiones, entre las que se encuentran
    - 2G/4G/SMS/Línea Telefónica: Es un comunicador que hace uso de la red celular para enviar y recibir los reportes de estado. El precio de compra es de U$S 200.

- WiFi: Es un comunicador que hace uso de internet para enviar y recibir los reportes de estado. El precio de compra es de U$S 85.

6 Conclusiones y Anexos

Se puede concluir, a la luz de los resultados, que las tecnologías LPWAN, y en este caso particular LoRaWAN es capaz de cumplir satisfactoriamente con los requerimientos establecidos por el solicitante del proyecto.

Estos resultados en conjunto con el análisis de cobertura sirven como puntapié inicial para la implementación en campo del sistema, donde deberán enfrentar otros desafíos tales como la arquitectura y dimensionamiento de la red.

La utilización de partes comercialmente disponibles y de componentes de código abierto hacen que lo realizado en este proyecto sea fácilmente reproducido y/o modificado para cumplir objetivos similares.

El conocimiento técnico e ingenieril que contempla el desarrollo del proyecto previamente descrito, engloba múltiples de las áreas de la ingeniería electrónica además de abarcar temáticas como la gestión de sistemas y aspectos legales.

7 Bibliografías y referencias bibliográficas

[1] *DSC - DSC (Digital Security Controls) es líder mundial en seguridad electrónica y es la principal marca con la que trabaja el solicitante del proyecto. (2024)*
https://www.dsc.com/index.php

[2] *LoRa Alliance - LoRa Alliance es una asociación abierta y sin fines de lucro para promover e impulsar el éxito del estándar LoRaWAN como el estándar para conectividad IoT LPWAN. (2024)*
https://lora-alliance.org/

[3] *LoRaWAN Security Whitepaper - Este documento técnico explica cómo se maneja la seguridad en la especificación LoRaWAN. (2024)*
https://lora-alliance.org/resource_hub/lorawan-security-whitepaper/

[4] *Chirpstack - ChirpStack es un servidor de red LoRaWAN de código abierto que se puede utilizar para configurar redes LoRaWAN. (2024)*
https://www.chirpstack.io/

[5] *The things Industries - The Things Industries es un proveedor de soluciones LoRaWAN de servicio completo. (2024)*
https://www.thethingsindustries.com

[6] *Mosquitto - Eclipse Mosquitto es un intermediario de mensajes de código abierto que implementa el protocolo MQTT. (2024)*
https://mosquitto.org/

[7] *Redis - Redis es un motor de base de datos en memoria, basado en el almacenamiento en tablas de hashes pero que opcionalmente puede ser usada como una base de datos durable o persistente. (2024)*
https://redis.io/

[8] *PostgreSQL - PostgreSQL es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto. (2024)*
https://www.postgresql.org/

[9] *Mikrotik WAP lr9 - El Kit wAP LR9 es una solución lista para usar para utilizar la tecnología LoRa. (2024)*
https://mikrotik.com/product/wap_lr9_kit

[10] *Mikrotik Winbox - Winbox es una utilidad que permite la administración de MikroTik RouterOS mediante una GUI rápida y sencilla. (16/11/2020)*
https://wiki.mikrotik.com/wiki/Manual:Winbox

[11] *LoRaMac Node - El objetivo de este proyecto es mostrar un ejemplo de implementación de una pila LoRaWAN en un dispositivo final. (2024)*
https://github.com/Lora-net/LoRaMac-node

[12] *Platformio - PlatformIO es una herramienta profesional multiplataforma, multiarquitectura y marco múltiple para ingenieros de sistemas integrados y desarrolladores de software que escriben aplicaciones para productos integrados. (2024)*
https://platformio.org/

[13] *Semtech SX1276 - Los transceptores SX1276 cuentan con un módem de largo alcance LoRa que proporciona comunicación de espectro ensanchado de alcance ultra largo y alta inmunidad a interferencias al tiempo que minimiza el consumo de corriente. (2024)*
https://www.semtech.com/products/wireless-rf/lora-core/sx1276

[14] *TTN Conference Workshop Radio Planning - Este repositorio contiene el contenido del taller de planificación de radio en The Things Conference de enero de 2020 en Ámsterdam.. (01/2020)*
https://github.com/pe1mew/TTN_Conference_WorkshopRadioPlanning

[15] *Decoding LoRA - Esta página trata sobre cómo comprender el formato de modulación de RF LoRa. (11/5/2020)*
https://revspace.nl/DecodingLora